Symantec™ Endpoint Protection on Oracle Cloud Infrastructure as a Service

Overview

Moving to the Oracle Cloud promotes business agility and reduces IT costs. But what about security? Symantec Endpoint Protection protects Oracle Cloud instances on Oracle Compute and Bare Metal Cloud platforms in several ways. It offers antivirus capabilities and detects and blocks unknown malware with reputation-based analysis and real-time behavioral monitoring that applies machine learning heuristics. It also provides policy lockdown features, such as application control, for your Oracle Infrastructure as a Service instances. Drawing on the world's largest civilian threat intelligence network, Symantec Endpoint Protection effectively protects against targeted attacks and advanced threats, and facilitates more accurate detection without slowing down Oracle Cloud platform performance.

Unrivaled, Complete Security

Keep your Oracle Infrastructure as a Service instances free from malware and viruses: Symantec Endpoint Protection stops targeted attacks and advanced persistent threats with intelligent security and layered protection.

Symantec Endpoint Protection:

- Sees and protects against the latest security threats by analyzing telemetry pulled from our Global Intelligence Network: 175 million endpoints and 98 million attack sensors in 175 countries.
- Analyzes incoming and outgoing traffic and blocks threats while they travel through the network—before hitting endpoints. Stops web-based attacks with rules-based firewall and browser protection.
- Controls file and registry access, and how processes are allowed to run. Restricts access to select hardware and controls what types of devices can upload or download information.
- Neutralizes zero-day exploits that have not been patched by the vendor. This signature-less technology works regardless of the flaw, bug, or vulnerability.

- Correlates tens of billions of linkages between users, files, and websites to preempt more threats and defend against rapidly mutating malware. Analyzes key attributes to accurately identify good and bad, and assign a reputation score before the file arrives at the endpoint.
- Eradicates malware—viruses, worms, Trojans, spyware, bots, adware, rootkits—using signature-based antivirus and file heuristics capabilities.
- Uses advanced machine learning to stop new and unknown threats, reducing our dependence on signatures.
- Monitors application behavior in real time to determine file risk and stop targeted attacks zero-day threats, and rapidly mutating malware, regardless of how they attack your endpoint.
- Uses a high-speed emulator to detect malware hidden using polymorphic custom packers; runs each file in milliseconds in a lightweight virtual machine, causing threats to reveal themselves.

Blazing Performance

Get performance so fast your users won't know it is there: Symantec Endpoint Protection safeguards your Oracle

Infrastructure as a Service instances while ensuring they execute and scale quickly.

Symantec Endpoint Protection:

- Downloads only the newest threat information, reducing signature definition file sized by up to 70 percent, which in turn reduces bandwidth usage; rapid scan techniques include pipelining, trust propagation, and batched queries.
- Minimizes disruption due to false positives.
- Reduces the number of managed agents on endpoints because the single lightweight agent combines. technologies and capabilities—machine learning, exploit mitigation, endpoint detection and response, and antimalware— normally only obtained through multiple agents. Also reduces the burden on IT and lowers total cost of ownership.
- Ensures only at-risk files are scanned, effectively eliminating significant scan overhead.

Easy Integration for an Orchestrated Response

Easily control your Oracle Cloud instances on Oracle Compute and Bare Metal Cloud: Symantec Endpoint Protection enhances management with granular policy control and a single console and agent for physical and virtual platforms.

Symantec Endpoint Protection includes:

- Power Eraser: Uses aggressive scanning technology to eliminate persistent threats and tenacious malware that traditional antivirus tools don't always detect. Can be triggered remotely.
- Host Integrity: Ensures endpoints are protected and compliant by enforcing policies, detecting unauthorized changes, and conducting damage assessments; can isolate a managed system that does not meet your requirements. Use with threat detection to quarantine an infected endpoint, quickly stopping the spread of infection until you can remediate or re-image the endpoint.
- System Lockdown: Allows whitelisted 'good' applications to run, and blocks blacklisted 'bad' applications (known to be bad) from running.
- Secure Web Gateway Integration: Uses new programmable REST APIs to integrate with existing security infrastructure, including Secure Web Gateway, orchestrating a response at the endpoint that quickly stops the spread of infection.
- EDR Console Integration: Integrated with Symantec Advanced Threat Protection: Endpoint (ATP:Endpoint), which quickly detects and blocks targeted attacks and advanced persistent threats by prioritizing attacks. Endpoint detection and response (EDR) is built into Symantec Endpoint Protection, making it unnecessary to deploy additional agents.

POWER ERASER	HOST INTEGRITY	SYSTEM LOCKDOWN	SECURE WEB GATEWAY INTEGRATION	EDR CONSOLE (ATP:ENDPOINT)
Aggressive remediation of hard-to-remove infections	Quarantine and detect unauthorized change, conduct damage assessment and ensure compliance	Part of Application Control—harden endpoint security with whitelisting and blacklisting	Use APIs to orchestrate a response from Secure Web Gateway	Orchestrate a response from Symantec ATP:Endpoint. EDR capabilities are built into the SEP agent

INOCULATION

Client Workstation and Server System Requirements

Windows® Operating Systems	Virtual Environments
Windows Vista (32-bit, 64 bit)	Microsoft Azure
Windows 7 (32-bit, 64-bit, RTM and SP1)	Amazon WorkSpaces
Windows 7 Embedded Support	VMware WS 5.0, GSX 3.2, ESX 2.5 or later
Windows 8 (32-bit, 64-bit)	VMware ESXi 4.1 – 5.5
Windows 8 Embedded (32-bit)	VMware ESX 6.0
Windows 8.1	Microsoft Virtual Server 2005
Windows 10	Microsoft Enterprise Desktop Virtualization (MED-V)
Windows Server 2008 (32-bit, 64-bit, including R2)	Microsoft Windows Server 2008, 2012, and 2012 R2 Hyper-V
Windows Essentials Business Server 2008 (64-bit)	Citrix XenServer 5.6 or later
Windows Small Business Server 2011 (64-bit)	Oracle Cloud
Windows Server 2012 (64-bit, including R2)	Virtual Box by Oracle
Windows 2016	**Linux Operating System (32-bit and 64-bit versions)**
Windows Hardware Requirements	RedHat Enterprise Linux
1GHz CPU or higher	SuSE Linux Enterprise (server/desktop)
512 MB of RAM (1 GB recommended)	Oracle Linux (OEL)
1.5 GB of free space on the hard disk	CentOS
Macintosh® Operating Systems	Ubuntu
Mac OS X 10.9, 10.10, 10.11, 10.12	Debian
Mac Hardware Requirements	Fedora
64-bit Intel Core 2 Duo or later	**Linux Hardware Requirements**
2 GB of RAM	Intel Pentium 4 (2 GHz CPU or higher)
500 MB of free space on the hard disk	1 GB of RAM
	7 GB of free space on the hard disk

Manager System Requirements

Windows® Operating Systems	Hardware
Windows Server 2008 (64-bit, including R2)	Intel Pentium Dual-Core or equivalent minimum
Windows Server 2012 (R2)	2 GB of RAM (8 GB recommended)
Windows Server 2016	8 GB or more free space on the hard disk
Web Browser	**Database**
Microsoft Internet Explorer	Embedded database included or choose from the following:
Mozilla Firefox	SQL Server 2008 R2, SP3, SP4
Google Chrome	SQL Server 2012, RTM - SP1; SP2
Microsoft Edge	SQL Server 2014, RTM and SP1
	SQL Server 2016

More Information

Try It Now for FREE

Try the world's most complete endpoint protection by downloading a free 60-day trial today.

Read third-party reviews and find out why Gartner ranks Symantec as a leader in the Endpoint Protection Platform Magic Quadrant: https://www.symantec.com/products/performance-center

Visit Our Website

Symantec home page: www.symantec.com
Symantec Endpoint Protection: go.symantec.com/sep

Speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745-6054

Speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website: http://www.symantec.com/contact-us

✔ Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

SYMC_DS_SEP_on_Oracle_Cloud_Infrastructure_EN_v1a