Case Study

Global Security Management Made Easier for Leading IT Service Provider

An information security engineer and his team defend this global IT service provider and its many clients much more easily and efficiently thanks to the centralized management of McAfee® ePolicy Orchestrator® (McAfee ePO™) software and the Intel® Security unified platform.

Computer Sciences Corporation

Customer profile
Global MSSP for a Global Entertainment company.

Industry
Entertainment.

IT environment
200,000 endpoints in 70 countries, with 'every flavor' of operating system.

Challenges
- Lack of visibility across endpoints due to diverse security environment with multiple point solutions.
- Protecting geographically vast enterprise and multiple clients.
- Lack of centralized security management.

McAfee solutions
- McAfee VirusScan Enterprise software
- McAfee VirusScan for Storage software
- McAfee Host Intrusion Prevention for Servers
- McAfee ePolicy Orchestrator software

Results
- Easier management, reporting, and deployment thanks to centralized control.
- Real-time visibility across all endpoints worldwide.
- Faster detection of incidents and remediation of threats.
- Time savings from more efficient, effective administration.

As an information security engineer at Computer Sciences Corporation (CSC), one of the world's leading IT service providers, Christopher Sacharok manages day-to-day endpoint security for client organizations as well as troubleshoots security issues for other teams of CSC consultants. As major data breaches have become national headlines, Sacharok has seen CSC clients, from large federal government agencies to small corporations, increasingly devote more resources to security.

"The good thing that has resulted from these very public breaches is that security is moving to its rightful place as a top priority," says Sacharok. "At CSC, our first priority is to provide a secure environment that safeguards data, ensures business continuity, and complies with all necessary regulations. Making sure our clients' operations run as efficiently and effectively as possible comes next, but security comes first."

Point Solutions Pose Management Burden

"One of the biggest challenges I see in most IT environments is getting security solutions to talk to one another," states Sacharok. "Security Ops has to spend a ton of energy trying to get data from all the various homegrown and third-party software and hardware products to a central place where they can be managed efficiently. It's also extremely difficult to manage and protect assets or comply with PCI and other regulations."

With multiple vendors' point solutions protecting its own endpoints, CSC used to have the same problem. Without central management, there was no way to see the security status across all of its 200,000 endpoints scattered across 70 locations and four continents. Demonstrating compliance with regulations ranging from PCI and HIPAA to Sarbanes-Oxley was difficult and time-consuming. It's also beneficial to have a single pane of glass to view similar endpoint protection products for different operating systems. It's an added bonus that the individual products that report into McAfee ePO software are better than standard OS protections.

Solution: Unified Security Platform with Central Management

After researching endpoint protection options, CSC turned to Intel Security solutions for a unified security platform with easy-to-use, centralized management. CSC implemented McAfee VirusScan® Enterprise software to protect its 200,000 endpoints worldwide from malware and spyware, and McAfee VirusScan for Storage to extend protection to 18 network-attached storage devices. In addition, the company deployed McAfee Host Intrusion Prevention for Servers to proactively protect about 5,600 servers against known and new zero-day attacks, and McAfee Vulnerability Manager, to immediately detect system vulnerabilities.

What sets these products apart, however, is the McAfee ePO software central management console that comes bundled with each of them and enables them to be managed from a single, common screen. "McAfee ePO software stands out compared to other solutions," says Sacharok, who has seen his share of

"McAfee ePO software stands out compared to other solutions. It is a one stop shop for our endpoint protection. I can see everything I need to see for all of our McAfee products from one pane of glass. Its easy-to-use dashboards and built-in functionality make everything—visibility, reporting, deployment, updating, maintenance, decision making—so much easier."

—Christopher Sacharok, Information Security Engineer, Computer Sciences Corporation

Proof of Concepts for a wide range of security products. "It is a one stop shop for our endpoint protection. I can see everything I need to see for all of our McAfee products from one pane of glass. Its easy-to-use dashboards and built-in functionality make everything—visibility, reporting, deployment, updating, maintenance, decision making—so much easier."

How McAfee ePO Software Makes Security Operations Easier and More Efficient

Besides Sacharok, seven others on his team and two security administrators on other CSC teams rely on McAfee ePO software for a centralized view of security status across all 200,000 corporate and client endpoints. They also depend on it for reporting—regularly scheduled reports for compliance purposes as well as on-the-fly queries. Sacharok and the others often refer to a number of the out-of-the-box reports, including top threats by internal organization, top 10 computers with malware detection, and a listing of all new security incidents.

On average, the company sees 200 unique threat events every 24 hours and 4,100 each month. "For daily operations, the intuitive McAfee ePO dashboards are simply the best," claims Sacharok. "I can see instantly if an event needs my attention and drill down for details. McAfee ePO software makes me more efficient and alleviates a lot of headaches."

Sacharok's team also uses McAfee ePO software to scan regularly for vulnerabilities, push out security software updates, and perform troubleshooting or remediation activities. When other CSC information security teams—the firewall team, the email gateway team, and so on—need endpoint protection troubleshooting, they call Sacharok's team. "Whether we need to write a new exclusion rule or update DATs or HIPS for instance, or any time a security incident happens on the network, we're immediately able to detect where and what is happening in real-time and take corrective action," he says.

Time Savings from High Level of Granularity, Built-In Tools

Sacharok also cites the ability within McAfee ePO software to use a system tree and sort dynamically at a very granular level as extremely helpful. He can view endpoint status information by continent, city, building, or even floor, so it's easy to pinpoint exactly where to remediate if physical intervention is necessary. "You don't see that level of granularity of management in many other security tools," notes Sacharok. "It definitely gives Intel Security an edge."

Remediation tools built into McAfee ePO software also facilitate more streamlined security operations. For instance, with the software Sacharok can transfer an endpoint directly from one internal organization into a different one and apply the latter's policies to it or run a high-priority antivirus scan against it. "Being able to perform many remediation acts remotely via McAfee ePO software also alleviates the need to have a deskside technician and the subsequent degree of separation between my team and the end user," adds Sacharok. "Less in-person time saves Security Operations significant time and resources."

Strong Support and a Strategy for the Future

In addition to Intel Security technology, Sacharok and others at CSC depend on Intel Security Platinum Support. "We have been very pleased with the level of support we receive," notes Sacharok. "Whenever we have a question, we check the support knowledge base, and on the rare occasions that we need to talk with someone, the turnaround is always very fast."

Just as McAfee ePO software stands apart in Sacharok's mind, so does Intel Security the company. "When you are looking at security vendors, strategy ranks above everything else," explains Sacharok. "The vendor obviously needs to have a cost-efficient product that works well, but at the end of the day, the vendor also needs to have a strategy to make your environment more secure than anyone else can. Intel Security has by far the most comprehensive security vision and strategy of any vendor I've seen."

Sacharok is referring to the Intel Security strategy of an open, interconnected security architecture that simplifies the threat defense lifecycle to help organizations resolve more threats, faster, with fewer people. "In the near future, integrating our different solutions together even further is definitely going to be critical to making us a more holistic security company," says Sacharok. "I expect Intel Security will have a key role in this process."

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