SONDA®
make it easy

DESCRITIVO ENDPOINT PROTECTION

ÍNDICE

1. Versão do Produto

Versão	Escopo	Data de Atualização
Versão 01	Criação do documento	-

2. Descrição Resumida

O serviço de antivírus é uma proteção para endpoints que previnem exploração de agentes mal-intencionados. O Antivírus protege contra atividades maliciosas ou ataques, visando garantir a conformidade de segurança dos endpoints com padrão de segurança de dados.

A solução de próxima geração para antivírus, possibilita a substituição do antivírus tradicional combinando as tecnologias de prevenção mais eficazes e a visibilidade total de ataques com inteligência de ameaças integrada, alterando a forma de atuação de assinatura para comportamento.

O Next-Generation Antivírus (NGAV), comprovou interromper o malware, com inteligência de ameaças integrada e resposta imediata, com um único agente leve que opera sem a necessidade de atualizações de assinatura constantes, infraestrutura de gerenciamento local ou integrações complexas.

3. Objetivo

A solução de NGAV fornecida pela **SONDA** é líder na proteção de endpoint. Utilizando inteligência artificial (IA), a plataforma oferece visibilidade e proteção instantâneas a toda a empresa evitando ataques aos endpoints dentro ou fora da rede. A solução unifica perfeitamente o antivírus de última geração com a melhor detecção e resposta de endpoint do mercado, com um time de serviços gerenciados e busca de ameaças 24 horas por dia, sete dias por semana. Sua infraestrutura de nuvem e arquitetura de agente único eliminam a complexidade e adicionam escalabilidade, capacidade de gerenciamento e velocidade.

A plataforma protege os **CLIENTES** contra todos os tipos de ataques cibernéticos, usando tecnologia de inteligência artificial, sem necessidade de assinaturas. Baseado em Indicadores de Ataque (IoA) bloqueia ameaças conhecidas e desconhecidas em tempo real.

4. Benefícios

Impedir através de inteligência de ameaças integradas e resposta imediata que malwares comprometam o ambiente de TI, evitando:

- Perda de dados devido a criptografia realizada pelos malwares;
- Vazamento de informação da organização.

4.1. Diferenciais Comerciais

Visando o cenário atual de ameaças Cibernéticas a **SONDA** tem como benefícios:

- Experiência nas melhores tecnologias de mercado baseados nos resultados das melhores empresas de pesquisa e testes do mundo;
- Acesso remoto em tempo real para ação imediata a qualquer incidente;
- Equipe com certificações nas tecnologias;
- Administração Centralizada.

5. Escopo de Atuação

- Protege contra malwares conhecidos e desconhecidos, e ataques sem arquivos ou malware;
- Elimina ransomware;
- Fornece visibilidade e alerta de contexto inigualáveis;
- Desvenda um ataque inteiro em uma única árvore de processos de fácil compreensão, repleta de dados contextuais e de inteligência de ameaças;
- Proteção contra vírus, spywares, cavalos de tróia, worms, bots e rootkits;
- Prevenção contra táticas de rápida mudança, técnicas e procedimentos (TTPs) usados pelos adversários para violar organizações - incluindo malware básico, malware de dia zero e até ataques avançados sem malware;
- Segurança de firewall defende contra hackers graças ao firewall bidirecional silencioso;
- Segurança no uso de dispositivos USB;
- Gerenciamento **SONDA**;
- Console centralizada Web, com controles de acesso e segurança granular;
- Configuração de políticas de antivírus, firewall e de exceções específicas para o **CLIENTE** ou para grupo de máquinas.

5.1. Relatórios entregáveis

O **CLIENTE** tem disponível os relatórios abaixo, para confecção do relatório o **CLIENTE** deve abrir uma requisição de serviço.

- Relatórios de riscos por máquina ou por usuário;
- Relatório de inventário do antivírus;
- Relatório executivo.

6. Ofertas

O serviço oferta o EndPoint Protection para os servidores com as funcionalidades abaixo, garantindo a segurança e prevenção de invasão:

Prevent: um novo conceito em prevenção, combina de maneira única uma série de métodos para fornecer prevenção contra táticas de rápida mudança, técnicas e procedimentos (TTPs) usados pelos adversários para violar organizações - incluindo malware básico, malware de dia zero e até ataques avançados sem malware;

Threat Intelligence: realiza uma análise profunda de ameaças evasivas e desconhecidas, enriquece os resultados com inteligência de ameaças. Análises mais sofisticadas são necessárias para descobrir malwares evasivos e avançados. A tecnologia de Análise Híbrida expõe comportamentos ocultos, neutraliza malware evasivo e fornece mais IOCs, para melhorar a eficácia de toda a infraestrutura de segurança, permitindo que a equipe de segurança compreenda melhor os ataques sofisticados de malware e fortaleça suas defesas;

- **Endpoint Integration:** Todos os arquivos quarentenados podem ser automaticamente investigados;
- **Malware Analysis:** Toda a análise de arquivos é feita pelo Falcon Sandbox;
- **Malware Search:** Automaticamente descobre famílias de Malwares e campanhas de ataque para proteger os endpoints contra-ataques similares;
- **Custom Inteligence:** Gera IOCs através de análise Sandbox para que sejam utilizadas e compartilhadas com outras ferramentas de segurança;
- **Threat Inteligence:** Mostra quem está por trás de um ataque e aprende sobre as técnicas utilizadas pelo ator malicioso para o desenvolvimento de contramedidas.

Device Control: permite que os administradores controlem os dispositivos USB usados em seus ambientes e reduzam os riscos associados. O Falcon Device Control fornece a visibilidade e o controle granular necessários para permitir o uso seguro de dispositivos USB em toda a organização, permitindo que o **CLIENTE** monitore como os dispositivos USB são usados em seu ambiente. Determina com precisão quais dispositivos são permitidos ou restritos e o nível granular de acesso concedido a cada dispositivo;

Control Respond: fornece a capacidade de se conectar em host para conter e investigar sistemas comprometidos. A funcionalidade garante acesso remoto em tempo real para ação imediata a qualquer incidente;

Assinatura	Tipo	Serviços
1	Standard	• Endpoint Protection, Threat Intelligence, Control and Respond, Device Control. • Gerenciamento 24x7 **SONDA.**

7. Segurança – Serviços de Segurança Gerenciados

Os Serviços de Segurança Gerenciados da **SONDA** têm como objetivo o princípio de defesa em profundidade onde é aplicado em cada camada, tecnologia, processos e controles baseados no framework CIS (Center of Internet Security Framework) e a na norma ISO/IEC 27000.

8. Monitoramento

Para atuar de forma preventiva e preditiva, a **SONDA** oferece o serviço de Monitoramento que coleta dados dos itens monitorados e identifica condições que indicam a saúde do ambiente, sinalizando possíveis riscos ou sucessos operacionais.

O **CLIENTE** tem acesso ao portal da ferramenta de monitoramento, onde pode visualizar dados e relatórios detalhados, garantindo total transparência e a certeza de que o ambiente está sendo continuamente gerido e acompanhado pela equipe **SONDA**.

Além disso, o serviço conta com integração entre nosso ITSM e o Monitoramento por meio da ferramenta de Enterprise Application Integration (EAI), permitindo a abertura automática de chamados sempre que uma anomalia for detectada. Isso reduz significativamente o tempo de resposta a qualquer irregularidade no ambiente.

- **Monitoramento padrão**

Item	Regra
Servidores	UP/DOWN de Serviços da solução de Endpoint Security.
Segurança	Eventos de Segurança reportado pelo o EndPoint Protection.

9. Premissas e Requisitos

- A **SONDA** não se responsabiliza por definições dos requisitos de negócio para as políticas de proteção, firewall, prevenção contra intrusões, controle de dispositivos e aplicativos e exceções;
- A **SONDA** não se responsabiliza por possíveis prejuízos causados por eventuais acessos legítimos do **CLIENTE**;
- O **CLIENTE** deve indicar um profissional como responsável pelo fornecimento de informações sobre o ambiente;
- Este serviço não contempla a instalação dos agentes nos recursos ou configurações no SO, caso o **CLIENTE** desejar contratar este serviço deve contratar o serviço de Professional Services de SO;
- Para utilização do serviço deve ser avaliado a compatibilidade com os sistemas.

9.1. Compatibilidade da Solução de Endpoint

A consulta da compatibilidade da Solução de Endpoint deve ser feita diretamente pelo site do fabricante, devido as constantes atualizações de Sistemas Operacionais, abaixo consta o link a ser consultado no item de DEPLOYMENT:
https://www.crowdstrike.com/products/faq/?srsltid=AfmBOoq4tzZuVH_VCvfpTZQnpyYDAdUE9HIPylx5WLPchMIwAAqKD0fG

10.Matriz de Responsabilidades

Para um melhor entendimento a matriz de responsabilidade será classificada com base na metodologia RASICO, onde: **R** - Responsável; **A** - Aprovador; **S** - solicita; **I** – Informado; **C** – Consulta e **O** - Opcional.

Atividades	SONDA	CLIENTE
Geração de relatórios do ambiente do **CLIENTE**	R	S
Criação e alteração de políticas de Segurança	R	S
Definição dos requisitos de negócio para as políticas de Prevenção contra Intrusões	I	R
Criação e alteração de políticas de Exceções	R	S
Definição dos requisitos de negócio para as políticas de Exceções	I	R

11.Requisição de Serviço

A tabela abaixo lista as requisições de serviços disponíveis para solicitações dos **CLIENTES** assim como seu tempo de solução e horário de cobertura.

Requisição	Classificação	Tempo de Solução
Criar política	C	Conforme TS contratado
Alterar política	C	Conforme TS contratado
Liberar arquivo bloqueado	A	Conforme TS contratado
Analisar computador infectado	B	Conforme TS contratado
Gerar relatório	D	Conforme TS contratado

12.Nível de Serviço

Serviço	Nome	Descrição	Meta
EndPoint Protection	Disponibilidade do sistema	Percentual de tempo que o serviço estará disponível, incluindo acessibilidade e funcionalidade, excluindo desse tempo as atividades de paralisação programada e demais exceções mencionadas em contrato.	99,48%


SONDA
make it easy