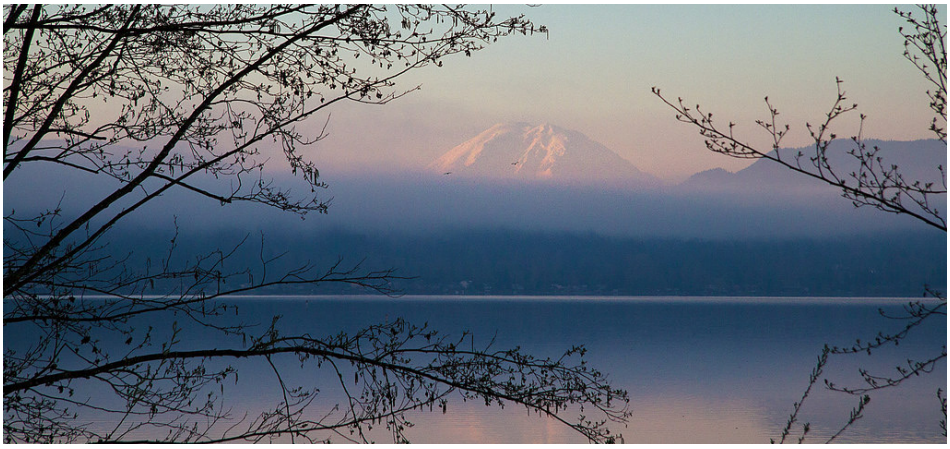
CUSTOMER STORY

Community Recovers After Ransomware Attack

City of Sammamish Deploys FireEye Solutions to Create Resilient Infrastructure



The City of Sammamish often is cited as one of the United States' most idyllic towns. A strong sense of community, wealth of local amenities and outdoor recreational space, admirable public-school system, family-oriented neighborhoods, and comfortable quality of life have garnered Sammamish honors such as being named Forbes "Friendliest Town in the U.S." and one of CNN Money's "Best Places to Live".

The city provides a wide range of public services, including passport and building permit issuance, while contracting out a select few others, including water, sewage, fire and police. Most City Hall functions are supported using a Windows-based environment comprised of 130 endpoints and servers virtualized using VMware, while Amazon Web Services enables the remaining city operations.

Not Business as Usual

On one eventful day, as employees first arrived at work, they struggled to log into email accounts and connect to the Internet. Normally a well-organized, highly functional organization, the whole of City Hall was shocked to find business had come to a grinding halt. Less than three hours into the workday the IT department issued a blanket shutdown of all systems; something serious had seized control of the network.

Ransomware messages monopolized server consoles, rendering all the city's online services unusable. City staff had to revert to pencil-and-paper processing and their services were only accessible to those residents that visited City Hall in person.

FACTS AT A GLANCE

INDUSTRY

Local Government

SOLUTIONS

- FireEye Email Security—Cloud Edition
- FireEye Network Security
- FireEye Endpoint Security—Cloud Service
- FireEye Helix

BENEFITS

- Efficient solution deployment generates immediate protection
- Contextual threat intelligence-powered forensic analysis provides deep situational awareness
- Proactive file analysis detects and prevents phishing and malware execution

CUSTOMER PROFILE

Nestled between Lake Sammamish and Snoqualmie Valley, and a short drive from Seattle, lays the City of Sammamish. It is the 13th largest city in the state of Washington with a population of 65,000 and ranked 1st in Forbes 2012 list of the "Friendliest Towns in the United States". The City of Sammamish is overseen by a seven-member, publicly elected City Council and served by 130 city employees.

> "The best way to prevent an attack like we suffered is to be proactive, and the type of protection that FireEye offers is exactly what an organization needs in order to stay one step ahead of the enemy."
>
> — **Stephen Schommer**, Interim IT Director, City of Sammamish

Sammamish's city manager immediately jumped into action, declaring an emergency to expedite the process of contracting cyber security consultants to help remediate the situation. The FBI also was informed of the incident. A full cohort of security experts and federal agents were onsite by nightfall.

United Against a Common Foe

Two days later, a call to the local emergency management network brought community members out in droves to offer their support to the restoration efforts. Volunteers from nearby Microsoft offices, the University of Washington, and even the water districts and utilities of adjacent cities all came together to lend their expertise. By the end of the week, Stephen Schommer—a cyber security expert who came out of retirement to help the city—had joined the undertaking and was quickly offered the position of interim IT Director to help lead resurrection of the environment.

"One of my first priorities—based on positive experiences at a previous employer—was to reach out to FireEye, and the response was tremendous: Things started happening immediately," recalled Schommer. "FireEye Network Security was very easily configured and implemented with help from FireEye's technical support department. FireEye Email Security and FireEye Endpoint Security are cloud-based, so getting those into place was rather simple too. I was able to start the remediation process almost immediately because deploying the core security infrastructure was so rapid."

The forensic consultants the city contracted at the onset of the emergency found that the earliest indication of the malware's presence occurred a month prior to the actual ransomware event as remote desktop protocol activity on a single PC. To further investigate the attack's behavior and effectively remediate, the city needed to be able to efficiently correlate and analyze security data from various sources. The solution to this problem was FireEye Helix, a security operations platform that brings cloud-native benefits to security practitioners. FireEye Helix can use the AWS Athena service to perform ad hoc queries on large datasets with results in seconds. The City of Sammamish harnessed the power of FireEye security coupled with AWS storage, compute and analytics to perform advanced forensic analysis for their VMware and AWS environments. This analysis determined the exact endpoint the malware exploited and revealed that an employee had clicked a malicious email link and enabled the ransomware to gain residency and access.

FireEye Email Security is designed to continually and proactively adapt defenses to protect against exactly the type of email-borne threats that the city suffered. Schommer explained, "FireEye Email Security reads every email, opens every attachment and follows every link it finds to analyze the data for malicious content. It blocks dangerous files from executing while allowing clean files into the network. It's a great product for protecting the email threat vector."

Back on Track

The remediation was a success: The ransomware was eradicated across the city's environment and online services resurrected. "Forensic analysis confirmed that no personal information was compromised at the city during the attack. Going forward, the residents of Sammamish can take confidence in knowing that the city now has

> "One of my first priorities—based on positive experiences at a previous employer—was to reach out to FireEye, and the response was tremendous: Things started happening immediately."
>
> — **Stephen Schommer**, Interim IT Director, City of Sammamish

an integrated suite of state-of-the-art security solutions protecting all of their data," declared Schommer.

As FireEye solutions monitor activity across all threat vectors, there is a constant exchange of threat intelligence that helps ensure a unified response in the event of a suspected breach. Schommer stated, "The value that FireEye brings to the city greatly exceeds the costs we would have incurred had the ransom been paid."

Schommer knew from his prior experience working with FireEye that the company was the right resource for Sammamish in its hour of need. He enthused, "FireEye employees are very receptive and responsive, and they take cyber security very seriously. The professional relationships I've developed with the staff at FireEye give me confidence to know that if I call them, I'll get answers that will work; they understand the landscape and know how to quickly remediate the problems we're dealing with."

Reflecting on the event, Schommer acknowledged how much the city has learned through the experience and is now applying towards keeping the community's services safe in the future. "The City Council was already pursuing a path to scale the city's IT department and infrastructure, and they continue to remain very supportive of the effort," shared Schommer. "New processes and procedures have been implemented to keep the environment secure. Everyone who does business with the city, as well as employees and contractors, is now made to take ongoing cyber security awareness training."

One Step Ahead with FireEye

"I really like FireEye cyber security solutions because of the company's depth of expertise, and for its track-record in successfully protecting a huge variety of environments," concluded Schommer.

"Cyber criminals are only going to get progressively more resourceful and more aggressive. Nobody is immune from getting hit, and reacting to a threat is frequently very difficult and painful. The best way to prevent an attack like we suffered is to be proactive, and the type of protection that FireEye offers is exactly what an organization needs in order to stay one step ahead of the enemy."

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™