Case Study

Government Statistics Agency Embraces Enterprise Security Connected Strategy

Customer profile
A federal census and statistics agency.

Industry
Government Agency.

Challenges
A lack of a comprehensive security infrastructure, with disjointed solutions provided by many vendors.

Intel Security solutions
- McAfee Endpoint Protection Enterprise.
- McAfee Network Security Platform.
- McAfee Vulnerability Manager.
- McAfee Enterprise Security Manager.
- McAfee Data Center Security Suite for Databases.
- McAfee Asset Manager.
- McAfee ePO software.

Results
- Provides enterprise-level integration and control to stop threats in their tracks.
- Offers enhanced visibility into overall security posture.
- Provides a trusted partnership for evolving the security infrastructure into the future.

This South American government agency is responsible for collecting and processing statistical data. The agency conducts the country's census and other sociodemographic and economic surveys, and also analyzes and reports economic and social indicators such as inflation rate, consumer price index, and unemployment figures.

Filling In Security Gaps

In 2012, the government mandated a large-scale modernization of all federal resources including the IT and security infrastructure. For the agency, this was an opportunity to identify gaps in protection and adopt a more comprehensive and integrated security platform.

"Prior to 2012, we had no real security infrastructure and our IT ecosystem was a diverse collection of solutions and servers. Our antivirus protection was outdated, and we had only a software firewall at the network perimeter," explains the agency's systems director.

"We were also dealing with several highly publicized malware attacks. We realized we needed a holistic security approach, rather than trying to deal with threats in an isolated fashion," remarks the agency's network security manager. "We were looking for much more than antivirus; we also needed to address policy enforcement, security of servers and storage, and a lack of visibility into our overall security posture."

The network security manager adds, "We needed a security partner that could sustain and support us proactively as our needs evolved. Previous security vendors could not offer that level of support."

He gave the example of a previous antivirus solution that had not been updated for more than two years. "The vendor never checked in on the status of our deployment, and it was not a flexible organization to work with. In general, it was neither a collaborative nor a supportive relationship," he says.

A Security Connected Choice

To address these requirements, the agency chose an integrated suite of McAfee® solutions, part of the Intel® Security product line. In addition to McAfee Endpoint Protection—Enterprise, the agency has deployed McAfee Network Security Platform, McAfee Vulnerability Manager, McAfee Enterprise Security Manager, McAfee Data Center Security Suite for Databases, and McAfee Asset Manager. McAfee ePolicy Orchestrator® (McAfee ePO™) software provides a single, unified point of control for the complete Intel Security suite.

"With the Intel Security solutions tied together within the McAfee ePO management console, we're able to deploy a single-vendor platform to cover all points of vulnerability and provide enterprise protection," the systems director notes. "Each Intel Security tool is able to work with data supplied by other tools, and feed information to other tools, for more effective and comprehensive threat resolution. Intel Security is the only vendor that can provide that degree of integrated, connected security."

Another key factor in the agency's choice of Intel Security is its local presence in the region, including in-country engineering and support personnel.

Holistic Threat Visibility and Protection

Since deploying the integrated suite of Intel Security solutions, the agency has noticed a steep drop-off in malware attacks, and threats that do enter the network can be detected and mitigated quickly.

"Previously we had no visibility into our overall security posture, so we had no way of knowing the volume or character of attacks, whether

intel Security

> *"With Intel Security as our long-term security partner, we have the confidence we need to ensure business continuity and deliver a security platform that we can continue to build on into the future."*
>
> —Systems Director

they were viruses, botnets, or information theft attempts. Now, with Intel Security, we know what's happening on the network, and where and when," the systems director says. "With the heightened visibility of the Intel Security tools, we can be proactive and shut the threats down immediately before they have a chance to do damage."

He adds that the enhanced visibility into risks is an important tool for security analysis and management. "We can use the security data from the Intel Security tools to better understand our vulnerabilities and continually strengthen our infrastructure. Plus, the automation of security processes and integration of the tools gives us the control we need to adapt our environment in a security landscape that changes constantly."

A Solid Approach to SIEM

Another important weapon in the agency's security strategy is McAfee Enterprise Security Manager, a security information and event management (SIEM) tool. McAfee Enterprise Security Manager continually gathers data in 'listener' mode at highly sensitive information points in the network, such as server logs. Using this data, the agency can constantly fine-tune the monitoring and alerts needed to proactively stop threats and comply with government standards and policies. "Intel Security gives us intelligence we've never had before. The speed and quality of the SIEM reports is excellent and continually improving as we continue to adapt our use of the tool," says the network security manager.

Proactive Database Security

In addition, the agency migrated from a standalone database security system to McAfee Data Center Security Suite for Databases—also under the complete control of McAfee ePO software.

The agency has a mixed data environment with databases from many different vendors, and with varying degrees of vulnerability to exploits. Regardless of the database type, the Intel Security database security solution stops exploits from executing without the need to apply aggressive patches.

A Security Partner for the Long Haul

The agency's partnership with Intel Security Professional Services has played a critical role in getting it up and running quickly on the Intel Security solutions, and in reaping maximum benefit from the deployment. "The team's expertise has saved us a lot of time both in knowledge transfer and in implementation, and in showing how to get the most out of the products," the network security manager says.

The systems director adds, "The chief difference between Intel Security and other vendors we've worked with is that their solutions have been effective from day one at stopping malware threats on many levels. With other brands, we've had to iron out many implementation problems—but not so with Intel Security."

"With Intel Security as our long-term security partner, we have the confidence we need to ensure business continuity and deliver a security platform that we can continue to build on into the future."

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

Intel and the Intel and McAfee logos, ePolicy Orchestrator, and McAfee ePO are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. Copyright © 2015 McAfee, Inc. 62201cs_govt-stat_1215_fnl_ETMG