Case Study

Rapidly Deployed, Robust Web Protection with a Hybrid Security Solution

Global Manufacturer

Customer profile
Multinational diversified manufacturer.

Industry
Manufacturing.

IT environment
50,000 endpoints across more than 600 sites worldwide.

Challenges
- Limited IT security staff to protect global enterprise.
- Excessive time spent remediating endpoints from web-borne malware.
- Unprotected intellectual property.
- Compliance with Sarbanes-Oxley, PCI, and HIPAA.

Intel Security solutions
- McAfee Web Gateway
- McAfee SaaS Web Protection
- McAfee Client Proxy
- McAfee Complete Endpoint Protection—Enterprise
- McAfee ePolicy Orchestrator (McAfee ePO) Software

Results
- Reduced malware-related IT helpdesk tickets 20%.
- Accelerated time-to-web protection for onsite and offsite employees and contractors.
- Streamlined MPLS network usage.
- Improved end-user productivity.

By implementing McAfee® Software-as-a-Service (SaaS) Web Protection, this Intel® Security customer was able to quickly protect its onsite employees, remote employees, and contractors from web-borne malware across its global enterprise. By phasing in on-premises McAfee Web Gateway appliances and creating a hybrid environment, the company enabled a more comprehensive defense.

This global manufacturer makes and distributes a very diverse range of products for industrial giants as well as individual consumers. Consequently, the company has plenty of physical and intellectual property (IP) assets to protect, amidst a world of ever-increasing cyber threats. The company's IT security manager and his small team face this challenge every day as they support the entire global enterprise's IT security needs, from desktop to network, across more than 50 manufacturing plants and 600 offices, warehouses, and repair centers worldwide.

Defense Against Web-Borne Malware Couldn't Wait

In the past, the company's IT field engineers spent hours each day dealing with malware on laptops and other devices. They literally had more than 100 help tickets every day, a huge portion originating from Internet-based malware. As a result, the company's CIO decreed web security a top priority that simply could not wait.

The Best Solution Also the Fastest

The company quickly narrowed down its search for a web protection solution to four different security vendors. Both the CIO and the IT security manager had extensive experience with web filtering solutions that were not from Intel Security, so those two vendors' solutions initially topped the list. However, as the security team compared solutions against the company's requirements—including speed of deployment—Intel Security rose to the top.

Unlike the other vendors, Intel Security offers SaaS via the cloud combined with on-premises hardware, or a hybrid environment. With McAfee SaaS Web Protection, the security team quickly provided web filtering and malware detection for everyone—onsite employees, remote employees, employees using their smartphones or tablets, and contractors. In a follow-on phase, the security team plans to add gateway hardware and seamless authentication. Only Intel Security gives them an immediate widespread web protection solution, plus meets all of their longer-term requirements.

Accelerated Time to Enterprise-wide Web Protection

Within one month after initializing McAfee SaaS Web Protection, nearly 75% of the organization's 50,000 nodes were protected by advanced web filtering and malware detection. The solution blocks both known and zero-day malware before reaching an endpoint.

The company simply port-forwards all traffic hitting its major firewalls as a point of egress to McAfee SaaS Web Protection. There is no need for internal network configurations or network beams that complicate the internal network. If

intel Security

employees or contractors use their phone on the network and traverse through one of the data centers as the egress point, they are routed through the cloud service without needing a client configuration.

Phased-In Approach to a Hybrid Environment

After the success of the SaaS Web Protection deployment, the security team then deployed McAfee Web Gateway appliances for on-premises web protection. They also added authentication, providing visibility into users' Internet access. Before activation, the security team did not know what sites people were visiting—now they know exactly who is looking at what sites and when.

In order to protect mobile workers while traveling on- and off-premises, the security team deployed the location-aware McAfee Client Proxy on their devices. When these users are inside the corporate network, McAfee Client Proxy directs Internet traffic to the appropriate McAfee Web Gateway appliance. When mobile workers move outside the firewall, Client Proxy redirects web traffic from their device to the cloud-based McAfee SaaS Web Protection, maintaining consistent protection.

Initially the company had two separate management consoles, one for its seven McAfee Web Gateway appliances and one for McAfee SaaS Web Protection. The security team plans to manage all policies for the gateways and cloud protection from one central console, and apply the same policies to the remote and on-premises users.

Tremendous Time and Cost Savings for Both IT and End Users

After the company implemented McAfee SaaS Web Protection, it experienced a 20% decrease in IT help-desk tickets. Where field engineers were once consumed with hunting down or remediating malware, the company now easily saves more than $1 million per year in manpower thanks to the Intel Security infrastructure.

Fewer malware incidents minimize negative impact on productivity for the manufacturer's end users because they seldom experience interruption in their workday.

Easy Management and Reporting with a High Level of Granularity

Using the McAfee Content Security Reporter—included with McAfee Web Protection and integrated with the McAfee ePolicy Orchestrator® (McAfee ePO™) central management console—the IT security manager and his team quickly and easily generate reports on web usage trends, most-visited IP addresses, top Internet users, policy enforcement actions, and so on. With the McAfee Web Protection solution, the level of granularity available for analysis and policy-setting exceeds that of competitive products. The extreme power of the McAfee Web Gateway rules enables the team to customize rules for various groups. The SaaS logs also stream into McAfee Content Security Reporter, providing cloud visibility.

Streamlining Network Bandwidth for Additional Savings

With the McAfee Content Security Reporter web traffic reports, the company's security team better controls network bandwidth across the enterprise. The reports show what sites are being visited, when, and by whom. Rather than upgrading their MPLS, users are educated to stay away from certain sites or are restricted from visiting sites that put an undue burden on bandwidth. Streamlining MPLS usage is a side benefit that alleviates additional expenditure and enables a faster, more responsive network.

Flexible Licensing and Dependable Support

The IT security manager also appreciates the flexible licensing that Intel Security provides. Rather than being forced into a per-user pricing model for a device with sporadic users, or a per-device model when users may have four or five devices, Intel Security offers licensing that makes sense for the company.

"After we implemented the McAfee SaaS Web Protection Service, we experienced a 20% decrease in IT help desk tickets. Our field engineers used to be constantly tied up either hunting down or remediating malware. In my mind, we are easily saving more than $1 million a year in manpower thanks to the Intel Security infrastructure."

— IT Service Manager, Global Manufacturer and Intel Security Customer

The security team is also impressed with the Intel Security Platinum Support offering and the quality of the support they receive from their Intel Security contacts. For instance, the company meets regularly with the Intel Security Support team, and they listen closely to what the customer has to say. The vast majority of the time they troubleshoot their own issues, but on rare occasions when the security team needs to call for help, they know they can count on Intel Security.

Future Plans to Fortify Threat Defense

To strengthen its threat defense in the near future, the company plans to deploy McAfee Advanced Threat Defense for sophisticated sandboxing detection of zero-day threats, and McAfee Threat Intelligence Exchange. Threat Intelligence Exchange combines multiple internal and external threat information sources and instantly shares the data with all of the security solutions that are connected to the McAfee Data Exchange Layer (DXL). The company rolled out McAfee DXL across all of its Intel Security web protection, endpoint, and network intrusion prevention system (IPS) solutions in anticipation of the benefits delivered by enabling McAfee Advanced Threat Defense and its other McAfee security solutions.

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