SMART DEFENDER: análise de ameaças em tempo real

HSC

Sumário

Introdução

Frente à crescente evolução do cibercrime e o aumento do número de ataques de fraude e engenharia social, é imprescindível que os sistemas de proteção estejam preparados para lidar com ameaças mais sofisticadas.

O Smart Defender é um Cloud APT, motor que integra todos os sistemas de segurança da HSC em uma rede global. Busca proteger organizações e seus usuários em tempo real, utilizando as mais avançadas tecnologias.

A solução já vem integrada nos produtos HSC e também pode ser contratada à parte e integrada a plataformas de terceiros ou agregadas em serviços de NOC e SOC.

A importância de investir em cibersegurança

Ataques como phishing, ransomware, links direcionados à sites falsos, documentos maliciosos, ataques de engenharia social por email ou Business Email Compromise (BEC, na sigla em inglês), malware evasion, PDFs com boletos e ordens de pagamento adulterados e tantas outras ameaças atormentam qualquer organização.

Estes tipos de ataques cresceram mais de 43% somente em 2020. Com a adoção em massa do Home-Office e Cloud Office, cada vez mais organizações se tornaram alvos de criminosos e hackers. Entretanto, grande parte delas não está preparada para isso.

Tendo isso em mente, é preciso projetar uma infraestrutura de proteção que conte com soluções que vão além do tradicional.

Através de técnicas de engenharia social, criminosos estudam o comportamento humano para explorar brechas. Monitorando redes sociais de funcionários, por exemplo, é possível descobrir seus hábitos, preferências e a quem estes se reportam dentro da hierarquia corporativa, oportunizando a criação de ataques de phishing personalizados. Um único clique pode comprometer a segurança de toda a organização. Soluções inteligentes como o Smart Defender se tornaram essenciais, pois usam tecnologias de Inteligência Artificial, Machine Learning e Behavior Analysis para detectar e eliminar essas ameaças em tempo real.

Como Funciona o Smart Defender

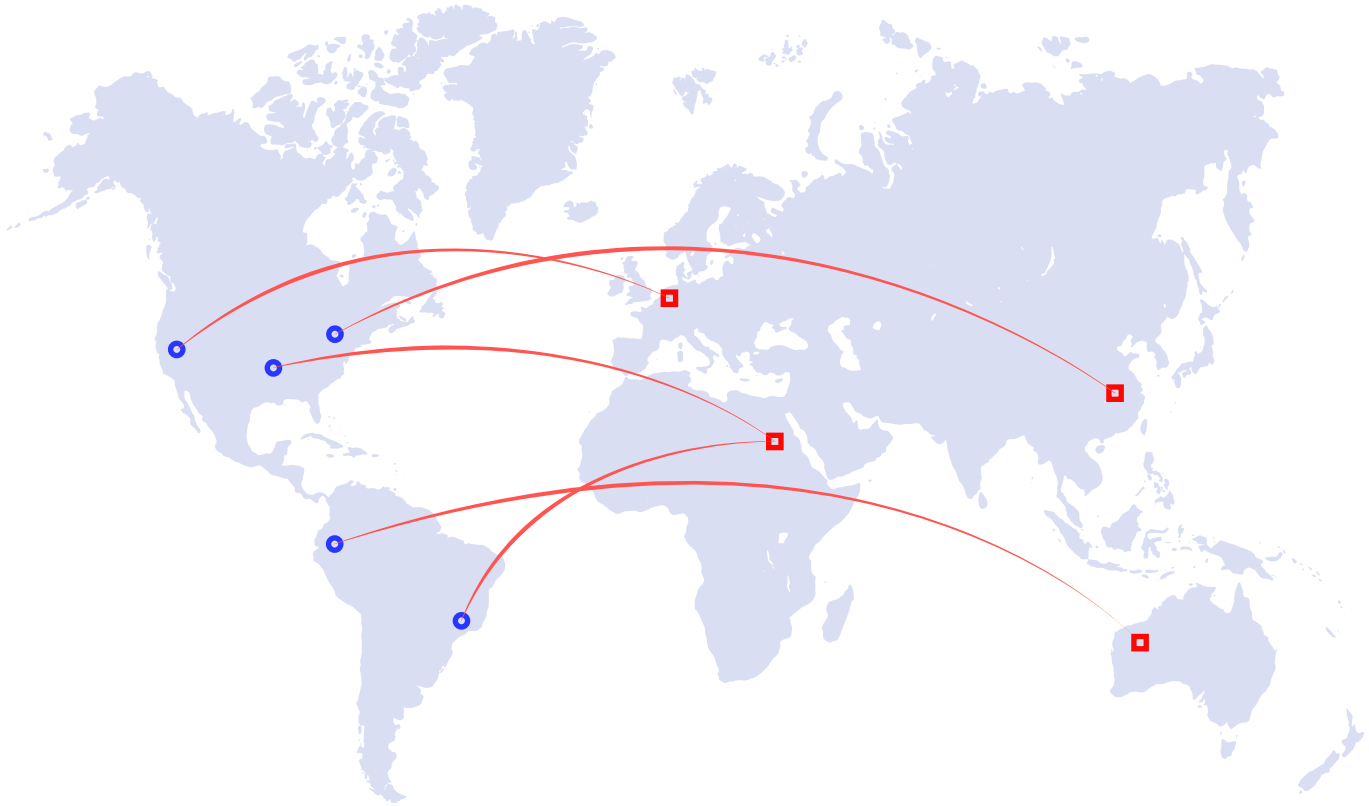
O Smart Defender é um solução de Advanced Threat Protection (APT) que funciona na Nuvem e está integrada aos produtos da HSC. Também pode ser incorporada em sistemas de terceiros através de sua API. Seu objetivo é viabilizar a análise de IPs, URLs e arquivos e seus metadados.

Seu funcionamento é flexível e adaptável. Além disso, é possível implantar módulos como o Sandbox, tanto localmente quanto através da nuvem da própria HSC. Com o Cloud Sandbox, é possível detectar e conter ameaças de hora-Zero, emulação de códigos maliciosos e de registro, entre outras aplicações com base no comportamento. Tudo isso de forma transparente e online, sem depender de vacinas.

Pesquisas apontam que 90% dos ataques às organizações começam com um e-mail direcionado ao usuário final, hoje o principal alvo dos ataques baseados em Engenharia social.

O Smart Defender possui uma rede global capaz de analisar, em tempo real, a reputação de arquivos, URLs e IPs. Sua base é atualizada dinamicamente fazendo com que, em menos de 60 segundos, todos os clientes já estejam protegidos contra uma nova ameaça.

O Smart Defender conta com as tecnologias de Sandbox Cloud e Local para documentos, arquivos e URLs. Além disso, seu Smart Crawler simula a ação do usuário ao clicar em um link, seguindo a URL até seu destino e identificando possíveis ameaças através da tecnologia Behavior Analysis.



Principais funcionalidades

Os links são uma porta de entrada para as mais variadas ameaças. Por isso, o Smar Defender adota estratégias específicas para lidar com eles. Entre elas, podemos destacar:

- Classificação e pontuação dos links dentro de e-mails
- SandBox Local ou em Nuvem
- Inteligência Artificial e Machine Learning
- Análise da reputação de origem e anexos de e-mails
- Proteção de Urls "On-Click" através de Behavior analysis
- Integração com plataformas de e-mail, como MS365, Gsuite, etc

O Smart Defender potencializa as soluções da HSC, provendo segurança e visibilidade de ameaças e incidentes para uma melhor gestão e resposta rápida por parte do administrador.

Ferramentas de proteção

Categorização de URLs

Análise, detecção e categorização links. Atualmente são mais de 100 milhões de URLs cadastradas em 150 categorias. As URLs são analisadas e categorizadas automaticamente, permitindo que o administrador possa reportar ou sugerir recategorização para a HSC de forma automática.

Reputação

O Smart Defender está ligado a uma rede global de colaboração de segurança. Por isso, consegue realizar consultas em tempo real acerca da reputação de URL's e links dentro de e-mails, endereços de IPs e arquivos, através da análise do arquivo completo ou processando somente de seus metadados. Tudo isso de forma anônima e sem comprometer dados sensíveis de usuários.

Cloud SandBox

Possui a capacidade de detecção e proteção contra ameaças em tempo real, executando os arquivos em um ambiente seguro, isolado e controlado, através de máquinas virtuais que podem funcionar em um Appliance ou 100% na nuvem da HSC. Essas máquinas são compatíveis com diferentes sistemas operacionais como Windows, Linux, Android, entre outros.

Além de analisar arquivos, como executáveis e compactados (.apk, .exe. dlls, .ZIP, .rar e outros), aplicações e documentos do Office (.odf,.docx, .doc, .pptx, ppt, xlsx, .xls, entre outros), o Smart Defender realiza o Sandboxing de URLs através do HSC Smart Crawler, que simula a ação do usuário clicando nos links e seguindo o caminho da URL até conseguir identificar sua real intenção. Essa tecnologia é chamada de Behavior Analysis e com ela é possível identificar ameaças de "hora-zero", sem a necessidade de assinaturas prévias

Local File SandBox

Uso de engenharia reversa de malware para neutralizar as ameaças.

URL SandBox

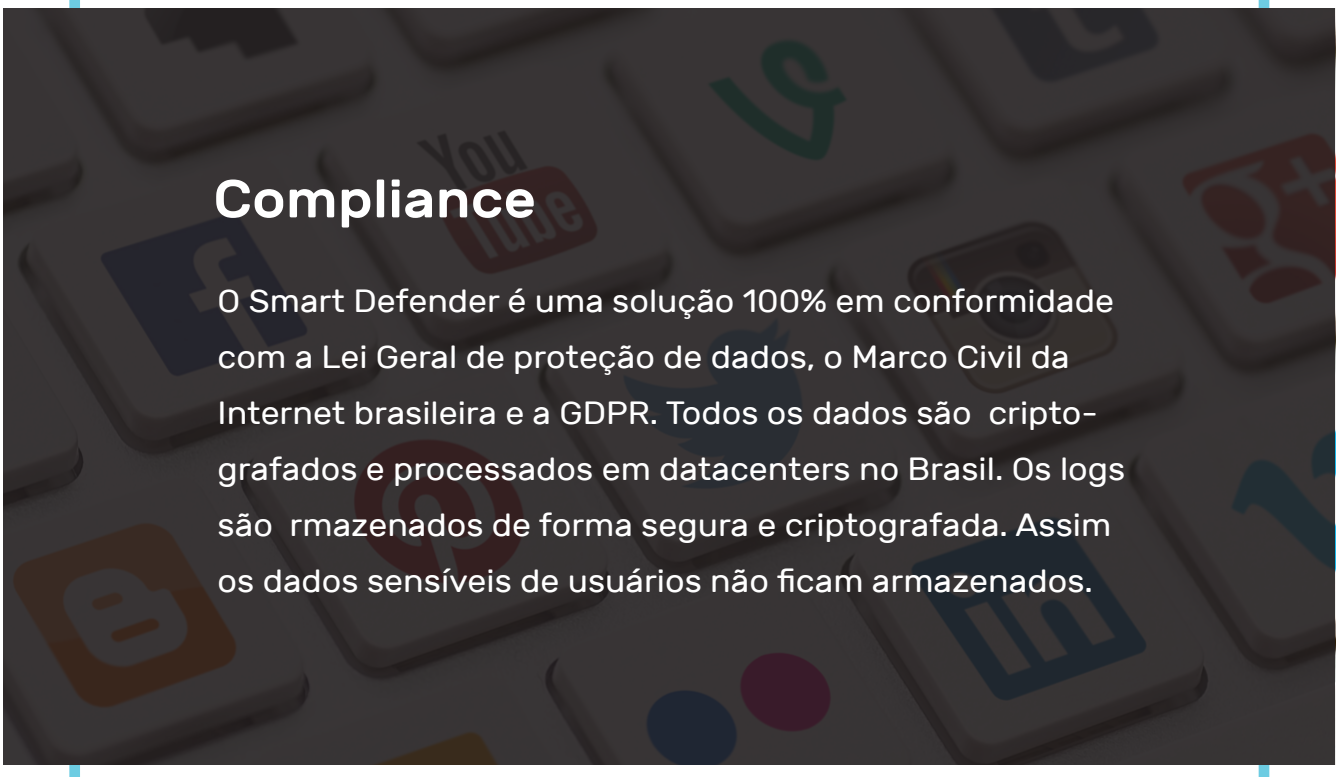
O Smart Crawler usa tecnologias de Behavior Analysis para simular a ação do usuário ao clicar em uma URL e mapear sua intenção em tempo real. Conhecida como análise On-Click, essa ação é realizada em segundos, no momento em que um usuário clica em um link recebido por e-mail.

File Reputation

Utiliza metadados gerados localmente para comparação com BigData na nuvem.

Análise de Imagens pornográficas

O Smart Defender verifica se a imagem está cadastrada em uma rede global de imagens pornográficas. Após essa verificação, é acionado o modelo de Inteligência Artificial, que através de métodos de machine learning, modelos matemáticos, redes neurais e deep learning, verifica de forma automatizada diferentes parâmetros da imagem (incluindo o contexto da mensagem), para detectar a probabilidade da imagem ser um conteúdo pornográfico.



Compliance

O Smart Defender é uma solução 100% em conformidade com a Lei Geral de proteção de dados, o Marco Civil da Internet brasileira e a GDPR. Todos os dados são cripto-grafados e processados em datacenters no Brasil. Os logs são rmazenados de forma segura e criptografada. Assim os dados sensíveis de usuários não ficam armazenados.

HSC Smart Defender em números

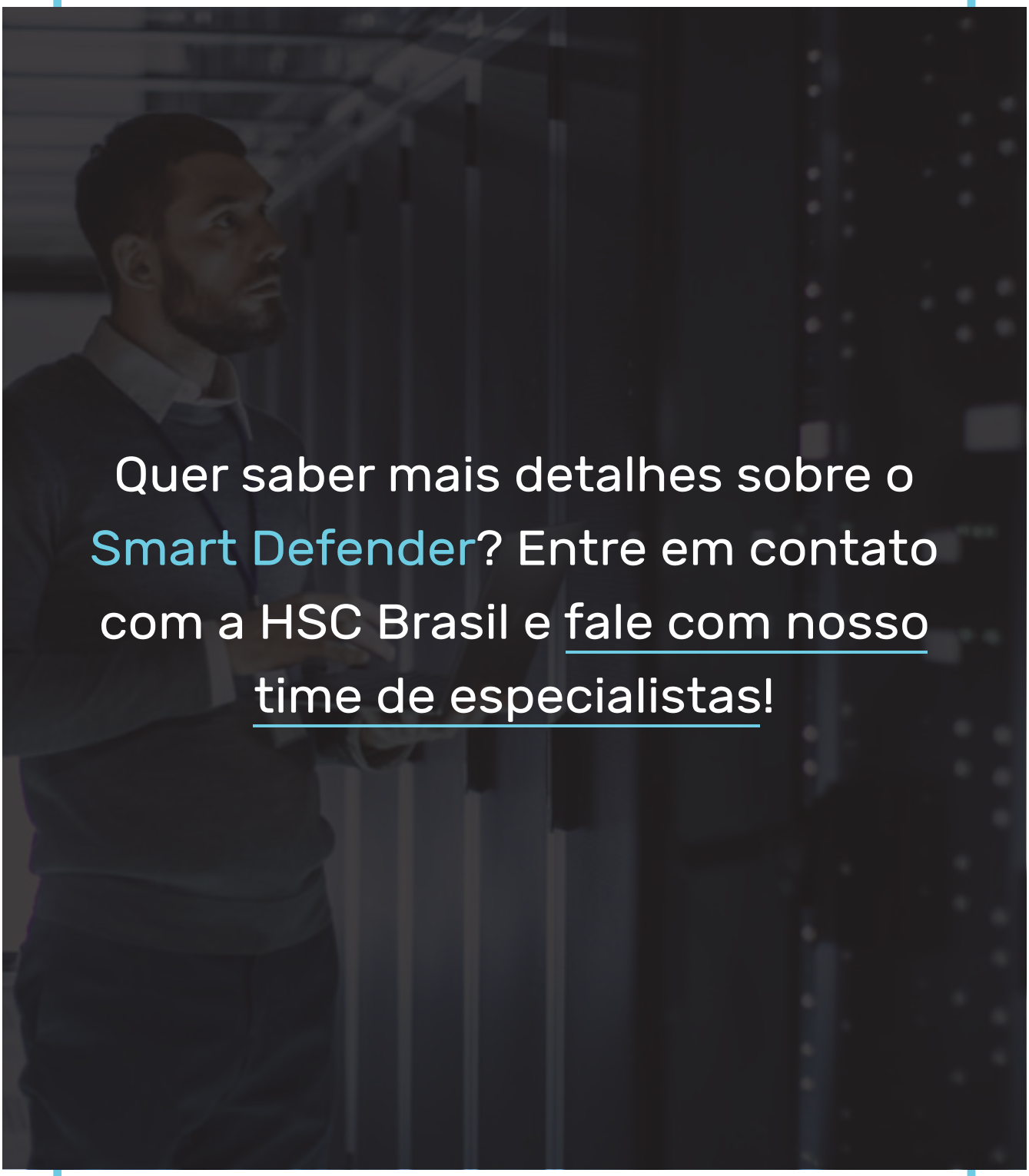
3 engines de Antivirus

Além de uma engine proprietária, o Smart Defender conta ainda com as engines de antivírus da ESET Node e da BitDefender, duas das mais difundidas empresas de antivírus do mundo. Alguns dados importantes da tecnologia:

- 10 Bilhões de IOCs processados diariamente por nossos sistemas;
- 500 milhões de emails filtrados todos os dias, através do HSC Mailinspector que está ligado ao Smart Defender;
- 15 milhões de Mailboxes protegidas por nossas soluções;
- 60 segundos é o tempo que levamos para identificar uma ameaça e atualizar base em todos os clientes conectados a nossa nuvem.

Através da Smart Defender, a HSC consegue prover ao mercado soluções que protegem organizações, usuários e dados contra os mais diversos tipos de ameaças e através de diferentes plataformas conectadas a nossa base global de inteligência contra o cibercrime.

O Smart Defender já vem integrado nas soluções HSC Mailinspector, Mailinspector Cloud e HSC Internet Secure Suite. Também possui a capacidade de conexão com outras plataformas, através de uma API da HSC, que permite integração com outras soluções de segurança e proteção. Isso aumenta ainda mais seu potencial para blindar empresas e organizações contra criminosos e hackers.


Quer saber mais detalhes sobre o Smart Defender? Entre em contato com a HSC Brasil e fale com nosso time de especialistas!


SMART
DEFENDER