Trellix

DATASHEET

Trellix Management for Optimized Virtual Environments AntiVirus

Security for your private cloud without sacrificing performance

Traditional antivirus does not play well with virtualized infrastructure. Trellix Management for Optimized Virtual Environments AntiVirus (Trellix MOVE AntiVirus) brings optimized, advanced malware protection to your virtualized desktops and servers. Implement across multiple hypervisors, or choose an agentless, tuned option for VMware NSX. Either way, you get top-rated security for instant threat detection and containment with minimal impact on virtual machine (VM) performance. Trellix MOVE AntiVirus optimizes anti-malware protection for virtualized deployments, freeing hypervisor resources while ensuring up-to-date security scans are run according to policy.

Key Advantages

- **Offloads malware scanning:** Instant protection with low impact on memory and processing
- **Prevents antivirus storms:** Options include on-access and on-demand scans
- **Enables flexible deployment:** Multiplatform (all major hypervisors, Windows VMs) or agentless (VMware, Windows, and Linux VMs)
- **Improves resource optimization:** Elastic provisioning of offline scanners with event notifications (multiplatform)
- **Blocks zero-day, unknown threats in seconds:** Local reputation intelligence combined with behavioral analytics in a sandbox (multiplatform, additional module sold separately)
- **Leverages Trellix ePolicy Orchestrator (Trellix ePO) console:** End-to-end visibility and control across physical, virtual, and cloud deployments

Optimized Scanning Control

The dynamic nature of guest desktops and virtual servers requires careful handling. Images must be malware-free when users initiate a session. This can be challenging, since users often begin work in groups, causing peak-demand "antivirus storms" that consume resources and prevent users from obtaining a session.

To eliminate scanning bottlenecks and delays, Trellix MOVE AntiVirus offloads scanning, configuration, and DAT update operations from individual guest images to an offload scan server. We build and maintain a global cache of scanned files to ensure that once a file is scanned and confirmed to be clean, subsequent VMs accessing the file won't have to wait for a scan.

Memory resource allocation for each VM decreases and can be released back to the resource pool for more effective utilization.

Trellix MOVE AntiVirus allows separate policies for on-access and on-demand scanning to enable finetuned security execution. For instance, administrators can assume some reasonable level of risk for real-time, on-access scans to avoid degrading performance and then use on-demand scanning with more rigid policies running at a later time when there's less impact.

Complete End-to-End Visibility Across All Clouds

Poor visibility makes it difficult to implement proper security policies for virtualized environments. Trellix Cloud Workload Security (Trellix CWS) spans on-premise, private, and public cloud environments—including VMware and OpenStack—to provide complete visibility into virtual data centers and populate key properties such as servers, hypervisors, and VMs into the Trellix ePO console. Once administrators gain visibility into the security status of all VMs and can monitor hypervisor-to-VM relationships in near real time, securing your virtual data center becomes a lot easier. A customizable dashboard displays security scan status, executive overviews, and historical security data on assets.

Trellix CWS Essentials and Trellix CWS Advanced extend visibility and control across Amazon Web Services (AWS) and Microsoft Azure public clouds and physical servers.

Fine-Grained Policy Management

The familiar Trellix ePO console lets you configure policies and controls for Trellix MOVE AntiVirus. You can roll up virtual data with data from your physical systems and public clouds to provide unified dashboards and reports. Administrators are able to configure a unique policy per VM, cluster, or data center through

Trellix MOVE AntiVirus Configurations

Trellix MOVE AntiVirus for Virtual Servers

- Trellix MOVE AntiVirus:

  –Multiplatform deployment

  –Agentless deployment
- Cloud Workload Security for private cloud such as VMware, XenServer, OpenStack and Hyper-V
- Cloud Workload Security for public cloud such as AWS, Azure, and Kubernetes
- Trellix ePO software

Trellix MOVE AntiVirus for Virtual Desktops

- Trellix MOVE AntiVirus:

  –Multiplatform deployment

  –Agentless deployment
- Cloud Workload Security for public and private cloud
- Trellix Host Intrusion Prevention System
- Trellix SiteAdvisor® Enterprise
- Memory Protection, and Web Application Protection
- Trellix ePO software

Trellix Cloud Workload Discovery, adapting security specifically according to the makeup of the data center.

Additional Trellix MOVE AntiVirus Features

Management and visibility:

- Instantly schedule an on-demand scan on a VM or group of VMs.
- Increase scanning precision with targeted on-demand scans.
- Automatically deploy an offload scanner on each hypervisor through integration with VMware NSX Service Composer.
- Stay on top of issues with dashboards, reports, and email alerts.

Simplified deployment and configuration:

- Deploy and configure an offload scanner on multiple hypervisors (agentless).
- Restore quarantined files using the Trellix ePO console (multiplatform).
- Detailed diagnostics for antivirus performance tuning.
- Seamless agentless and multiplatform policy management.

Agentless Option for VMware

Trellix MOVE AntiVirus leverages VMware NSX for better efficiency. In agentless deployments, these use the hypervisor as a high-speed connection to allow the Trellix MOVE AntiVirus security virtual machine (SVM) to scan VMs from outside the guest image. As it scans, the SVM will direct VMware NSX to cache good files and either delete, deny access to, or quarantine malicious files.

After you install and configure the SVM and VMware NSX components, along with installing the VMware NSX endpoint driver on guest VMs, every image is automatically protected without installing Trellix software on each client VM. Our vMotion-aware implementation means that your VMs can move from one host to another and be seamlessly protected by the SVM on the target host, with no impact on scans or the user experience.

Integration of Trellix products with VMware allows you to monitor SVM status within VMware vCenter and receive alerts if the SVM loses connectivity. The Trellix ePO console receives event data detailing the specific VM affected in the event a VM is infected. Deep integration with VMware NSX synchronizes policies created in the Trellix ePO console and rules assigned in VMware NSX. Tagging of vulnerable machines with no anti-malware protection or machines with malware enables immediate quarantining of VMs through the VMware NSX firewall.

Multiplatform for All Major Hypervisors

In multiplatform installations, including vSphere, Hyper-V, KVM, and XenServer, the Trellix MOVE AntiVirus agent—a lightweight endpoint component—communicates to the SVM to broker the antivirus processing on behalf of each VM. Trellix MOVE AntiVirus agent maintains a local cache and manages policies and scanning functions. You can designate and scan a gold image for use as a clean master. Prepopulating the local cache with clean images delivers the fastest VM boot-up time.

Upon file access, the Trellix MOVE AntiVirus offload scan server performs an on-access scan, providing a response back to the VM. Users are notified of issues through a pop-up alert and can then take action to either delete, deny access to, or quarantine malicious files.

As scanning demand fluctuates in multiplatform deployments, SVMs can automatically be added to or removed from the resource pool to scale your power up or down for unlimited scale and efficient resource utilization. Event notifications help administrators understand SVM usage trends to optimize resource management.

Trellix MOVE AntiVirus in multiplatform deployments can enhance global reputation intelligence from Trellix Global Threat Intelligence (Trellix GTI) with local data from Trellix Threat Intelligence Exchange, an additional module sold separately, to instantly identify and combat ever-increasing unique malware samples. Using Trellix Threat Intelligence Exchange, Trellix MOVE AntiVirus coordinates with Trellix Advanced Threat Defense to dynamically analyze the behavior of unknown applications in a sandbox and automatically immunizes all endpoints from newly detected malware. Trellix MOVE AntiVirus integration with Trellix Network Security Platform through Trellix Threat Intelligence Exchange provides a layered security approach for unified perimeter and virtual machine protection.

Unified Policy Management for Agentless and Multiplatform

Many organizations may want to take advantage of the ability of Trellix MOVE AntiVirus to support both agentless and multiplatform deployments.

Trellix MOVE AntiVirus gives security administrators the ability to define and manage consistent security policies using one extension point in the Trellix ePO console so that management of these different methods is seamless and easy.

Architecture	Multiplatform Deployment	Agentless Deployment
Hypervisor/platform support	All major hypervisors, including VMware, Citrix, Hyper-V, and KVM	VMware
Scanning platform	Windows 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 8.1, Windows 10, Windows 11	Linux Ubuntu 18.04
Deployment scalability	One SVM can protect VMs from multiple hypervisors. SVMs can be elastically provisioned.	One SVM per ESXi host
Communication to VMs	Over the network	Over the hypervisor
Virtual machine protection	Windows	Windows and Linux