CASE STUDY

Leading Latin American University Fortifies Security for Institution and Students

Faster incident response with McAfee Enterprise Security Manager

Universidad de Las Américas Puebla (UDLAP)

Customer Profile
Private university in Mexico

Industry
Higher education

IT Environment
- One main campus supporting more than 750 staff members and 8,000 students.
- 2,500 endpoints, not including student devices

One of the most prestigious universities in Latin America relies on McAfee and its security incident and events management (SIEM) solution to provide widespread visibility and greater control, enable faster detection and response to security threats, and safeguard its own assets as well as those of its students.

Chief Information Officer Fernando Thompson de la Rosa is passionate about using technology to improve operations at Universidad de Las Américas (University of the Americas) , or UDLAP, in Puebla, Mexico. At the prestigious undergraduate university, he deals with IT operations on a daily basis—from enterprise resource planning (ERP) and learning management systems to a distance teaching portal and the Wi-Fi network. Of all his challenges, protecting the university from cyberthreats tops the list.

Secure University Assets and Student Devices

Maintaining a secure environment in a university setting has become much more difficult in recent years. "Ten years ago, our main network was the LAN, and the only devices we had to protect belonged to the university," explains Thompson de la Rosa. "Today, the main network is Wi-Fi, and we have to enable access to thousands of devices—laptops, smartphones, and tablets, with numerous operating systems and versions—that don't belong to us. If we only protect the 2,000 laptops owned by the university, we are going to fail."

UDLAP has 8,000 undergraduate students, each with an average of 2.8 personal devices. That's more than 22,000 devices among students alone. Approximately 40,000 devices connect to UDLAP networks daily.

"We have to protect the devices of millennials who don't realize that they need to be protected in order to prevent them from putting the university and others at risk," he explains. "Consequently, educating our users is at the core of our security strategy—as is widespread visibility and early detection. We need to be able to see and understand what is going on across our networks and be able to respond as quickly as possible to threats."

McAfee Enterprise Security Manager: Lowest TCO and Highest ROI

Previously, UDLAP had implemented McAfee® Complete Endpoint Protection for Business for antivirus and antispyware protection, web filtering, host intrusion prevention, and disk, file, and folder encryption—all managed from the McAfee ePolicy Orchestrator® (McAfee ePO™) central management console. As devices proliferated and the challenge of complying with data privacy regulations increased, Thompson de la Rosa recognized the need to add a SIEM system to provide greater visibility and control across the university's infrastructure, which includes a tier 3 data center, 10 networks, and 120 physical and virtual servers.

After evaluating solutions from several leading SIEM vendors, he and his team had an easy decision. "We chose the McAfee Enterprise Security Manager because it helps us consume and process security information faster, so we can identify and respond to incidents in a very short period of time," says Thompson de la Rosa. "It also cost less than some of the other SIEMs. The decision was a 'no-brainer.' McAfee clearly offered the lowest TCO and best return on investment. McAfee Enterprise Security Manager is one of our best tools."

UDLAP implemented McAfee Enterprise Security Manager to dramatically improve the university's ability to protect, detect, and correct future cyberthreats.

Challenges

- Protect not only the university's IT infrastructure and data, but also personal devices
- Average of 2.8 personal devices per student
- 40,000 devices connect to network daily
- Limited budget and staffing resources
- Comply with privacy regulations

McAfee Solution

- McAfee Advanced Correlation Engine
- McAfee Anti-Spyware Student
- McAfee Enterprise Log Manager
- McAfee Complete Data Protection—Advanced
- McAfee Complete Endpoint for Business
- McAfee Enterprise Security Manager
- McAfee Event Receiver
- McAfee Global Threat Intelligence for McAfee Enterprise Security Manager
- McAfee Network Security Platform
- McAfee VirusScan® Student
- McAfee ePolicy Orchestrator

The university also implemented McAfee Advanced Correlation Engine to identify and score threat events in real time, using both rules- and risk-based logic, and McAfee Global Threat Intelligence (McAfee GTI) for McAfee Enterprise Security Manager to deliver a constantly updated, rich feed of threat intelligence data.

Improves Security Posture and Enables Faster Incident Response

"We now review a huge amount of data in a very short amount of time," notes Thompson de la Rosa. "With fast analysis from all the critical data sources, alerts are triggered sooner, and we can detect and respond to suspicious incidents faster." In addition to endpoint data from McAfee ePO software and network traffic data from McAfee Network Security Platform, the McAfee Enterprise Security Manager receives information from firewalls, a sandboxing appliance, Microsoft Active Directory, web gateways, databases, routers, and other systems. McAfee GTI also helps determine risk level and prioritization of incidents.

To stay ahead of advanced threats, UDLAP has defined a number of key behavioral correlations and is in the process of creating new correlation rules to trigger automated alerts. "McAfee Advanced Correlation Engine is a magnificent tool. It provides a ton of intelligence about what is happening in our networks," claims Thompson de la Rosa. "With this capability, we have been able to detect ransomware before it locks up our systems."

Granular, Centralized Reporting Facilitates Compliance

Thompson de la Rosa's security administrators use reports from both McAfee ePO software and McAfee Enterprise Security Manager's dashboard—standard, out-of-the-box reports, such as the Top 10 Infected Systems and Top 10 Detected Threats, as well as customized reports. "If we need to drill down to a deep granular level to obtain detailed information on a specific event, we can easily build a custom report on the fly," explains Thompson de la Rosa.

The McAfee Enterprise Security Manager's reporting functionality also facilitates compliance. "Before McAfee Enterprise Security Manager, demonstrating compliance with privacy laws was extremely difficult and time-consuming, but now it is often simply a matter of printing out several reports," he notes. "In addition, with McAfee Enterprise Security Manager, we can conduct trend analysis and more easily detect irregular trends."

Data Protection for the University and Its Students

UDLAP also uses the McAfee Complete Data Protection—Advanced software suite to protect computers that have access to sensitive information. The university is currently in the process of using this solution to encrypt hard drives across university-owned laptops and PCs and is testing other forms of encryption. As for student devices, the university offers all of its students McAfee VirusScan® Student and McAfee AntiSpyware Student free of charge.

Results

- Improved security posture with faster incident response
- Lowest TCO, highest ROI
- Easier, faster proof of compliance
- Invaluable support, including educating users on how to maintain security best practices

An Extremely Supportive Partner and Ecosystem

"Partnering with McAfee these past several years has dramatically improved our security posture," says Thompson de la Rosa. "McAfee has knowledgeable people who work very closely with us and understand the specific security needs of higher education. They have even helped us increase awareness of security best practices among our students—a task that is absolutely essential because the weakest part of the security defense for a university is its user population, not its technical infrastructure."

"Competitors are constantly approaching us, but we feel very good about partnering with McAfee," adds Thompson de la Rosa. "I also love being part of the McAfee ecosystem." For instance, Thompson de la Rosa, who has been in Mexico's CIO 100 for seven years, finds the annual McAfee FOCUS user conferences (now called MPOWER) extremely worthwhile for learning and discussing security strategies. "We have had a very successful partnership, and I hope to work with McAfee for years to come."

> "We chose the McAfee Enterprise Security Manager because it helps us consume and process security information faster, so we can identify and respond to incidents in a very short period of time … The decision was a 'no-brainer.' McAfee clearly offered the lowest TCO and best return on investment."
>
> —Fernando Thompson de la Rosa, CIO, Universidad de Las Américas Puebla

McAfee
Together is power.

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