FireEye
SECURITY REIMAGINED

U.C. Berkeley EECS engages FireEye for advanced malware protection

CUSTOMER STORY

SECURITY REIMAGINED

KEY COMPONENTS

- FireEye Network Threat Prevention Platform
- FireEye Threat Intelligence
- FireEye Forensics Analysis Platform

Located adjacent to San Francisco Bay, University of California Berkeley is ranked as the world's premier public university according to a recent U.S. News & World Report. As the university's largest single department, Electrical Engineering and Computer Science (EECS) is home to more than 1,500 undergraduate and graduate students. The pace of innovation and leading-edge research within the department combine to form a dynamic and stimulating environment for students, staff and faculty. For the EECS information technology team, attaining a balance that continues to foster learning, creativity and breakthrough thinking, without imposing unduly restrictive policies, is a constant challenge.

ACHIEVING RESULTS WHEN OTHERS FAILED

Following a successful proof of concept evaluation, a FireEye® Network Threat Prevention Platform was deployed to help protect the department. Fred Archibald, computing infrastructure manager for EECS, recalled, "We looked closely at several competing products,

COMPANY	UC Berkeley
INDUSTRY	Education
DESCRIPTION	The University of California, Berkeley is internationally recognized for excellence and pioneering achievements across many disciplines. The university has over 1,700 full-time faculty members and 35,000 students. The Department of Electrical Engineering and Computer Science (EECS) offers one of the strongest research and instructional programs anywhere in the world.
CHALLENGE	• Identify and deploy solution to address shortcomings in existing security product portfolio, while minimizing operational overhead and impact on users. To achieve the highest possible level of threat detection and remediation precision.
SOLUTION	• Deployment of FireEye Network Threat Prevention Platform, FireEye Threat Intelligence and FireEye Forensics Analysis Platform.
BENEFITS	• Highly accurate malware detection with nominal false positives, and real-time confirmation of malicious activity, independent of known signature- and pattern-based threats. Easy implementation, requiring no changes to existing processes or infrastructure, and low operational overhead.

> "FireEye keeps us ahead of the onslaught of continually escalating Web-based threats. I trust FireEye to give me the definitive expert view on how to protect our very unique environment."
>
> — **Fred Archibald, Computing Infrastructure Manager,** Department of Electrical Engineering and Computer Science, University of California, Berkeley

but the FireEye platform was very compelling. It was extremely easy to install, actually taking less than half an hour in total but more importantly it was immediately able to identify threats that had not been detected by the existing multiple layers of protection."

The FireEye Network Threat Prevention Platform is specifically designed to be deployed alongside other security gateways to identify zero-day threats that policy- and signature-based firewalls, Web gateways, intrusion prevention and anti-virus systems, fail to detect. A highly sophisticated virtual execution engine identifies both unknown and known malware.

Archibald observed, "Cyber criminals are making substantial and ever-increasing investments in malware, and new threats are constantly being introduced: There is no way that even a really good suite of traditional security applications can cope. The FireEye Network Threat Prevention Platform is so effective because it doesn't rely on existing signatures or patterns. It searches in real-time for any unusual or suspicious activities to determine if a behavior poses a legitimate threat. Once something malicious is detected, specific details are shared with subscribers of the FireEye® Threat Intelligence: Being a member of the worldwide FireEye community gives us a truly global perspective on malware outbreaks."

IRREFUTABLE PROOF

A consequence of working for a world-renowned university is the inherent expertise of the user population. Archibald explained, "Many of our users possess a highly detailed knowledge of computer science-related fields. This sometimes leads to requests for tangible proof for the reasons a potentially malicious piece of code has been intercepted or isolated.

Unlike conventional defenses, the FireEye platform actually confirms malicious activity and provides detailed descriptions of what was found. In addition, we can use the FireEye® Forensics Analysis Platform to do a forensic investigation and this enables me to convince even the most skeptical of users that an attack was real, and our remediation actions justified."

The FireEye Network Threat Prevention Platform has a well deserved reputation for its effectiveness and extremely low operational overhead. Archibald concurred, "Four years on and FireEye continues to deliver outstanding protection. It requires minimal routine management and delivers precision results with negligible false positives. It does the job so well that I can focus on other tasks, feeling confident that we are protected."

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**