Gleicimara Chagas Lustosa

De: Andre Wilson Pimenta Santana
Enviado em: terça-feira, 30 de novembro de 2021 10:43
Para: Gleicimara Chagas Lustosa
Assunto: ENC: solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)
Anexos: Proposta Comercial FUNASA - DLP - 29-11-2021.pdf

De: Andre Oliveira [mailto:andre.oliveira@arvvo.com.br]
Enviada em: segunda-feira, 29 de novembro de 2021 17:08
Para: Andre Wilson Pimenta Santana <andre.pimenta@funasa.gov.br>
Assunto: Re: solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

Prezado Sr. André, boa tarde!

Segue anexa proposta comercial conforme solicitado.

ARVVO TECNOLOGIA
ANDRÉ OLIVEIRA
DIRETOR
(61) 3553-9006 / 9 9272-4997
ANDRE.OLIVEIRA@ARVVO.COM.BR
BRASÍLIA-DF
SHN QUADRA 1 BLOCO A SALA 1114
ED LE QUARTIER - CEP 70.701 010
WWW.ARVVO.COM.BR

De: Andre Wilson Pimenta Santana <andre.pimenta@funasa.gov.br>
Data: segunda-feira, 29 de novembro de 2021 09:02
Para: André Oliveira <andre.oliveira@arvvo.com.br>, "vitor.costa@ish.com.br" <vitor.costa@ish.com.br>, "gerson.cezar@dsr9.com" <gerson.cezar@dsr9.com>
Assunto: solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

Prezado,

solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

Licenciamento para 36 meses

OBJETO DA CONTRATAÇÃO

1.1. Aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP), contemplando licenciamento, garantia, suporte e implantação, de acordo com as quantidades e especificações descritas neste Termo de Referência. **Licenciamento para 36 meses**

item	Descrição	Unidade	Quantidade
1	Aquisição de licenças de software de solução de prevenção de vazamento de dados – Data Loss Prevention – DLP.	UN	3,190
2	Treinamento	UN	3

1. Descrição da Solução de Tecnologia da Informação

Este Anexo especifica as características técnicas da solução de Data Loss Prevention / DLP a ser adquirida para implementação no ambiente do FUNASA. Detalhamos neste Anexo os componentes da solução de DLP.

ITEM	ESPECIFICAÇÕES TÉCNICAS E REQUISITOS MÍNIMOS
01	Aquisição de licenças de software de solução de prevenção de vazamento de dados - Data Loss Prevention (DLP) para 3190 usuarios

2.

1. **Console de Gerenciamento e Plataforma**

1. O licenciamento da solução proposta deve contemplar todo o software, ou seja, todas as funcionalidades descritas neste Termo de referência
2. As configurações de todos os módulos devem possuir integração nativa com a console central.
3. Deve ter console de gerenciamento via tecnologia Web (HTTP ou HTTPS).
4. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, nos sistemas operacionais:
    1. Microsoft Windows Server;
5. Suportar funcionamento em sistemas de virtualização.
6. A solução deve possuir ou integrar com sistemas de monitoramento de atividades do usuário baseado na nuvem (UAM), usando indicadores comportamentais (IOB) e fornecendo visibilidade significativa sobre comportamentos de risco do usuário, a fim de automatizar as políticas de proteção de dados em nível de usuário.
7. Capacidade de excluir incidentes em lote para gestão eficiente de epaço utilizado pela base de dados.
8. Suportar funcionamento em plataformas de Single Sign-On (SSO)
9. A solução deverá criptografar toda a comunicação que ocorre entre os servidores de gerenciamento e os agentes instalados em terminais.
10. A solução deverá criptografar a comunicação entre o servidor principal e os servidores adicionais da plataforma.
11. Possuir registros detalhados de auditoria de atividades de sistema.
12. Permitir a instalação em Sistema Operacional restrito, com serviços e configurações de porta limitados (Hardening).
13. Deve ter a capacidade de bloquear o acesso, movimentação, tráfego e cópia de informações confidenciais detectadas;
14. Deve possuir módulos de detecção distintos, para:
    - Localizar dados confidenciais armazenados em servidores de arquivos, bancos de dados e servidores de email;
    - Localizar dados confidenciais armazenados em desktops e laptops;
    - Detectar dados confidenciais em trânsito na rede, em protocolos TCP/IP;
    - Detectar vazamento de dados a partir de conexão direta com servidores de email;
    - Detectar vazamento de dados a partir de conexão direta com appliances responsáveis pelo processsamento de tráfego WEB (Proxy ou UTM);

1. Capacidade de obter a “impressão digital” de dados estruturados e não estruturados.
2. Capacidade de normalizar variações comuns de apresentação de dados para aprimorar a precisão de políticas de monitoramento.
3. Capacidade de identificar dados estruturados e não estruturados, sem necessidade de utilização de servidores adicionais ou dedicados para este fim.
4. Detectar documentos não estruturados, após usar capacidades nativas de aprendizado automático, a partir da análise de um conjunto de amostras.
5. Permite a criação de padrão de identificação utilizando dados internos da instituição de modo a customizar a ferramenta.
6. Permitir detecção de acordo com expressões regulares configuráveis.
7. Permitir detecção por tipo de arquivo, por nome e extensão de arquivo, remetente/destinatário e protocolo de transmissão.

8. Capacidade de integrar diretamente com LDAP (MS Active Directory) para criar regras de detecção de terminal baseadas em usuário ou grupo. Políticas diferentes podem ser aplicadas de acordo com o usuário que fez o login, mesmo em uma máquina compartilhada.
9. Possuir mecanismo de envio de notificações personalizadas por e-mail aos administradores.
10. Permitir a criação de perfis para administração de servidores, administração de usuário, criação e edição de política.
11. Armazenar e exibir a mensagem original ou arquivo que gerou o incidente.
12. Exibir todo o histórico do incidente, inclusive as alterações e edições referentes ao mesmo.
13. Permitir a exportação da lista de incidentes no formato HTML, PDF ou CSV.
14. Interface de administração única para vizualização de todos os incidentes.
15. Possuir interface WEB, compatível, no mínimo, com os navegadores Internet Explorer, Mozilla Firefox e Google Chrome.
16. Permitir a configuração de ações automáticas, dependendo da quantidade de dados expostos.
17. Deve possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuários envolvidos num incidente detectado.
18. Deve possuir integração com Active Directory, para autenticação de usuários da solução.
19. Deve possuir logs detalhados de auditoria de alterações de políticas.
20. A solução deve ter capacidade de descoberta de vazamento de dados nos seguintes canais:
    - Nuvem;
    - Email;
    - Web;
    - Terminais;
    - Smartphones (A partir de um APP a ser instalado);
    - Plataforma de armazenamento de dados.
21. Proteger os dados contra exposição ou roubo em tempo real.
22. Deve suportar a verificação de arquivos compactados recursivos (exemplos .zip, .rar dentro de .zip, .rar).
23. Deve suportar de forma comprovada a detecção de dados no idioma português brasileiro.
24. Deve ter a capacidade de analisar conteúdo de arquivos grandes (maiores que 20MB) anexados em e-mails.
25. Deve identificar informações confidenciais sem a necessidade de acrescentar tags, etiquetas e afins nos arquivos de origem.
26. Deve identificar conteúdos armazenados em colunas específicas de planilhas eletrônicas e em bancos de dados.
27. Deve possuir capacidade para identificar conteúdos específicos com base em um padrão pré-determinado, para no mínimo:
    - CPF;
    - CNPJ;
    - Cartões de Crédito;
    - Número de eleitor;
    - RG;
    - IBAN;
    - Dados de tecnologia com o IP Address, Mac Address e IMEI de telefones.
28. Deve detectar o arquivo pelo seu conteúdo real, e não apenas pela extensão do arquivo.
29. A solução deve possuir integrada na console a funcionalidade de workflow (Condições de acionamento) resposta a incidentes.
30. Devem ser exibidas na console de gerenciamento todas as informações a respeito do incidente para, no mínimo:
    - Dados para análise como: Origem, Destino, detalhes de qual Canal de detecção foi acionado e nome/caminho do arquivo;

- Dados de qual regra foi acionada;
- Dados de qual informação acionou a regra;
- Severidade do incidente;
- Status do incidente;
- Nome da aplicação;
- Data e hora do evento;
- Volume de dados trafegados no incidente;
- Nome do usuário referenciado no incidente;
- Atributos do usuário coletados do Active Directory;
- Nome da estação de trabalho;
- Informações de destino para qual o dado seria copiado;
- Histórico completo de alteração de incidentes.

31. Deve ter a capacidade de importar um conjunto de pré-configurações do sistema otimizadas para verticais das indústrias específicas, contando com dados de pesquisa em português.
32. A solução deve ser agnóstica a linguística. Todos os mecanismos de identificação de dados, por exemplo: palavras, dicionários e Machine Learning, devem funcionar de forma igual em qualquer linguagem.
33. A solução deve proteger documentos em pelo menos 40 tipos de idiomas.
34. A solução deve incluir um mecanismo de análise de segurança, que é exclusivamente responsável pela modelagem estatística de dados e análise de comportamento suspeito dos usuários, com o objetivo de identificar e agrupar incidentes comuns a um determinado usuário ou estação de trabalho, automaticamente e usando uma pontuação de risco atribuída.
35. Deve permitir que sejam visualizados e identificados rapidamente os usuários ou estações de trabalho com o mais alto nível de risco para a organização, como resultado dos incidentes de segurança associados a eles.
36. A solução deve possuir, com mais de 1700 modelos de políticas predefinidos agrupados por localização geográfica e tipo de organização para identificar regras, regulamentos ou leis que a organização deve cumprir e aplicar as políticas correspondentes sem a necessidade de impressão digital dos dados envolvidos.
37. Deve possibilitar a realização de backup e restore de configurações, incidentes e políticas da plataforma.
38. Deve possibilitar integração nativa com soluções de classificação da informação, de forma a monitorar o uso de dados classificados nos canais de detecção e também a possibilidade de imposição de classificação durante a descoberta de dados em servidores de arquivos, por exemplo.

2. **Criação de Políticas e Detecção de Conteúdo Confidencial**
    1. Deve ter a capacidade de utilizar, no mínimo, os critérios abaixo para criação de políticas:
        - Palavra ou conjunto de palavras chave;
        - Identificadores pré existentes o customizados (CPF, CNPJ, Cartão de crédito, etc.);
        - Expressões regulares com possibilidade de adaptação para qualquer padrão de dados existentes;
        - Nível de classificação da informação;
        - Tipo de arquivo;
        - Nome e extensão de arquivos;
        - Bases de indexação previamente carregadas;
        - Tamanho de dados trafegados;
        - Quantidade de anexos de um e-mail;

- Usuários/E-mails internos;
- Estações de trabalho/servidores específicos;
- Localização da estação de trabalho (Dentro ou fora da rede interna);
- Tipo de estação (Laptop ou desktop);
- E-mails ou domínios externos;
- Direção do tráfego (Entrada ou saída);
- Protocolos de rede ou canais da estação;
- E-mails em dispositivos móveis;
- Dados enviados para impressora;
- Qualquer aplicação em execução na estação de trabalho;
- Cópias para caminhos de rede.

2. Deve possibilitar criação de regras de exclusões para as políticas de acordo com grupos de usuários fornecidos pelo active directory.
3. O produto deve possuir modelos de políticas de detecção com base em regulamentações e melhores práticas de mercado, para no mínimo:
    - SOX;
    - PCI;
    - HIPAA;
    - GDPR.
4. A solução deve possibilitar a criação de regras para adequação a LGPD.
5. A solução deve possuir templates de políticas de detecção, para no mínimo os seguintes temas:
    - Imagens com conteúdo inapropriado;
    - Linguagem ofensiva ou racismo;
    - Cyber Bullying;
    - Problemas relacionados a jogos de azar;
    - Dados confidenciais e propriedade intelectual;
    - Dados que envolvem segurança de redes;
    - Busca de informações relacionadas a indicadores de comprometimento.
6. Deve ter a capacidade para análise de conteúdo nos mais diversos tipos de arquivos, para no mínimo:
    - Texto (TXT, ASC, HTML, DOC, DOCX, SWX, ODT);
    - Compactados (ZIP, RAR, GZ, LHA, HQX, JAR, 7z);
    - CAD (DWG, DXF, VSD, DGN);
    - Planilhas (XLS, XLSX, 123, SXC, ODS, CSV);
    - Apresentações (PPT, PPTX, SXI, SXP, ODP);
    - Outros (PDF, MDB).
7. Deve permitir criar políticas que combinam várias tecnologias e regras de detecção com regras "E/OU" lógicas e de exceção.
8. Permitir a escrita de expressões lógicas para configuração das regras de detecção, exemplo:("Condição 1" OU "Condição 2") E NÃO "Condição 3".
9. Deve ter a capacidade de construir políticas de detecção, configurando-se o grau de severidade adotado para cada regra criada, conforme o número de correspondências que se deseja encontrar em cada possível violação.
10. A solução deve fornecer a implantação de políticas DLP corporativas de forma unificada, ou seja, uma única política de DLP pode ser aplicada a todos os módulos (network, endpoints e aplicações em cloud).
11. As políticas de detecção devem possuir, no mínimo:
    - A capacidade de normalização de todas as variações comuns de apresentação de dados (por exemplo, se a extração de dados contiver "123456789", deverá ter como correspondente "123-45-6789", "123456789", "123.45.6789", etc.);

- A capacidade de detecção usando palavras e frases-chave totalmente configuráveis;
- A capacidade de colocar múltiplas palavras/frases em uma única regra de detecção.
- A capacidade nativa de detectar documentos de identificação e números de impostos internacionais, para no mínimo, os países EUA, França e Brasil.
- A capacidade de detectar faixas de números válidos para determinados tipos de dados, tal como no mínimo, número de cartão de crédito válido.

12. A solução deve incluir mecanismos de proteção de dados contra vazamentos lentos e sofisticados (DRIP DLP), ou seja, deve monitorar a perda lenta de dados em eventos cumulativos;
13. A solução deve fornecer políticas predefinidas para identificar expressões potenciais que são indicativas de bullying cibernético, padrões de pensamento suicida ou conteudo malicioso;
14. A solução deve ter inteligência artificial composta de técnicas que permitem aprender com exemplos de dados em vez de regras de dados pré-classificadas. O produto deve trabalhar com algoritmos de aprendizagem supervisionados e algoritmos de aprendizagem não-Supervisados para classificar e aprender com as informações descobertas nos endpoints;

3. **Resposta a incidentes**

1. Deve possuir notificações personalizáveis através de e-mail em caso de violação de política.
2. A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviados nas notificações.
3. Deve permitir tomar ações automáticas pré-definidas na detecção de incidentes, para no mínimo:
    - Permitir o envio, deletar anexos, quarentenar ou criptografar e-mails;
    - Permitir ou bloquear tráfego de dados sensíveis via FTP;
    - Permitir ou bloquear tráfego de dados sensíveis via HTTP/HTTPs;
    - Através do agente, permitir, bloquear ou solicitar justificativa para o tráfego em pelo menos: Qualquer tipo de aplicação executada pelo Sistema operacional, cópia para armazenamentos de rede, impressão de arquivos, E-mails enviados, upload para páginas Web e cópias para dispositivos USB.
    - Permitir a possibilidade de busca ou não de detalhes sobre o incidente durante o registro;
    - Execução de atividades customizadas;
    - Enviar mensagens para servidores de syslog;
    - Enviar notificações por e-mail;
    - Manipular arquivos durante a descoberta de rede.
4. Deve permitir vários botões de reposta na interface gráfica dos incidentes totalmente configuráveis.
5. Os botões de resposta na interface gráfica dos incidentes devem possibilitar no mínimo:
    - Designar o incidente para resposta de alguém específico;
    - Modificar o status do incidente;
    - Modificar a severidade do incidente;
    - Ignorar o incidente;
    - Adicionar TAG no incidente;
    - Adicionar comentários no incidente;
    - Fazer Download do incidente;
    - Deletar o incidente;
    - Acionar scripts ou tarefas customizadas;

- Escalar o incidente para o gerente do usuário envolvido;
- Escalar o incidente para uma pessoa específica.

6. Deve exibir todos os detalhes do incidente em uma única página.
7. Deve permitir exibir partes específicas da mensagem ou arquivo que violou as políticas, através de uma visualização rápida na tela do incidente, sem a necessidade de usar software externo.
8. Deve permitir armazenar a mensagem e o arquivo original que gerou o incidente.
9. Deve exibir todo o histórico do incidente, incluindo alterações, edições e respostas executadas automaticamente e manualmente.

4. **Relatórios**
    1. Deve exibir relatórios personalizáveis sobre os incidentes e utilizar filtros, no mínimo de:
        - Ação aplicada;
        - Responsável pela análise;
        - Nome da aplicação;
        - Departamento;
        - Canal de detecção;
        - Nível de classificação da informação;
        - Destino de tráfego da informação;
        - Tipo estação (Desktop ou Laptop);
        - ID do incidente
        - Hora do incidente
        - Nome do arquivo trafegado;
        - Histórico do incidente;
        - Incidentes marcados como ignorados;
        - TAGs de incidentes;
        - Quantidade de informação sensível trafegada;
        - Propriedades do arquivo;
        - Política acionada;
        - Nome da regra acionada;
        - Severidade do incidente;
        - Origem do incidente;
        - Status do incidente;
        - Tamanho da transação;
        - Dados relacionados as violações encontradas.
    2. Deve exportar relatórios para os formatos HTML, PDF e CSV.
    3. Deve apresentar um painel para visualização dos relatórios.
    4. Deve ter a capacidade para configurar, salvar relatórios e painéis personalizados por usuário.
    5. Deve possuir painéis (Dashboards) para, no mínimo os seguintes itens:
        - Incidentes criados nos últimos X dias;
        - Políticas mais acionadas;
        - Incidentes por severidade;
        - Incidentes por ação tomada;
        - Incidentes por canais de detecção;
        - Incidentes por origem/destino;
        - Usuários que mais violam políticas.
    6. A solução deve se integrar nativamente a solução de comportamento dos usuários e correlacionar as informações;

7. A solução deve exibir informações dos usuários, com pelo menos 20 incidentes durante o período analisado em conjunto com número de correspondências, tamanho da transação, conteúdo e políticas infringidas;

5. **Módulo de Área de Armazenamento**
    1. Deve verificar existência de conteúdo confidencial em file systems sem a necessidade de agentes de coleta (agent-less) para no mínimo CIFS, NFS, SMB e NTFS.
    2. Deve permitir a análise dos file systems através de agentes ou sem agente em sistemas operacionais, para no mínimo:
        - Windows Server 2008 R2;
        - Windows Server 2012;
        - Windows Server 2016;
        - Red Hat Enterprise Linux 6 e demais releases da versão;
        - Red Hat Enterprise Linux 7 e demais releases da versão.
    3. Deve analisar conteúdo sigiloso armazenado em ambientes complexos, para no mínimo:
        - Microsoft Sharepoint;
        - Lotus Notes;
        - Microsoft SQL Server;
        - Oracle;
        - MySQL
        - Microsoft Exchange;
    4. Deve analisar conteúdo sigiloso em aplicações em nuvem:
        - Salesforce,
        - AW
        - ServiceNow
        - Facebook Workplace
        - G-Suite
        - Google Cloud Platform
        - Azure.
        - One Drive
        - Trello
        - Dropbox
        - Slack
        - GitHub
        - LinkedIn
    5. Deve possuir a capacidade de verificar arquivos Microsoft "PST", possibilitando executar varreduras tanto nas mensagens, assim como, nos arquivos anexos as mensagens.
    6. Possibilidade de mover para quarentena arquivos que violam políticas de segurança.
    7. Deve manter o arquivo no local original, substituindo seu conteúdo por uma mensagem customizável, como aviso e orientação para o usuário.
    8. Permitir a remoção do arquivo que está em quarentena e restaurá-lo de volta ao local original.
    9. Deve permitir coleta automática de arquivos que violem políticas para análise legal (evidência).
    10. Permitir a criação de respostas personalizadas para incidentes.
    11. Exibir detalhes, no incidente, dos arquivos que violam as políticas.
    12. Permitir a visualização das permissões do arquivo.
    13. Deve possibilitar notificação através de e-mail e alerta Syslog em caso de violação de política.
    14. Deve permitir agendamento de varreduras automáticas.

15. Possuir mecanismo de verificação incremental, na qual apenas arquivos novos, ou alterados, sejam verificados.
16. Deve permitir configurar janelas de tempo para verificações, interrompendo o processo automaticamente ao fim do período configurado.
17. Preservar os atributos originais do arquivo, inclusive o atributo "Acessado em", enquanto realiza a verificação.
18. Possuir capacidade de pausar, manualmente, a verificação.
19. Deve utilizar técnicas de paralelismo e controle de banda.
20. Permitir o controle da velocidade das verificações para limitar o uso da largura de banda da rede.
21. Deve ter a capacidade de reutilizar uma única credencial (nome de usuário/senha) em múltiplos alvos a serem verificados.
22. Permitir a verificação simultânea em várias fontes distintas.
23. Permitir limitar quais portas de comunicação serão utilizadas entre o sistema-alvo e o servidor que faz a verificação.
24. Deve permitir aplicar filtros para verificar na varredura de arquivos de um determinado tipo ou em certo diretório.
25. Deve permitir aplicar filtros para verificar na varredura de arquivos a idade E/ou o tamanho de arquivos.

6. **Módulo de Terminal de Usuário**
    1. Capacidade de descobrir fuga de informações sensíveis, por meio de agente.
    2. Possibilidade de aplicação de políticas mesmo quando o agente não tem comunicação com o servidor de gerenciamento.
    3. Possibilidade de armazenamento em cache, dos arquivos que causaram o incidente até que o usuário se conecte, novamente, à rede corporativa.
    4. A solução possuir a funcionalidade de OCR em arquivos do tipo imagem, no mínimo para:
        - Jpeg
        - Bmp
        - Png
        - Gif
        - Tiff
    5. Monitorar e bloquear dados copiados para dispositivos de armazenamento removível (USB).
    6. A solução deverá possuir capacidade de analisar arquivos menos de 1 kbyte.
    7. Possibilidade de criptografar dados sensíveis copiados para dispositivos USB, sem a necessidade de soluções adicionais.
    8. A solução deve ser capaz de detectar e proteger informações estruturadas de dados, por exemplo, de bancos de dados.
    9. a solução de ponto final deve ser capaz de descobrir e proteger informações estruturadas de dados sem exigir uma conexão com o servidor remoto
    10.
    11. Permitir a monitoração e bloqueio para dados copiados para CD/DVD.
    12. Permitir a monitoração e bloqueio para dados enviados a qualquer tipo de impressora local e de rede.
    13. Permitir a monitoração e bloqueio para ações de copiar e colar.
    14. Permitir a monitoração e bloqueio de dados sensíveis trafegados via e-mail corporativo.
    15. Permitir a monitoração e bloqueio para transmissões HTTPS pelo menos nos seguintes navegadores:
        - Internet Explorer;

- Microsoft Edge;
- Mozilla Firefox;
- Google Chrome;
- Safari.

16. Permitir a monitoração e bloqueio para transmissões HTTP.
17. Permitir a monitoração e bloqueio para transmissões via FTP.
18. Permitir a monitoração e bloqueio para uso de dados confidenciais por qualquer aplicativo, incluindo programas de criptografia não autorizados.
19. Permitir a monitoração e bloqueio para dados copiados para compartilhamentos de rede pelo Windows Explorer.
20. A Solução deve possuir monitoramento, por padrão, para pelo menos os seguintes aplicativos:
    - Chrome;
    - Firefox;
    - Internet Explorer (IE);
    - Microsoft Edge;
    - Opera;
    - Safari;
    - Tor;
    - Torch;
    - Acoustica MP3 CD Burner;
    - Alcohol 120%;
    - CD-Mate;
    - Disk Utility;
    - iTunes;
    - Nero Burning ROM;
    - Roxio – Easy Media Creator;
    - Windows Media Player;
    - Amazon Cloud Drive;
    - Box;
    - Dropbox;
    - Egnyte;
    - Google Drive;
    - iCloud;
    - OneDrive;
    - Salesforce Files;
    - ShareFile;
    - Syncplicity;
    - WatchDox;
    - Apple Mail;
    - Eudora;
    - Lotus Notes;
    - MailMate;
    - Microsoft Outlook;
    - Microsoft Outlook Express;
    - Mozilla Thunderbird;
    - Pegasus Mail;
    - Postbox;
    - Sparrow;
    - Windows Live Mail;
    - Windows Mail;

- DK2 Network Server Remote Monitor - DK2 DESkey;
- File Encryption XP;
- Windows Privacy Tray (WinPT);
- Core FTP LE;
- Cute FTP Home 8.2;
- File Transfer Program (Microsoft Utility);
- FileZilla FTP Client;
- Flash FXP 3.6 build 1240;
- FTP Voyager 15;
- Ipswitch WS FTP Home;
- Leech FTP;
- Serv-U;
- Smart FTP Client;
- Adium;
- AIM;
- Apple Messages;
- Camfrog;
- Cisco WebEx;
- GoToMeeting;
- ICQ;
- Jabber Messenger;
- ManyCam;
- Microsoft Lync 2010;
- Miranda IM;
- ooVoo;
- Pidgin;
- Skype for Business;
- TeamViewer;
- Teccent QQ;
- Trillian;
- Viber;
- Yahoo! Instant Messenger;
- Adobe Reader;
- Bean;
- Eclipse;
- Emacs;
- Evernote;
- Keynote;
- LibreOffice/Apache OpenOffice;
- Mellel;
- Microsoft Office Access;
- Microsoft Office Excel;
- Microsoft Office InfoPath;
- Microsoft OneNote;
- Microsoft Office PowerPoint;
- Microsoft Office Project;
- Microsoft Office Publisher;
- Microsoft Office Visio;
- Microsoft Office Word;
- Notepad;
- Numbers;

- OpenOffice.org Calc;
- OpenOffice.org Draw;
- OpenOffice.org Math;
- OpenOffice.org Writer;
- Pages;
- Reminders;
- Stickies;
- TextEdit;
- WordPad;
- AllegianceMD;
- eClinicalWorks;
- ECLIPSYS;
- INGENIX;
- inteGreat;
- Sequel;
- Ares;
- Azureus;
- BearShare;
- BitComet;
- BitLord;
- BitTornado;
- BitTorrent;
- eMule;
- FrostWire;
- Kazaa Lite;
- LimeWire;
- Pando;
- Transmission;
- uTorrent;
- 7-Zip File Manager;
- iArchiver;
- WinRAR;
- WinZip;
- Bluetooth Stack COM Server - BTStackServer;
- Fsquirt;
- iTunes;
- Wireless Link File Transfer App – Irftp;
- WCESMgr;
- Aplicor (online);
- CRM.com;
- HostAnalytics;
- Intacct;
- NetSuite;
- Oracle CRM on demand;
- RightNow;
- Salesforce;
- WorkDay;
- FoxPro;
- Ld;
- MSTSC;
- NT backup tool;

- Vista backup tool;
- VMWare.

21. A solução deve permitir a criação de qualquer aplicativo existente que não venha cadastrado por padrão.
22. Definir dispositivos removíveis individuais, ou grupos de dispositivos, como confiáveis e criar exceções de políticas para esses dispositivos.
23. A solução deve suportar a integração com o Microsoft RMS (Azure Information Protection), para descriptografar e analisar arquivos do tipo Office (Word, Excel, Power Point entre outros) que foram previamente criptografados pelo Azure RMS ou RD (Active Directory) RMS.
24. O agente deverá suportar, no mínimo, Windows 7 (32 e 64 bits), Windows 2008 R2 Enterprise (64bit), Windows 10, Windows Server 2012, Windows Server 2016 e Apple MacOS.
25. Todas as funções devem ser executadas por um único agente.
26. Permitir a desativação do agente pela console de gerenciamento.
27. Possuir mecanismo que reinicie o agente caso o usuário tente interromper o serviço.
28. Possuir proteção contra desinstalação do agente.
29. Capacidade de apresentar as mensagens de notificações em português.
30. Possuir a capacidade de envio de notificação automática, por e-mail, para o usuário e administrador durante a ocorrência de um incidente.
31. Possuir a capacidade de gerenciamento da saúde dos agentes.
32. Deve permitir a distribuição do agente através de GPO ou por ferramenta de terceiros.
33. Deve ter a capacidade de permitir ao usuário justificar a movimentação de conteúdo confidencial, a partir do alerta em “pop-up”, escolhendo opções de justificativa configuráveis pelo administrador da ferramenta.
34. O agente deve executar varredura local para verificar se a estação do usuário possui conteúdo confidencial.
35. A solução deve ser capaz de proteger informações de impressão digital de dados estruturados offline e sem a necessidade de qualquer comunicação com servidores de administração ou gerenciamento ou repositórios de impressões digitais
36. O endpoint deve poder pode permitir automaticamente a transferência de informações específicas em forma criptografada, configurados pelo administrador;
37. O endpoint deve permitirá que o usuário defina sua própria senha para criptografia e arquivos criptografados.
38. A solução deve permitir que o arquivo criptografado possa ser visualizado ou aberto em computadores onde o endpoint não está instalado usando a senha original do emissor do documento.
    1. Essa funcionalidade deve ser atendida através do próprio agente sem a necessidade de adicionar uma solução de terceiros;

1.
2. Deve permitir realizar verificações incrementais, apenas em arquivos novos e alterados.
3. Permitir a instalação do agente de modo oculto ou em modo de interação com o usuário.
4. Quando utilizado em modo interativo, permitir sincronização de políticas de forma manual, através de acionamento de botão no agente.
5. A solução deve suportar integração dinâmica com o User Behavior Analytics ou plataformas UAM.
6. Deve permitir incluir na solução de UAM ou User Behavior Analytics a coleta de eventos produzidos pela solução DLP e posterior análise e modelagem realizada pelo UAM ou User Behavior Analytics, com o objetivo de calcular um nível de risco por usuário.

7. Deve permitir atraves do nível de risco obtido pelos algoritmos do UAM ou User Behaivior Analytics , esses resultados devem ser devolvidos à solução DLP original para aplicar ações imediatas ou dinâmicas, sem a intervenção humana do administrador da solução.
8. Alimentar a console de gerenciamento, com pelo menos, as seguintes informações do agente:
    - Nome do computador;
    - IP Address;
    - Usuário logado;
    - Última vez que o agente se comunicou com a o servidor central;
    - Identificador do grupo de políticas utilizados;
    - Campo que informa se o agente está em sincronismo com as últimas políticas/configurações disponibilizadas pelo administrador;
    - Versão do agente;
    - Versão da política instalada.

1. **Módulo de rede**
    1. Permitir a monitoração/bloqueio do e-mail corporativo, evitando que e-mails com dados sigilosos sejam enviados para fora da organização, inclusive em smartphones e tablets.
    2. Possibilidade de colocar mensagens de correio eletrônico em quarentena para análise.
    3. Permitir a monitoração/bloqueio de tráfego WEB, evitando que dados sigilosos saiam da organização por este canal, inclusive em smartphones e tablets.
    4. Capacidade de monitorar/bloquear o tráfego informações sensíveis em posts de redes sociais.
    5. Permitir a monitoração de qualquer protocolo baseado em TCP, como o SMTP, inclusive anexos; HTTP, inclusive arquivos de upload; FTP ativo e passivo.
    6. Capacidade de monitorar o vazamento de dados por meio de softwares de Mensagens Instantâneas.
    7. Permitir a classificação dos protocolos, mesmo quando executados em portas que não são padrão.
    8. Capacidade de filtrar o tráfego da rede para inspeção, segundo o protocolo, faixa de IP e remetente/destinatário de e-mail.

2. **Módulo de Classificação da informação**
    1. A solução deve ter integração nativa com soluções de Data Loss Prevention;
    2. A solução deve ter capacidade de realizar a rotulagem de informações recém criadas ou pré-existentes sem a necessidade de alterar as propriedades do arquivo, somente seus metadados;
    3. A solução de deve ter a capacidade de automaticamente classificar arquivos no mínimo para os seguintes tipos de arquivo;
        - Word, Excel, PowerPoint, Outlook, Project e Microsoft Office.
        - Open Office
        - PDF
        - ZIP
        - MSG, TIF e EML files
        - JPEG
        - HTML

4. A solução deve ter a capacidade de proporcionar ao usuário a classificar a informação recém-criada de forma que as soluções integradas possam usufruir desta classificação e incluí-las de forma automática dentro de políticas previamente criadas;
5. A solução deve permitir que as soluções integradas detectem os metadados do Classificador, a fim de evitar que o arquivo seja copiado e notificar o usuário/administrador.
6. A solução deve possuir integração com o sistema operacional Windows, permitindo que as ações de classificação do usuário sejam logadas pelo sistema operacional;
7. A solução deve possibilitar a classificação da informação pelo usuário, possibilitando classificar a informação recém-criada em no mínimo:
    - Informação Pública;
    - Informação Restrita;
    - Informação Interna;
    - Informação Confidencial
    - Informação Pessoal.
8. A solução deve possibilitar classificar tanto a informação recém-criada, como pré-existentes;
9. A solução deve ter integração para classificação da informação pelo usuário para no mínimo:
    - Word, Excel, PowerPoint, Outlook, Project e Microsoft Office.
    - Open Office
    - PDF
    - ZIP
10. A solução deve ser capaz de analisar o comportamento malicioso do usuário, priorizando alertas correlacionados com diversas soluções de segurança em produção, contendo desta forma as ameaças, possibilitando a partir de um único relatório indicar um possível ataque;
11. A solução deve ter a capacidade de analisar as informações em conformidade com normas e regulamentações, para no mínimo GDPR, PCI, DSS, SOX, HIPAA;
12. A solução deve basear o coeficiente comportamental de risco, indicando a priorização das ações e identificando se o comportamento malicioso é interno ou se é externo, correlacionando para isso informações de no mínimo:
    - Incidentes recebidos da solução de DLP local;
    - Incidentes recebidos pela solução de criptografia, na tentativa de acesso aos dados sensíveis;
    - Incidentes de classificação de documentos/informação por parte do usuário final;
    - Incidentes recebidos da rede de inteligência mundial do fabricante da solução;
13. A solução deve ser capaz de identificar os usuários expostos aos maiores níveis de risco e possibilitar a partir desta informação refinar as políticas de proteção dos dados;
14. A solução deve permitir que as soluções integradas possam gerar um relatório sobre as marcas de metadados do Classificador, permitindo no mínimo:
    - Localização de arquivo por classificação;
    - Alteração na permissão dos arquivos;
    - Adicionar criptografia no arquivo;
15. A solução deve ser capaz de inserir marcações visuais em e-mails (ex. Outlook) para o cabeçalho ou rodapé;
16. A solução deve classificar e-mails enviados com arquivos anexados de acordo com a classificação do anexo. Esta classificação deve ser realizada antes do envio.
17. solução deve ter a capacidade de calcular a pontuação de risco de cada usuário a partir do comportamento do passado e do presente;
18. A solução deve ter a capacidade de criar relatórios de risco, baseados nos maiores infratores;
19. A solução deve ter a capacidade de criar políticas de alerta e bloqueio, conforme segue:

- Políticas de Alerta: É enviado um alerta ao usuário, no entanto, é possível ao usuário salvar o arquivo e enviá-lo por e-mail;
- Políticas de Bloqueio: É enviado um alerta ao usuário, independentemente do nível de classificação do arquivo, onde não será possível salvar, nem tão pouco enviar o arquivo;

20. A solução deverá possibilitar no mínimo formas de:
    - Descoberta de Informações;
    - O fluxo da informação;
    - Proteger contra a exfiltração da informação, quer seja intencional, quer seja inadvertida;
    - Assegurar conformidade com as políticas de acesso e políticas de segurança;
    - Possibilitar a manutenção da trilha de auditoria por razões de controle e conformidade;
    - Possibilitar alertar aos usuários quando da criação de informações, sobre as políticas de gerenciamento da informação;
    - Possibilitar o rastreio de "onde" os dados não estruturados estão sendo criados e "quem" os estão criando;
21. A solução deve permitir forçar a aplicação de políticas antes que os dados saiam da gerência do Órgão, para no mínimo:
    - Políticas de TAG;
    - Políticas de introdução de cabeçalhos (append headers);
    - Políticas de inclusão de metadados (add metadata);
22. A solução deve ser capaz de implementar gráficos comparativos de risco comportamental entre no mínimo:
    - Usuários sob o mesmo Gerente;
    - Usuários do mesmo departamento;
    - Comportamento dos endpoints;
    - Comportamento das informações marcadas com TAG de dados sensíveis;
    - Frequência com que as políticas de proteção dos documentos são violadas;
    - Envio de informações sensíveis por e-mail e web;

Gleicimara Chagas Lustosa

De: Andre Wilson Pimenta Santana
Enviado em: terça-feira, 30 de novembro de 2021 10:43
Para: Gleicimara Chagas Lustosa
Assunto: ENC: solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)
Anexos: 202111-9217 - Proposta FUNASA - DLP Forcepoint.pdf

De: Arthur Andrade [mailto:arthur.andrade@dsr9.com]
Enviada em: segunda-feira, 29 de novembro de 2021 18:14
Para: Andre Wilson Pimenta Santana <andre.pimenta@funasa.gov.br>
Assunto: FW: solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

Boa tarde André, tudo bem?

Segue como solicitado a proposta do DLP.

Quaisquer dúvidas estou à disposição.
Abraço.

Arthur Andrade
dsr9
arthur.andrade@dsr9.com | skype: arthurandrade4 | www.dsr9.com | +55 (11) 97323-9868
Av. Paulista, 1337 - Edifício Paulista I - Conj. 12 - 1º And. - São Paulo - SP - CEP: 01311-200 - Tel.: +55 (11) 3628-7880

Symantec. FUJITSU CYBERARK VERITAS FORTINET Guardicore

From: Andre Wilson Pimenta Santana <andre.pimenta@funasa.gov.br>
Date: Monday, 29 November 2021 09:03
To: "andre.oliveira@arvvo.com.br" <andre.oliveira@arvvo.com.br>, "vitor.costa@ish.com.br" <vitor.costa@ish.com.br>, Gerson Cezar Jr <gerson.cezar@dsr9.com>
Subject: solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

Prezado,

solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

Licenciamento para 36 meses

OBJETO DA CONTRATAÇÃO

1.1. Aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP), contemplando licenciamento, garantia, suporte e implantação, de acordo com as quantidades e especificações descritas neste Termo de Referência. **Licenciamento para 36 meses**

item	Descrição	Unidade	Quantidade
1	Aquisição de licenças de software de solução de prevenção de vazamento de dados – Data Loss Prevention – DLP.	UN	3,190
2	Treinamento	UN	3

1. Descrição da Solução de Tecnologia da Informação

Este Anexo especifica as características técnicas da solução de Data Loss Prevention / DLP a ser adquirida para implementação no ambiente do FUNASA. Detalhamos neste Anexo os componentes da solução de DLP.

ITEM	ESPECIFICAÇÕES TÉCNICAS E REQUISITOS MÍNIMOS
01	Aquisição de licenças de software de solução de prevenção de vazamento de dados - Data Loss Prevention (DLP) para 3190 usuarios

2.

1. **Console de Gerenciamento e Plataforma**

1. O licenciamento da solução proposta deve contemplar todo o software, ou seja, todas as funcionalidades descritas neste Termo de referência
2. As configurações de todos os módulos devem possuir integração nativa com a console central.
3. Deve ter console de gerenciamento via tecnologia Web (HTTP ou HTTPS).
4. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, nos sistemas operacionais:
    1. Microsoft Windows Server;
5. Suportar funcionamento em sistemas de virtualização.
6. A solução deve possuir ou integrar com sistemas de monitoramento de atividades do usuário baseado na nuvem (UAM), usando indicadores comportamentais (IOB) e fornecendo visibilidade significativa sobre comportamentos de risco do usuário, a fim de automatizar as políticas de proteção de dados em nível de usuário.
7. Capacidade de excluir incidentes em lote para gestão eficiente de epaço utilizado pela base de dados.
8. Suportar funcionamento em plataformas de Single Sign-On (SSO)
9. A solução deverá criptografar toda a comunicação que ocorre entre os servidores de gerenciamento e os agentes instalados em terminais.
10. A solução deverá criptografar a comunicação entre o servidor principal e os servidores adicionais da plataforma.
11. Possuir registros detalhados de auditoria de atividades de sistema.
12. Permitir a instalação em Sistema Operacional restrito, com serviços e configurações de porta limitados (Hardening).
13. Deve ter a capacidade de bloquear o acesso, movimentação, tráfego e cópia de informações confidenciais detectadas;
14. Deve possuir módulos de detecção distintos, para:
    - Localizar dados confidenciais armazenados em servidores de arquivos, bancos de dados e servidores de email;
    - Localizar dados confidenciais armazenados em desktops e laptops;
    - Detectar dados confidenciais em trânsito na rede, em protocolos TCP/IP;
    - Detectar vazamento de dados a partir de conexão direta com servidores de email;
    - Detectar vazamento de dados a partir de conexão direta com appliances responsáveis pelo processsamento de tráfego WEB (Proxy ou UTM);

1. Capacidade de obter a “impressão digital” de dados estruturados e não estruturados.
2. Capacidade de normalizar variações comuns de apresentação de dados para aprimorar a precisão de políticas de monitoramento.
3. Capacidade de identificar dados estruturados e não estruturados, sem necessidade de utilização de servidores adicionais ou dedicados para este fim.
4. Detectar documentos não estruturados, após usar capacidades nativas de aprendizado automático, a partir da análise de um conjunto de amostras.
5. Permite a criação de padrão de identificação utilizando dados internos da instituição de modo a customizar a ferramenta.
6. Permitir detecção de acordo com expressões regulares configuráveis.
7. Permitir detecção por tipo de arquivo, por nome e extensão de arquivo, remetente/destinatário e protocolo de transmissão.
8. Capacidade de integrar diretamente com LDAP (MS Active Directory) para criar regras de detecção de terminal baseadas em usuário ou grupo. Políticas diferentes podem ser aplicadas de acordo com o usuário que fez o login, mesmo em uma máquina compartilhada.
9. Possuir mecanismo de envio de notificações personalizadas por e-mail aos administradores.

10. Permitir a criação de perfis para administração de servidores, administração de usuário, criação e edição de política.
11. Armazenar e exibir a mensagem original ou arquivo que gerou o incidente.
12. Exibir todo o histórico do incidente, inclusive as alterações e edições referentes ao mesmo.
13. Permitir a exportação da lista de incidentes no formato HTML, PDF ou CSV.
14. Interface de administração única para vizualização de todos os incidentes.
15. Possuir interface WEB, compatível, no mínimo, com os navegadores Internet Explorer, Mozilla Firefox e Google Chrome.
16. Permitir a configuração de ações automáticas, dependendo da quantidade de dados expostos.
17. Deve possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuários envolvidos num incidente detectado.
18. Deve possuir integração com Active Directory, para autenticação de usuários da solução.
19. Deve possuir logs detalhados de auditoria de alterações de políticas.
20. A solução deve ter capacidade de descoberta de vazamento de dados nos seguintes canais:
    - Nuvem;
    - Email;
    - Web;
    - Terminais;
    - Smartphones (A partir de um APP a ser instalado);
    - Plataforma de armazenamento de dados.
21. Proteger os dados contra exposição ou roubo em tempo real.
22. Deve suportar a verificação de arquivos compactados recursivos (exemplos .zip, .rar dentro de .zip, .rar).
23. Deve suportar de forma comprovada a detecção de dados no idioma português brasileiro.
24. Deve ter a capacidade de analisar conteúdo de arquivos grandes (maiores que 20MB) anexados em e-mails.
25. Deve identificar informações confidenciais sem a necessidade de acrescentar tags, etiquetas e afins nos arquivos de origem.
26. Deve identificar conteúdos armazenados em colunas específicas de planilhas eletrônicas e em bancos de dados.
27. Deve possuir capacidade para identificar conteúdos específicos com base em um padrão pré-determinado, para no mínimo:
    - CPF;
    - CNPJ;
    - Cartões de Crédito;
    - Número de eleitor;
    - RG;
    - IBAN;
    - Dados de tecnologia com o IP Address, Mac Address e IMEI de telefones.
28. Deve detectar o arquivo pelo seu conteúdo real, e não apenas pela extensão do arquivo.
29. A solução deve possuir integrada na console a funcionalidade de workflow (Condições de acionamento) resposta a incidentes.
30. Devem ser exibidas na console de gerenciamento todas as informações a respeito do incidente para, no mínimo:
    - Dados para análise como: Origem, Destino, detalhes de qual Canal de detecção foi acionado e nome/caminho do arquivo;
    - Dados de qual regra foi acionada;
    - Dados de qual informação acionou a regra;
    - Severidade do incidente;
    - Status do incidente;

- Nome da aplicação;
- Data e hora do evento;
- Volume de dados trafegados no incidente;
- Nome do usuário referenciado no incidente;
- Atributos do usuário coletados do Active Directory;
- Nome da estação de trabalho;
- Informações de destino para qual o dado seria copiado;
- Histórico completo de alteração de incidentes.

31. Deve ter a capacidade de importar um conjunto de pré-configurações do sistema otimizadas para verticais das indústrias específicas, contando com dados de pesquisa em português.
32. A solução deve ser agnóstica a linguística. Todos os mecanismos de identificação de dados, por exemplo: palavras, dicionários e Machine Learning, devem funcionar de forma igual em qualquer linguagem.
33. A solução deve proteger documentos em pelo menos 40 tipos de idiomas.
34. A solução deve incluir um mecanismo de análise de segurança, que é exclusivamente responsável pela modelagem estatística de dados e análise de comportamento suspeito dos usuários, com o objetivo de identificar e agrupar incidentes comuns a um determinado usuário ou estação de trabalho, automaticamente e usando uma pontuação de risco atribuída.
35. Deve permitir que sejam visualizados e identificados rapidamente os usuários ou estações de trabalho com o mais alto nível de risco para a organização, como resultado dos incidentes de segurança associados a eles.
36. A solução deve possuir, com mais de 1700 modelos de políticas predefinidos agrupados por localização geográfica e tipo de organização para identificar regras, regulamentos ou leis que a organização deve cumprir e aplicar as políticas correspondentes sem a necessidade de impressão digital dos dados envolvidos.
37. Deve possibilitar a realização de backup e restore de configurações, incidentes e políticas da plataforma.
38. Deve possibilitar integração nativa com soluções de classificação da informação, de forma a monitorar o uso de dados classificados nos canais de detecção e também a possibilidade de imposição de classificação durante a descoberta de dados em servidores de arquivos, por exemplo.

2. **Criação de Políticas e Detecção de Conteúdo Confidencial**
    1. Deve ter a capacidade de utilizar, no mínimo, os critérios abaixo para criação de políticas:
        - Palavra ou conjunto de palavras chave;
        - Identificadores pré existentes o customizados (CPF, CNPJ, Cartão de crédito, etc.);
        - Expressões regulares com possibilidade de adaptação para qualquer padrão de dados existentes;
        - Nível de classificação da informação;
        - Tipo de arquivo;
        - Nome e extensão de arquivos;
        - Bases de indexação previamente carregadas;
        - Tamanho de dados trafegados;
        - Quantidade de anexos de um e-mail;
        - Usuários/E-mails internos;
        - Estações de trabalho/servidores específicos;
        - Localização da estação de trabalho (Dentro ou fora da rede interna);
        - Tipo de estação (Laptop ou desktop);

- E-mails ou domínios externos;
- Direção do tráfego (Entrada ou saída);
- Protocolos de rede ou canais da estação;
- E-mails em dispositivos móveis;
- Dados enviados para impressora;
- Qualquer aplicação em execução na estação de trabalho;
- Cópias para caminhos de rede.

2. Deve possibilitar criação de regras de exclusões para as políticas de acordo com grupos de usuários fornecidos pelo active directory.
3. O produto deve possuir modelos de políticas de detecção com base em regulamentações e melhores práticas de mercado, para no mínimo:
    - SOX;
    - PCI;
    - HIPAA;
    - GDPR.
4. A solução deve possibilitar a criação de regras para adequação a LGPD.
5. A solução deve possuir templates de políticas de detecção, para no mínimo os seguintes temas:
    - Imagens com conteúdo inapropriado;
    - Linguagem ofensiva ou racismo;
    - Cyber Bullying;
    - Problemas relacionados a jogos de azar;
    - Dados confidenciais e propriedade intelectual;
    - Dados que envolvem segurança de redes;
    - Busca de informações relacionadas a indicadores de comprometimento.
6. Deve ter a capacidade para análise de conteúdo nos mais diversos tipos de arquivos, para no mínimo:
    - Texto (TXT, ASC, HTML, DOC, DOCX, SWX, ODT);
    - Compactados (ZIP, RAR, GZ, LHA, HQX, JAR, 7z);
    - CAD (DWG, DXF, VSD, DGN);
    - Planilhas (XLS, XLSX, 123, SXC, ODS, CSV);
    - Apresentações (PPT, PPTX, SXI, SXP, ODP);
    - Outros (PDF, MDB).
7. Deve permitir criar políticas que combinam várias tecnologias e regras de detecção com regras "E/OU" lógicas e de exceção.
8. Permitir a escrita de expressões lógicas para configuração das regras de detecção, exemplo:("Condição 1" OU "Condição 2") E NÃO "Condição 3".
9. Deve ter a capacidade de construir políticas de detecção, configurando-se o grau de severidade adotado para cada regra criada, conforme o número de correspondências que se deseja encontrar em cada possível violação.
10. A solução deve fornecer a implantação de políticas DLP corporativas de forma unificada, ou seja, uma única política de DLP pode ser aplicada a todos os módulos (network, endpoints e aplicações em cloud).
11. As políticas de detecção devem possuir, no mínimo:
    - A capacidade de normalização de todas as variações comuns de apresentação de dados (por exemplo, se a extração de dados contiver "123456789", deverá ter como correspondente "123-45-6789", "123456789", "123.45.6789", etc.);
    - A capacidade de detecção usando palavras e frases-chave totalmente configuráveis;
    - A capacidade de colocar múltiplas palavras/frases em uma única regra de detecção.
    - A capacidade nativa de detectar documentos de identificação e números de impostos internacionais, para no mínimo, os países EUA, França e Brasil.

- A capacidade de detectar faixas de números válidos para determinados tipos de dados, tal como no mínimo, número de cartão de crédito válido.

12. A solução deve incluir mecanismos de proteção de dados contra vazamentos lentos e sofisticados (DRIP DLP), ou seja, deve monitorar a perda lenta de dados em eventos cumulativos;
13. A solução deve fornecer políticas predefinidas para identificar expressões potenciais que são indicativas de bullying cibernético, padrões de pensamento suicida ou conteudo malicioso;
14. A solução deve ter inteligência artificial composta de técnicas que permitem aprender com exemplos de dados em vez de regras de dados pré-classificadas. O produto deve trabalhar com algoritmos de aprendizagem supervisionados e algoritmos de aprendizagem não-Supervisados para classificar e aprender com as informações descobertas nos endpoints;

3. **Resposta a incidentes**

1. Deve possuir notificações personalizáveis através de e-mail em caso de violação de política.
2. A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviados nas notificações.
3. Deve permitir tomar ações automáticas pré-definidas na detecção de incidentes, para no mínimo:
    - Permitir o envio, deletar anexos, quarentenar ou criptografar e-mails;
    - Permitir ou bloquear tráfego de dados sensíveis via FTP;
    - Permitir ou bloquear tráfego de dados sensíveis via HTTP/HTTPs;
    - Através do agente, permitir, bloquear ou solicitar justificativa para o tráfego em pelo menos: Qualquer tipo de aplicação executada pelo Sistema operacional, cópia para armazenamentos de rede, impressão de arquivos, E-mails enviados, upload para páginas Web e cópias para dispositivos USB.
    - Permitir a possibilidade de busca ou não de detalhes sobre o incidente durante o registro;
    - Execução de atividades customizadas;
    - Enviar mensagens para servidores de syslog;
    - Enviar notificações por e-mail;
    - Manipular arquivos durante a descoberta de rede.
4. Deve permitir vários botões de reposta na interface gráfica dos incidentes totalmente configuráveis.
5. Os botões de resposta na interface gráfica dos incidentes devem possibilitar no mínimo:
    - Designar o incidente para resposta de alguém específico;
    - Modificar o status do incidente;
    - Modificar a severidade do incidente;
    - Ignorar o incidente;
    - Adicionar TAG no incidente;
    - Adicionar comentários no incidente;
    - Fazer Download do incidente;
    - Deletar o incidente;
    - Acionar scripts ou tarefas customizadas;
    - Escalar o incidente para o gerente do usuário envolvido;
    - Escalar o incidente para uma pessoa específica.
6. Deve exibir todos os detalhes do incidente em uma única página.

7. Deve permitir exibir partes específicas da mensagem ou arquivo que violou as políticas, através de uma visualização rápida na tela do incidente, sem a necessidade de usar software externo.
8. Deve permitir armazenar a mensagem e o arquivo original que gerou o incidente.
9. Deve exibir todo o histórico do incidente, incluindo alterações, edições e respostas executadas automaticamente e manualmente.

4. **Relatórios**
    1. Deve exibir relatórios personalizáveis sobre os incidentes e utilizar filtros, no mínimo de:
        - Ação aplicada;
        - Responsável pela análise;
        - Nome da aplicação;
        - Departamento;
        - Canal de detecção;
        - Nível de classificação da informação;
        - Destino de tráfego da informação;
        - Tipo estação (Desktop ou Laptop);
        - ID do incidente
        - Hora do incidente
        - Nome do arquivo trafegado;
        - Histórico do incidente;
        - Incidentes marcados como ignorados;
        - TAGs de incidentes;
        - Quantidade de informação sensível trafegada;
        - Propriedades do arquivo;
        - Política acionada;
        - Nome da regra acionada;
        - Severidade do incidente;
        - Origem do incidente;
        - Status do incidente;
        - Tamanho da transação;
        - Dados relacionados as violações encontradas.
    2. Deve exportar relatórios para os formatos HTML, PDF e CSV.
    3. Deve apresentar um painel para visualização dos relatórios.
    4. Deve ter a capacidade para configurar, salvar relatórios e painéis personalizados por usuário.
    5. Deve possuir painéis (Dashboards) para, no mínimo os seguintes itens:
        - Incidentes criados nos últimos X dias;
        - Políticas mais acionadas;
        - Incidentes por severidade;
        - Incidentes por ação tomada;
        - Incidentes por canais de detecção;
        - Incidentes por origem/destino;
        - Usuários que mais violam políticas.
    6. A solução deve se integrar nativamente a solução de comportamento dos usuários e correlacionar as informações;
    7. A solução deve exibir informações dos usuários, com pelo menos 20 incidentes durante o período analisado em conjunto com número de correspondências, tamanho da transação, conteúdo e políticas infringidas;

5. **Módulo de Área de Armazenamento**
    1. Deve verificar existência de conteúdo confidencial em file systems sem a necessidade de agentes de coleta (agent-less) para no mínimo CIFS, NFS, SMB e NTFS.
    2. Deve permitir a análise dos file systems através de agentes ou sem agente em sistemas operacionais, para no mínimo:
        - Windows Server 2008 R2;
        - Windows Server 2012;
        - Windows Server 2016;
        - Red Hat Enterprise Linux 6 e demais releases da versão;
        - Red Hat Enterprise Linux 7 e demais releases da versão.
    3. Deve analisar conteúdo sigiloso armazenado em ambientes complexos, para no mínimo:
        - Microsoft Sharepoint;
        - Lotus Notes;
        - Microsoft SQL Server;
        - Oracle;
        - MySQL
        - Microsoft Exchange;
    4. Deve analisar conteúdo sigiloso em aplicações em nuvem:
        - Salesforce,
        - AW
        - ServiceNow
        - Facebook Workplace
        - G-Suite
        - Google Cloud Platform
        - Azure.
        - One Drive
        - Trello
        - Dropbox
        - Slack
        - GitHub
        - LinkedIn
    5. Deve possuir a capacidade de verificar arquivos Microsoft "PST", possibilitando executar varreduras tanto nas mensagens, assim como, nos arquivos anexos as mensagens.
    6. Possibilidade de mover para quarentena arquivos que violam políticas de segurança.
    7. Deve manter o arquivo no local original, substituindo seu conteúdo por uma mensagem customizável, como aviso e orientação para o usuário.
    8. Permitir a remoção do arquivo que está em quarentena e restaurá-lo de volta ao local original.
    9. Deve permitir coleta automática de arquivos que violem políticas para análise legal (evidência).
    10. Permitir a criação de respostas personalizadas para incidentes.
    11. Exibir detalhes, no incidente, dos arquivos que violam as políticas.
    12. Permitir a visualização das permissões do arquivo.
    13. Deve possibilitar notificação através de e-mail e alerta Syslog em caso de violação de política.
    14. Deve permitir agendamento de varreduras automáticas.
    15. Possuir mecanismo de verificação incremental, na qual apenas arquivos novos, ou alterados, sejam verificados.

16. Deve permitir configurar janelas de tempo para verificações, interrompendo o processo automaticamente ao fim do período configurado.
17. Preservar os atributos originais do arquivo, inclusive o atributo "Acessado em", enquanto realiza a verificação.
18. Possuir capacidade de pausar, manualmente, a verificação.
19. Deve utilizar técnicas de paralelismo e controle de banda.
20. Permitir o controle da velocidade das verificações para limitar o uso da largura de banda da rede.
21. Deve ter a capacidade de reutilizar uma única credencial (nome de usuário/senha) em múltiplos alvos a serem verificados.
22. Permitir a verificação simultânea em várias fontes distintas.
23. Permitir limitar quais portas de comunicação serão utilizadas entre o sistema-alvo e o servidor que faz a verificação.
24. Deve permitir aplicar filtros para verificar na varredura de arquivos de um determinado tipo ou em certo diretório.
25. Deve permitir aplicar filtros para verificar na varredura de arquivos a idade E/ou o tamanho de arquivos.

6. **Módulo de Terminal de Usuário**
    1. Capacidade de descobrir fuga de informações sensíveis, por meio de agente.
    2. Possibilidade de aplicação de políticas mesmo quando o agente não tem comunicação com o servidor de gerenciamento.
    3. Possibilidade de armazenamento em cache, dos arquivos que causaram o incidente até que o usuário se conecte, novamente, à rede corporativa.
    4. A solução possuir a funcionalidade de OCR em arquivos do tipo imagem, no mínimo para:
        - Jpeg
        - Bmp
        - Png
        - Gif
        - Tiff
    5. Monitorar e bloquear dados copiados para dispositivos de armazenamento removível (USB).
    6. A solução deverá possuir capacidade de analisar arquivos menos de 1 kbyte.
    7. Possibilidade de criptografar dados sensíveis copiados para dispositivos USB, sem a necessidade de soluções adicionais.
    8. A solução deve ser capaz de detectar e proteger informações estruturadas de dados, por exemplo, de bancos de dados.
    9. a solução de ponto final deve ser capaz de descobrir e proteger informações estruturadas de dados sem exigir uma conexão com o servidor remoto
    10.
    11. Permitir a monitoração e bloqueio para dados copiados para CD/DVD.
    12. Permitir a monitoração e bloqueio para dados enviados a qualquer tipo de impressora local e de rede.
    13. Permitir a monitoração e bloqueio para ações de copiar e colar.
    14. Permitir a monitoração e bloqueio de dados sensíveis trafegados via e-mail corporativo.
    15. Permitir a monitoração e bloqueio para transmissões HTTPS pelo menos nos seguintes navegadores:
        - Internet Explorer;
        - Microsoft Edge;
        - Mozilla Firefox;

- Google Chrome;
- Safari.

16. Permitir a monitoração e bloqueio para transmissões HTTP.
17. Permitir a monitoração e bloqueio para transmissões via FTP.
18. Permitir a monitoração e bloqueio para uso de dados confidenciais por qualquer aplicativo, incluindo programas de criptografia não autorizados.
19. Permitir a monitoração e bloqueio para dados copiados para compartilhamentos de rede pelo Windows Explorer.
20. A Solução deve possuir monitoramento, por padrão, para pelo menos os seguintes aplicativos:
    - Chrome;
    - Firefox;
    - Internet Explorer (IE);
    - Microsoft Edge;
    - Opera;
    - Safari;
    - Tor;
    - Torch;
    - Acoustica MP3 CD Burner;
    - Alcohol 120%;
    - CD-Mate;
    - Disk Utility;
    - iTunes;
    - Nero Burning ROM;
    - Roxio – Easy Media Creator;
    - Windows Media Player;
    - Amazon Cloud Drive;
    - Box;
    - Dropbox;
    - Egnyte;
    - Google Drive;
    - iCloud;
    - OneDrive;
    - Salesforce Files;
    - ShareFile;
    - Syncplicity;
    - WatchDox;
    - Apple Mail;
    - Eudora;
    - Lotus Notes;
    - MailMate;
    - Microsoft Outlook;
    - Microsoft Outlook Express;
    - Mozilla Thunderbird;
    - Pegasus Mail;
    - Postbox;
    - Sparrow;
    - Windows Live Mail;
    - Windows Mail;
    - DK2 Network Server Remote Monitor - DK2 DESkey;
    - File Encryption XP;

- Windows Privacy Tray (WinPT);
- Core FTP LE;
- Cute FTP Home 8.2;
- File Transfer Program (Microsoft Utility);
- FileZilla FTP Client;
- Flash FXP 3.6 build 1240;
- FTP Voyager 15;
- Ipswitch WS FTP Home;
- Leech FTP;
- Serv-U;
- Smart FTP Client;
- Adium;
- AIM;
- Apple Messages;
- Camfrog;
- Cisco WebEx;
- GoToMeeting;
- ICQ;
- Jabber Messenger;
- ManyCam;
- Microsoft Lync 2010;
- Miranda IM;
- ooVoo;
- Pidgin;
- Skype for Business;
- TeamViewer;
- Teccent QQ;
- Trillian;
- Viber;
- Yahoo! Instant Messenger;
- Adobe Reader;
- Bean;
- Eclipse;
- Emacs;
- Evernote;
- Keynote;
- LibreOffice/Apache OpenOffice;
- Mellel;
- Microsoft Office Access;
- Microsoft Office Excel;
- Microsoft Office InfoPath;
- Microsoft OneNote;
- Microsoft Office PowerPoint;
- Microsoft Office Project;
- Microsoft Office Publisher;
- Microsoft Office Visio;
- Microsoft Office Word;
- Notepad;
- Numbers;
- OpenOffice.org Calc;
- OpenOffice.org Draw;

- OpenOffice.org Math;
- OpenOffice.org Writer;
- Pages;
- Reminders;
- Stickies;
- TextEdit;
- WordPad;
- AllegianceMD;
- eClinicalWorks;
- ECLIPSYS;
- INGENIX;
- inteGreat;
- Sequel;
- Ares;
- Azureus;
- BearShare;
- BitComet;
- BitLord;
- BitTornado;
- BitTorrent;
- eMule;
- FrostWire;
- Kazaa Lite;
- LimeWire;
- Pando;
- Transmission;
- uTorrent;
- 7-Zip File Manager;
- iArchiver;
- WinRAR;
- WinZip;
- Bluetooth Stack COM Server - BTStackServer;
- Fsquirt;
- iTunes;
- Wireless Link File Transfer App – Irftp;
- WCESMgr;
- Aplicor (online);
- CRM.com;
- HostAnalytics;
- Intacct;
- NetSuite;
- Oracle CRM on demand;
- RightNow;
- Salesforce;
- WorkDay;
- FoxPro;
- Ld;
- MSTSC;
- NT backup tool;
- Vista backup tool;
- VMWare.

21. A solução deve permitir a criação de qualquer aplicativo existente que não venha cadastrado por padrão.
22. Definir dispositivos removíveis individuais, ou grupos de dispositivos, como confiáveis e criar exceções de políticas para esses dispositivos.
23. A solução deve suportar a integração com o Microsoft RMS (Azure Information Protection), para descriptografar e analisar arquivos do tipo Office (Word, Excel, Power Point entre outros) que foram previamente criptografados pelo Azure RMS ou RD (Active Directory) RMS.
24. O agente deverá suportar, no mínimo, Windows 7 (32 e 64 bits), Windows 2008 R2 Enterprise (64bit), Windows 10, Windows Server 2012, Windows Server 2016 e Apple MacOS.
25. Todas as funções devem ser executadas por um único agente.
26. Permitir a desativação do agente pela console de gerenciamento.
27. Possuir mecanismo que reinicie o agente caso o usuário tente interromper o serviço.
28. Possuir proteção contra desinstalação do agente.
29. Capacidade de apresentar as mensagens de notificações em português.
30. Possuir a capacidade de envio de notificação automática, por e-mail, para o usuário e administrador durante a ocorrência de um incidente.
31. Possuir a capacidade de gerenciamento da saúde dos agentes.
32. Deve permitir a distribuição do agente através de GPO ou por ferramenta de terceiros.
33. Deve ter a capacidade de permitir ao usuário justificar a movimentação de conteúdo confidencial, a partir do alerta em “pop-up”, escolhendo opções de justificativa configuráveis pelo administrador da ferramenta.
34. O agente deve executar varredura local para verificar se a estação do usuário possui conteúdo confidencial.
35. A solução deve ser capaz de proteger informações de impressão digital de dados estruturados offline e sem a necessidade de qualquer comunicação com servidores de administração ou gerenciamento ou repositórios de impressões digitais
36. O endpoint deve poder pode permitir automaticamente a transferência de informações específicas em forma criptografada, configurados pelo administrador;
37. O endpoint deve permitirá que o usuário defina sua própria senha para criptografia e arquivos criptografados.
38. A solução deve permitir que o arquivo criptografado possa ser visualizado ou aberto em computadores onde o endpoint não está instalado usando a senha original do emissor do documento.
    1. Essa funcionalidade deve ser atendida através do próprio agente sem a necessidade de adicionar uma solução de terceiros;

1.
2. Deve permitir realizar verificações incrementais, apenas em arquivos novos e alterados.
3. Permitir a instalação do agente de modo oculto ou em modo de interação com o usuário.
4. Quando utilizado em modo interativo, permitir sincronização de políticas de forma manual, através de acionamento de botão no agente.
5. A solução deve suportar integração dinâmica com o User Behavior Analytics ou plataformas UAM.
6. Deve permitir incluir na solução de UAM ou User Behavior Analytics a coleta de eventos produzidos pela solução DLP e posterior análise e modelagem realizada pelo UAM ou User Behavior Analytics, com o objetivo de calcular um nível de risco por usuário.
7. Deve permitir atraves do nível de risco obtido pelos algoritmos do UAM ou User Behaivior Analytics , esses resultados devem ser devolvidos à solução DLP original para aplicar ações imediatas ou dinâmicas, sem a intervenção humana do administrador da solução.

8. Alimentar a console de gerenciamento, com pelo menos, as seguintes informações do agente:
    - Nome do computador;
    - IP Address;
    - Usuário logado;
    - Última vez que o agente se comunicou com a o servidor central;
    - Identificador do grupo de políticas utilizados;
    - Campo que informa se o agente está em sincronismo com as últimas políticas/configurações disponibilizadas pelo administrador;
    - Versão do agente;
    - Versão da política instalada.

1. **Módulo de rede**
    1. Permitir a monitoração/bloqueio do e-mail corporativo, evitando que e-mails com dados sigilosos sejam enviados para fora da organização, inclusive em smartphones e tablets.
    2. Possibilidade de colocar mensagens de correio eletrônico em quarentena para análise.
    3. Permitir a monitoração/bloqueio de tráfego WEB, evitando que dados sigilosos saiam da organização por este canal, inclusive em smartphones e tablets.
    4. Capacidade de monitorar/bloquear o tráfego informações sensíveis em posts de redes sociais.
    5. Permitir a monitoração de qualquer protocolo baseado em TCP, como o SMTP, inclusive anexos; HTTP, inclusive arquivos de upload; FTP ativo e passivo.
    6. Capacidade de monitorar o vazamento de dados por meio de softwares de Mensagens Instantâneas.
    7. Permitir a classificação dos protocolos, mesmo quando executados em portas que não são padrão.
    8. Capacidade de filtrar o tráfego da rede para inspeção, segundo o protocolo, faixa de IP e remetente/destinatário de e-mail.

2. **Módulo de Classificação da informação**
    1. A solução deve ter integração nativa com soluções de Data Loss Prevention;
    2. A solução deve ter capacidade de realizar a rotulagem de informações recém criadas ou pré-existentes sem a necessidade de alterar as propriedades do arquivo, somente seus metadados;
    3. A solução de deve ter a capacidade de automaticamente classificar arquivos no mínimo para os seguintes tipos de arquivo;
        - Word, Excel, PowerPoint, Outlook, Project e Microsoft Office.
        - Open Office
        - PDF
        - ZIP
        - MSG, TIF e EML files
        - JPEG
        - HTML
    4. A solução deve ter a capacidade de proporcionar ao usuário a classificar a informação recém-criada de forma que as soluções integradas possam usufruir desta classificação e incluí-las de forma automática dentro de políticas previamente criadas;

5. A solução deve permitir que as soluções integradas detectem os metadados do Classificador, a fim de evitar que o arquivo seja copiado e notificar o usuário/administrador.
6. A solução deve possuir integração com o sistema operacional Windows, permitindo que as ações de classificação do usuário sejam logadas pelo sistema operacional;
7. A solução deve possibilitar a classificação da informação pelo usuário, possibilitando classificar a informação recém-criada em no mínimo:
    - Informação Pública;
    - Informação Restrita;
    - Informação Interna;
    - Informação Confidencial
    - Informação Pessoal.
8. A solução deve possibilitar classificar tanto a informação recém-criada, como pré-existentes;
9. A solução deve ter integração para classificação da informação pelo usuário para no mínimo:
    - Word, Excel, PowerPoint, Outlook, Project e Microsoft Office.
    - Open Office
    - PDF
    - ZIP
10. A solução deve ser capaz de analisar o comportamento malicioso do usuário, priorizando alertas correlacionados com diversas soluções de segurança em produção, contendo desta forma as ameaças, possibilitando a partir de um único relatório indicar um possível ataque;
11. A solução deve ter a capacidade de analisar as informações em conformidade com normas e regulamentações, para no mínimo GDPR, PCI, DSS, SOX, HIPAA;
12. A solução deve basear o coeficiente comportamental de risco, indicando a priorização das ações e identificando se o comportamento malicioso é interno ou se é externo, correlacionando para isso informações de no mínimo:
    - Incidentes recebidos da solução de DLP local;
    - Incidentes recebidos pela solução de criptografia, na tentativa de acesso aos dados sensíveis;
    - Incidentes de classificação de documentos/informação por parte do usuário final;
    - Incidentes recebidos da rede de inteligência mundial do fabricante da solução;
13. A solução deve ser capaz de identificar os usuários expostos aos maiores níveis de risco e possibilitar a partir desta informação refinar as políticas de proteção dos dados;
14. A solução deve permitir que as soluções integradas possam gerar um relatório sobre as marcas de metadados do Classificador, permitindo no mínimo:
    - Localização de arquivo por classificação;
    - Alteração na permissão dos arquivos;
    - Adicionar criptografia no arquivo;
15. A solução deve ser capaz de inserir marcações visuais em e-mails (ex. Outlook) para o cabeçalho ou rodapé;
16. A solução deve classificar e-mails enviados com arquivos anexados de acordo com a classificação do anexo. Esta classificação deve ser realizada antes do envio.
17. solução deve ter a capacidade de calcular a pontuação de risco de cada usuário a partir do comportamento do passado e do presente;
18. A solução deve ter a capacidade de criar relatórios de risco, baseados nos maiores infratores;
19. A solução deve ter a capacidade de criar políticas de alerta e bloqueio, conforme segue:
    - Políticas de Alerta: É enviado um alerta ao usuário, no entanto, é possível ao usuário salvar o arquivo e enviá-lo por e-mail;

- Políticas de Bloqueio: É enviado um alerta ao usuário, independentemente do nível de classificação do arquivo, onde não será possível salvar, nem tão pouco enviar o arquivo;

20. A solução deverá possibilitar no mínimo formas de:
    - Descoberta de Informações;
    - O fluxo da informação;
    - Proteger contra a exfiltração da informação, quer seja intencional, quer seja inadvertida;
    - Assegurar conformidade com as políticas de acesso e políticas de segurança;
    - Possibilitar a manutenção da trilha de auditoria por razões de controle e conformidade;
    - Possibilitar alertar aos usuários quando da criação de informações, sobre as políticas de gerenciamento da informação;
    - Possibilitar o rastreio de "onde" os dados não estruturados estão sendo criados e "quem" os estão criando;
21. A solução deve permitir forçar a aplicação de políticas antes que os dados saiam da gerência do Órgão, para no mínimo:
    - Políticas de TAG;
    - Políticas de introdução de cabeçalhos (append headers);
    - Políticas de inclusão de metadados (add metadata);
22. A solução deve ser capaz de implementar gráficos comparativos de risco comportamental entre no mínimo:
    - Usuários sob o mesmo Gerente;
    - Usuários do mesmo departamento;
    - Comportamento dos endpoints;
    - Comportamento das informações marcadas com TAG de dados sensíveis;
    - Frequência com que as políticas de proteção dos documentos são violadas;
    - Envio de informações sensíveis por e-mail e web;

Gleicimara Chagas Lustosa

De: Andre Wilson Pimenta Santana
Enviado em: terça-feira, 30 de novembro de 2021 10:44
Para: Gleicimara Chagas Lustosa
Assunto: ENC: solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)
Anexos: 2021112901 - Funasa - Proposta aquisição DLP.pdf

De: Hélio Ferreira da Silva Junior [mailto:helio.ferreira@ish.com.br]
Enviada em: segunda-feira, 29 de novembro de 2021 18:53
Para: Andre Wilson Pimenta Santana <andre.pimenta@funasa.gov.br>
Assunto: Re: solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

Andre,
Boa noite.

Conforme solicitado, segue em anexo nossa proposta de preço.

Coloco-me a disposição em caso de duvida.

Atenciosamente,

HELIO FERREIRA
Executivo de Negócios

+55 61 3029 8666 | +55 61 98588 8
Helio.ferreira@ish.com.br
www.ish.com.br

De: Andre Wilson Pimenta Santana <andre.pimenta@funasa.gov.br>
Data: terça-feira, 16 de novembro de 2021 16:17
Para: Vitor Teixeira Costa <vitor.costa@ish.com.br>, "andre.oliveira@arvvo.com.br" <andre.oliveira@arvvo.com.br>, "contato@grgtech.io" <contato@grgtech.io>, "thiago@vonk.com.br" <thiago@vonk.com.br>, "renata@niva.com.br" <renata@niva.com.br>, "gerson.cezar@dsr9.com.br" <gerson.cezar@dsr9.com.br>, "hugobsa@algartech.com" <hugobsa@algartech.com>, "alex@cdti.com.br" <alex@cdti.com.br>, "franco.damata@servix.com" <franco.damata@servix.com>, "emilio@netway.com.br" <emilio@netway.com.br>
Assunto: solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

Prezado,

solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

Licenciamento para 36 meses

OBJETO DA CONTRATAÇÃO

1.1. Aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP), contemplando licenciamento, garantia, suporte e implantação, de acordo com as quantidades e especificações descritas neste Termo de Referência. **Licenciamento para 36 meses**

item	Descrição	Unidade	Quantidade
1	Aquisição de licenças de software de solução de prevenção de vazamento de dados – Data Loss Prevention – DLP.	UN	3,190
2	Treinamento	Turma	1

1. Descrição da Solução de Tecnologia da Informação

Este Anexo especifica as características técnicas da solução de Data Loss Prevention / DLP a ser adquiridapara implementação no ambiente do FUNASA. Detalhamos neste Anexo os componentes da solução de DLP.

ITEM	ESPECIFICAÇÕES TÉCNICAS E REQUISITOS MÍNIMOS
01	Aquisição de licenças de software de solução de prevenção de vazamento de dados - Data LossPrevention (DLP)

2. Solução

2.1.1. Deverá ser em multicamada, permitindo escalabilidade para um ambiente computacional distribuídoem áreas geográficas diferentes;

2.1.2. Tolerância a links de alta latência para servidores remotos, permitindo o suporte a locais remotos viaWAN e mecanismos de recuperação automática integrados ao servidor;

2.1.3. Atualizações dos softwares da solução serão centralizadas, a partir de um console, para os servidores eos terminais;

2.1.4. Possuir relatórios de tráfego e de desempenho do sistema e indicadores de rendimento;

2.1.5. Permitir a utilização de Banco de dados em alta disponibilidade e suporte ao clustering;

2.1.6. Capacidade de excluir incidentes como um todo, desejável que se possa eliminar detalhes específicosde incidentes do banco de dados;

2.2. Enviar alertas em tempo real, por e-mail, sobre as condições do nível do sistema;

2.3. Suportar sistema de virtualização VMware e/ou RHEV;

2.4. Suportar integração do cliente integrado com o Microsoft Active Directory;

2.5. A solução deverá criptografar os dados na captura - monitoração, servidores de descoberta e agentes;

2.6. Armazenamento de dados no banco de dados de incidentes, em formato criptografado;

2.7. Os canais de comunicação entre componentes do sistema deverão ser autenticados e criptografados;

2.8. Todas as senhas do sistema deverão ser criptografadas, incluindo as credenciais de logon para varredurade arquivos;

2.9. Possuir registros detalhados de auditoria de atividades de transações do banco de dados e alterações depolíticas;

2.10. Desejável ter capacidade de obter a "impressão digital" de dados estruturados e não estruturados (MSOffice docs, PDFs, EMC Documentum, diagramas CAD/CAM, código-fonte, etc.);

2.11. Capacidade de especificar quais colunas dos dados estruturados identificados são necessárias paralocalizar uma correspondência, como por exemplo, utilizar nome, sobrenome e CPF;

2.12. Opção de permitir que qualquer um, ou todos, os proprietários de dados enviem seus dados pessoaispara fora da rede corporativa, sem violar uma regra de detecção;

2.13. Capacidade para detectar, nos documentos não estruturados identificados, as extrações ou derivaçõesdos documentos;

2.14. Capacidade de normalizar todas as variações comuns de apresentação de dados;

2.15. Detectar documentos não estruturados de um tipo específico, como código-fonte protegido, contratos,ou outros tipos de conteúdo especificados pelo contratante, após usar capacidades nativas de aprendizado

automático para analisar um conjunto de amostras;

2.16. Permitir detectar documentos não estruturados;

2.17. Permite a criação de padrão de identificação utilizando dados internos da instituição de modo acustomizar a ferramenta;

2.18. Permite personalizar padrões pré-configurados de identificação de dados;

2.19. Realizar detecção de acordo com expressões regulares configuráveis;

2.20. Detectar por tipo de arquivo, por nome e extensão de arquivo e protocolo de transmissão;

2.21. Permitir a criação de assinaturas personalizadas de tipos de arquivos que não são suportadas porpadrão;

2.22. Capacidade de integrar diretamente com LDAP (MS Active Directory) para criar regras de detecção determinal baseadas em usuário ou grupo. Políticas diferentes podem ser aplicadas de acordo com o usuário que fez o login, mesmo em uma máquina compartilhada;

2.23. Permitir a exportação/importação das regras de detecção existentes;

2.24. Possuir mecanismo de envio de notificações personalizadas por e-mail aos administradores;

2.25. Permitir a configuração de respostas automáticas com base na severidade, contagem de combinações epolítica;

2.26. Permitir a criação de perfis para administração de servidores, administração de usuário, criação eedição de política;

2.27. Permitir atribuir de modo automático e manual, proprietários de dados por incidente e agendar o envioautomatizado de listas de incidentes personalizadas para os respectivos proprietários;

2.28. Armazenar e exibir a mensagem original ou arquivo que gerou o incidente;

2.29. Em um determinado incidente, permitir a verificação por assunto, remetente, destinatário, nome dearquivo, proprietário do arquivo, nome de usuário e política;

2.30. Exibir todo o histórico do incidente, inclusive as alterações e edições referentes ao mesmo;

2.31. Permitir a exportação da lista de incidentes em ao menos 1 destes formatos: HTML, XML, TXT, PDF;

2.32. Interface de administração única para todos os incidentes de armazenamento, rede e terminal deusuário;

2.33. Possuir interface WEB, compatível, no mínimo, com os navegadores Internet Explorer, Mozilla Firefoxe Google Chrome;

2.34. Relatório de incidentes e tendências por empresa, departamento e usuário, utilizando o LDAP (MSActive Directory) corporativo;

2.35. Permitir agrupar, filtrar e classificar relatórios;

2.36. A solução possuir a funcionalidade de Discovery em arquivos do tipo imagem, no mínimo para:

2.36.1. Jpeg;

2.36.2. Bmp;

2.36.3. Png;

2.37. Capacidade de enviar relatórios por e-mail via agendamento;

2.38. Capacidade de exportar os relatórios no formato HTML, XML, TXT, PDF;

2.39. Permitir executar relatórios em banco de dados, mantendo o desempenho da ferramenta.

3. Gerenciamento

3.1. As configurações de todos os módulos de detecção e criação de relatórios deverão ser realizadas atravésda mesma console;

3.2. Deve ter console de gerenciamento via tecnologia Web (HTTP e/ou HTTPS);

3.3. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, nomínimo, nos sistemas operacionais:

3.3.1. Microsoft Windows Server;

3.3.2. RedHat Enterprise Linux

3.4. Deverá possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuáriosenvolvidos num incidente detectado;

3.5. Deverá possuir integração com Active Directory, para autenticação de usuários da solução;

3.6. Deverá ter a capacidade para criação das contas de usuário no console de gerenciamento com diferentesníveis de acesso, para no mínimo, administração e operação;

3.7. Deverá utilizar criptografia para comunicação, no mínimo, entre console de gerenciamento e monitores,scanners e agentes;

3.8. Deverá armazenar no banco de dados do produto, de forma cifrada, todos os dados relativos a incidentes;

3.9. Deverá manter um histórico de todas as alterações em configurações e acompanhamentos de incidentes,tanto no console quanto na base de dados;

3.10. Deverá permitir criptografar os dados no momento da captura (monitoração, servidores e agentes);

3.11. Deverá possuir canais de comunicação autenticados e criptografados entre os componentes do sistema;

3.12. Deverá possuir as senhas do sistema com hash e criptografadas e armazenamento seguro das credenciaisde acesso aos repositórios de dados;

3.13. Desejável ter a capacidade de indexação off-line de dados armazenados em sistemas em redes isoladas,sem conectividade pelo DLP;

3.14. Desejável possuir logs detalhados de auditoria de atividade de transações do banco de dados;

3.15. Deverá possuir logs detalhados de auditoria de alterações de políticas;

3.16. Desejável utilizar somente portas de rede padrão, determinadas, fixas e conhecidas;

3.17. Deverá ter suporte a servidores com hardware x86 e sistema operacional Windows e Linux, nãorequerendo a utilização de appliance;

4. Criação de Políticas e Detecção

4.1. Deverá ser fornecido em formato de hardware dedicado (Appliance);

4.2. Deverá possuir módulos de detecção distintos, licenciados de forma independente, gerenciados porconsole único, para:

4.3. Localizar dados confidenciais armazenados em servidores de arquivos, intranets e bancos de dados;

4.4. Localizar dados confidenciais armazenados em estações de trabalho;

4.5. Detectar dados confidenciais em trânsito na rede, em protocolos TCP/IP, capturando tráfego em modopromíscuo;

4.6. Deverá ter a capacidade de bloquear o acesso, movimentação, tráfego e cópia de informaçõesconfidenciais detectadas, sem impacto no Proxy utilizado na infraestrutura;

4.7. Toda política criada na solução deve ser única, compatível e válida para aplicação em qualquer um dosmódulos (agente, monitor de rede, scanner de dado armazenado);

4.8. Deverá ter a capacidade de utilizar, no mínimo, os critérios abaixo para criação de políticas:

4.8.1. Conteúdo detectado em arquivos e tráfego de rede (protocolos);

4.8.2. Remetente e destinatário de correio;

4.8.3. Tipo real (baseado em cabeçalho, não extensão), nome e tamanho do arquivo;

4.9. Protocolo de comunicação utilizado;

4.10. Deverá permitir alterar a criticidade do incidente, baseado em valores de referência e limitesconfiguráveis para, no mínimo:

4.10.1. Quantidade de dados expostos;

4.10.2. Dados específicos expostos;

4.10.3. Arquivos específicos expostos;

4.10.4. Remetente de correio específico;

4.10.5. Destinatário de correio específico;

4.10.6. Protocolo de comunicação utilizado.

4.11. Deverá criar regras de exclusões para as políticas de acordo com grupos de usuários fornecidos peloserviço de diretório, seja AD (Active Directory) quanto LDAP;

4.12. Deverá ter a capacidade para análise de conteúdo nos mais diversos tipos de arquivos, para no mínimo:

4.12.1. Compactados (ZIP, RAR, GZ, LHA, HQX, JAR);

4.12.2. CAD (DWG, DXF, VSD, DGN);

4.12.3. Planilhas (XLS, XLSX, 123, SXC, ODS);

4.12.4. Texto (TXT, ASC, HTML, DOC, DOCX, SWX, ODT);

4.12.5. Apresentações (PPT, PPTX, SXI, SXP, ODP);

4.12.6. Outros (PDF, MDB).

4.13. Deverá ser entregue pelo fornecedor ferramentas e metodologia para extração de cabeçalho com base emamostragem de arquivos;

4.14. A ferramenta deverá ter a capacidade de detectar o formato do documento correto, possibilitandoextrair os dados internos e deixar somente um aviso de confidencialidade, por exemplo.

4.15. Deverá detectar o arquivo pelo seu conteúdo real, e não apenas pela extensão do arquivo;

4.16. Deverá ter a capacidade de indexar através de impressão digital (hash) para dados não estruturados;

4.17. Deverá ter a capacidade de definir o percentual do documento indexado para validar a detecção (porexemplo, 10% do documento indexado);

4.18. Deverá ter a capacidade de normalizar todas as variações comuns de apresentação de dados (por exemplo, se a extração de dados contiver "123456789", deverá ter como correspondente "123-45-6789","123456789",

"123.45.6789", etc.);

4.19. Deverá possuir capacidade de detecção usando palavras e frases-chave totalmente configuráveis;

4.20. Deverá possuir capacidade de colocar múltiplas palavras/frases em uma única regra de detecção;

4.21. Deverá ter a capacidade nativa de detectar uma grande variedade de padrões de dados que representamdados confidenciais (por exemplo, CPFs, depósitos, dados da tarja magnética, IBAN);

4.22. Deverá ter a capacidade nativa de detectar documentos de identificação e outros padrões numéricos dedocumentos oficiais brasileiros, tais como: impostos, CNPJ e afins;

4.23. Deverá permitir detectar faixas de números válidos para determinados tipos de dados, tal como nomínimo, número de cartão de crédito válido;

4.24. Desejável ter a capacidade de excluir automaticamente faixas de números inválidos para tipos de dadosespecíficos, como "ranges" de teste, para no mínimo, cartão de crédito;

4.25. Desejável possuir minimamente modelos de políticas preexistentes que incluem palavras chave epadrões de dados, para no mínimo, as principais normas internacionais Cobit, ISO 27002 e FISMA;

4.26. A atividade de detecção deve ser realizada de forma distribuída, por cada um dos módulos da solução (servidores, agentes e monitores de rede), não podendo ser realizada pelo servidor de gerenciamento central;

4.27. Deverá permitir criar políticas que combinam várias tecnologias e regras de detecção com regras "E/OU"lógicas e de exceção;

4.28. Deverá ter a capacidade de integrar diretamente com AD para criar regras de detecção de endpoint baseada em usuário e grupo. Políticas diferentes podem ser aplicadas de acordo com o usuário que fez ologin, mesmo em uma máquina compartilhada;

4.29. Deverá ter a capacidade de exportar e importar com facilidade as políticas existentes, pela interfacegráfica do console;

4.30. Deverá permitir ocultar certos dados, como informações de identidade do remetente, durante avisualização do Incidente na tela do Console, dependendo do nível de acesso dado ao operador daferramenta, para no mínimo, os seguintes tópicos:

4.30.1. Endereço de e-mail;

4.30.2. Nome de usuário;

4.30.3. Proprietário do arquivo;

4.31. Deverá permitir criar funções de administração separadas, para dados armazenados e dados em uso,estejam na rede ou no endpoint, no mínimo para:

4.31.1. Administração dos servidores;

4.31.2. Administração de usuários;

4.31.3. Criação e edição de políticas;

4.31.4. Solução de incidentes;

4.32. Deverá suportar a verificação de arquivos compactados recursivos (exemplos .zip, .rar dentro de .zip,
.rar);

4.33. Deverá suportar de forma comprovada a detecção de dados no idioma português brasileiro;

4.34. Deverá ter a capacidade de analisar conteúdo de arquivos grandes (maiores que 20MB) anexados em e-mails;

4.35. Deverá identificar informações confidenciais sem a necessidade de acrescentar tags, etiquetas e afins nosarquivos de origem;

4.36. Deverá identificar conteúdos armazenados em colunas específicas de planilhas eletrônicas e em bancosde dados;

4.37. Deverá ser capaz de gerar incidentes para detecção apenas se após um determinado percentual de cópiado conteúdo for atingido;

4.38. Deverá possuir capacidade para identificar conteúdos específicos com base em um padrão pré-determinado, para no mínimo:

4.38.1. CPF;

4.38.2. Carteira de Identidade;

4.38.3. CNPJ;

4.38.4. Cartões de Crédito;

4.39. Deverá possibilitar a utilização de expressões regulares para identificação de conteúdo;

4.40. Deverá possuir notificações personalizáveis através de e-mail em caso de violação de política;

4.41. A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviadosnas notificações;

4.42. Deverá ser possível a notificar automaticamente o remetente e o gerente ou superior hierárquico dousuário envolvido no incidente;

4.43. Deverá permitir tomar ações automáticas pré-definidas na detecção de incidentes, para no mínimo:

4.43.1. Bloqueio de mensagem;

4.43.2. Quarentena de arquivo;

4.43.3. Notificação ao usuário;

4.43.4. Bloqueio do acesso web, bloqueio de cópia e impressão;

4.44. Deverá disponibilizar interface de resposta totalmente personalizável que permita combinações de váriasações de reparo e reação, através do acionamento de um único botão na interface gráfica do Incidente.

4.45. Deverá permitir vários botões de reposta na interface gráfica dos incidentes totalmente configuráveis;

4.46. Desejável exibir todos os detalhes do incidente em uma única página;

4.47. Deverá permitir destacar na tela do incidente os dados confidenciais detectados;

4.48. Deverá permitir exibir partes específicas da mensagem ou arquivo que violou as políticas, através de umavisualização rápida na tela do incidente, sem a necessidade de usar software externo;

4.49. Deverá permitir armazenar a mensagem e o arquivo original que gerou o incidente;

4.50. Deverá possibilitar a exibição na tela do Incidente no console um link que possibilite o download e aabertura destes itens usando um software externo;

4.51. Deverá exibir todo o histórico do incidente, incluindo alterações, edições e respostas executadasautomaticamente e manualmente;

4.52. Deverá ter a capacidade de importar um conjunto de pré-configurações do sistema (incluindo políticas,relatórios, funções e workflow);

4.53. A solução deve possuir integrada no console a funcionalidade de workflow para tratamento e escaladados incidentes;

4.54. As informações detectadas nos incidentes devem ser possíveis de serem visualizadas através da consolede gerenciamento;

4.55. Deverá ser possível ocultar a visualização de evidências de acordo com o nível de permissão atribuído aooperador da ferramenta;

4.56. Devem ser exibidas na console de gerenciamento todas as informações a respeito do incidente para, nomínimo:

4.56.1. Timestamp;

4.56.2. Método de detecção;

4.56.3. Remetente e destinatário;

4.56.4. Mensagens e anexos;

4.56.5. Protocolo e endereço IP;

4.57. Deverá agregar diversos incidentes em um caso para investigação mais detalhada;

4.58. Permitir a exportação dos incidentes para ao menos os formatos: HTML, XML, PDF, TXT, DOCX, deforma que não exista necessidade de credenciais de acesso para visualização off-line das informações;

4.59. Deverá segregar acesso aos incidentes de acordo com características, para no mínimo:

4.59.1. Unidade de negócio;

4.59.2. País;

4.59.3. Gerente do usuário envolvido;

4.59.4. Severidade.

5. Relatórios

5.1. Deverá fornecer relatórios de tendências com gráficos distribuídos em uma linha de tempo;

5.2. Devera exportar relatórios ao menos para dois dos seguintes formatos: HTML, XML, PDF, TXT, DOCX eCSV;

5.3. Devera agendar relatórios para envio automático através de e-mail (datas específicas e periodicamente);

5.4. Devera apresentar um painel de controle para visualização dos relatórios;

5.5. Devera permitir gerar relatórios resumidos por níveis, agrupados, sumarizados e com capacidade dedetalhamento;

5.6. Desejável possuir API para permitir que aplicações de terceiros extraiam dados de incidentes da base dedados do DLP;

5.7. Devera ter a capacidade para configurar, salvar relatórios e painéis de controle personalizados por usuário;

5.8. Devera possibilitar a execução de relatórios em todo o histórico de incidentes armazenados na base dedados e via console web.

6. Módulo de Área de Armazenamento

6.1. Permitir a verificação de sistemas de arquivo do Windows via CIFS, do Unix via NFS e Linux;

6.2. Permitir a verificação de Bancos de dados Oracle e SQL Server;

6.3. Desejável permitir a verificação de servidores MS-SharePoint por meio da API Windows SharePointServices (WSS);

6.4. Devera permitir a análise dos file systems através de agentes em sistemas operacionais, para no mínimo:

6.4.1. Linux;

6.4.2. Windows servers 2008 e superiores;

6.5. Devera analisar conteúdo armazenado em ambientes complexos, para no mínimo:

6.5.1. Microsoft File Server;

6.5.2. Microsoft Sharepoint;

6.5.3. Microsoft SQL Server;

6.5.4. Oracle;

6.5.5. Microsoft Exchange on-premise e Nuvem;

6.5.6. Office365;

6.6. Desejável possuir API para permitir a verificação de repositório de dados;

6.7. Copiar e realocar em quarentena, automaticamente, os arquivos que violam as políticas;

6.8. Coletar, automaticamente, arquivos que correspondem aos critérios da política;

6.9. Desejável permitir a colocação de arquivos personalizados no lugar de arquivos que foram colocados emquarentena;

6.10. Permitir a criação de respostas personalizadas para incidentes

6.11. Permitir a remoção do arquivo que está em quarentena e restaurá-lo de volta ao local original;

6.12. Exibir o local do arquivo e as informações do proprietário dos arquivos que violam as políticas;

6.13. Exibir detalhes do incidente dos arquivos que violam as políticas;

6.14. Permitir a emissão de relatórios dos maiores usuários gerais que editaram arquivos que violam aspolíticas;

6.15. Permitir a emissão de relatórios dos maiores leitores dos arquivos que violam as políticas;

6.16. Permitir a emissão de relatórios do histórico completo de acesso, de todos os usuários, aos arquivos queviolam as políticas;

6.17. Permitir a emissão de relatórios dos arquivos que um usuário específico acessou no último ano;

6.18. Permitir a visualização das permissões efetivas, do Windows e no nível NTFS;

6.19. Permitir a emissão de alertas aos administradores sobre acesso excessivo a pastas ou arquivos, com acapacidade de realizar autorização dos usuários;

6.20. Possuir um único console centralizado para administração;

6.21. Possuir mecanismo de verificação incremental, na qual apenas arquivos novos, ou alterados, sejamverificados;

6.22. Preservar os atributos originais do arquivo, inclusive o atributo "Acessado em", enquanto realiza averificação;

6.23. Possuir capacidade de pausar, manualmente, a verificação;

6.24. Permitir o controle da velocidade das verificações para limitar o uso da largura de banda da rede;

6.25. Permitir a verificação simultânea em vários dispositivos;

6.26. Permitir limitar quais portas de comunicação serão utilizadas entre o sistema-alvo e o servidor que faz averificação.

7. Módulo de Terminal de Usuário

7.1. Possuir opções de verificação, com agente e sem agente;

7.2. Descoberta, baseada em agente, de dados confidenciais em terminais, incluindo relatórios sobre as listasde controle de acesso para os arquivos que violam as políticas;

7.3. O agente deve permitir o armazenamento em cache, dos arquivos que causaram o incidente até que ousuário se conecte, novamente, à rede corporativa;

7.4. Monitorar dados gravados na unidade local;

7.5. Monitorar e bloquear dados copiados para dispositivos de armazenamento removível dos tipos USB;

7.6. Definir dispositivos removíveis individuais, ou grupos de dispositivos, como confiáveis e criar exceçõesde políticas para esses dispositivos;

7.7. Criptografar, automaticamente, os dados confidenciais ao copiá-los para um dispositivo externo dearmazenamento;

7.8. A solução deverá possuir capacidade de analisar arquivos menos de 1 kbyte;

7.9. Permitir a monitoração e bloqueio para dados copiados para unidade de CD/DVD;

7.10. Permitir a monitoração e bloqueio para transmissões HTTP;

7.11. Permitir a monitoração e bloqueio para transmissões HTTPS pelo Internet Explorer, Mozilla Firefox eGoogle Chrome sem a utilização do Proxy da infraestrutura;

7.12. Permitir a monitoração e bloqueio para Transmissões via FTP;

7.13. Permitir a monitoração e bloqueio para dados enviados a qualquer tipo de impressora local e de rede;

7.14. Permitir a monitoração e bloqueio para ações de copiar e colar feitas através da área de transferência doWindows;

7.15. Permitir a monitoração e bloqueio para dados copiados para e a partir de compartilhamentos de redepelo Windows Explorer;

7.16. Permitir a monitoração e bloqueio para uso de dados confidenciais por qualquer aplicativo, incluindoprogramas de criptografia não autorizados e aplicativos com protocolos proprietários;

7.17. O agente deverá suportar, no mínimo, Windows 7 (32 e 64 bits), Windows 2008 R2 Enterprise (64-bit),Windows 10, Windows Server 2012 e Windows Server 2016 e posteriores;

7.18. Todas as funções devem ser executadas por um único agente, inclusive a verificação de terminais e amonitoração e bloqueio de dados que saem do terminal;

7.19. Permitir a implementação de agente por grupos do LDAP;

7.20. Permite a reinicialização e desligamento do agente, ativação e desativação do agente a partir do consolecentral;

7.21. Possuir mecanismo que reinicie o agente caso o usuário tente interromper o serviço;

7.22. A comunicação entre o agente e o servidor devem ser criptografadas e autenticadas;

7.23. Possuir proteção contra desinstalação do agente;

7.24. Possuir capacidade para executar verificações de filtro com base no tamanho, tipo e local do arquivo;

7.25. Possuir capacidade de verificar e executar somente quando a máquina estiver ociosa;

7.26. Capacidade de apresentar as mensagens de notificações em português;

7.27. Possuir a capacidade de notificação automática, por e-mail, para o usuário e administrador durante aocorrência de um incidente;

7.28. Permitir a imposição de criptografia de arquivos confidenciais copiados para dispositivos removíveis,como dispositivos USB, por exemplo;

7.29. Caso a solução necessite de gateway de criptografia externa, este deverá ser fornecido comlicenciamento adequado para toda a solução;

7.30. Possuir a capacidade de gerenciamento da saúde dos agentes;

7.31. Possuir ferramenta para recuperação de agentes com mau funcionamento por meio de scripts de completa remoção e permitindo que seja feita uma nova instalação padrão remota dos agentes de formaautomatizada;

7.32. A operação não deixará quaisquer resquícios como licenças perdidas, lista de clientes pendentes ouduplicadas na console, etc.

8. Módulo de Rede

8.1. Permitir a monitoração do e-mail corporativo e o acesso à web de smartphones e tablets executando oGoogle Android e Apple iOS;

8.2. Permitir a monitoração de qualquer protocolo baseado em TCP, como o SMTP, inclusive anexos; HTTP,inclusive arquivos de upload; FTP ativo e passivo;

8.3. Capacidade de monitorar protocolo de Mensagens Instantâneas, além de classificar a passagem dotráfego destes protocolos de MI encapsulado em HTTP;

8.4. Permitir a classificação dos protocolos, mesmo quando executados em portas que não são padrão;

8.5. Permitir a monitoração de porta ethernet, com no mínimo, 1 gigabit, sem perda de pacotes;

8.6. Capacidade para controlar picos de tráfego, tráfego de buffer e fornecer informação de pacotes que nãopodem ser processados;

8.7. Capacidade de filtrar o tráfego da rede para inspeção, segundo o protocolo, faixa de IP eremetente/destinatário de e-mail;

8.8. Fornecer estatísticas de tráfego detalhadas e resultados gerais de dados, nº de mensagens e nº deincidentes, com base em cada protocolo;

8.9. Bloquear, redirecionar e colocar em quarentena, condicionalmente, as mensagens SMTP, com base noconteúdo;

8.10. Bloquear, condicionalmente, as mensagens HTTP, com base no conteúdo;

8.11. Remover, condicionalmente, o conteúdo de publicações HTTP e sites de redes sociais, suportando, nomínimo, Facebook, Twitter e Instagram;

8.12. Bloquear, condicionalmente, transmissões da Internet criptografadas (HTTP sobre SSL), com base noconteúdo da mensagem;

8.13. Bloquear, condicionalmente, as mensagens FTP, com base no conteúdo.

9. Módulo de Análise de Comportamento de Alto Risco com Fusão de Dados Estruturados e Não-estruturados

9.1. A Solução Deverá identificar fontes potenciais de vazamento de dados e perda de propriedade intelectualcrítica;

9.2. Deverá possuir Single SignOn (SSO);

9.3. As definições de configurações devem ser no formato JSON;

9.4. A solução deverá possuir um motor específico para análise de arquivos do tipo PST;

9.5. O módulo de análise comportamental deve ser integrada a solução de vazamento de informações usandoa pontuações analíticas de riscos para alterar dinamicamente as políticas de do DLP;

9.6. Deverá possuir integração com SIEM;

9.7. Deverá possuir NLP, Natural Language Processing;

9.8. Deverá possuir integração com soluções de EDRs;

9.9. Deverá priorizar eventos de interesse e alertas com base em análise de conteúdo e padrões de metadados.

10. Módulo de Classificação de Dados

10.1. Solução deve ser capaz de implementar em no mínimo:

10.1.1. Windows 7;

10.1.2. Windows 8;

10.1.3. Windows 8.1;

10.1.4. Windows 10;

10.1.5. MacOS 10.10, 10.11 e 10.12;

10.2. A solução deve ter integração nativa com soluções de Data LossPrevention;

10.3. A solução deve ter a capacidade de automaticamente classificar arquivos no mínimo para os seguintestipos de arquivo:

10.3.1. Word, Excel, PowerPoint e Project Microsoft Office;

10.3.2. Open Office;

10.3.3. PDF;

10.3.4. ZIP;

10.3.5. MSG, TIF e EML files;

10.3.6. JPEG;

10.3.7. HTML;

10.4. A solução deve ter a capacidade de proporcionar ao usuário a classificar a informação recém-criada de forma que as soluções integradas possam usufruir desta classificação e incluí-las de forma automática dentrode políticas previamente criadas;

10.5. A solução deve possibilitar a customização de graus de sigilo/categorias para a classificação dainformação pelo usuário, possibilitando classificar a informação recém-criada em no mínimo:

10.5.1. Informação Pública;

10.5.2. Informação Restrita;

10.5.3. Informação Interna;

10.5.4. Informação Confidencial;

10.5.5. Informação Pessoal;

10.6. A solução deve possibilitar classificar tanto a informação recém-criada, como as já existentes;

10.7. A solução deve ter integração para classificação da informação pelo usuário para no mínimo:

10.7.1. Word, Excel, PowerPoint e Project Microsoft Office;

10.7.2. Open Office;

10.7.3. PDF;

10.7.4. ZIP.

10.8. A solução deve ser capaz de analisar o comportamento malicioso do usuário, priorizando alertascorrelacionados com diversas soluções de segurança em produção, contendo desta forma as ameaças,possibilitando a partir de um único relatório indicar um possível ataque;

10.9. A solução deve ter a capacidade de analisar as informações em conformidade com normas eregulamentações da LGPD;

10.10. A solução deve basear o coeficiente comportamental de risco, indicando a priorização das ações e identificando se o comportamento malicioso é interno ou se é externo, correlacionando para isso informaçõesde no mínimo:

10.10.1. Incidentes recebidos da solução de DLP local;

10.10.2. Incidentes de classificação de documentos/informação por parte do usuário final;

10.10.3. Incidentes recebidos da rede de inteligência mundial do fabricante da solução;

10.11. A solução deve ser capaz de identificar os usuários expostos aos maiores níveis de risco e possibilitara partir desta informação refinar as políticas de proteção dos dados;

10.12. A solução deve ter a capacidade de calcular a pontuação de risco de cada usuário a partir docomportamento do passado e do presente;

10.13. A solução deve ter a capacidade de criar relatórios de risco, baseados nos maiores infratores;

10.14. A solução deve ter a capacidade de criar políticas de alerta e bloqueio, conforme segue:

10.14.1. Políticas de Alerta: É enviado um alerta ao usuário, no entanto, é possível ao usuário salvar oarquivo e enviá-lo por e-mail;

10.14.2. Políticas de Bloqueio: É enviado um alerta ao usuário, independentemente do nível de classificaçãodo arquivo, onde não será possível salvar, nem tão pouco enviar o arquivo;

10.15. A solução deverá possibilitar no mínimo formas de:

10.15.1. Descoberta de Informações;

10.15.2. O fluxo da informação;

10.15.3. Proteger contra o vazamento de informações, quer seja intencional, quer seja inadvertido;

10.15.4. Assegurar conformidade com as políticas de acesso e políticas de segurança;

10.15.5. Possibilitar a manutenção da trilha de auditoria por razões de controle e conformidade;

10.15.6. Possibilitar alertar aos usuários quando da criação de informações, sobre as políticas degerenciamento da informação;

10.15.7. Possibilitar o rastreio de "onde" os dados não estruturados estão sendo criados e "quem" os estãocriando;

10.16. A solução deve permitir forçar a aplicação de políticas antes que os dados saiam da gerência doÓrgão, para no mínimo:

10.16.1. Políticas de TAG;

10.16.2. Políticas de introdução de cabeçalhos (appendheaders);

10.16.3. Políticas de inclusão de metadados (addmetadata);

10.17. A solução deve ser capaz de implementar gráficos comparativos de risco comportamental entre nomínimo:

10.17.1. Usuários sob o mesmo Gerente;

10.17.2. Usuários do mesmo departamento;

10.17.3. Comportamento dos endpoints;

10.17.4. Comportamento das informações marcadas com TAG de dados sensíveis;

10.17.5. Frequência com que as políticas de proteção dos documentos são violadas;

10.17.6. Envio de informações sensíveis por e-mail e web.

Aviso de Confidencialidade: Esta comunicação deve ser lida apenas pelo seu destinatário e não pode ser retransmitida sem autorização formal. Caso seja recebida indevidamente, por favor destrua-a. Qualquer reprodução, alteração, distribuição e/ou publicação é estritamente proibida.

Notice of Confidentiality: This document should only be read by those persons to whom it is addressed and can not be relayed without formal permission. If you have received this e-mail message in error, please destroy it. Any form of reproduction, modification, distribution and/or publication of this e-mail message is strictly prohibited.

Gleicimara Chagas Lustosa

De: Andre Wilson Pimenta Santana
Enviado em: terça-feira, 30 de novembro de 2021 18:14
Para: Gleicimara Chagas Lustosa
Assunto: ENC: Solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

De: Andre Wilson Pimenta Santana
Enviada em: segunda-feira, 29 de novembro de 2021 09:04
Para: contato@grgtech.io
Assunto: Solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

Prezado,
solicito cotação para possível aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP)

Licenciamento para 36 meses

OBJETO DA CONTRATAÇÃO

1.1. Aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Preventiom – DLP), contemplando licenciamento, garantia, suporte e implantação, de acordo com as quantidades e especificações descritas neste Termo de Referência. **Licenciamento para 36 meses**

item	Descrição	Unidade	Quantidade
1	Aquisição de licenças de software de solução de prevenção de vazamento de dados – Data Loss Prevention – DLP.	UN	3,190
2	Treinamento	UN	3

1. Descrição da Solução de Tecnologia da Informação

Este Anexo especifica as características técnicas da solução de Data Loss Prevention / DLP a ser adquirida para implementação no ambiente do FUNASA. Detalhamos neste Anexo os componentes da solução de DLP.

ITEM	ESPECIFICAÇÕES TÉCNICAS E REQUISITOS MÍNIMOS
01	Aquisição de licenças de software de solução de prevenção de vazamento de dados - Data Loss Prevention (DLP) para 3190 usuarios

2.

1. **Console de Gerenciamento e Plataforma**

1. O licenciamento da solução proposta deve contemplar todo o software, ou seja, todas as funcionalidades descritas neste Termo de referência
2. As configurações de todos os módulos devem possuir integração nativa com a console central.
3. Deve ter console de gerenciamento via tecnologia Web (HTTP ou HTTPS).
4. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, nos sistemas operacionais:
    1. Microsoft Windows Server;
5. Suportar funcionamento em sistemas de virtualização.
6. A solução deve possuir ou integrar com sistemas de monitoramento de atividades do usuário baseado na nuvem (UAM), usando indicadores comportamentais (IOB) e fornecendo visibilidade significativa sobre comportamentos de risco do usuário, a fim de automatizar as políticas de proteção de dados em nível de usuário.
7. Capacidade de excluir incidentes em lote para gestão eficiente de epaço utilizado pela base de dados.
8. Suportar funcionamento em plataformas de Single Sign-On (SSO)
9. A solução deverá criptografar toda a comunicação que ocorre entre os servidores de gerenciamento e os agentes instalados em terminais.
10. A solução deverá criptografar a comunicação entre o servidor principal e os servidores adicionais da plataforma.
11. Possuir registros detalhados de auditoria de atividades de sistema.
12. Permitir a instalação em Sistema Operacional restrito, com serviços e configurações de porta limitados (Hardening).
13. Deve ter a capacidade de bloquear o acesso, movimentação, tráfego e cópia de informações confidenciais detectadas;
14. Deve possuir módulos de detecção distintos, para:
    - Localizar dados confidenciais armazenados em servidores de arquivos, bancos de dados e servidores de email;
    - Localizar dados confidenciais armazenados em desktops e laptops;
    - Detectar dados confidenciais em trânsito na rede, em protocolos TCP/IP;
    - Detectar vazamento de dados a partir de conexão direta com servidores de email;
    - Detectar vazamento de dados a partir de conexão direta com appliances responsáveis pelo processsamento de tráfego WEB (Proxy ou UTM);

1. Capacidade de obter a “impressão digital” de dados estruturados e não estruturados.
2. Capacidade de normalizar variações comuns de apresentação de dados para aprimorar a precisão de políticas de monitoramento.

3. Capacidade de identificar dados estruturados e não estruturados, sem necessidade de utilização de servidores adicionais ou dedicados para este fim.
4. Detectar documentos não estruturados, após usar capacidades nativas de aprendizado automático, a partir da análise de um conjunto de amostras.
5. Permite a criação de padrão de identificação utilizando dados internos da instituição de modo a customizar a ferramenta.
6. Permitir detecção de acordo com expressões regulares configuráveis.
7. Permitir detecção por tipo de arquivo, por nome e extensão de arquivo, remetente/destinatário e protocolo de transmissão.
8. Capacidade de integrar diretamente com LDAP (MS Active Directory) para criar regras de detecção de terminal baseadas em usuário ou grupo. Políticas diferentes podem ser aplicadas de acordo com o usuário que fez o login, mesmo em uma máquina compartilhada.
9. Possuir mecanismo de envio de notificações personalizadas por e-mail aos administradores.
10. Permitir a criação de perfis para administração de servidores, administração de usuário, criação e edição de política.
11. Armazenar e exibir a mensagem original ou arquivo que gerou o incidente.
12. Exibir todo o histórico do incidente, inclusive as alterações e edições referentes ao mesmo.
13. Permitir a exportação da lista de incidentes no formato HTML, PDF ou CSV.
14. Interface de administração única para vizualização de todos os incidentes.
15. Possuir interface WEB, compatível, no mínimo, com os navegadores Internet Explorer, Mozilla Firefox e Google Chrome.
16. Permitir a configuração de ações automáticas, dependendo da quantidade de dados expostos.
17. Deve possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuários envolvidos num incidente detectado.
18. Deve possuir integração com Active Directory, para autenticação de usuários da solução.
19. Deve possuir logs detalhados de auditoria de alterações de políticas.
20. A solução deve ter capacidade de descoberta de vazamento de dados nos seguintes canais:
    - Nuvem;
    - Email;
    - Web;
    - Terminais;
    - Smartphones (A partir de um APP a ser instalado);
    - Plataforma de armazenamento de dados.
21. Proteger os dados contra exposição ou roubo em tempo real.
22. Deve suportar a verificação de arquivos compactados recursivos (exemplos .zip, .rar dentro de .zip, .rar).
23. Deve suportar de forma comprovada a detecção de dados no idioma português brasileiro.
24. Deve ter a capacidade de analisar conteúdo de arquivos grandes (maiores que 20MB) anexados em e-mails.
25. Deve identificar informações confidenciais sem a necessidade de acrescentar tags, etiquetas e afins nos arquivos de origem.
26. Deve identificar conteúdos armazenados em colunas específicas de planilhas eletrônicas e em bancos de dados.
27. Deve possuir capacidade para identificar conteúdos específicos com base em um padrão pré-determinado, para no mínimo:
    - CPF;
    - CNPJ;
    - Cartões de Crédito;
    - Número de eleitor;
    - RG;

- IBAN;
- Dados de tecnologia com o IP Address, Mac Address e IMEI de telefones.

28. Deve detectar o arquivo pelo seu conteúdo real, e não apenas pela extensão do arquivo.
29. A solução deve possuir integrada na console a funcionalidade de workflow (Condições de acionamento) resposta a incidentes.
30. Devem ser exibidas na console de gerenciamento todas as informações a respeito do incidente para, no mínimo:
    - Dados para análise como: Origem, Destino, detalhes de qual Canal de detecção foi acionado e nome/caminho do arquivo;
    - Dados de qual regra foi acionada;
    - Dados de qual informação acionou a regra;
    - Severidade do incidente;
    - Status do incidente;
    - Nome da aplicação;
    - Data e hora do evento;
    - Volume de dados trafegados no incidente;
    - Nome do usuário referenciado no incidente;
    - Atributos do usuário coletados do Active Directory;
    - Nome da estação de trabalho;
    - Informações de destino para qual o dado seria copiado;
    - Histórico completo de alteração de incidentes.
31. Deve ter a capacidade de importar um conjunto de pré-configurações do sistema otimizadas para verticais das indústrias específicas, contando com dados de pesquisa em português.
32. A solução deve ser agnóstica a linguística. Todos os mecanismos de identificação de dados, por exemplo: palavras, dicionários e Machine Learning, devem funcionar de forma igual em qualquer linguagem.
33. A solução deve proteger documentos em pelo menos 40 tipos de idiomas.
34. A solução deve incluir um mecanismo de análise de segurança, que é exclusivamente responsável pela modelagem estatística de dados e análise de comportamento suspeito dos usuários, com o objetivo de identificar e agrupar incidentes comuns a um determinado usuário ou estação de trabalho, automaticamente e usando uma pontuação de risco atribuída.
35. Deve permitir que sejam visualizados e identificados rapidamente os usuários ou estações de trabalho com o mais alto nível de risco para a organização, como resultado dos incidentes de segurança associados a eles.
36. A solução deve possuir, com mais de 1700 modelos de políticas predefinidos agrupados por localização geográfica e tipo de organização para identificar regras, regulamentos ou leis que a organização deve cumprir e aplicar as políticas correspondentes sem a necessidade de impressão digital dos dados envolvidos.
37. Deve possibilitar a realização de backup e restore de configurações, incidentes e políticas da plataforma.
38. Deve possibilitar integração nativa com soluções de classificação da informação, de forma a monitorar o uso de dados classificados nos canais de detecção e também a possibilidade de imposição de classificação durante a descoberta de dados em servidores de arquivos, por exemplo.

2. **Criação de Políticas e Detecção de Conteúdo Confidencial**
    1. Deve ter a capacidade de utilizar, no mínimo, os critérios abaixo para criação de políticas:
        - Palavra ou conjunto de palavras chave;

- Identificadores pré existentes o customizados (CPF, CNPJ, Cartão de crédito, etc.);
- Expressões regulares com possibilidade de adaptação para qualquer padrão de dados existentes;
- Nível de classificação da informação;
- Tipo de arquivo;
- Nome e extensão de arquivos;
- Bases de indexação previamente carregadas;
- Tamanho de dados trafegados;
- Quantidade de anexos de um e-mail;
- Usuários/E-mails internos;
- Estações de trabalho/servidores específicos;
- Localização da estação de trabalho (Dentro ou fora da rede interna);
- Tipo de estação (Laptop ou desktop);
- E-mails ou domínios externos;
- Direção do tráfego (Entrada ou saída);
- Protocolos de rede ou canais da estação;
- E-mails em dispositivos móveis;
- Dados enviados para impressora;
- Qualquer aplicação em execução na estação de trabalho;
- Cópias para caminhos de rede.

2. Deve possibilitar criação de regras de exclusões para as políticas de acordo com grupos de usuários fornecidos pelo active directory.
3. O produto deve possuir modelos de políticas de detecção com base em regulamentações e melhores práticas de mercado, para no mínimo:
    - SOX;
    - PCI;
    - HIPAA;
    - GDPR.
4. A solução deve possibilitar a criação de regras para adequação a LGPD.
5. A solução deve possuir templates de políticas de detecção, para no mínimo os seguintes temas:
    - Imagens com conteúdo inapropriado;
    - Linguagem ofensiva ou racismo;
    - Cyber Bullying;
    - Problemas relacionados a jogos de azar;
    - Dados confidenciais e propriedade intelectual;
    - Dados que envolvem segurança de redes;
    - Busca de informações relacionadas a indicadores de comprometimento.
6. Deve ter a capacidade para análise de conteúdo nos mais diversos tipos de arquivos, para no mínimo:
    - Texto (TXT, ASC, HTML, DOC, DOCX, SWX, ODT);
    - Compactados (ZIP, RAR, GZ, LHA, HQX, JAR, 7z);
    - CAD (DWG, DXF, VSD, DGN);
    - Planilhas (XLS, XLSX, 123, SXC, ODS, CSV);
    - Apresentações (PPT, PPTX, SXI, SXP, ODP);
    - Outros (PDF, MDB).
7. Deve permitir criar políticas que combinam várias tecnologias e regras de detecção com regras "E/OU" lógicas e de exceção.
8. Permitir a escrita de expressões lógicas para configuração das regras de detecção, exemplo:("Condição 1" OU "Condição 2") E NÃO "Condição 3".

9. Deve ter a capacidade de construir políticas de detecção, configurando-se o grau de severidade adotado para cada regra criada, conforme o número de correspondências que se deseja encontrar em cada possível violação.
10. A solução deve fornecer a implantação de políticas DLP corporativas de forma unificada, ou seja, uma única política de DLP pode ser aplicada a todos os módulos (network, endpoints e aplicações em cloud).
11. As políticas de detecção devem possuir, no mínimo:
    - A capacidade de normalização de todas as variações comuns de apresentação de dados (por exemplo, se a extração de dados contiver "123456789", deverá ter como correspondente "123-45-6789", "123456789", "123.45.6789", etc.);
    - A capacidade de detecção usando palavras e frases-chave totalmente configuráveis;
    - A capacidade de colocar múltiplas palavras/frases em uma única regra de detecção.
    - A capacidade nativa de detectar documentos de identificação e números de impostos internacionais, para no mínimo, os países EUA, França e Brasil.
    - A capacidade de detectar faixas de números válidos para determinados tipos de dados, tal como no mínimo, número de cartão de crédito válido.
12. A solução deve incluir mecanismos de proteção de dados contra vazamentos lentos e sofisticados (DRIP DLP), ou seja, deve monitorar a perda lenta de dados em eventos cumulativos;
13. A solução deve fornecer políticas predefinidas para identificar expressões potenciais que são indicativas de bullying cibernético, padrões de pensamento suicida ou conteudo malicioso;
14. A solução deve ter inteligência artificial composta de técnicas que permitem aprender com exemplos de dados em vez de regras de dados pré-classificadas. O produto deve trabalhar com algoritmos de aprendizagem supervisionados e algoritmos de aprendizagem não-Supervisados para classificar e aprender com as informações descobertas nos endpoints;

3. **Resposta a incidentes**

1. Deve possuir notificações personalizáveis através de e-mail em caso de violação de política.
2. A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviados nas notificações.
3. Deve permitir tomar ações automáticas pré-definidas na detecção de incidentes, para no mínimo:
    - Permitir o envio, deletar anexos, quarentenar ou criptografar e-mails;
    - Permitir ou bloquear tráfego de dados sensíveis via FTP;
    - Permitir ou bloquear tráfego de dados sensíveis via HTTP/HTTPs;
    - Através do agente, permitir, bloquear ou solicitar justificativa para o tráfego em pelo menos: Qualquer tipo de aplicação executada pelo Sistema operacional, cópia para armazenamentos de rede, impressão de arquivos, E-mails enviados, upload para páginas Web e cópias para dispositivos USB.
    - Permitir a possibilidade de busca ou não de detalhes sobre o incidente durante o registro;
    - Execução de atividades customizadas;
    - Enviar mensagens para servidores de syslog;
    - Enviar notificações por e-mail;
    - Manipular arquivos durante a descoberta de rede.
4. Deve permitir vários botões de reposta na interface gráfica dos incidentes totalmente configuráveis.

5. Os botões de resposta na interface gráfica dos incidentes devem possibilitar no mínimo:
    - Designar o incidente para resposta de alguém específico;
    - Modificar o status do incidente;
    - Modificar a severidade do incidente;
    - Ignorar o incidente;
    - Adicionar TAG no incidente;
    - Adicionar comentários no incidente;
    - Fazer Download do incidente;
    - Deletar o incidente;
    - Acionar scripts ou tarefas customizadas;
    - Escalar o incidente para o gerente do usuário envolvido;
    - Escalar o incidente para uma pessoa específica.
6. Deve exibir todos os detalhes do incidente em uma única página.
7. Deve permitir exibir partes específicas da mensagem ou arquivo que violou as políticas, através de uma visualização rápida na tela do incidente, sem a necessidade de usar software externo.
8. Deve permitir armazenar a mensagem e o arquivo original que gerou o incidente.
9. Deve exibir todo o histórico do incidente, incluindo alterações, edições e respostas executadas automaticamente e manualmente.

4. **Relatórios**
    1. Deve exibir relatórios personalizáveis sobre os incidentes e utilizar filtros, no mínimo de:
        - Ação aplicada;
        - Responsável pela análise;
        - Nome da aplicação;
        - Departamento;
        - Canal de detecção;
        - Nível de classificação da informação;
        - Destino de tráfego da informação;
        - Tipo estação (Desktop ou Laptop);
        - ID do incidente
        - Hora do incidente
        - Nome do arquivo trafegado;
        - Histórico do incidente;
        - Incidentes marcados como ignorados;
        - TAGs de incidentes;
        - Quantidade de informação sensível trafegada;
        - Propriedades do arquivo;
        - Política acionada;
        - Nome da regra acionada;
        - Severidade do incidente;
        - Origem do incidente;
        - Status do incidente;
        - Tamanho da transação;
        - Dados relacionados as violações encontradas.
    2. Deve exportar relatórios para os formatos HTML, PDF e CSV.
    3. Deve apresentar um painel para visualização dos relatórios.
    4. Deve ter a capacidade para configurar, salvar relatórios e painéis personalizados por usuário.
    5. Deve possuir painéis (Dashboards) para, no mínimo os seguintes itens:

- Incidentes criados nos últimos X dias;
- Políticas mais acionadas;
- Incidentes por severidade;
- Incidentes por ação tomada;
- Incidentes por canais de detecção;
- Incidentes por origem/destino;
- Usuários que mais violam políticas.

6. A solução deve se integrar nativamente a solução de comportamento dos usuários e correlacionar as informações;
7. A solução deve exibir informações dos usuários, com pelo menos 20 incidentes durante o período analisado em conjunto com número de correspondências, tamanho da transação, conteúdo e políticas infringidas;

5. **Módulo de Área de Armazenamento**
    1. Deve verificar existência de conteúdo confidencial em file systems sem a necessidade de agentes de coleta (agent-less) para no mínimo CIFS, NFS, SMB e NTFS.
    2. Deve permitir a análise dos file systems através de agentes ou sem agente em sistemas operacionais, para no mínimo:
        - Windows Server 2008 R2;
        - Windows Server 2012;
        - Windows Server 2016;
        - Red Hat Enterprise Linux 6 e demais releases da versão;
        - Red Hat Enterprise Linux 7 e demais releases da versão.
    3. Deve analisar conteúdo sigiloso armazenado em ambientes complexos, para no mínimo:
        - Microsoft Sharepoint;
        - Lotus Notes;
        - Microsoft SQL Server;
        - Oracle;
        - MySQL
        - Microsoft Exchange;
    4. Deve analisar conteúdo sigiloso em aplicações em nuvem:
        - Salesforce,
        - AW
        - ServiceNow
        - Facebook Workplace
        - G-Suite
        - Google Cloud Platform
        - Azure.
        - One Drive
        - Trello
        - Dropbox
        - Slack
        - GitHub
        - LinkedIn
    5. Deve possuir a capacidade de verificar arquivos Microsoft "PST", possibilitando executar varreduras tanto nas mensagens, assim como, nos arquivos anexos as mensagens.
    6. Possibilidade de mover para quarentena arquivos que violam políticas de segurança.
    7. Deve manter o arquivo no local original, substituindo seu conteúdo por uma mensagem customizável, como aviso e orientação para o usuário.

8. Permitir a remoção do arquivo que está em quarentena e restaurá-lo de volta ao local original.
9. Deve permitir coleta automática de arquivos que violem políticas para análise legal (evidência).
10. Permitir a criação de respostas personalizadas para incidentes.
11. Exibir detalhes, no incidente, dos arquivos que violam as políticas.
12. Permitir a visualização das permissões do arquivo.
13. Deve possibilitar notificação através de e-mail e alerta Syslog em caso de violação de política.
14. Deve permitir agendamento de varreduras automáticas.
15. Possuir mecanismo de verificação incremental, na qual apenas arquivos novos, ou alterados, sejam verificados.
16. Deve permitir configurar janelas de tempo para verificações, interrompendo o processo automaticamente ao fim do período configurado.
17. Preservar os atributos originais do arquivo, inclusive o atributo "Acessado em", enquanto realiza a verificação.
18. Possuir capacidade de pausar, manualmente, a verificação.
19. Deve utilizar técnicas de paralelismo e controle de banda.
20. Permitir o controle da velocidade das verificações para limitar o uso da largura de banda da rede.
21. Deve ter a capacidade de reutilizar uma única credencial (nome de usuário/senha) em múltiplos alvos a serem verificados.
22. Permitir a verificação simultânea em várias fontes distintas.
23. Permitir limitar quais portas de comunicação serão utilizadas entre o sistema-alvo e o servidor que faz a verificação.
24. Deve permitir aplicar filtros para verificar na varredura de arquivos de um determinado tipo ou em certo diretório.
25. Deve permitir aplicar filtros para verificar na varredura de arquivos a idade E/ou o tamanho de arquivos.

6. **Módulo de Terminal de Usuário**
    1. Capacidade de descobrir fuga de informações sensíveis, por meio de agente.
    2. Possibilidade de aplicação de políticas mesmo quando o agente não tem comunicação com o servidor de gerenciamento.
    3. Possibilidade de armazenamento em cache, dos arquivos que causaram o incidente até que o usuário se conecte, novamente, à rede corporativa.
    4. A solução possuir a funcionalidade de OCR em arquivos do tipo imagem, no mínimo para:
        - Jpeg
        - Bmp
        - Png
        - Gif
        - Tiff
    5. Monitorar e bloquear dados copiados para dispositivos de armazenamento removível (USB).
    6. A solução deverá possuir capacidade de analisar arquivos menos de 1 kbyte.
    7. Possibilidade de criptografar dados sensíveis copiados para dispositivos USB, sem a necessidade de soluções adicionais.
    8. A solução deve ser capaz de detectar e proteger informações estruturadas de dados, por exemplo, de bancos de dados.

9. a solução de ponto final deve ser capaz de descobrir e proteger informações estruturadas de dados sem exigir uma conexão com o servidor remoto
10.
11. Permitir a monitoração e bloqueio para dados copiados para CD/DVD.
12. Permitir a monitoração e bloqueio para dados enviados a qualquer tipo de impressora local e de rede.
13. Permitir a monitoração e bloqueio para ações de copiar e colar.
14. Permitir a monitoração e bloqueio de dados sensíveis trafegados via e-mail corporativo.
15. Permitir a monitoração e bloqueio para transmissões HTTPS pelo menos nos seguintes navegadores:
    - Internet Explorer;
    - Microsoft Edge;
    - Mozilla Firefox;
    - Google Chrome;
    - Safari.
16. Permitir a monitoração e bloqueio para transmissões HTTP.
17. Permitir a monitoração e bloqueio para transmissões via FTP.
18. Permitir a monitoração e bloqueio para uso de dados confidenciais por qualquer aplicativo, incluindo programas de criptografia não autorizados.
19. Permitir a monitoração e bloqueio para dados copiados para compartilhamentos de rede pelo Windows Explorer.
20. A Solução deve possuir monitoramento, por padrão, para pelo menos os seguintes aplicativos:
    - Chrome;
    - Firefox;
    - Internet Explorer (IE);
    - Microsoft Edge;
    - Opera;
    - Safari;
    - Tor;
    - Torch;
    - Acoustica MP3 CD Burner;
    - Alcohol 120%;
    - CD-Mate;
    - Disk Utility;
    - iTunes;
    - Nero Burning ROM;
    - Roxio – Easy Media Creator;
    - Windows Media Player;
    - Amazon Cloud Drive;
    - Box;
    - Dropbox;
    - Egnyte;
    - Google Drive;
    - iCloud;
    - OneDrive;
    - Salesforce Files;
    - ShareFile;
    - Syncplicity;
    - WatchDox;
    - Apple Mail;

- Eudora;
- Lotus Notes;
- MailMate;
- Microsoft Outlook;
- Microsoft Outlook Express;
- Mozilla Thunderbird;
- Pegasus Mail;
- Postbox;
- Sparrow;
- Windows Live Mail;
- Windows Mail;
- DK2 Network Server Remote Monitor - DK2 DESkey;
- File Encryption XP;
- Windows Privacy Tray (WinPT);
- Core FTP LE;
- Cute FTP Home 8.2;
- File Transfer Program (Microsoft Utility);
- FileZilla FTP Client;
- Flash FXP 3.6 build 1240;
- FTP Voyager 15;
- Ipswitch WS FTP Home;
- Leech FTP;
- Serv-U;
- Smart FTP Client;
- Adium;
- AIM;
- Apple Messages;
- Camfrog;
- Cisco WebEx;
- GoToMeeting;
- ICQ;
- Jabber Messenger;
- ManyCam;
- Microsoft Lync 2010;
- Miranda IM;
- ooVoo;
- Pidgin;
- Skype for Business;
- TeamViewer;
- Teccent QQ;
- Trillian;
- Viber;
- Yahoo! Instant Messenger;
- Adobe Reader;
- Bean;
- Eclipse;
- Emacs;
- Evernote;
- Keynote;
- LibreOffice/Apache OpenOffice;
- Mellel;

- Microsoft Office Access;
- Microsoft Office Excel;
- Microsoft Office InfoPath;
- Microsoft OneNote;
- Microsoft Office PowerPoint;
- Microsoft Office Project;
- Microsoft Office Publisher;
- Microsoft Office Visio;
- Microsoft Office Word;
- Notepad;
- Numbers;
- OpenOffice.org Calc;
- OpenOffice.org Draw;
- OpenOffice.org Math;
- OpenOffice.org Writer;
- Pages;
- Reminders;
- Stickies;
- TextEdit;
- WordPad;
- AllegianceMD;
- eClinicalWorks;
- ECLIPSYS;
- INGENIX;
- inteGreat;
- Sequel;
- Ares;
- Azureus;
- BearShare;
- BitComet;
- BitLord;
- BitTornado;
- BitTorrent;
- eMule;
- FrostWire;
- Kazaa Lite;
- LimeWire;
- Pando;
- Transmission;
- uTorrent;
- 7-Zip File Manager;
- iArchiver;
- WinRAR;
- WinZip;
- Bluetooth Stack COM Server - BTStackServer;
- Fsquirt;
- iTunes;
- Wireless Link File Transfer App – Irftp;
- WCESMgr;
- Aplicor (online);
- CRM.com;

- HostAnalytics;
- Intacct;
- NetSuite;
- Oracle CRM on demand;
- RightNow;
- Salesforce;
- WorkDay;
- FoxPro;
- Ld;
- MSTSC;
- NT backup tool;
- Vista backup tool;
- VMWare.

21. A solução deve permitir a criação de qualquer aplicativo existente que não venha cadastrado por padrão.
22. Definir dispositivos removíveis individuais, ou grupos de dispositivos, como confiáveis e criar exceções de políticas para esses dispositivos.
23. A solução deve suportar a integração com o Microsoft RMS (Azure Information Protection), para descriptografar e analisar arquivos do tipo Office (Word, Excel, Power Point entre outros) que foram previamente criptografados pelo Azure RMS ou RD (Active Directory) RMS.
24. O agente deverá suportar, no mínimo, Windows 7 (32 e 64 bits), Windows 2008 R2 Enterprise (64bit), Windows 10, Windows Server 2012, Windows Server 2016 e Apple MacOS.
25. Todas as funções devem ser executadas por um único agente.
26. Permitir a desativação do agente pela console de gerenciamento.
27. Possuir mecanismo que reinicie o agente caso o usuário tente interromper o serviço.
28. Possuir proteção contra desinstalação do agente.
29. Capacidade de apresentar as mensagens de notificações em português.
30. Possuir a capacidade de envio de notificação automática, por e-mail, para o usuário e administrador durante a ocorrência de um incidente.
31. Possuir a capacidade de gerenciamento da saúde dos agentes.
32. Deve permitir a distribuição do agente através de GPO ou por ferramenta de terceiros.
33. Deve ter a capacidade de permitir ao usuário justificar a movimentação de conteúdo confidencial, a partir do alerta em “pop-up”, escolhendo opções de justificativa configuráveis pelo administrador da ferramenta.
34. O agente deve executar varredura local para verificar se a estação do usuário possui conteúdo confidencial.
35. A solução deve ser capaz de proteger informações de impressão digital de dados estruturados offline e sem a necessidade de qualquer comunicação com servidores de administração ou gerenciamento ou repositórios de impressões digitais
36. O endpoint deve poder pode permitir automaticamente a transferência de informações específicas em forma criptografada, configurados pelo administrador;
37. O endpoint deve permitirá que o usuário defina sua própria senha para criptografia e arquivos criptografados.
38. A solução deve permitir que o arquivo criptografado possa ser visualizado ou aberto em computadores onde o endpoint não está instalado usando a senha original do emissor do documento.
    1. Essa funcionalidade deve ser atendida através do próprio agente sem a necessidade de adicionar uma solução de terceiros;

1.
2. Deve permitir realizar verificações incrementais, apenas em arquivos novos e alterados.
3. Permitir a instalação do agente de modo oculto ou em modo de interação com o usuário.
4. Quando utilizado em modo interativo, permitir sincronização de políticas de forma manual, através de acionamento de botão no agente.
5. A solução deve suportar integração dinâmica com o User Behavior Analytics ou plataformas UAM.
6. Deve permitir incluir na solução de UAM ou User Behavior Analytics a coleta de eventos produzidos pela solução DLP e posterior análise e modelagem realizada pelo UAM ou User Behavior Analytics, com o objetivo de calcular um nível de risco por usuário.
7. Deve permitir atraves do nível de risco obtido pelos algoritmos do UAM ou User Behaivior Analytics , esses resultados devem ser devolvidos à solução DLP original para aplicar ações imediatas ou dinâmicas, sem a intervenção humana do administrador da solução.
8. Alimentar a console de gerenciamento, com pelo menos, as seguintes informações do agente:
    - Nome do computador;
    - IP Address;
    - Usuário logado;
    - Última vez que o agente se comunicou com a o servidor central;
    - Identificador do grupo de políticas utilizados;
    - Campo que informa se o agente está em sincronismo com as últimas políticas/configurações disponibilizadas pelo administrador;
    - Versão do agente;
    - Versão da política instalada.

1. **Módulo de rede**
    1. Permitir a monitoração/bloqueio do e-mail corporativo, evitando que e-mails com dados sigilosos sejam enviados para fora da organização, inclusive em smartphones e tablets.
    2. Possibilidade de colocar mensagens de correio eletrônico em quarentena para análise.
    3. Permitir a monitoração/bloqueio de tráfego WEB, evitando que dados sigilosos saiam da organização por este canal, inclusive em smartphones e tablets.
    4. Capacidade de monitorar/bloquear o tráfego informações sensíveis em posts de redes sociais.
    5. Permitir a monitoração de qualquer protocolo baseado em TCP, como o SMTP, inclusive anexos; HTTP, inclusive arquivos de upload; FTP ativo e passivo.
    6. Capacidade de monitorar o vazamento de dados por meio de softwares de Mensagens Instantâneas.
    7. Permitir a classificação dos protocolos, mesmo quando executados em portas que não são padrão.
    8. Capacidade de filtrar o tráfego da rede para inspeção, segundo o protocolo, faixa de IP e remetente/destinatário de e-mail.

2. **Módulo de Classificação da informação**
    1. A solução deve ter integração nativa com soluções de Data Loss Prevention;

2. A solução deve ter capacidade de realizar a rotulagem de informações recém criadas ou pré-existentes sem a necessidade de alterar as propriedades do arquivo, somente seus metadados;
3. A solução de deve ter a capacidade de automaticamente classificar arquivos no mínimo para os seguintes tipos de arquivo;
    - Word, Excel, PowerPoint, Outlook, Project e Microsoft Office.
    - Open Office
    - PDF
    - ZIP
    - MSG, TIF e EML files
    - JPEG
    - HTML
4. A solução deve ter a capacidade de proporcionar ao usuário a classificar a informação recém-criada de forma que as soluções integradas possam usufruir desta classificação e incluí-las de forma automática dentro de políticas previamente criadas;
5. A solução deve permitir que as soluções integradas detectem os metadados do Classificador, a fim de evitar que o arquivo seja copiado e notificar o usuário/administrador.
6. A solução deve possuir integração com o sistema operacional Windows, permitindo que as ações de classificação do usuário sejam logadas pelo sistema operacional;
7. A solução deve possibilitar a classificação da informação pelo usuário, possibilitando classificar a informação recém-criada em no mínimo:
    - Informação Pública;
    - Informação Restrita;
    - Informação Interna;
    - Informação Confidencial
    - Informação Pessoal.
8. A solução deve possibilitar classificar tanto a informação recém-criada, como pré-existentes;
9. A solução deve ter integração para classificação da informação pelo usuário para no mínimo:
    - Word, Excel, PowerPoint, Outlook, Project e Microsoft Office.
    - Open Office
    - PDF
    - ZIP
10. A solução deve ser capaz de analisar o comportamento malicioso do usuário, priorizando alertas correlacionados com diversas soluções de segurança em produção, contendo desta forma as ameaças, possibilitando a partir de um único relatório indicar um possível ataque;
11. A solução deve ter a capacidade de analisar as informações em conformidade com normas e regulamentações, para no mínimo GDPR, PCI, DSS, SOX, HIPAA;
12. A solução deve basear o coeficiente comportamental de risco, indicando a priorização das ações e identificando se o comportamento malicioso é interno ou se é externo, correlacionando para isso informações de no mínimo:
    - Incidentes recebidos da solução de DLP local;
    - Incidentes recebidos pela solução de criptografia, na tentativa de acesso aos dados sensíveis;
    - Incidentes de classificação de documentos/informação por parte do usuário final;
    - Incidentes recebidos da rede de inteligência mundial do fabricante da solução;
13. A solução deve ser capaz de identificar os usuários expostos aos maiores níveis de risco e possibilitar a partir desta informação refinar as políticas de proteção dos dados;
14. A solução deve permitir que as soluções integradas possam gerar um relatório sobre as marcas de metadados do Classificador, permitindo no mínimo:

- Localização de arquivo por classificação;
- Alteração na permissão dos arquivos;
- Adicionar criptografia no arquivo;

15. A solução deve ser capaz de inserir marcações visuais em e-mails (ex. Outlook) para o cabeçalho ou rodapé;
16. A solução deve classificar e-mails enviados com arquivos anexados de acordo com a classificação do anexo. Esta classificação deve ser realizada antes do envio.
17. solução deve ter a capacidade de calcular a pontuação de risco de cada usuário a partir do comportamento do passado e do presente;
18. A solução deve ter a capacidade de criar relatórios de risco, baseados nos maiores infratores;
19. A solução deve ter a capacidade de criar políticas de alerta e bloqueio, conforme segue:
    - Políticas de Alerta: É enviado um alerta ao usuário, no entanto, é possível ao usuário salvar o arquivo e enviá-lo por e-mail;
    - Políticas de Bloqueio: É enviado um alerta ao usuário, independentemente do nível de classificação do arquivo, onde não será possível salvar, nem tão pouco enviar o arquivo;
20. A solução deverá possibilitar no mínimo formas de:
    - Descoberta de Informações;
    - O fluxo da informação;
    - Proteger contra a exfiltração da informação, quer seja intencional, quer seja inadvertida;
    - Assegurar conformidade com as políticas de acesso e políticas de segurança;
    - Possibilitar a manutenção da trilha de auditoria por razões de controle e conformidade;
    - Possibilitar alertar aos usuários quando da criação de informações, sobre as políticas de gerenciamento da informação;
    - Possibilitar o rastreio de "onde" os dados não estruturados estão sendo criados e "quem" os estão criando;
21. A solução deve permitir forçar a aplicação de políticas antes que os dados saiam da gerência do Órgão, para no mínimo:
    - Políticas de TAG;
    - Políticas de introdução de cabeçalhos (append headers);
    - Políticas de inclusão de metadados (add metadata);
22. A solução deve ser capaz de implementar gráficos comparativos de risco comportamental entre no mínimo:
    - Usuários sob o mesmo Gerente;
    - Usuários do mesmo departamento;
    - Comportamento dos endpoints;
    - Comportamento das informações marcadas com TAG de dados sensíveis;
    - Frequência com que as políticas de proteção dos documentos são violadas;
    - Envio de informações sensíveis por e-mail e web;

Gleicimara Chagas Lustosa

De: Andre Wilson Pimenta Santana
Enviado em: quarta-feira, 1 de dezembro de 2021 14:52
Para: Gleicimara Chagas Lustosa
Assunto: Enc: Renovação da solução de DLP

De: Andre Wilson Pimenta Santana
Enviado: quinta-feira, 25 de novembro de 2021 15:23
Para: alexsander.bastos@broadcom.com
Assunto: Renovação da solução de DLP

Prezado,
Conforme acordado em reunião, solicito a indicação de revenda para possível aquisição de DLP para a Funasa
Nosso ambiente conta com 214 servidores virtuais e 3190 usuários.