

FIREEYE AND FORESCOUT GET TOP MARKS FROM HILLSBOROUGH COMMUNITY COLLEGE



CUSTOMER PROFILE

Tampa, Florida-based Hillsborough Community College (HCC) successfully educates more than 44,000 students annually across 160 academic programs. The college is made up of five campuses comprising 64 buildings and 1.719 million square feet of space, spread over a total of 850 acres.

“I already had a really good experience with FireEye and knew the NX Series could deliver the information I needed to determine the exact nature of any malware challenges we were facing.”

— **Ken Compres**, Senior Network Security and Integration Engineer, HCC

A recent campus-wide “bring your own device” (BYOD) policy has given HCC students pervasive access to internal and online resources. With each user typically using smart phones and tablets or laptops to access information, the college experienced a massive spike in endpoint numbers and diversity.

The initiative emphasized the need for a robust security strategy to protect the extensive HCC network infrastructure that encompasses multiple server farms with several thousand access points. The person tasked with ensuring the integrity of the environment was Ken Compres, senior network security and integration engineer for HCC. He commented, “My top priorities were to achieve a level of visibility that enables us to classify devices and to begin tightening network access controls across the entire infrastructure.”

ACCESS AND PROTECTION

To further compound the challenges, Compres had to find the right balance between imposing severe access restrictions and creating an environment that was conducive to learning. He recalled, “My goal is always to facilitate convenient access to information and resources but

simultaneously provide an appropriately high-level of protection for everyone on the network without unnecessarily impacting the user experience.”

SEEING IS BELIEVING

To achieve his goal of pervasive visibility, one of the first components Compres deployed into the overhauled HCC environment was the FireEye® NX Series network security solution. He explained, “I already had a really good experience with FireEye and knew the NX could deliver the information I needed to determine the exact nature of any malware challenges we were facing.

“As soon as the FireEye solution came online we realized we had a major problem: We could see that hundreds of our devices were infected with malware, and it rapidly became obvious that our team wouldn’t be able to perform remediation fast enough to keep up.”

Compres was able to take the detailed FireEye Network Security information and use it to conclusively demonstrate to upper management that further investments would be needed to protect the college across all of its threat vectors. “Once I had

the FireEye data, I was able to accurately quantify the problem and get buy-in that we needed to take additional steps to secure our campuses,” stated Compres.

FORESCOUT TO THE FOREFRONT

One of the next elements in the college’s defense strategy was the selection of ForeScout CounterACT®. Compres elaborated, “We conducted an extensive study into the best solution for network access control, and ForeScout clearly stood out from the competition. The agentless approach enables us to quickly discover, classify and assess every device on our network, and then automatically remedy any issues.”

THE POWER OF TWO

HCC became one of the first organizations to recognize the potential of combining the strengths of the individual FireEye and ForeScout solutions. “It dawned on us that we could channel the information coming from NX over to CounterACT to further elevate our visibility and situational

awareness of connected devices across the entire infrastructure,” declared Compres.

HCC’s security team began creating the necessary interconnectivity between the solutions and shared its findings with engineers from both companies. The effectiveness of the pairing became the catalyst for the creation of a formal partnership between ForeScout and FireEye, and led to a joint release of ForeScout Extended Modules to facilitate data exchange and automated response between both solutions.

The power of the integrated approach was quickly demonstrated: One of the college systems became infected with CryptoLocker ransomware but its attempts to propagate across the HCC network were immediately detected by FireEye NX. Information relating to the attack was instantly communicated to CounterACT and the infected system isolated. “It was amazing to watch the scenario unfold,” observed Compres. “This malware could have encrypted all of the files accessible to this user — including network shares and documents — across our whole network. In the end, we had to only reimage one system.”

“My goal is always to facilitate convenient access to information and resources but simultaneously provide an appropriately high-level of protection for everyone on the network without unnecessarily impacting the user experience.”

— **Ken Compres**, Senior Network Security and Integration Engineer, HCC

ACCURACY, AUTOMATION AND EFFECTIVENESS

In another incident, a Hillsborough user inadvertently downloaded a malicious payload via email. “We started seeing a higher than normal volume of messages being sent from that person’s mailbox,” Compres recounted. “Following an instant exchange between ForeScout and FireEye, it was quickly determined the system was attempting malicious attacks against other network resources, and we were able to immediately halt things before any damage was done. The identical attack hit

a neighboring county and brought down a critical departmental email server for two days: That’s proof enough for me!”

The integration between FireEye and ForeScout provides Hillsborough Community College with the ability to respond to breaches in real-time, as well as enabling visibility into every device connected to its network. Compres summarized, “We don’t have a huge security team but the accuracy of the alerts and the automated response to issues really make a difference in our ability to protect an infrastructure of this scale.”

“Following an instant exchange between ForeScout and FireEye, it was quickly determined the system was attempting malicious attacks against other network resources, and we were able to immediately halt things before any damage was done...that’s proof enough for me!”

— **Ken Compres**, Senior Network Security and Integration Engineer, HCC

To learn more about FireEye,
visit: www.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 has over 5,300 customers across 67 countries, including more than 825 of the Forbes Global 2000.

FireEye, Inc.

1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com