Case Study

State Agency Secures Expansive Virtualized Environment with Intel Security

Large State Agency

Customer profile
Organization charged with managing key functions such as procurement, real estate, and transportation for other state agencies.

Industry
State Government.

IT environment
Six managed solution centers supporting more than 360 virtual machines.

Challenges
The need to streamline and expand security for virtual machines and provide more comprehensive and centralized endpoint security.

Intel Security solution

- McAfee Data Center Security Suite
- McAfee Complete Endpoint Protection—Enterprise
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator
- McAfee Management for Optimized Virtual Environments AntiVirus
- McAfee Active Response
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense

This Intel® Security customer serves as the business manager for a large US state. The agency helps the state government better serve residents by providing services to other agencies including procurement and acquisition solutions, real estate management, leasing and design services, environmentally friendly transportation, and architectural oversight and funding for the construction of safe schools. The agency is organized across 15 divisions and has more than 4,000 employees.

Protecting a Virtual Environment

The agency's IT environment is now more than 90% virtualized under VMware vShield and VMware NSX, with four vShield hypervisors managing approximately 360 virtual machines (VMs) across six managed solutions centers.

"As an IT organization, our goals are centered on supporting our customers' requirements through faster time to deployment, timely support for end users, and ease of tracking requested changes in systems," comments the agency's enterprise architect in charge of virtualization. "Through virtualization, we can be much more nimble when requests come in for server or network deployments, security and systems scans, and any other type of support issue."

Security is a critical requirement for such a large virtualized infrastructure. The agency needed a security solution maximized for virtualization—one that could offer advanced protection from malware on each VM while streamlining management.

At the same time, the agency sought to strengthen and integrate its endpoint security. "With standalone virus scanning software on each of our systems, our environment had become too difficult to manage and keep updated," explains the agency's security operations manager. "We needed an integrated, centralized platform that could offer greater security from vulnerabilities."

A Connected Choice

To address these ongoing security requirements, the agency is migrating its infrastructure to an integrated suite of solutions from Intel Security. This includes the McAfee® Data Center Security Suite including McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus, delivering advanced virus protection to all VMs. In addition, the agency has adopted McAfee Complete Endpoint Protection Enterprise—a comprehensive suite of solutions that include endpoint security, dynamic application control, intrusion prevention, global threat intelligence, web and email security, and data protection.

The agency has also implemented McAfee Enterprise Security Manager, the Intel Security acclaimed security information and event management (SIEM) solution, that provides real-time visibility into all activity on systems, networks, databases, and applications.

Comprehensive Protection for Virtual Machines

The agency operates MOVE AntiVirus in agentless mode for most of its environment, extending comprehensive protection to VMware vShield without burdening each VM with a local scan engine. In multiplatform mode, MOVE gives the agency the ability to install an agent on a select group of administrative servers that require deeper-level scans. MOVE AntiVirus delivers seamless integration with VMware NSX and enables the agency to deploy virtual appliances protected by McAfee security from the NSX console.

intel Security

With McAfee ePO software providing 'single-pane-of-glass' visibility and the integration of the entire McAfee suite, this customer is confident that it is providing maximum protection for its infrastructure.

Results

- Reduced OPEX and faster response to customer VM requests.
- Protected 360 VMs from advanced threats.
- Gained complete visibility into all security-related events.
- Enhanced reporting and management through centralized dashboard.

MOVE AntiVirus in agentless mode continuously protects the organization's VMs from advanced threats without consuming local processing power and without impacting system performance. In addition, MOVE AntiVirus gives the organization the flexibility to deploy local agents when needed. Since MOVE AntiVirus operates as a deployable service in NSX, the agency can set up a single security profile that can be applied every time a new server is added in the protected environment. By default, the new server gets all of the predefined protections, enabling the team to respond instantly to service requests and go live much faster. Not only can the agency support its customers better, but its operational costs are reduced along with the management overhead.

Enhanced Visibility into Security Events

With McAfee Enterprise Security Manager, the agency is now armed with comprehensive visibility into potential security events and risks. The SIEM solution collects and correlates an average of 178 events per second, with almost 15.4 million events collected to date. These events come from application security logs for virtually every device and system in the organization including switches, firewalls, and Windows servers.

McAfee Enterprise Security Manager is a significant improvement over the previous environment, since the agency had been relying on a syslog server for event information. Not only is the organization much better equipped to respond to security audits and meet compliance requirements, but it now has a baseline for anomalous activities that lets it be more proactive about threats and remedy misconfigured system accounts faster.

Centralized Management

Within the McAfee Complete Endpoint Protection—Enterprise suite, McAfee VirusScan® Enterprise software now protects more than 2,500 endpoints including PCs, laptops, smartphones, and tablets. Moving forward, the agency will deploy McAfee Threat Intelligence Exchange, McAfee Advanced Threat Defense, and McAfee Active Response for strengthened detection and protection against advanced targeted threats. McAfee ePolicy Orchestrator® (McAfee ePO™) software provides a single, centralized console for the agency to manage policies, compliance, and reporting for all McAfee security components.

With McAfee ePO software, the agency has complete visibility into its entire security environment. The security team is able to make custom queries to monitor different aspects of security, and the McAfee ePO platform makes it easy to ensure that all clients are running the most up-to-date software.

The agency is also developing a set of reports to keep management updated on security activities such as stats on suspicious emails and intercepted malware. With McAfee ePO software providing 'single-pane-of-glass' visibility and the integration of the entire McAfee suite, this customer is confident that it is providing maximum protection for its infrastructure.

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