FIREEYE™

CUSTOMER STORY

# USC Slashes Incident Resolution Time by 75% with FireEye Endpoint Security

UNIVERSITY OF SOUTH CAROLINA

## FACTS AT A GLANCE

**INDUSTRY**

Education

## CUSTOMER PROFILE

With a focus on enabling higher education and research, the University of South Carolina (USC) covers eight campuses across the state of South Carolina supporting 44,000 students with 10,000 faculty and staff. Founded in 1801, it is one of only 32 public universities to earn the Carnegie Foundation's top-tier designations in research activity and community engagement, and is a top producer of U.S. Fulbright scholarship students.

USC fosters an open learning environment that encourages online access to technical and educational resources. Without active and effective stewardship of key data — including medical data, credit card information, research data, intellectual property, government contracts. and other types of personally identifiable information (PII) — USC could be a serious target for cyber criminals.

"FireEye truly understands the challenges we face today. The wealth of experience and expertise built into its tools make us more effective in managing and executing our security strategy."

— **James D. Perry II**, Chief Information Security Officer. University of South Carolina

James D. Perry 11, USC's chief information security officer, shared, "In today's environment it's really a matter of when, not if, there will be a cyber security incident. Ensuring that our endpoints are configured securely and kept up to date — and that we understand what's happening to those devices — is critical to adequately protecting our information assets."

**Securing 60,000 endpoints**

USC has 60,000 endpoint devices distributed across its widespread environments with operating systems spanning Microsoft Windows. Mac OS, and Linux. And a range of hardware including desktops, laptops, tablets and mobile phones. While the university had a legacy endpoint security forensics tool, it lacked threat detection or automated deployment capabilities. The sheer number of endpoints creates a challenge, and in the event of an alert, Perry's team spent a significant amount of time simply trying to identify a point of contact let alone resolve an incident quickly.

Perry reflected, "We were looking for strategies and tools that could help us with swift incident response so we can immediately mitigate risk threats without being too resource-intensive. We also needed a central solution that could help us investigate and determine the broader picture across the entire infrastructure. Our evaluation of solutions led us to FireEye® Endpoint Security (HX)."

Tom Webb, USC's director of the information security operations team, recalled, "With HX we found the combination of both the forensic and the detection tools that we were looking for: It's a great value from that perspective."

He continued, "Implementation of HX was pretty easy; there's no detectible performance impact and it is seamless and transparent to users. New users easily understood how it would benefit them as we explained the process, and since it provides automatic upgrades to new software versions, there was no need for any additional user training."

**Automated updates and reduced detection time**

FireEye Endpoint Security delivers accurate alerts, Webb described, "HX produces very few false positives: When we do get a hit, we're confident that it's a true incident that we should immediately act on. With HX we have the ability to instantly quarantine an individually affected endpoint, which prevents the spread of any malware. With the detection capabilities we have from FireEye, we've been able to slash the industry average 'time to detection' by almost 98%!"

**Measuring the value of HX**

Prior to the installation of FireEye Endpoint Security, Perry's team would identify an average of 100 intrusion incidents a year. With HX in place, the team's ability to detect endpoint threats has increased significantly; with the elevated visibility uncovering an average of 250 breach attempts annually that potentially might not have been caught by traditional security solutions.

The reduction in time to detection has been accompanied by a similarly impressive drop in the time needed to resolve an incident once it has been identified. Webb noted, "With the introduction of FireEye Endpoint Security we've reduced our average resolution time by 75%! HX is able to rapidly pinpoint an affected machine, enabling investigation and remediation to begin immediately. Obviously the faster we eliminate a cyber attack, the better."

Perry concurred, "The ability for our team to respond quickly and return key IT assets back into service after an alert has enabled us to get critical buy-in from our faculty and researchers." USC has been able to save around 2,000 hours of the USC IT team's time spent just on intrusion investigation; equivalent to one full-time employee. Webb estimated, "It amounts to $100,000 worth of labor that we are able to utilize in more strategic ways."

> "IT is a strategic enabler that drives our ability to effectively educate our students. Utilizing FireEye Endpoint Security ensures that our IT assets are available, highly functioning, and secure, which is critical to achieving our mission."
>
> — **James D. Perry II**, Chief Information Security Officer. University of South Carolina

**Strategic value from an industry leader**

FireEye's monthly delivery of 'new threat trends' notes and its ongoing Indicators of Compromise (IOC) updates add value to USC's investment in HX. "Understanding what's happening from a global perspective gives us the edge over new types of attacks," stated Webb.

Perry summarized, "My experience with FireEye has been fantastic. It is recognized as an industry leader with the credentials that demonstrate it understands the issues we face. In fact, in many cases it pioneers the technology and processes that later become best practices. FireEye Endpoint Security enables me to promote good security practices and improve their adoption throughout USC. Consequently, it's been a critical part of our success in developing and achieving substantial systemic improvement."

To learn more about FireEye, visit: **www.FireEye.com**

**FireEye, Inc.**
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com



**About FireEye, Inc.**

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™