

# SentinelOne EPP

## Ficha Técnica

► **Proteção Autônoma de Endpoint Que Economiza Tempo**

O SentinelOne Endpoint Protection Platform (EPP) unifica prevenção, detecção e resposta em um único agente empoderado por machine learning e automação. Fornecendo prevenção e detecção de ataques vindos dos maiores vetores, rápida eliminação de ameaças com capacidade de resposta totalmente automatizada acionada por políticas e uma completa visibilidade em contexto amplo do ambiente do endpoint e análises forenses em tempo real.

A suíte de próxima geração do futuro – iniciada no endpoint e orquestrada por IA



EPP	EDR	Gestão	Serviços	Intel. de Cloud
<ul style="list-style-type: none"><li>IA Estática</li><li>IA Comportamental</li><li>Anti-Exploitation</li><li>Movimentação Lateral</li><li>Prevenção de roubo de credenciais</li></ul>	<ul style="list-style-type: none"><li>Caça de Ameaças</li><li>Pesquisa IOC</li><li>Remediação</li><li>Visibilidade de tráfego Criptografado</li><li>Confinamento e Rollback</li></ul>	<ul style="list-style-type: none"><li>Controle de Dispositivos</li><li>API e SDK</li><li>Inventário de Aplicações</li><li>Monitoramento de Integridade de Arquivos</li><li>Gestão de Patches e Vulnerabilidades</li></ul>	<ul style="list-style-type: none"><li>Vigilância MDR</li></ul>	<ul style="list-style-type: none"><li>Alimentação de ameaças</li><li>Reputação de IPs</li><li>Análises Automatizadas</li><li>Inteligência Compartilhada</li></ul>

**SentinelOne**

### CLIENTES ENDPOINT USUÁRIOS

Windows XP, 7, 8, 8.1, 10  
Mac OSX 10.9.x, 10.10.x, 10.11x, macOS 10.12x  
macOS 10.13 (High Sierra)  
CentOS 6.5, 7.0, 7.2  
Red Hat Enterprise Linux 6.5, 7.0, 7.2  
Ubuntu 12.04, 14.04, 16.04, 16.10  
openSUSE 42.2

### SERVER ENDPOINT CLIENTS

Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016  
CentOS 6.5, 7.0, 7.2  
Red Hat Enterprise Linux 6.5, 7.0, 7.2  
Ubuntu 12.04, 14.04, 16.04, 16.10  
SUSE Linux Enterprise Server 12SP1  
Oracle Linux 6.5 - 6.9, 7.0+  
Amazon Linux (AMI) 2016.09+, 2017.03+

### AMBIENTES VIRTUAIS

Citrix XenApp, XenDesktop  
Microsoft Hyper-V  
Oracle VirtualBox  
VMware vSphere  
VMware Workstation  
VMware Fusion  
VMware Horizon



## SentinelOne EPP Ficha Técnica

### ► Proteção

- Prevenção autônoma multi-camadas que cobrem todos os vetores de ataque, mesmo off-line
- Tecnologia machine learning que não depende de assinaturas e não requerem atualizações diárias / semanais ou scans recorrentes
- Mitigação de atividade maliciosa em contexto amplo, reduzindo tempo e custo de reparo de dispositivos infectados
- Fornecendo análises forenses. Bloquear não é o bastante. Clientes querem saber de onde as ameaças vieram e o que elas tentaram fazer.

### ► Visibilidade

- Visibilidade dos endpoints entre diferentes plataformas – nós vamos além dos limites do EPP e EDR com funcionalidades de valor agregado como dados de IT Hygiene.
- Visibilidade de tráfego criptografado – porque todos os usuários estão expostos a phishing e 70% do tráfego da web é criptografado
- Visibilidade de todas as aplicações e processos em execução

### ► Simplicidade

- Um agente único e leve fornece as seguintes funcionalidades:
  - EPP
  - EDR
  - HIPS
  - Monitoramento de integridade de arquivos
  - Gerenciamento de riscos e vulnerabilidades
- Console de gerenciamento hospedado em cloud, on premise ou de modo híbrido
- Alta eficácia, baixo impacto de performance e excelente experiência para o usuário final

### ► Automação

- A plataforma SentinelOne é construída no conceito de API-first e possui integrações com SonicWall, Fortnet, Splunk, Qradar, LogRhythm, Demisto, Phantom e inclusive com Alexa apenas para citar algumas!
- Automaticamente isola os dispositivos infectados e imuniza os demais
- Recupera arquivos mesmo em casos como ransomware. Com 44% das empresas enfrentando infecções de ransomware nos últimos 12 meses, recuperar e retornar ao estado anterior torne-se uma funcionalidade indispensável

#### Perfil do avaliador

##### Gerente de redes

Indústria Educação

Cargo Infraestrutura e Operações

Porte da empresa

Última Atualização 29 de outubro de 2017

<http://bit.ly/s1-edu111>



*Não desperdice seu tempo com outros fornecedores. Depois de 20 anos implementando e usando endpoint software, SentinelOne lidera o grupo*

