The SentinelOne Endpoint Protection Platform (EPP) unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

**Autonomous Endpoint Protection That Saves You Time**

The next-gen suite of the future - born from the endpoint and orchestrated by AI

<table>
<thead>
<tr>
<th>EPP</th>
<th>EDR</th>
<th>Manageability</th>
<th>Services</th>
<th>Cloud Intel.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static AI</td>
<td>Threat Hunting</td>
<td>Device Control</td>
<td>Vigilance MDR</td>
<td>Threat Feeds</td>
</tr>
<tr>
<td>Behavior AI</td>
<td>IOC Search</td>
<td>API and SDK</td>
<td></td>
<td>IP Reputation</td>
</tr>
<tr>
<td>Anti-Exploitation</td>
<td>Remediation</td>
<td>Application Inventory</td>
<td></td>
<td>Automated Analysis</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>Encrypted Traffic Visibility</td>
<td>File Integrity Monitoring</td>
<td>Shared Intelligence</td>
<td></td>
</tr>
<tr>
<td>Credential Theft Prevention</td>
<td>Containment and Rollback</td>
<td>Vulnerability &amp; Patch Management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**USER ENDPOINT CLIENTS**

- Windows XP, 7, 8, 8.1, 10
- Mac OS X 10.9.x, 10.10.x, 10.11.x, 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**

- 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+

**VIRTUAL ENVIRONMENTS**

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

- Autonomous multi-layered prevention that covers all attack vectors, even when offline
- Machine learning technology that does not rely on signatures and does not require daily/weekly updates or recurring scans
- Mitigation of the full context of malicious activity, reducing time and cost of fixing up infected devices
- Providing the right forensics. Blocking is not enough. Customers want to know where threats come from and what they tried to do

Visibility

- Cross-platform visibility into endpoints - we go beyond the limits of EPP and EDR with value added capabilities such as IT hygiene data
- Visibility into encrypted traffic - because all users are exposed to phishing and 70% of web traffic is encrypted
- Visibility on all applications and running processes

Simplicity

- One lightweight agent provides the following functionality -
  - EPP
  - EDR
  - HIPS
  - File Integrity Monitoring
  - Vulnerability/Risk Management
- Managed console hosted in the cloud, on-premise, or in a hybrid model
- Higher efficacy, lower system impact, and an optimal end-user experience

Automation

- The SentinelOne platform is built with an API-first approach and has integrations with SonicWall, Fortinet, Splunk, QRadar, LogRhythm, Demisto, Phantom, and even Alexa to name a few!
- Automatically isolate infected devices and immunize the remaining of the endpoint estate
- Recover files in the highly unlikely case of ransomware. With 44% of businesses facing ransomware infections in the last 12 month, recovery and rollback is a convenient capability

BEFORE

| Static AI | Prevent attacks | Pre-execution |

DURING

| Behavioral AI | Constantly monitor and map each running process for incongruous behaviors |

AFTER

| Automated EDR | Automate remediation and response...even rollback |

Reviewer Profile

Network Manager
Industry Education
Role Infrastructure and Operations
Firm Size Gov't/PS/ED 5,000 - 50,000 Employees
Last Update October 29, 2017

Don't waste your time with other vendors. Coming from 20 years of deploying and using endpoint software, SentinelOne leads the pack