Data Sheet

Symantec Endpoint Protection Cloud

Proteger usuários e seus dispositivos é crítico para organizações de todos os tamanhos. Para negócios com profissionais de TI limitados, a tarefa de proteger endpoints e controlar todos os dispositivos de seus usuários (desktops, laptops, tablets e smartphones) pode ser assustadora. A necessidade de lidar com ameaças avançadas com recursos limitados requer uma solução que simplifique a proteção de endpoints e o gerenciamento de dispositivos.

Proteção Avançada de Endpoints Facilitada

Symantec Endpoint Protection Cloud (SEP Cloud) é um serviço de segurança fácil de utilizar, que protege e gerencia PCs, Macs, dispositivos móveis e servidores em um único console, tornando-se a solução ideal para organizações com recursos de segurança de TI limitados. SEP Cloud efetivamente protege de ransomwares, ameaças de dia-zero e outros ataques sofisticados, utilizando tecnologias multicamadas avançadas, incluindo machine learning e análise de comportamento. Utilizando as configurações padrão de segurança do SEP Cloud e as capacidades de implementação facilitadas, essa solução protege rapidamente seus endpoints.

Proteção inteligente para Ameaças Emergentes

Uma combinação poderosa de tecnologias de detecção impede ameaças avançadas e malwares com rápidas mutações, não importa como eles ataquem o seu endpoint - tudo em um agente leve e de alta performance.

- **Machine Learning avançado** bloqueia ameaças novas e emergentes, utilizando trilhões de amostras de arquivos bons e ruins da Rede de Inteligência Global Symantec para melhorar os resultados de machine-learning.
- **Monitoramento de comportamento** determina o risco do arquivo, monitorando aproximadamente 1.400 arquivos, enquanto eles estão em execução, para bloquear arquivos maliciosos.
- **A mitigação de exploração de memória** neutraliza malwares de dia-zero em softwares populares que não tenham sido atualizados pelo fabricante, utilizando uma tecnologia sem assinatura, que funciona não importa a falha, bug ou vulnerabilidade.
- **A tecnologia de emulação de alta velocidade** detecta malware escondido por pacotes polimórficos customizados. Um scanner estático de dados roda em cada arquivo em milissegundos, em uma máquina virtual leve, para forçar as ameaças a se revelarem, melhorando as taxas de detecção e a performance.
- **A tecnologia de firewall de rede e prevenção de intrusões** analisa os tráfegos de entrada e saída e bloqueia ameaças enquanto elas trafegam pela rede, antes de chegarem aos endpoints. O firewall baseado em regras e a proteção de navegadores protegem contra ataques baseados em web. Com uma proteção de rede forte, você pode detectar a maioria das ameaças antes delas alcançarem os endpoints.
- **Análise de reputação de arquivo** identifica se um arquivo é bom ou ruim e determina uma pontuação de reputação através da inspeção de atributos chave, como a frequência de download, data de download, e localização do download - tudo antes do arquivo alcançar o endpoint.

Impeça ataques direcionados e ameaças de Dia-Zero com uma proteção em camadas

PESQUISA EM TEMPO REAL PATENTEADA PARA TODOS OS ARQUIVOS ESCANEADOS							
Machine-learning avançado	**Monitoramento de comportamento**	**Mitigação de exploração de memória**	**Emulador**	**Firewall e prevenção de intrusão**	**Reputação de arquivo**	**Antivírus**	**Controle de dispositivos**
Detecção de pré-execução de ameaças novas e emergentes	Monitora e bloqueia arquivos que exibam comportamentos suspeitos	Bloqueia explorações de dia-zero contra vulnerabilidades em softwares populares	Máquina virtual detecta malware escondido, utilizando pacotes customizados	Bloqueia malware antes que se espalhe para seu computador e controla o tráfego	Determina a segurança dos arquivos e websites utilizando o conhecimento da comunidade	Scaneia e elimina malware que chega ao sistema	Bloqueia infecções de dispositivos USB, prevenindo roubo de dados

- A **proteção de antivírus** utiliza assinaturas e heurística avançada de arquivos para analisar e eliminar malware em endpoints, incluindo vírus, worms, Trojans, spyware, bots, adware e rootkits. A pesquisa baseada em nuvem durante escaneamentos provém informações atualizadas e protege contra surtos de malwares novos e emergentes.

Segurança e gerenciamento de dispositivos móveis

A defesa abrangente contra ameaças está integrada no SEP Cloud para dispositivos iOS e Android, para entregar proteção superior contra uma gama extensa de ameaças existentes e desconhecidas. O SEP Cloud utiliza uma abordagem em camadas para proteger proativamente dispositivos móveis contra malware, ameaças de rede, e vulnerabilidades de app/SO.

- **Defesa contra malware** provém uma defesa proativa contra aplicativos maliciosos de dia-zero baseados em assinaturas, análise dinâmica/estática, comportamento, estrutura, permissões, fonte e resposta em tempo real.
- **Defesa de rede** entrega um escudo eficiente contra redes Wi-fi maliciosas, e bloqueia ataques man-in-the-middle, SSL downgrading, e ataques de manipulação de conteúdo, com uma tecnologia patenteada de honeypot.
- **Defesa de vulnerabilidades** monitora dispositivos em vulnerabilidades conhecidas de atualizações, e revela vulnerabilidades de dia-zero em apps e sistemas operacionais.
- **Proteção de senhas** previne acesso não autorizado a dispositivos, forçando os requerimentos de senha e controles de dispositivos, como o controle de câmera poder limitar o acesso ou desativar a utilização.
- Capacidades de **bloqueio e limpeza de dispositivos** protege os dados da organização em dispositivos móveis, em casos em que o dispositivo é perdido ou roubado, remotamente bloqueando o acesso ou limpando os dados contidos nos dispositivos.
- **Políticas de e-mail e Wi-fi** controlam o acesso a redes internas baseado na propriedade dos dispositivo (da empresa ou pessoal) e no status de segurança do dispositivo.

Configuração e gerenciamento baseados em nuvem, fácil de usar

O gerenciamento altamente intuitivo do SEP Cloud permite a você garantir a segurança e gerenciar uma grande variedade de dispositivos na nuvem, incluindo: PCs, laptops, smartphones, tablets e servidores com suporte aos SOs (mascOS, Windows, iOS e Android). A configuração inicial leva 5 minutos, utilizando as políticas de configuração padrão.

Pronto para proteger os usuários em menos de 5 minutos

Configuração de Políticas Intuitiva	Dashboard de Ação Rápida	Sempre Atualizado
Crie políticas baseadas em usuários ou grupos, que são aplicadas facilmente a todos os dispositivos.	Encontre e remedeie dispositivos infectados em 3 cliques e traga dispositivos à conformidade facilmente, baseado em status e distribuição.	Fique à frente de ameaças com um serviço de segurança que é automaticamente atualizado sempre.
Arquitetura baseada em nuvem, sempre disponível		
Gerenciamento baseado em nuvem, portal de usuário, dashboard em tempo real e proteção avançada para endpoints		
		

- Um **dashboard intuitivo** que provém uma visualização rápida de todos os dispositivos da sua organização, seus status e distribuição, com a habilidade de gerar relatórios e tomar ações rapidamente para remediar dispositivos, mantendo-os seguros e em conformidade.
- A **configuração de políticas com um clique** possibilita a criação de políticas cross-platform que protegem usuários em qualquer dispositivo. A política é criada apenas uma vez, e a configuração da política é aplicada em qualquer dispositivo ou sistema operacional, simplificando o gerenciamento e implementação de políticas.
- **Implementação self-service** permite que os usuários incluam seus dispositivos corporativos e pessoais em minutos, utilizando um portal online.
- **Atualização automatizada de agentes**, entregues pelo serviço do SEP Cloud, garantem que as informações mais recentes estão sendo transferidas para os dispositivos e que estes estão sempre atualizados.
- **A Descoberta de dispositivos** garante que todos os seus dispositivos estão protegidos, continuamente escaneando sua rede para dispositivos desprotegidos, e integrando automaticamente esses dispositivos com um único clique.
- **Agente de implementação** automatizada com pacotes de instalação para Windows e macOS, que podem ser forçados, utilizando ferramentas de distribuição populares.
- **Integração com Provedores de Identidade** como Azure AD, Okta, Oracle IDCS e VIP Access Manager torna simples sincronizar usuários com o SEP

Cloud. Para organizações sem Azure AD, é possível integrar usuários em massa a partir de um arquivo em Excel ou .CSV.

- **REST APIs** tornam possível a desenvolvedores integrarem o SEP Cloud com outras tecnologias de segurança, relatórios, informação e eventos.
- **Ferramentas de gerenciamento de parceiros** provém aos revendedores e provedores de serviços de gerenciamento, uma visualização agregada do SEP Cloud de seus clientes, para monitoramento e gerenciamento de serviços em sua custódia. A Symantec provém um console de gerenciamento baseado em nuvem para parceiros (PMC), e integração com ferramentas populares de gerenciamento e monitoramento, incluindo ConnectWise.

Opções de Assinatura Flexíveis para Suprir as Necessidades do seu Negócio

O SEP Cloud oferece opções de assinatura flexíveis por usuário ou por dispositivo, com termos mensais ou anuais. Com uma assinatura por usuário, você pode obter suporte a múltiplos dispositivos (PC, Mac ou dispositivos móveis), com uma base por usuário, sem taxa mínima, e evitando despesas surpresa. Uma assinatura por dispositivo garante a proteção para um único PC, Mac ou dispositivo móvel, que é utilizado por vários usuários. Com o SEP Cloud, o serviço de proteção do seu endpoint está sempre atualizado, com as ferramentas mais atuais habilitadas, e inclui suporte técnico 24x7. A tabela de comparação abaixo detalha as ferramentas inclusas em cada opção de assinatura:

SYMANTEC ENDPOINT PROTECTION CLOUD			
Opções de assinatura	Por usuário (até 5 dispositivos)	Por dispositivo	Por servidor
Ferramentas			
Windows e macOS	O	O	Windows Server
Firewall & Prevenção de Intrusão	O	O	
Bloqueia Ameaças de Dia-Zero Contidas na Memória	O	O	O
Escaneamento Antivírus	O	O	O
Detecção em Máquina Virtual de Ameaças Ocultas em Arquivos e Executáveis	O	O	O
Detecção de Pré-Execução de Ameaças utilizando Machine Learning	O	O	O
iOS e Android			
Defesa Contra Malware	O	O	
Defesa de Rede	O	O	
Defesas de Vulnerabilidades de Apps/SO	O	O	
Gerenciamento de Dispositivos Móveis	O	O	
Add-Ons			
Gerenciamento de Encriptação de Dispositivo	O		

A Symantec é consistentemente nomeada líder em proteção de endpoints

- Líder Gartner Magic Quadrant pelos últimos 16 anos
- Prêmio de melhor proteção de endpoints, AV-TEST, 2017
- Vendedor de Segurança de Endpoint do Ano, Frost & Sullivan, 2017
- Líder de Segurança Contra Ameaças em Dispositivos Móveis do Mercado, IDC MarketScape, 2017

Para mais informações a respeito do **Symantec Endpoint Protection Cloud**, visite: www.r2sis.com.br

Symantec

R2SIS TECNOLOGIA