



Maximum Server Protection, Maximum Performance.

SentinelOne Next-Generation Server Protection

BENEFITS

- Provides complete protection against advanced malware, exploit and stealthy insider-based threats
- Protects against dangerous vulnerabilities; buys valuable time to implement new patches while maintaining compliance
- Preserves valuable compute resources through lightweight out-of-band monitoring
- Automatically mitigates threats, stopping attacks in real time
- Provides complete visibility into server activity
- Deployable across large-scale physical, virtual and cloud-based compute environments

SentinelOne extends its leadership in next-generation endpoint protection with an entirely new platform built from the ground up to protect the most critical servers.

Today's mission critical servers require complete protection against advanced malware and exploit-based attacks. More traditional technologies such as antivirus or host-based IPS can only protect against known threats – and even then protection comes at a significant cost to server performance. The SentinelOne Critical Server Protection Platform (CSPP) offers the broadest level of support for both known and unknown threats, and does so while preserving valuable compute resources.

Microsoft Partner
Virus Information Alliance



SentinelOne is a certified replacement for AV-based solutions.

SentinelOne Critical Server Protection Platform – How it Works

COMPLETE PROTECTION AGAINST KNOWN AND UNKNOWN THREATS

Continuous System-Level Monitoring

Deployed on each Windows or Linux-based server (physical, virtual or cloud), the SentinelOne Critical Server Protection Platform consists of a lightweight agent that monitors all system-level activity for suspicious processes used by malware and exploit-based attacks. The unique out-of-band architecture ensures that SentinelOne never degrades performance while providing superior detection.

Behavioral-Based Detection of Advanced Malware and Exploits

The Dynamic Behavior Tracking (DBT) Engine that sits at the core of the SentinelOne Critical Server Protection Platform utilizes sophisticated algorithms to map suspicious processes into malicious patterns, which is compared against a full context view of normal server and application behavior.

MITIGATE ATTACKS IN REAL-TIME

Zero-Touch Mitigation

Automatically mitigates attacks according to user-customizable policies, allowing for a decisive response that instantly kills and quarantines all malicious processes and files.

Robust Containment of “Patient Zero”

Upon detection of an attack, the SentinelOne Critical Server Protection Platform immediately removes an infected server from the network, eliminating any potential for lateral spread.

Auto-Immunization shares critical

insights of the attack across your compute network to prevent any further infection by the newly identified threat.

Real-Time Forensic Analysis with Attack

Storyline Visualization

A complete 360-degree view of an attack, along with a detailed storyline view of the steps taken, ensures incident response teams have the information they need to quickly remediate against any attempts.

COMPLIANCE AND SCALABLE PROTECTION FOR PHYSICAL, VIRTUAL & CLOUD-BASED DATA CENTERS

Certified Antivirus Replacement

The SentinelOne Critical Server Protection Platform is a certified replacement for antivirus, and is PCI and HIPAA certified.

Simple Management and Seamless Scalability

Robust, single-pane-of-glass management featuring policy structures that easily apply across complex enterprise-scale data center environments.

Specifications and System Requirements

CLIENTS

Operating Systems: Windows Server 2008 R2, 2012 R2
Red Hat Linux, CentOS 6.5 or higher
Ubuntu 12.04 and 14.04 LTS

Virtual Environments: vSphere
Microsoft Hyper-V
Citrix XenServer
Xen Desktop
Xen App

Hardware: 1 GHz Dual-core CPU or better
1 GB RAM or higher if required
by OS (recommended 2 GB)
2 GB free disk space

MANAGEMENT SERVER (ON-PREMISE)

Operating System: Linux Ubuntu 12.04 and 14.04 LTS Server
Red Hat Linux

Hardware: 4-core Intel Xeon E5-2680v2,
2.8 GHz or better
8 GB RAM
500 GB free disk space



Secure ERP, Inc.

Not Just ERP Software,
Real Business Problems Solved!™

For more information about SentinelOne Endpoint Protection and the future of endpoint protection, please contact Secure ERP at info@secureerpinc.com or (317) 290-8702.

© 2016 SentinelOne, Inc. All rights reserved.