Data Sheet

Symantec Endpoint Security

Implementar uma estratégia de segurança de endpoint coesa é mais importante do que nunca

Introdução

Os endpoints são o alvo principal de ataques cibernéticos. Em 2018, o número de novas ameaças para endpoint cresceu significativamente, variantes de malware para dispositivos móveis surgiram, e a frequência de ataques cresceu. Em resposta, muitas empresas tentaram aumentar as suas defesas, adicionando múltiplos produtos de proteção de endpoints. Infelizmente, essa nova abordagem deixa a postura de segurança da organização fragilizada.

O Ponemon Institute descobriu que as organizações instalam, em média, sete agentes de endpoint diferentes, para dar suporte ao gerenciamento de segurança e de TI. Cada agente opera independentemente, com seu próprio console e conjunto de regras e políticas - todos os quais precisam ser configurados, implementados e gerenciados. Além de criar mais despesas gerais e de TI, vários produtos apresentam falhas e erros de segurança, aumentando as chances de você perder uma ameaça.

A prevenção é importante, pois as ameaças cibernéticas globais estão mais agressivas do que nunca e podem ter um impacto impressionante nos negócios. No tempo em que você leva para ler este datasheet, uma empresa inteira pode ficar comprometida. O ataque NotPetya supostamente paralisou uma das maiores companhias de transporte do mundo em apenas 7 minutos, juntamente com milhares de outras organizações. É essencial evitar ataques o quanto antes, pois a janela de detecção e reação a um ataque moderno é muito curta. Investir na resposta a incidentes também é fundamental para criar uma postura de segurança reforçada para evitar futuros ataques.

Com a Symantec, você pode encerrar os compromissos. Por que escolher entre a melhor segurança e maior simplicidade quando você pode ter os dois?

Visão Geral da Solução

O Endpoint Security oferece a plataforma de segurança de endpoints mais completa e integrada do planeta. Como uma solução local, híbrida ou baseada em nuvem, a plataforma Symantec de único agente protege todos os pontos de extremidade tradicionais e móveis, fornecendo intertravamento de defesas a nível de dispositivo, aplicativo e rede, e usa inteligência artificial (IA) para otimizar decisões de segurança. Um sistema de gerenciamento unificado baseado em nuvem simplifica a proteção, detecção e resposta a todas as ameaças avançadas, direcionadas aos endpoints.

Segurança endpoint sem comparações para a sua organização

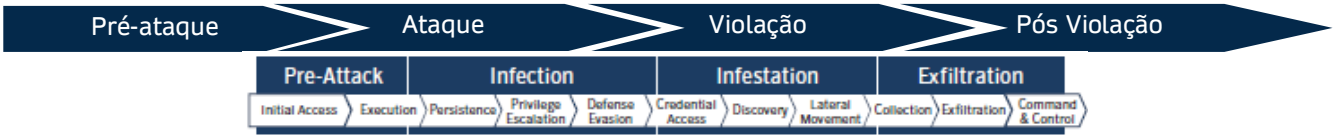
O Symantec Endpoint Security fornece à sua organização a melhor segurança de enpoints para dispositivos móveis e tradicionais, nas três fases de ataque - pré-ataque, ataque e pós-ataque - com ênfase na prevenção em toda a cadeia de ataques para contenção rápida. A redução proativa da superfície de ataque e as tecnologias inovadoras de prevenção de ataques, fornecem uma defesa mais forte contra as ameaças mais difíceis de detectar, como malware furtivo, roubo de credenciais, desaparecimento de arquivos, e ataques “living off the land”. O Symantec também previne grandes vazamentos antes que o roubo de arquivos possa ocorrer. A análise sofisticada de ataques, análise forense de comportamento, investigação automatizada de playbooks, e o primeiro movimento lateral da indústria de prevenção de ataques a roubo de dados, provém detecções precisas e busca proativa para conter o atacante e remediar ameaças persistentes em tempo real.

Redução da superfície de ataques

A Symantec oferece defesa proativa de endpoints com recursos de redução de superfície pré-ataque, baseados em avançados controles de políticas e tecnologias que procuram continuamente vulnerabilidades e configurações incorretas entre aplicativos, AD e dispositivos. Com a redução da superfície de ataque, muitas táticas de ataque não alcançarão os seus endpoints.

- A **correção de vulnerabilidades** aprimora sua postura de segurança, fornecendo visibilidade e inteligência sobre vulnerabilidades e seus riscos associados. As vulnerabilidades descobertas são classificadas por sua gravidade com base no CVSS (Common Vulnerability

Segurança Completa do Symantec Endpoint



Redução da Superfície de Ataques

- Avaliação de violação
- Remediação de vulnerabilidades
- Controle de dispositivos
- Isolamento e controle

Prevenção de Ataques

- Prevenção de malware
- Proteção de exploit
- Prevenção baseada em comportamento
- Conexão segura: Integridade de Wi-fi e redes, e Smart VPN

Prevenção de Violações

- Fraude
- Defesa para AD
- Políticas auto-gerenciáveis
- Firewall de rede e prevenção de intrusões

Resposta & Detecção

- Análise de ataques direcionados
- Forensics de comportamento
- Investigador expert SOC
- Busca de ameaças e

Agente Único: Agente Symantec para Win, Win S Mode, macOS, Linux, Androis, iOS

Gerenciamento Flexível: Consoles de gerenciamento Cloud, Híbrido e Local

Rede de Inteligência Global: A maior rede mundial de inteligência de usuários

Defesa Cibernética Integrada: Integrações com Symantec e serviços de terceiros

Opções de Serviço:

- Execute por nós
- Nós queremos ajudar
- Nós iremos gerenciar independentemente

Scoring System), juntamente com a identificação do número de dispositivos afetados, para garantir que as ameaças mais críticas sejam corrigidas primeiro.

- A **avaliação de violação** investiga continuamente o AD para configurações incorretas de domínio, vulnerabilidades e persistência, utilizando simulações de ataques para identificar riscos, permitindo a mitigação imediata com recomendações sobre remediação.
- O **controle de dispositivos** especifica políticas de permissões em diferentes tipos de dispositivos, que conectam-se com computadores, como USB, infravermelho e FireWire, para reduzir o risco de ameaças e roubo de arquivos.
- O **isolamento e controle de aplicativos** permite que apenas aplicações confiáveis sejam executadas, além de proteger as vulnerabilidades de aplicações já conhecidas. Também isola aplicações desconhecidas para parar comportamentos maliciosos, como ações com privilégios elevados em arquivos.

Prevenção de ataques

A prevenção multicamadas da Symantec protege imediatamente e efetivamente contra ataques baseados em arquivos e métodos de ataque fileless. Suas capacidades de machine-learning e inteligência artificial utilizam esquemas avançados de detecção de dispositivos, para identificar ameaças crescentes entre tipos de dispositivos, sistemas operacionais e aplicações. Os ataques são bloqueados em tempo real, para que seja possível manter a integridade dos seus endpoints e evitar impactos negativos.

- **Prevenção de malware** combina detecção de pré-execução e bloqueio de ameaças novas e crescentes (machine-learning avançado, sandboxing para detectar malware oculto em pacotes personalizados, e monitoramento/bloqueio de comportamento suspeito em arquivos), e métodos baseados em assinaturas (análise de reputação de arquivos/sites e escaneamento de malware).
- O **Exploit Prevention** bloqueia exploits de dia-zero baseados em memória, de softwares populares.
- A **proteção intensiva** permite o ajuste granulado do nível de detecção e bloqueio separadamente, para otimizar a proteção e obter visibilidade aprimorada de arquivos suspeitos.
- A **segurança de conexão de rede** identifica redes de Wi-fi rogue e utiliza uma tecnologia de reputação de hotspot, além de entregar uma VPN baseada em política para proteger as conexões de rede e atender à conformidade.

Prevenção de Violação

A abordagem de prevenção da Symantec envolve conter atacantes o mais cedo possível - no endpoint - antes que eles tenham a oportunidade de persistir

na rede. Várias tecnologias de prevenção de fraudes e intrusões baseadas em IA trabalham juntas para impedir a persistência de rede antes, imediatamente e após o comprometimento do terminal - antes que uma violação completa possa ocorrer.

- **Firewall e Prevenção de Intrusões** bloqueia ataques conhecidos de rede e baseados em browser, utilizando regras e políticas, e previne a instalação de controles e comandos com um blacklisting automático de endereços de IP.
- O **sistema de fraudes** utiliza de iscas - arquivos falsos, credenciais, compartilhamentos de rede, entradas de cache, solicitações web e endpoints - para expor, determinar a intenção e as táticas do atacante, com o objetivo de adiar os invasores, através de visibilidade inicial.
- A **Segurança de Active Directory** defende a camada primária de ataque contra roubos de credenciais de administrador de domínio, controlando a percepção do atacante sobre os recursos do AD - do endpoint -, utilizando ofuscamento ilimitado (criação de credenciais e ativos falsos). Com ofuscação, o atacante se entrega enquanto interage com "ativos falsos", ou tenta usar credenciais de administrador de domínio que não serão válidas.
- **Políticas auto gerenciadas**, baseadas em avançados IA e ML, combinam exclusivamente indicadores de compromisso e anomalias históricas, para continuamente adaptar os limites ou regras das políticas de endpoints, e mantê-las atualizadas e em conformidade com os riscos atuais da sua organização.

Remediação e resposta pós violação

A Symantec combina tecnologias de detecção e resposta de endpoint (EDR) e a experiência de analistas de security operations center (SOC), dando a você as ferramentas necessárias para encerrar rapidamente os incidentes de endpoint e minimizar os impactos de ataques. Capacidades integradas de EDR em um único agente, que cobrem tanto endpoints tradicionais quanto modernos, detecta precisamente ataques avançados, provém análises em tempo real e tornam possível a você ativamente buscar ameaças e conduzir investigações forenses e a remediação.

- A **análise de ataques direcionados** fornece detecções precisas de testes realizados pela Symantec por 3.000 pesquisadores, com base na atividade global do bom e do mau, em todas as empresas que compõem o nosso conjunto de telemetria. Incidentes em tempo real são gerados - com uma análise detalhada do atacante, técnicas, máquinas impactadas e orientação de remediação.
- A **forense de comportamento** fornece a capacidade de registrar e analisar o comportamento do endpoint para identificar técnicas avançadas de ataques, que podem estar utilizando aplicações legítimas para fins maliciosos. Esses dados são enriquecidos com o framework MITRE ATT&CK para ajudar a orientar respondedores de incidentes durante investigações.
- As **ferramentas avançadas de detecção de ameaças** inclusas nos playbooks integrados Symantec EDR, encapsulam as melhores práticas de detecção e busca de comportamento anormal. Os respondentes de incidentes podem procurar em toda a organização por IOCs, para incluírem a consulta direta ao endpoint.
- A **resposta integrada** executa uma ação direta no endpoint para remediar - recuperar e excluir arquivos, isolando endpoints e incluindo-os em blacklist. O Symantec EDR oferece suporte a envio automático de arquivos suspeitos identificados pelo sandboxing para análise completa de malware, incluindo exposição de malware que é compatível com VM.
- O **investigador expert SOC** é uma serviço de investigação e busca forense 24x7, que emprega os analistas SOC Symantec para detectar ativamente ataques furtivos e examinar habilmente atividades suspeitas. Esses analistas usam a Symantec Endpoint Detection and Response (EDR), juntamente com análise de machine-learning e inteligência global de rede da Symantec.

Tenha controle dos dados em uso nos endpoints

Com a integração do Symantec Endpoint DLP com o Symantec Endpoint Security, você pode impedir o manuseio inadequado ou roubo de dados confidenciais em tempo real, independentemente se os endpoints estão dentro ou fora da sua rede, enquanto fornece ampla cobertura de perda de dados entre aplicativos, dispositivos e plataformas.

- **Gerenciamento 100% baseado em nuvem**: Investigue e corrija incidentes de segurança de um mesmo console de gerenciamento, utilizado pelo Symantec Endpoint Security (Gerenciador de segurança cibernética integrado), para gerenciamento simplificado e controle de política de dados.
- **Proteção de dados sensível à ameaças**: Combata o roubo de dados por aplicações malicio-

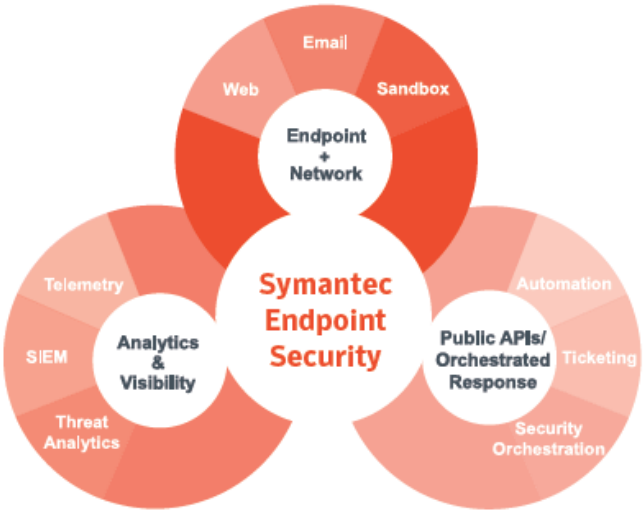
sas e com baixa reputação, com os recursos do Symantec Endpoint Security App Control de controle de aplicativos, que interrompem aplicativos e processos não confiáveis de acessar e extrair dados confidenciais.

- **Empacotamento de agente comum** e gerenciamento de dispositivos: Mantenha seguros os seus endpoints em um único controle, com um único pacote de implementação para DLP e segurança de endpoints.

Proteja facilmente o seu ambiente dinâmico de endpoint

Um único agente reduz o seu footprint de segurança, enquanto integra (e coordena) as melhores tecnologias de prevenção, detecção e resposta. Gerencie tudo de um sistema integrado, baseado em nuvem (Gerenciador de defesa cibernética integrado), minimizando o tempo, recursos e esforços para configurar, implementar, gerenciar e manter a sua postura de segurança. Tudo o que você precisa está acessível a um clique ou dois, aumentando a produtividade dos administradores e melhorando os tempos de resposta para eventos de segurança.

- O **gerenciamento de segurança guiado por IA**, é atualizado com políticas de precisão, com menos configurações incorretas, para melhorar a sua segurança.
- **Fluxos de trabalho simplificados** garantem que tudo funcione em conjunto para aumentar o desempenho, eficiência e produtividade.
- **Recomendações sensíveis ao contexto** ajudam a obter desempenho, eliminando tarefas rotineiras e melhorando a tomada de decisões.
- O **gerenciamento de segurança autônomo** aprende continuamente dos comportamentos do administrador e do usuário, para melhorar as avaliações de ameaças, ajustar as respostas e fortalecer sua capacidade geral de segurança.



Reduza a complexidade com o amplo portifólio da Symantec e integrações de terceiros

O Symantec Endpoint Security é uma solução fundamental que facilita a integração para que as equipes de segurança de TI possam detectar ameaças em qualquer lugar da rede e trate essas ameaças com uma resposta orquestrada. O Symantec Endpoint Security trabalha em conjunto com outras soluções da Symantec e com produtos de terceiros, por meio de aplicativos dedicados e APIs, para fortalecer sua postura de segurança. Nenhum outro fornecedor oferece uma solução que orquestra uma resposta no endpoint (blacklist e remediação) desencadeadas pela detecção de uma ameaça nos gateways de segurança da web e de e-mail. Integrações específicas incluem:

- **Symantec Web Security Service**: Redireciona o tráfego da web de usuários do Symantec Endpoint Security em roaming para o Symantec Web Security Service e Symantec SACB, usando um arquivo PAC.
- **Symantec Web Gateway**: APIs REST programáveis possibilitam a integração de segurança com infraestruturas de rede local.
- **Symantec Validation e ID Protection**: autenticação multifator, incluindo cartões inteligentes PIV/CAC para os consoles de gerenciamento local e em nuvem do Symantec Endpoint Security.
- **Symantec Content Analysis**: utiliza dinâmica de sandboxing local e mecanismos adicionais para uma melhor análise de ameaças e arquivos suspeitos, enviados pelo Symantec Endpoint Security.

Opções de Licenciamento			Symantec End-point Security Enterprise	Symantec End-point Security Complete
	Gerenciamento	SaaS/Nuvem pura	O	O
		Gerenciamento local	O	O
		Híbrido	O	O
	Sistemas Operacionais	Workstation (Windows/Mac)	O	O
		Mobile (iOS/Android)	O	O
		Servidores (Windows/Linux)		O
	Prevenção de Ataques	Prevenção de malware	O	O
		Prevenção de exploit	O	O
		Proteção intensiva	O	O
		Segurança de conexão de rede **	O	O
	Redução de Superfície de Ataque	Avaliação de violação		O
		Remediação de vulnerabilidades *		Add-On
		Controle e isolamento de aplicações *		O
		Controle de dispositivos	O	O
	Prevenção de Violação	Prevenção de intrusão	O	O
		Firewall	O	O
		Fraude *	O	O
		Segurança de Active Directory ***		O
		Políticas auto gerenciáveis		O
	Resposta e Remediação ***	Análise de ataques direcionados		O
		Forensics de comportamento		O
		Busca de ameaças & rápida resposta		O
	Busca de Ameaças	Centro de busca de ameaças		Add-On
	Serviços Gerenciados	Serviço de busca de ameaças		Add-On

Para mais informações, visite: www.r2sis.com.br

* Suportado em workstations Windows apenas

** Suportado apenas no Win 10, Win 10 em modo S, iOS e dispositivos Androis

*** Apenas gerenciamento local

Symantec

R2SIS TECNOLOGIA