Case Study

Global Retailer Secures Virtual Business Infrastructure with McAfee MOVE AntiVirus

Large Retail Chain

Customer profile
Global membership-style warehouse retailer.

Industry
Retail.

IT environment
More than 25,000 virtual clients, 5,000 virtual servers, and 50 VMware Host in three vCenters.

Challenges
Protect virtualized enterprise without hampering business.

McAfee solution
- McAfee Management for Optimized Virtual Environments AntiVirus
- McAfee Host Intrusion Prevention for Desktop
- McAfee VirusScan Enterprise
- McAfee Endpoint Encryption
- McAfee ePolicy Orchestrator

Results
- Protects 98% of virtualized desktops and servers against sophisticated threats.
- Delivers new efficiencies through centralized management.
- Provides global visibility to support compliance and protect customers.

This company is a large retailer with hundreds of locations worldwide. Like many other global enterprises, the company has made virtualization of its IT infrastructure a top priority. "Our server environment is now 98% virtualized, and any new servers are now deployed as virtual machines," says the company's endpoint security specialist.

The specialist is part of a Microsoft Windows core infrastructure group that works closely with the IT virtualization team to protect the company's networks. Together, both teams are continually challenged to ensure that the company's virtual computing environment can grow without being compromised by malware attacks. Recent highly publicized hacks of large retail chains, such as Home Depot and Target, have added even more urgency to the challenge.

McAfee Management for Optimized Virtual Environments AntiVirus: Protection for Virtual Endpoints

The company sought an antivirus solution that would not burden each virtual machine by requiring installation of a scan engine and at the same time was specifically designed for VMware-based virtual environments. Tuned specifically for VMware vShield, McAfee McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) deployed in agentless mode provided the ideal solution. In addition, the company deployed McAfee MOVE AntiVirus in multiplatform mode on their VMware infrastructure to leverage some of the additional features that McAfee, a part of Intel Security, offered in this mode. This also allows them to leverage the same offloaded antivirus capability on non-VMware hypervisors as they expand in the future.

McAfee MOVE AntiVirus brings optimized, advanced virus protection to the company's virtual enterprise. The solution integrates real-time threat intelligence and provides unified security management across the company's entire complement of Intel Security solutions through the McAfee ePO management platform. Other solutions that are included in McAfee Data Center Security Suites are McAfee VirusScan® Enterprise, McAfee Host Intrusion Prevention for Desktop, and McAfee Endpoint Encryption.

"We had tremendous buy-in right away for McAfee MOVE AntiVirus. Already, we had VMware tools and other agents running on every server, so our management was sold when they heard we would be able to remove the antivirus scan engine," the endpoint security specialist notes. "The agentless design of McAfee MOVE AntiVirus helps relieve the overhead of traditional endpoint security, while offering essential protection and performance for our global operation."

Virtualized Security Management Made Efficient

McAfee MOVE AntiVirus optimizes the industry-leading protection of McAfee VirusScan® Enterprise to virtual machines (VMs) by enabling the scanning to be offloaded to a security virtual appliance (SVA) that is shared by all the VMs on the hypervisor. The SVA is delivered as an open virtualization format (OVF) package. In the agentless deployment, the SVA uses the VMware vShield Endpoint API to receive scan requests from VMs running the VMware vSphere hypervisor. McAfee® ePolicy Orchestrator® (McAfee ePO™) software manages the security policy for each of the VMs, the McAfee MOVE AntiVirus configuration on the SVA, and provides reporting on malware discovered on the VMs.

intel Security

"With so many highly evolved and sophisticated threats, endpoint protection alone is no longer enough—we need to know our landscape and have comprehensive intelligence in order to assess our risk. Intel Security offers us that intelligence, in addition to the industry's best protection for virtualized environments."

—Endpoint Security Specialist, Global Retailer

"In a virtual environment, instead of updating 100 physical servers with .DAT files, you're actually updating the hypervisor times 100," the specialist explains. "With McAfee MOVE AntiVirus, we just need to update one SVA per hypervisor, instead of having to re-deploy and update software on each client. It's a huge time-saver."

McAfee ePO software provides near-real-time visibility into the entire virtual infrastructure—consisting of 25,000 virtual clients, 5,000 virtual servers, and 50 VMware Host in three vCenters. The McAfee Data Center Connector for VMware vCenter integrates the management feature of McAfee ePO software with the VMware vCenter server. This enables the specialist to discover and import each virtual machine and its protection status into the McAfee ePO software system tree.

"I can't say enough about McAfee Data Center Connector. It's an incredibly useful tool for me to view every vSphere connected through our data centers, which also saves me lots of time," the specialist comments.

A Security Connected Virtual Enterprise

With this suite of solutions under centralized management by McAfee ePO software, the company benefits from a fully integrated, enterprise-wide security strategy that also meets compliance requirements. McAfee Host Intrusion Prevention for Desktop offers additional protection for 25,000 endpoints against threats that might otherwise be unintentionally introduced or allowed by users. In addition, McAfee VirusScan Enterprise in tandem with McAfee Global Threat Intelligence protects 30,000 laptops, workstations, and servers. McAfee ePO software plays a critical role in the company's compliance with internal policy, as well as external standards, such as PCI and HIPAA, providing direct feeds into a security information and event management system for long-term analysis and correlation of security events. Using the data, the specialist is able to run monthly reports with statistics on malware interceptions that are shared with the company's management and information security team.

"McAfee ePO software and Security Connected solutions give us protection as well as visibility," the specialist says. "For instance, at this moment the McAfee ePO software dashboard is showing me the morning's status of .DAT deployments, today's detections from each Intel Security solution, disk encryption status on all laptops, the number of endpoints that are compliant with McAfee VirusScan Enterprise 8.8, and a host of other critical security information."

Enabling Tight Collaboration with the Virtualization Team

The specialist explains that the security team had once been a fairly autonomous organization, but that changed with the advent of virtualization. "As our environment became more and more virtualized, the virtualization team became more dependent on our group to provide appropriate security," he says. "With the deployment of McAfee MOVE AntiVirus, we were able to gain their confidence that the solution would secure the environment without slowing down the business—and we have the access and visibility we need to ensure that each and every virtual machine is protected."

Global Security for a Global Business

The company's IT department views its role as supportive, with a commitment to provide a safe and efficient environment for the company to go about its main business of selling products to consumers. "In the end, security is about protecting our end customers from threats when they entrust their credit card information to us. Everything else is secondary," the specialist comments. "With so many highly evolved and sophisticated threats, endpoint protection alone is no longer enough—we need to know our landscape and have comprehensive intelligence in order to assess our risk. Intel Security offers us that intelligence, in addition to the industry's best protection for virtualized environments."

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

61649cs_warehouse-retailer_0115_ETMG