

ANEXO VII - PLANILHA DE CONFORMIDADE TÉCNICA (PONTO A PONTO)

Instruções para a Licitante:

Esta planilha deve ser preenchida de forma completa e objetiva, servindo como um índice remissivo da proposta técnica. **A falta de preenchimento ou a apresentação de informações inverídicas poderá levar à desclassificação da proposta.** Na coluna "Comprovação (Descrição e Referência no Documento/Página)", descreva sucintamente como a sua solução/serviço atende ao requisito e indique claramente o número da página ou seção da proposta técnica, anexo, ou outro documento onde a evidência pode ser encontrada.

PLANILHA DE CONFORMIDADE TÉCNICA			
Item	Requisito Técnico do Termo de Referência	Referência no TR	Comprovação de Atendimento (Descrição e Referência no Documento/Página)
A	ESCOPO GERAL E MÓDULOS OBRIGATÓRIOS		
A.1	Anti-malware / NGAV multicamadas (assinaturas, heurística, comportamento e ML);	Anexo I – 1.1.1	
A.2	EDR com telemetria rica, busca (Threat Hunting), RCA e reconstrução de cadeias de ataque (kill-chain);	Anexo I – 1.1.2	
A.3	Firewall de endpoint e IPS de próxima geração com capacidade de virtual patching e bloqueio de explorações de rede;	Anexo I – 1.1.3	
A.4	Controle de aplicações (whitelisting/blacklisting por hash, caminho, certificado);	Anexo I – 1.1.4	
A.5	HIPS (Host-based Intrusion Prevention) e controles para proteção do SO (arquivos, chaves de registro, autorun, hosts);	Anexo I – 1.1.5	
A.6	Controle de dispositivos e DLP de endpoint com políticas granulares e inspeção de conteúdo;	Anexo I – 1.1.6	
A.7	Módulo especializado para proteção do Active Directory (detecção de abusos de Kerberos, movimentos laterais e mecanismos de deception);	Anexo I – 1.1.7	
A.8	Ferramentas de resposta remota (isolamento, execução remota de scripts, coleta forense, dump de memória) e automação por playbooks.	Anexo I – 1.1.8	

B	REQUISITOS DO AGENTE DE ENDPOINT		
B.1	Agente único e unificado: toda a funcionalidade essencial (EPP, EDR, DLP, HIPS, firewall, telemetria) deverá ser provida por um único agente sem dependência de agentes auxiliares para funcionalidades básicas.	Anexo I – 1.2.1	
B.2	Consumo e performance: Consumo médio de CPU em operação normal $\leq 1\%$; Consumo médio de CPU durante varredura completa $< 10\%$; Consumo médio de memória RAM em operação normal ≤ 200 MB; Consumo médio de memória durante atividades intensivas < 400 MB; Tráfego de rede típico gerado pelo agente em operação normal < 100 kbps.	Anexo I – 1.2.2	
B.3	Autoproteção (anti-tampering): o agente deve resistir a tentativas de desativação, modificação ou remoção não autorizada; a desinstalação só poderá ser efetuada mediante credenciais da console e processo protegido por autenticação forte (MFA).	Anexo I – 1.2.3	
B.4	Operação offline: o agente deve manter as últimas políticas e operar por, no mínimo, 30 dias sem conectividade com o console, executando controles DLP e políticas locais.	Anexo I – 1.2.4	
B.5	Atualizações e distribuição de assinaturas/engine: o agente e o console devem suportar atualização incremental automática (mínimo diário) e opção de distribuir atualizações via servidores internos ou clientes eleitos (peer distribution) com controle de banda, sem necessidade de reinicialização obrigatória.	Anexo I – 1.2.5	
B.6	Compatibilidade: o agente deve suportar versões e edições de Windows (estações e servidores) e Linux (principais distribuições corporativas).	Anexo I – 1.2.6	
C	REQUISITOS DA CONSOLE DE GERENCIAMENTO CENTRAL		
C.1	Arquitetura e certificações: console de gerenciamento central (plataforma SaaS) hospedada em nuvem segura com certificações ISO 27001 (ou equivalente) e	Anexo I – 1.3.1	

	SOC 2 Tipo II (ou equivalente); SLA de disponibilidade contratual mínimo 99,95%.		
C.2	Acesso e autenticação: acesso via HTTPS/TLS 1.2+; interface nativa em Português-BR; suporte a SAML 2.0, LDAP/AD, OAuth/OIDC; MFA obrigatória para administradores; possibilidade de restrição por ranges de IP; integração e entrega ao SIEM do CONTRATANTE para retenção de 1 ano.	Anexo I – 1.3.2	
C.3	RBAC e auditoria: Controle de Acesso Baseado em Função (RBAC) granular; perfis predefinidos e customizáveis; trilha de auditoria imutável com retenção mínima de 1 ano.	Anexo I – 1.3.3	
C.4	Gerenciamento de políticas e grupos: organização de endpoints em grupos dinâmicos e estáticos; aplicação de políticas por atributos; implantação remota e agendada de agentes; mecanismos de rollback e versionamento de políticas.	Anexo I – 1.3.4	
C.5	Dashboards e relatórios: dashboards em tempo real; relatórios customizáveis; suporte a exportação (CSV, JSON) e integração via APIs com SIEM/SOAR.	Anexo I – 1.3.5	
C.6	Integração: APIs REST bem documentadas, webhooks, syslog e conectores pré-construídos para SIEM/CMDB/ITSM.	Anexo I – 1.3.6	
D	REQUISITOS DE EPP / NGAV		
D.1	Proteção em tempo real (on-access): motor que combine assinaturas, heurística, análise comportamental e Machine Learning com atualização contínua de reputação.	Anexo I – 1.4.1	
D.2	Proteção fileless e scripts: detecção e bloqueio de técnicas sem arquivo, incluindo execução via PowerShell, WMI, macros e interpreters; capacidade de analisar comportamento em memória.	Anexo I – 1.4.2	
D.3	Verificação e tratamento de arquivos compactados recursivamente (suporte mínimo a 10 níveis de compactação) e análise de arquivos grandes (>20MB).	Anexo I – 1.4.3	

D.4	Ações configuráveis por categoria: permitir a definição de ações primárias e secundárias (alertar, limpar, quarentenar, apagar) por categoria de ameaça; lista de exclusões.	Anexo I – 1.4.4	
D.5	Capacidade de reversão: possibilidade de restaurar assinaturas/definições anteriores armazenadas no servidor (rollback de vacina).	Anexo I – 1.4.5	
D.6	Requisitos operacionais: suporte a planos de distribuição de atualizações, escolha de clientes para distribuição e controle de banda.	Anexo I – 1.4.6	
E	REQUISITOS DE EDR - TELEMETRIA, HUNTING E RESPOSTA		
E.1	Coleta de telemetria: coleta contínua e em tempo real de processos, rede, filesystem, registro, eventos de autenticação, carregamento de bibliotecas, linhas de comando e outros artefatos.	Anexo I – 1.5.1	
E.2	Retenção e pesquisa: telemetria online pesquisável por período mínimo de 90 dias e possibilidade de exportação para análise histórica.	Anexo I – 1.5.2	
E.3	Mapeamento MITRE ATT&CK: todos os alertas e eventos devem ser mapeados ao framework MITRE ATT&CK com visualização interativa.	Anexo I – 1.5.3	
E.4	Threat Hunting: interface com linguagem de consulta avançada para buscas proativas; suporte a consultas ad-hoc e saved searches.	Anexo I – 1.5.4	
E.5	RCA e reconstrução de cadeia de ataque: geração automática de árvores correlacionadas (causa raiz, origem, propagação, artefatos e timeline).	Anexo I – 1.5.5	
E.6	Ações remotas e orquestração: isolamento de rede, finalização de processos, quarentena/deleção de arquivos, modificação de chaves de registro, parada de serviços, reboot, execução remota de scripts (PowerShell/Bash) com log de output.	Anexo I – 1.5.6	
E.7	Coleta forense remota: coleta de arquivos,	Anexo I –	

	logs e dump de memória para análise forense com mecanismo de exportação segura.	1.5.7	
E.8	Automação (playbooks): criação de playbooks condicionais que executem sequências de ações baseadas em gatilhos, com versionamento e testes em ambiente controlado.	Anexo I – 1.5.8	
F	PROTEÇÃO CONTRA EXPLORAÇÃO DE MEMÓRIA		
F.1	Cobertura mínima: mitigar explorações em aplicações críticas (navegadores, runtime Java, pacotes Office, ambientes .NET e aplicações corporativas críticas).	Anexo I – 1.6.1	
F.2	Detectar e bloquear shellcode, técnicas de injeção de código e exploração baseada em memória, com alerta detalhado.	Anexo I – 1.6.2	
F.3	Permitir configuração de sensibilidade e tuning por aplicação e grupos de endpoints.	Anexo I – 1.6.3	
G	HARDENING, CONTROLE DE APLICAÇÕES E EXCEÇÕES		
G.1	Application Control: suporte a whitelisting/blacklisting por hash (MD5/SHA1/SHA256), caminho, fabricante e certificado digital.	Anexo I – 1.7.1	
G.2	Descoberta e catálogo: descoberta automática de aplicações instaladas para auxiliar na criação de políticas.	Anexo I – 1.7.2	
G.3	Trusted Updaters: definição de processos/atualizadores confiáveis (Windows Update, SVCHost, instaladores corporativos) com política de exceção.	Anexo I – 1.7.3	
G.4	Modo de simulação/auditoria: políticas aplicáveis em modo 'monitor' para avaliar impacto; workflow de solicitações de exceção com justificativa e aprovação registrada.	Anexo I – 1.7.4	
G.5	Application hardening: bloquear execução de aplicações não autorizadas mesmo com privilégios administrativos.	Anexo I – 1.7.5	

H	REDUÇÃO DA SUPERFÍCIE DE ATAQUE E LOTL		
H.1	Detecção contextual de LOTL: distinguir uso legítimo vs malicioso de ferramentas administrativas levando em conta usuário, processo pai, argumentos e comportamento subsequente.	Anexo I – 1.8.1	
H.2	Base de referência LOTL: oferecer base mínima de aplicações conhecidas (mínimo de 50) e mapear cada comportamento ao MITRE ATT&CK.	Anexo I – 1.8.2	
H.3	Auto-tune e prevalência: capacidade de auto-sintonização com histórico de prevalência de comportamento por, no mínimo, 6 meses; geração automática de recomendações e exceções.	Anexo I – 1.8.3	
H.4	Isolamento de aplicações não confiáveis: política de isolamento que impede exclusão/modificação de arquivos e pastas críticas, com modo de simulação e logs detalhados.	Anexo I – 1.8.4	
I	CONTROLE DE DISPOSITIVOS E DLP		
I.1	Controle granular de dispositivos USB por tipo, classe, fabricante, modelo e número de série; operações de leitura/escrita/execução configuráveis.	Anexo I – 1.9.1	
I.2	Controle de outras interfaces: Wi-Fi, Bluetooth, portas seriais, FireWire, CD/DVD, etc.	Anexo I – 1.9.2	
I.3	Políticas baseadas em localização e contexto: permitir políticas diferenciadas dependendo da rede, VLAN, OU do AD ou tag de inventário.	Anexo I – 1.9.3	
I.4	DLP de endpoint — Requisitos: Identificação de dados por palavras-chave, regex e dicionários; Impressão digital de documentos; Detecção por similaridade; Suporte a arquivos compactados e grandes (>20 MB); Detecção em Português-BR; Inspeção de conteúdo; Ações automáticas (quarentena, bloqueio, notificação); Monitoramento de clipboard e captura de	Anexo I – 1.9.4	

	tela; Monitoramento de clientes de e-mail; Notificações customizáveis.		
J	PROTEÇÃO E RESPOSTA AO ACTIVE DIRECTORY (AD)		
J.1	Detecção de ataques a credenciais: Kerberoasting, Pass-the-Hash, Pass-the-Ticket, Overpass-the-Hash, Forged PAC, DCSync, Golden Tickets e enumeração de sessão.	Anexo I – 1.10.1	
J.2	Monitoramento AD sem dependência exclusiva de agentes em DCs, correlacionando sinais de endpoints.	Anexo I – 1.10.2	
J.3	Deception e mascaramento de topologia: preferencialmente mecanismo nativo para implantar decoys e mascarar topologia.	Anexo I – 1.10.3	
J.4	Resposta automatizada no AD: ação com um clique para forçar redefinição de senha, invalidação de sessões e geração de relatório de avaliação de vulnerabilidades.	Anexo I – 1.10.4	
K	NÃO-FUNCIONAIS: DESEMPENHO, ESCALABILIDADE E LATÊNCIA		
K.1	Capacidade: suportar, em modo SaaS, gerenciamento de, no mínimo, 1.200 endpoints sem degradação; arquitetura escalável para 5.000 endpoints.	Anexo I – 1.11.1	
K.2	Latências máximas (SLAs técnicos): propagação de políticas ≤ 5 minutos; envio de telemetria crítica ≤ 30 segundos; execução de ações remotas (ex.: isolamento) ≤ 10 segundos.	Anexo I – 1.11.2	
K.3	Disponibilidade e resiliência: SLA da plataforma de 99,95% com planos de contingência e continuidade.	Anexo I – 1.11.3	
L	SEGURANÇA DA SOLUÇÃO E CADEIA DE SUPRIMENTOS (SDLC)		
L.1	Certificações: o fabricante deve demonstrar conformidade com padrões (ISO 27001 ou equivalente, SOC 2 Tipo II ou equivalente) e políticas de segurança da cadeia de	Anexo I – 12.1	

	suprimentos.		
L.2	SDLC e práticas de desenvolvimento seguro: o fornecedor deve apresentar documentação do SDLC, políticas de secure coding, resultados de testes de segurança (pen tests, SAST/DAST), e gestão de vulnerabilidades.	Anexo I – 1.12.2	
L.3	Auditoria e acesso a evidências: obrigação de fornecer evidências e permitir auditoria técnica (POC, logs, relatórios) mediante solicitação justificada.	Anexo I – 1.12.3	
M	INTEGRAÇÕES, EXPORTAÇÃO DE DADOS E FORMATOS		
M.1	APIs: APIs REST/JSON bem documentadas e estáveis; suporte a autenticação via tokens/credentials com rotação e expiração.	Anexo I – 1.13.1	
M.2	Exportação: suporte a exportações em CSV e JSON; integração via syslog e conectores para SIEM e SOAR.	Anexo I – 1.13.2	
M.3	Conectores: conectores pré-construídos para os principais SIEMs do mercado, com playbooks de ingestão e normalização.	Anexo I – 1.13.3	
N	REQUISITOS DE SERVIÇOS E HABILITAÇÃO		
N.1	Apresentação de no mínimo 1 (um) atestado de capacidade técnica comprovando experiência na prestação de serviços de fornecimento, implantação e suporte da solução de segurança de endpoint (EDR/XDR).	TR - 9.30.1	
N.2	Evidência de que o projeto referenciado no atestado possui características compatíveis com o objeto desta contratação, contemplando, no mínimo, gerenciamento centralizado e proteção para endpoints e servidores.	TR - 9.30.2	
N.3	Comprovação, por meio de atestados, de ter executado serviços de fornecimento, implantação e suporte de solução de EDR para um parque computacional de, no mínimo, 600 endpoints.	TR - 9.30.3	