Proposta Comercial Técnica – FUNASA

Forcepoint DLP

202111-9217-V3

São Paulo, 30 de novembro de 2021.

Prezados,

Sentimo-nos honrados em participar do processo de seleção para Aquisição de Licenças na Solução Forcepoint DLP, visando atender os requisitos e necessidades desta conceituada instituição.

A DSR9, é uma empresa do setor de TECNOLOGIA DA INFORMAÇÃO que oferece soluções voltadas para o mercado corporativo. Aceitamos o desafio de atender as necessidades tecnológicas da **FUNASA**, nos mais altos padrões de qualidade promovidos dentro da área de TI.

Estamos encaminhando para apreciação de V.Sas. os documentos abaixo relacionados, os quais compõem nossa proposta de prestação de serviços.

Colocamo-nos à disposição para quaisquer esclarecimentos que se fizerem necessários.

Atenciosamente,

_____

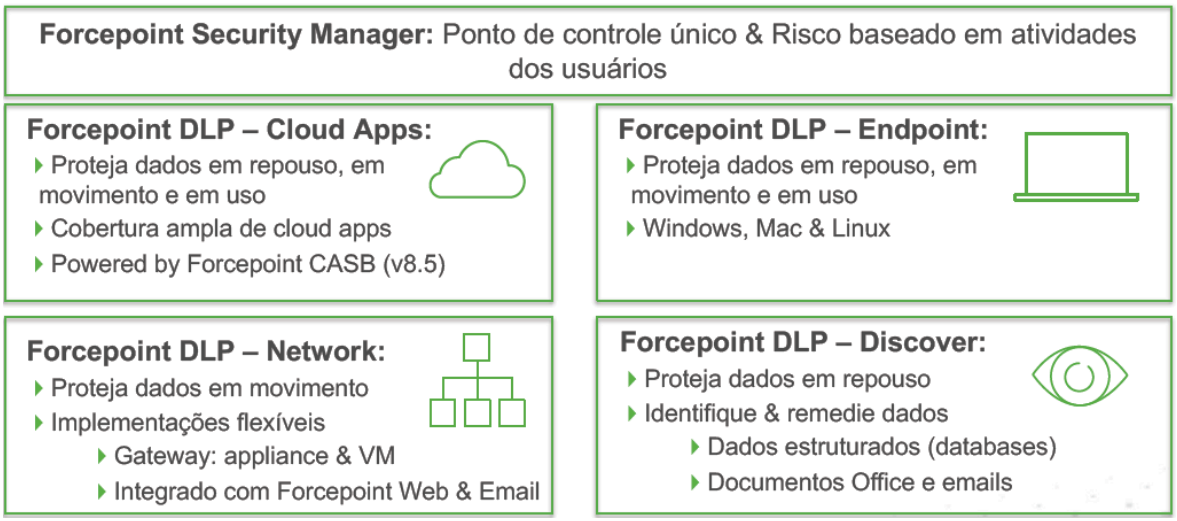
Arthur Andrade
arthur.andrade@dsr9.com

1. Objetivo da Proposta

A presente proposta tem como objetivo ofertar licenças do Forcepoint DLP, visando prevenir a perda e roubo de informações confidenciais da **FUNASA**.

2. Apresentação do Produto:

Desde danos a reputações até multas e penalidades de agências reguladoras, uma violação de dados pode ter consequências devastadoras. Forcepoint DLP habilita você a descobrir e proteger dados confidenciais não importa onde estejam – em pontos
de extremidade, na nuvem ou no local. Amplie os negócios e impulsione a inovação, adotando com segurança serviços de colaboração na nuvem como Microsoft Office 365 e Box. Proteja ativos críticos de informação em computadores portáteis Mac OS X e Microsoft Windows. Proteja dados pessoais e propriedade intelectual, e cumpra casos de uso de conformidade rapidamente, com uma biblioteca abrangente de políticas out-of-the-box, usando os recursos de DLP exclusivos do Forcepoint para impedir furto de dados.



Forcepoint DLP habilita os seus negócios

- Reduza o risco de furto de dados ao adotar serviços em nuvem como Microsoft Office 365 e Box com aumento da visibilidade de dados.
- Implemente controles de segurança eficaz que você pode auditar facilmente para cumprir requisitos de conformidade e regulatórios.
- Identifique dados confidenciais em imagens, como dados digitalizados e capturas de tela.
- Identifique e impeça ameaças internas com análises comportamentais.
- Localize facilmente e proteja arquivos armazenados em dispositivos Mac, Microsoft Windows e Linux.
- Unifique suas soluções de segurança, coordene as políticas para defesas, compartilhe inteligência em vários pontos e aproveite a gestão centralizada de sua segurança de dados.
- A central de gestão de incidentes e o fluxo de trabalho de e-mails habilitam as pessoas certas a revisar e responder a incidentes de perda de dados.

Principais Recursos

- Reconheça os dados confidenciais ocultos em imagens, documentos digitalizados e capturas de tela.
- Implemente com segurança os serviços na nuvem, como Microsoft Office 365 e Box, mantendo visibilidade e controle sobre dados confidenciais.
- O Drip DLP considera a transmissão cumulativa de dados para identificar pequenas quantidades de vazamentos de dados.
- Identifique funcionários de alto risco, identificando atividades que indicam furto de dados.
- Detecte dados com impressões digitais em dispositivos de ponto de extremidade dentro e fora da rede corporativa.
- Suporte para dispositivos de ponto de extremidade Mac OS X e Microsoft Windows.
- Detecte envio de dados confidenciais para fora da empresa por e-mail, uploads na web, mensagens instantâneas e clientes de serviços em nuvem. Inclui descriptografia SSL quando usado com Forcepoint Web Security

Recursos Forcepoint DLP

ADOTE A INOVAÇÃO COM CONFIANÇA

Atender as necessidades dos clientes e manter a competitividade requer inovar e habilitar sua força de trabalho para adotar novas tecnologias. Forcepoint DLP permite alavancar com segurança serviços potentes na nuvem, como Microsoft Office 365, Box e SalesForce. com, habilitando a sua empresa a continuar a crescer e inovar. Forcepoint DLP habilita sua força de trabalho em roaming, protegendo seus dados confidenciais e sua propriedade intelectual dentro e fora da rede.

CUMPRA E DEMONSTRE A CONFORMIDADE

Uma biblioteca abrangente de políticas out of- the-box torna fácil para seu pessoal de TI implementar rapidamente os controles para cumprir os requisitos regulatórios e proteger a propriedade intelectual. Você pode escolher as políticas apropriadas para cumprir seus requisitos de conformidade, e também as políticas necessárias para sua propriedade intelectual. Forcepoint fornece um conjunto de recursos de detecção de PI avançados, flexível o suficiente para cumprir as necessidades de proteção de dados com uma interface do usuário fácil de usar, que permite selecionar as políticas para proteger a sua propriedade intelectual e seus dados confidenciais em um único modelo. Forcepoint também ajuda a satisfazer auditores com relatórios personalizados, e habilita você a personalizar relatórios, conforme necessário.

LOCALIZE E PROTEJA DADOS CONFIDENCIAIS EM IMAGENS

Uma captura de tela maliciosa ou registros legados digitalizados e armazenados como imagens que apresentam pontos cegos para soluções DLP tradicionais, mas não para o Forcepoint DLP. Com o reconhecimento óptico de caracteres (OCR) da Forcepoint, você pode identificar de forma confiável e proteger dados confidenciais em uma imagem. Esse recurso exclusivo permite controlar o fluxo de informações confidenciais em capturas de tela, páginas de fax, fotos de smartphones e impressas, assim como documentos como cheques, recibos e arquivos legados digitalizados, protegendo contra-ataques avançados e ameaça interna de furto de dados. Outros recursos exclusivos podem identificar métodos de

criptografia personalizada e “Drip DLP” que são usados com frequência para evadir a detecção.

IDENTIFIQUE COMPORTAMENTOS DE USUÁRIO DE ‘ALTO RISCO’ E EDUQUE OS USUÁRIOS PARA AUMENTAR A CONSCIENTIZAÇÃO

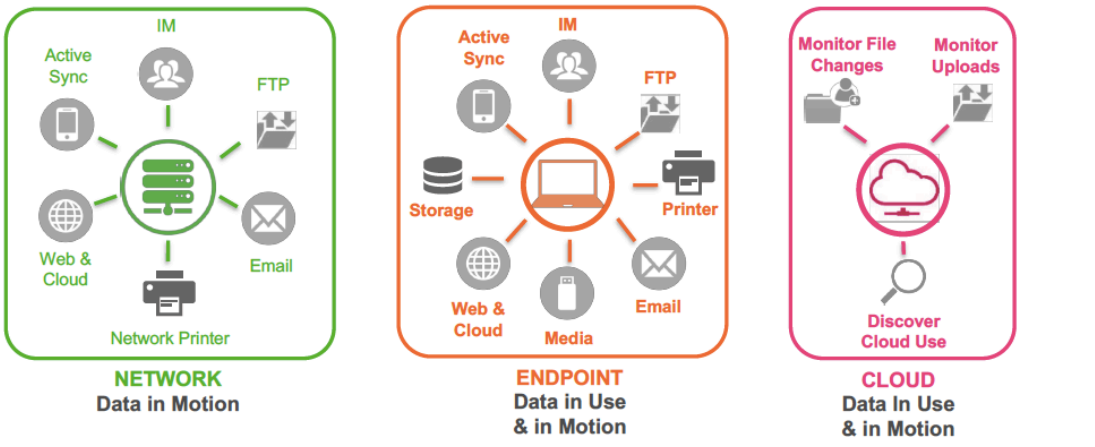
Desde erros de usuários até conteúdo malicioso, os usuários finais com frequência estão no coração dos incidentes de perda de dados. Forcepoint DLP usa dados analíticos comportamentais para identificar proativamente os usuários de alto risco:

- Usuários ingênuos com frequência geram risco, devido a maus hábitos que podem ser apontados e corrigidos antes que a perda de dados ocorra.
- Funcionários insatisfeitos podem ser identificados no início da atividade maliciosa.

Forcepoint DLP fornece com segurança para os usuários o acesso aos dados de que precisam para ajudar a impulsionar a empresa para a frente, mitigando simultaneamente as ameaças internas.

Componentes do Forcepoint DLP

Há duas opções principais do Forcepoint DLP, que podem ser implementadas juntas ou de forma independente para cumprir suas metas de segurança. Isso fornece flexibilidade para satisfazer as necessidades atuais e capacidade para crescer com a empresa.



PRODUTOS FORCEPOINT: DLP NETWORK, DLP ENDPOINT & DLP CLOUD APPS

FORCEPOINT DLP DISCOVERY

Para proteger dados, você deve ter capacidade para localizá-los onde quer que residam. Forcepoint DLP Discovery habilita você a localizar e proteger dados confidenciais na rede, e também os dados confidenciais armazenados em serviços na nuvem, como Microsoft Office 365 e Box. Com o acréscimo do Forcepoint DLP Endpoint, a potência do Forcepoint DLP Discovery pode ser ampliada para pontos de extremidade Mac OS X e Microsoft Windows dentro e fora da rede.

FORCEPOINT DLP NETWORK

A última chance para impedir o furto de dados é quando estão em movimento nos canais de E-mail e Web. Forcepoint DLP Network ajuda a identificar e impedir perda de dados maliciosa e acidental contra-ataques externos ou da crescente Ameaça Interna. Técnicas contra evasão de ameaças avançadas com OCR potente para reconhecer dados em

uma imagem. Use Drip DLP para impedir o furto de dados um registro de cada vez, e para monitoramento de comportamentos e anomalias para identificação de usuários de alto risco.

FORCEPOINT DLP ENDPOINT

Forcepoint DLP Endpoint estende OCR, 'Drip DLP' e outros controles contra perda de dados para os pontos de extremidade Mac OS X e Microsoft Windows, dentro e fora da rede. Forcepoint habilita o compartilhamento seguro de dados armazenados em dispositivos removíveis usando políticas para criptografia de arquivos. Monitoramento de uploads da web, incluindo HTTPS, e também uploads para serviços na nuvem, como Microsoft Office 365 e Box. Integração completa com Outlook, Notes e clientes de e-mail, usando a mesma interface de usuário das soluções Forcepoint Data, Web, E-mail e Endpoint.

MÓDULO DE ANÁLISE DE IMAGEM

Para cumprir obrigações regulatórias em muitas partes do mundo, ou simplesmente garantir um ambiente sem assédio, o módulo opcional de análise de imagem permite identificar imagens explícitas, como pornografia, armazenadas na rede da empresa ou em movimento por canais de E-mail ou Web.

ACE (Advanced Classification Engine)

Forcepoint ACE fornece defesas contextuais em linha e em tempo real para segurança Web, E-mail, de Dados e Móvel, usando pontuação de riscos composta e análises preditivas para fornecer a segurança mais eficaz disponível. Também fornece contenção ao analisar o tráfego de entrada e saída com defesas com reconhecimento de dados para proteção líder do setor contra furto de dados. Classificadores para análise de segurança, dados e conteúdo em tempo real, resultantes de anos de pesquisa e desenvolvimento, habilitam o ACE a detectar mais ameaças do que os mecanismos antivírus tradicionais todos os dias (a comprovação é atualizada diariamente em http://securitylabs.Forcepoint.com).

O ACE é a defesa primária por trás de todas as soluções Forcepoint TRITON Architecture e é apoiado pelo Forcepoint ThreatSeeker Intelligence.

CONJUNTO INTEGRADO DE RECURSOS DE AVALIAÇÃO DE DEFESAS EM 8 ÁREAS PRINCIPAIS.

- 10.000 dados analíticos disponíveis para apoiar inspeções profundas.
- Mecanismo de segurança preditivo que vê diversos movimentos à frente.
- A operação em linha não apenas monitora, mas **bloqueia** as ameaças.

Forcepoint ThreatSeeker Intelligence

O Forcepoint ThreatSeeker Intelligence, administrado pelo Forcepoint Security Labs, fornece a inteligência de segurança coletiva essencial para todos os produtos de segurança Forcepoint. Reúne mais de 900 milhões de pontos de extremidade, incluindo entradas do Facebook e, em conjunto com as defesas de segurança do Forcepoint ACE, analisa até 5 bilhões de solicitações ao dia. Esse reconhecimento abrangente de ameaças de segurança habilita o Forcepoint ThreatSeeker Intelligence a oferecer atualizações de segurança em tempo real que bloqueiam Ameaças Avançadas, malware, ataques de phishing, fraudes e scans, e fornecem as avaliações da Web mais recentes. O Forcepoint ThreatSeeker Intelligence é incomparável em alcance e no uso das defesas em tempo real do ACE para analisar dados coletivos. (Quando você faz upgrade para Forcepoint Web Security, o Forcepoint ThreatSeeker Intelligence ajuda a reduzir a sua exposição a ameaças da web e furto de dados.)

TRITON Architecture

Com segurança melhor da categoria, a arquitetura unificada Forcepoint TRITON Architecture oferece proteção no ponto de clique com defesas em linha e em tempo real do Forcepoint ACE. As defesas em tempo real incomparáveis do ACE são apoiadas pelo Forcepoint ThreatSeeker Intelligence e os conhecimentos dos pesquisadores do Forcepoint Security Labs. O resultado potente é uma arquitetura única, com uma interface de usuário unificada e inteligência de segurança unificada.

EXAMPLOS DE RELATÓRIOS QUE AUXILIAM NA INVESTIGAÇÃO

3. Serviço Especializado de Implantação na Solução ForcePoint Data Loss Prevent

Tarefa
Execução / kick off
Fase 1 - Mapeamento de pré-requisitos e definições instalação / Planejamento
• **Analise de topologia**
• **Analise do negocio**
• **Definição de parâmetros para classificação de informação**
• **Validar Pré-requisitos de Servidores DLP**
Portas de Comunicação
• **Validar as portas de comunicação Live Update**
• **Validar as portas de comunicação cliente/Servidor**
• **Desenhar Topologia com a implantação do DLP**
Fase 2 - Configuração Servidores
• **Instalação dos Servidores DLP:**
• **Protect for endpoint**
• **Atualização de Patches para a solução instalada**
Fase 3 - Configuração Politicas
• **Configuração de política de acordo com o negocio** • **Áreas envolvidas para análise de informação**
• **Validar as classificações importantes para o negócio da companhia**
• **Validar e Analisar padrões de documentos que não podem vazar (Inserir novas regras e documentos)**
• **Validar e Analisar palavras Chaves (Inserir novas palavras)**
Fase 4 - Acompanhamento e ajustes de Regras (Tunning)
• **Acompanhar regras existentes e monitorar as informações capturadas** • **Criar ajustes nas regras (Tunning)**
• **Varredura de Informação**
• **Criar novos Filtros de regras**
Fase 5 - Fechamento do Projeto
• **Documentação do projeto**
• **Hand-off para equipe técnica do cliente**
• **Entrega do Documentação**
• **Entrega do Projeto**

4. Serviço Especializado de Gerenciamento

Destacamos abaixo algumas das principais atividades que serão executadas através da contratação do serviço de gerenciamento, a critério e solicitação do cliente:

- Gerenciamento da solução 8x5;
- Revisão periódica dos servidores do DLP e console;
- Assessment Contínuo no Ambiente
- Análise do ambiente (disponibilidade e performance);
- Tratativa na melhoria de regras e políticas implementadas;
- Envio de e-mail mensal com status do ambiente;
- Manutenção preventiva dos servidores do DLP;
- Alterações administrativas pontuais no servidor Enforce;
- Envio de equipe especializada em caso de incidente crítico que venha a causar algum tipo de indisponibilidade no ambiente;
- Configuração de políticas quando solicitado;
- Atualização de Patches e Hotfix disponibilizados pelo fabricante;
- Gestão de licenças adquiridas;
- Gestão de backup relacionado ao Ambiente de infraestrutura do cliente;
- Reunião mensal para análise do ambiente (Problemas / Planejamento / Solução / Execução) e apresentação de relatório;
- Abertura de chamado com a Symantec em caso extremos e necessários;
- Criação de relatórios gerenciais mensais com todos os indicadores presentes na ferramenta;
- Suporte no desenvolvimento de política e sua aplicação.

4.1 SLA

Os incidentes poderão ser abertos automaticamente, via detecção pela ferramenta, ou manualmente, em caso de detecção pela equipe de gestão DSR9, em quaisquer casos, os mesmos terão tempo de acionamento conforme abaixo. Os tempos de acionamento referem-se ao prazo que a equipe de gestão DSR9 tem para alertar a equipe do cliente sobre o incidente.

Sev 1 ⇨ acionamento em até 2 horas
Incidentes de indisponibilidade total no dispositivo monitorado em uma ou mais localidades, causando impacto crítico ao negócio. P. ex: um servidor crítico está inacessível pela rede ou desligado.
Sev 2 ⇨ acionamento em até 4 horas
Incidentes que causem degradação de serviços ou funcionalidades no dispositivo monitorado em uma ou mais localidades, podendo causar impacto grave ao negócio. P. ex: um servidor crítico está com consumo excessivo de recursos, causando lentidão para os usuários.
Sev 3 e 4 ⇨ acionamento em até 24 horas
Incidentes que causem mal funcionamento de algum serviço ou funcionalidade no dispositivo monitorado, com médio ou baixo impacto no negócio. P. ex: um servidor não-crítico está com lentidão

4.2 Premissa

- A abrangência dos serviços a serem prestados é limitada pelos termos desta proposta, sem flexibilização;
- É necessário que sejam feitas todas as liberações físicas, lógicas e quaisquer outras restrições existentes no ambiente do cliente de forma que todos os acessos necessários já estejam disponíveis no momento das instalações e configurações, bem como no decorrer de todo o contrato;
- O cliente deve fornecer todos os dados necessários para a configuração correta dos equipamentos/tecnologias como endereços de instalação, mapa de Data Center, plano de endereçamento IP, definição de regras, políticas e outros;
- O cliente deve fornecer conectividade física e lógicas para os equipamentos através de links dedicados, links de Internet ou quaisquer outros que possuam funcionalidade similar, de forma que os equipamentos estejam perfeitamente acessíveis entre si.
- Não estão inclusas atividades de instalação e configuração de infraestrutura básica de Datacenter como obras civis, instalações elétricas e cabeamento estruturado.
- Também não estão inclusas a instalação e configuração de elementos de rede, servidores e quaisquer outros que não estejam especificados neste documento, bem como a execução de serviços que não foram contratados e não fazem parte dos serviços DSR9.

4.3 Benefícios

- Atuação local e ambientação do cliente;
- Mitigação dos riscos operacionais relacionados aos ativos do Symantec DLP;
- Segurança agregada à administração, manutenção e uso de todo o sistema;
- Mitigação da perda de dados em rápida atuação;
- Redução de custos para proteção de utilização indevida de dados;
- Maior controle das informações trafegadas;
- Enforcement da política de segurança da informação do cliente;
- Maior flexibilidade e escalabilidade do ambiente de segurança;
- Redução de custos operacionais;
- Manutenção do ambiente atualizado

5. Condição Comercial

Cenário 1 – DLP Forcepoint

ITEM	DESCRIÇÃO	UNIDADE	QUANT	UNIT.	TOTAL
1	Aquisição de licenças de software de solução de prevenção de vazamento de dados - Data Loss Prevention - DLP	UN.	3190	R$ 1.211,56	R$ 3.864.882,78
2	Treinamento	TURMA	1	R$ 53.627,20	R$ 53.627,20
VALOR TOTAL					R$ 3.918.509,98

Serviços

SERVIÇO ESPECIALIZADO (Opcional)	
Implantação da Solução Contratada Cenário 1	R$ 132.000,00
Gerenciamento da Solução Contratada (Mensal)	R$ 10.000,00

Obs: Cotação do dólar PTAX referente ao dia anterior do faturamento

6. Tributos

Os valores dos produtos e ou serviços incluem todos os tributos incidentes sobre o objeto desta proposta, de acordo com a legislação vigente na data de sua emissão.

7. Condição de Pagamento

Faturamento imediato com pagamento em até 30 dias**.** Sendo **software** sendo faturado pela Westcon Brasil LTDA - CNPJ:28.268.233/0007-84. E os **serviços** pela DSR9 TECNOLOGIA DA INFORMACAO LTDA - CNPJ: 10.656.232/0001-56

8. Validade da Proposta

Esta proposta é válida até 10/12/2021, caso expire este prazo, as condições descritas estarão sujeitas à confirmação.

9. Viagens

O Cliente deverá reembolsar toda e qualquer despesa com deslocamentos ou viagens para fora da Grande São Paulo. O reembolso se dará mediante apresentação de comprovantes e os limites para cada item de despesa serão os mesmos praticados pelo Cliente em situações semelhantes.

TERMO DE ACEITE DA PROPOSTA COMERCIAL Nº 202111-9217-V2

O aceite da presente proposta consiste na efetiva anuência de aquisição do objeto proposto, constituindo o acordo final entre a **DSR9** e a **FUNASA** substituindo todo e qualquer acordo anterior referente a esse objeto, seja ele por escrito ou verbal, sendo considerada nula a adoção de medidas diversas das condições aqui estabelecidas.

De acordo:

_____

FUNASA

Data: ___/___/___

_____
Arthur Andrade
arthur.andrade@dsr9.com

Testemunhas

_____
Nome:
RG:

_____
Nome:
RG: