CASE STUDY

Public University Automates Security to Mitigate Risk

Information security team does more with less, thanks to smarter, integrated security

Florida International University

Customer Profile
One of the largest public universities in the US

Industry
Higher education

IT Environment
Approximately 55,000 students and 15,000 staff scattered across two main campuses and satellite campuses overseas

With a layered defense based on a McAfee® integrated security architecture backbone, this large public university is shrinking the gap to containment and mitigating risk without adding staff.

Connect With Us

With approximately 55,000 students and 15,000 administrative and academic staff, Florida International University (FIU) is one of the largest universities in the US and the largest in the Florida public university system. Classified by the Carnegie Foundation as having the highest level of research activity, FIU conducts groundbreaking research and teaches students at its main campus in the Greater Miami area, as well as at campuses in China and Latin America and elsewhere in Florida.

Challenge: Protect Students and Staff Without Impacting Productivity or Increasing Headcount

As at universities everywhere, students pose one of FIU's largest information security risks: they can inadvertently click on a link or download an app that introduces malware into the environment. Furthermore, as a public university, the freedom to bring your own device is viewed as a right by students and staff alike. "In this type of open door, BYOD culture and environment, we can never ever stop being vigilant," says Chief Information Security Officer Helvetiella Longoria. "Of course, we must block as many threats as possible, but we also have to understand what kind of impact blocking them will have on our users and be prepared to contain and mitigate threats that make it into our environment as fast as possible."

"It's a constant balancing act," she continues. "We need to provide as robust a defense as possible, with 24/7 visibility across a network of students and staff constantly coming and going. But we also need to minimize any impact on student or staff productivity. And we need to keep operational overhead as low as possible, so we can juggle all the balls in the air and focus on what's important, without having to add staff."

Why McAfee: Ease of Management and Widespread Visibility

Over the past decade, the university has augmented its initial implementation of McAfee antivirus protection with endpoint encryption, host data loss prevention, and host intrusion prevention (HIPS), since all could be managed easily via the McAfee® ePolicy Orchestrator® (McAfee ePO™) central console. In more recent years, FIU also added to its arsenal McAfee Network Security Platform intrusion prevention systems (IPS) appliances, McAfee Threat Intelligence Exchange, and McAfee SIEM solutions, all of which also integrate with McAfee ePO software.

"One of the beauties of McAfee ePO software is the widespread visibility we get," states Longoria. "McAfee ePO provides so much valuable information at our fingertips. Its dashboards and reports help us determine exactly what needs attention or remediation. And, as we integrate additional technologies, McAfee ePO software becomes even beefier and better."

Two FIU information security managers use the McAfee ePO console to oversee endpoint security and McAfee SIEM solutions, but many others also rely on McAfee ePO software. For instance, academic department-level IT administrators regularly review department-specific

Challenges

- Allow freedom of bring you own device (BYOD), yet protect the environment from threats
- Keep students from accidentally introducing malware into environment
- Maintain widespread visibility
- Impact users minimally or not at all

McAfee solution

- McAfee® Advanced Threat Defense
- McAfee Complete Endpoint Threat Protection
- McAfee DLP Endpoint
- McAfee ePolicy Orchestrator
- McAfee Network Security Platform
- McAfee Policy Auditor
- McAfee SIEM solutions: McAfee Enterprise Security Manager, McAfee Log Manager, McAfee Advanced Correlation, McAfee Event Receiver, McAfee Global Threat Intelligence for McAfee Enterprise Security Manager
- McAfee Threat Intelligence Exchange

data loss prevention reports generated by McAfee ePO software, since what constitutes sensitive data varies by department. Many years ago, in a typically forward-looking move, Longoria and her staff worked to achieve buy-in across the university to install McAfee Host Data Loss Prevention (McAfee Host DLP) across McAfee ePO software-managed endpoints to prevent loss and leakage of sensitive data.

Migrating to McAfee Endpoint Security for a Leap in Performance and a Smaller Footprint

Although pleased with McAfee in general, and especially with McAfee ePO software, the university found that weekly Wednesday afternoon full virus scans impacted desktop performance to some extent, resulting in lower productivity. Consequently, FIU took advantage of the opportunity to migrate to a lighter endpoint security solution with a single agent per endpoint instead of multiple agents.

"The smaller footprint and improved system performance of McAfee Endpoint Security definitely piqued our interest," recalls Longoria. "We ran a very deep proof of concept to ensure that it was indeed slimmer and faster, and it definitely was. We also knew we wanted to use the new Dynamic Application Containment (DAC) functionality to quarantine unknown files, and the Real Protect machine learning technology. Traditional signature-based detection alone simply can't keep up with today's threats."

With the migration tool provided by McAfee and help from its longtime, trusted technology partner, Digital Arrow, FIU migrated to McAfee Endpoint Security in targeted waves. First, 500 desktops were migrated and then 1,000 at a time until all 8,000 endpoints were migrated. Some devices leave FIU premises for weeks, so it took a while to get them all checked in and fully migrated, but the effort was straightforward overall. Policy rules were migrated from McAfee Enterprise to the McAfee Endpoint Security Threat Prevention module and from McAfee HIPS to the McAfee Endpoint Security Firewall module.

"We experienced a dramatic difference in performance after implementing McAfee Endpoint Security," observes Longoria. With the new endpoint protection, FIU calculated that CPU memory utilization improved 51%. "Users are much happier. We haven't heard any complaints since the switch. Except for rare exceptions when a threat has been identified, malware scans now occur in the background when systems are idle. The weekly full scans are a thing of the past."

FIU migrated to McAfee Endpoint Security v10.2 and has begun upgrading to 10.5.3. They are eager to complete the upgrade on all endpoints as this will enable the university to take advantage of cloud-based Real Protect behavioral detection technology. "There's no question about it—machine learning is the way of the future and the way we are moving," says Longoria.

Results

- Faster containment of suspicious files or attacks, minimizing risk
- Stronger overall security posture without having to augment staff
- More robust endpoint protection with minimal impact on users
- Ease of management and enterprise-wide visibility

Superior Threat Detection but Transparent to Users

At FIU, threat detection and prevention also improved significantly after Longoria's team implemented McAfee Endpoint Security and McAfee Threat Intelligence Exchange. The latter uses the Data Exchange Layer (DXL), an open source platform that connects security components to share local and global threat information bi-directionally among all DXL-connected systems within the environment. Since McAfee Endpoint Security is built to leverage DXL, when an FIU endpoint protected by it encounters a suspicious or malicious file, that information is immediately conveyed to McAfee Threat Intelligence Exchange, which compares it to its reputation database. If the file is deemed malicious, it is immediately blocked, not only at "patient zero" but also across all endpoints. As soon as new threats are discovered, whether in the local environment or external sources, that information is added to the McAfee Threat Intelligence Exchange database.

In the future, FIU intends to implement McAfee Advanced Threat Defense for dynamic behavioral sandbox analysis. Then any file encountered by McAfee Endpoint Security that McAfee Threat Intelligence Exchange does not recognize will be sent automatically to McAfee Advanced Threat Defense. Meanwhile, as McAfee Advanced Threat Defense is analyzing the file, the DAC functionality of McAfee Endpoint Security quarantines the unknown file.

"By implementing McAfee Threat Intelligence, we have made our architecture much smarter," elaborates Longoria. "It helps our environment block thousands of threats each day, and users have no idea. Here's one example: recently, a back-door Trojan would have executed within our network if it had not been intercepted. McAfee Threat Intelligence works behind the scenes, doing its job phenomenally. We have only had to whitelist a handful of files."

Making the Most of the McAfee SIEM

To aid in continuous monitoring and incident response, three years ago FIU implemented McAfee SIEM solutions—McAfee Enterprise Security Manager, McAfee Log Manager, McAfee Advanced Correlation Engine, McAfee Event Receiver, and McAfee Global Threat Intelligence for McAfee Enterprise Security Manager. According to Longoria, McAfee SIEM made imminent sense because it seamlessly integrates with the university's existing McAfee solutions, as well as providing superior log management, ease of use, and advanced correlation capabilities.

"A SIEM is only as good as the information you feed it," she says. "With the McAfee SIEM, we log 650 million events daily from 102 diverse sources—firewalls, IPSs, and other network appliances and technologies, endpoints, DNS servers, Active Directory—as well as Windows logs and net flows from core routers and switches."

Logging all that data is one thing, but using it effectively and efficiently is what really counts. "I don't have a large team. I didn't want to have to add dedicated staff to oversee the SIEM," remarks Longoria. "So the SIEM had to be easy for my staff to learn to use. The McAfee SIEM interface is indeed very easy to use, and the system itself is powerful right out of the box. We used some of the built-in rule sets and saw benefits right away. And I didn't have to augment staff at all."

At FIU, two managers oversee both McAfee ePO software and SIEM solutions, though network managers and security analysts also use SIEM to query the data and take action. For instance, sometimes the university receives copyright infringement notices from the music industry. Using the SIEM, an administrator can easily track down violators. More importantly, however, SIEM is often used to identify compromised workstations, discover which users are connecting to which systems and how often, find errors on network ports, and more.

Working Smarter Through Automation

In addition to out-of-the-box SIEM rules and reports, Longoria's team has customized rules and automated actions to save time and mitigate risk. For example, if a McAfee ePO software report says that endpoint protection detected a malicious file but was unable to eradicate it—because the file had been loaded into memory, for instance—then the SIEM receives an "unhandled threat" alert, which kicks off a deep scan of the workstation. "The process is now completely automated, requiring no manual intervention," explains Longoria. "When we get a report that says there is a problem, an on-demand scan kicks off, and then either McAfee ePO software issues a report saying the problem was handled or a support ticket is opened for further investigation by a security specialist. No more having to schedule time with users, manually running the scans, and then checking back to make sure the scans dealt with the issue."

With the advent of this automated threat detection report, Longoria's staff realized that intrusive weekly full scans were no longer necessary. Today, a full scan is triggered only if the McAfee agent detects a potentially malicious file and is unable to clean it on the first pass. "We are essentially leveraging our SIEM investment to work smarter," says Longoria. "Minimizing the number of times full scans that are needed is a perfect example of this. "

Another way FIU works smarter is by tracking and comparing the current activity of networks and machines of interest in its environment against the previous year's historical data. Automatic alerts notify analysts when activity is deemed abnormal and include pertinent information about source and target involved in the anomaly. False positives are minimized because the past data is rolling data, comparing similar time periods one year later. FIU has also created automated reports to show which users and IP addresses are accessing which systems and is also working to automate the most common types of incident tickets.

> "By implementing McAfee Threat Intelligence, we have made our architecture much smarter. It helps our environment block thousands of threats each day, and users have no idea. Here's one example: recently, a back-door Trojan would have executed within our network if it had not been intercepted. McAfee Threat Intelligence works behind the scenes, doing its job phenomenally. We have only had to whitelist a handful of files."
>
> —Helvetiella Longoria, Chief Information Security Officer, Florida International University

Mitigating Risk Today and in the Future

"We will always face cyberthreats," says Longoria. "Our network is constantly scanned and probed. Our users receive attachments that are malicious and click on them. Thus, our main goal is to reduce risk, to block what threats we can and to make sure that, if there is a threat, we can contain it and mitigate it as quickly as possible. Besides educating our users, which we do a lot of, our main strategy is to maintain a multilayered, integrated, orchestrated, and sustainable defense."

To realize this vision, FIU continues to partner with Digital Arrow and with McAfee, both of which it deems critical to its future success. Next step is imminent deployment of McAfee Policy Auditor software to automate security audit processes, and McAfee Advanced Threat Defense for another level of threat analysis.

Automation will also continue to be a key element of the university's strategy to mitigate risk. "The ability to take needed action without having to manually intervene allows us to do more with less—and faster," notes Longoria. "The faster we can find out that there is a problem and contain it, the better. With everything integrated in McAfee ePO software and McAfee SIEM solutions, we don't have to spend a lot of time going over different applications and tools. The McAfee ePO software and SIEM dashboards allow us to quickly identify the problem, mitigate it—either by quarantining it or eradicating it—and determine exactly which system or systems are affected. Continuing to build in more automation will shrink the gap to containment even further."

"The faster we can find out that there is a problem and contain it, the better. With everything integrated in McAfee ePO software and the McAfee SIEM solutions, we don't have to spend a lot of time going over different applications and tools ... Continuing to build in more automation will shrink the gap to containment even further."

—Helvetiella Longoria, Chief Information Security Officer, Florida International University

McAfee

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com