FireEye
SECURITY REIMAGINED

Regional utility company uses FireEye to protect against advanced malware

CUSTOMER STORY

KEY COMPONENTS

- FireEye Network Threat Prevention Platform
- FireEye Central Management

Among the nation's largest publicly-owned utilities, providing energy to millions of electric and natural gas customers, the company understands the huge responsibility it has towards its own subscribers to ensure that its services are provided in a safe, reliable and responsible manner. To deliver on this commitment, there is a corporate-wide focus to lead the way to a secure energy future.

REPUTATION FOR FACILITATING REMEDIATION

In its quest to continually thwart the escalating plague of cyber-based attacks, the company explored the capabilities of the FireEye portfolio of malware protection platforms. The Utility's information security supervisor commented, "We were sufficiently impressed with the results of our research to implement a proof of concept using a FireEye® Network Threat Prevention Platform."

COMPANY	Regional Utility Company
INDUSTRY	Energy and Utilities
DESCRIPTION	Among the nation's largest regional utility companies, the organization provides energy services to millions of electric and natural gas customers throughout its multi-thousand square-mile territory.
CHALLENGE	• Identify easy to deploy solution to combat the next generation of threats, including zero-day and targeted APT attacks, to supplement legacy security defenses across corporate infrastructure. Need to optimize efficiency of information security team and maximize accuracy of detection and blocking.
SOLUTION	• FireEye Network Threat Prevention Platform • FireEye Central Management
BENEFITS	• Rapid deployment capabilities, centralized management and industry-leading levels of threat monitoring safeguard the integrity of the organization's extensive network and IT infrastructure. Exemplary false positive performance and highly detailed alert reporting enable the company's information security team to focus on remediating advanced malware.

> "Because of the business we're in, we have to be equipped to handle threats from anywhere across the globe. FireEye gives us visibility beyond that provided by other technologies."
>
> — **Information Security Supervisor**, Regional Utility Company

The FireEye Network Threat Prevention Platform can be deployed out-of-band or inline to monitor threats that legacy gateways allow to pass unimpeded. When used inline, unfamiliar code and suspicious web pages are stress tested using tightly controlled detonations to block polymorphic and zero-day malware and targeted APT attacks. The Utility's security team also evaluated the FireEye® Central Management (CM) that functions as a security event repository and facilitates the centralized management and operational control of distributed FireEye platforms.

FIRST IMPRESSIONS ARE LASTING ONES

The information security supervisor stated, "The FireEye Network Threat Prevention Platform was exceptionally easy to install and we found the FireEye CM interface to be very intuitive. The platform immediately affirmed the bulk of our infrastructure was clean but did detect the presence of a certain malware in our network and allowed us to zero in on a specific workstation for remediation. We ran the proof of concept for a few weeks and then purchased everything we were evaluating: It was an easy decision."

He added, "Since the very first day of deployment we have only ever seen one false positive! This has given us the confidence to aggressively pursue every threat alert in the knowledge that actual malicious potential has been detected."

The FireEye CM and initial FireEye Network Threat Prevention Platform were complemented by the purchase of additional NX Series platforms to provide comprehensive protection for the full network and infrastructure. To further enhance the effectiveness of the implementation, the team participates in the FireEye® Threat Intelligence that connects FireEye platforms and FireEye research feeds into a real-time global exchange of data on confirmed, emerging threats.

The information security supervisor concluded, "Because of the business we're in, we have to be equipped to handle threats from anywhere across the globe. FireEye gives us visibility beyond that provided by other technologies."

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