



CUSTOMER STORY

City and County of San Francisco

Comprehensive Threat Protection Provided by FireEye



FACTS AT A GLANCE

INDUSTRY



State and local government

SOLUTIONS

- FireEye Network Security
- FireEye Endpoint Security
- FireEye Email Security

BENEFITS

- Comprehensive threat protection
- FedRAMP authorized email security service
- Responsive support
- Easy to use

CUSTOMER PROFILE

The City and County of San Francisco is situated in Northern California and is world famous for being a cultural, commercial, financial, and tourism center. The city covers an area of 47.9 square miles on the north end of the San Francisco Peninsula. It is the thirteenth-most populous city in the United States with over 870,000 residents.



The government of the City and County of San Francisco is distinguished by being the only consolidated city-county in California. It has an annual budget of ten billion dollars that is overseen by an elected mayor, board of supervisors, and officers. The organization employs staff to support over 60 separate departments to serve the residents.

Nathan Sinclair, manager of the Cyber Security Defense Center for the City and County of San Francisco, plays a key role in protecting the city and maintaining multiple FireEye solutions. He explained, “We support the IT infrastructure for city departments; they connect to the internet via our network, and we’re effectively serving as an internal ISP for the city.”

Starting with FireEye Network Security

Sinclair and his team were looking for a way to boost network protection for the city. When he visited the FireEye booth at a security conference, Sinclair was intrigued by FireEye Network Security. “We started talking with FireEye and received a behind-the-scenes tour of how it works; the whole ‘nuts and bolts,’” Sinclair recalled.

“I really like the direction that FireEye is going. I like that it doesn’t just look at one aspect of security; everything is looked at as a whole.”

— **Nathan Sinclair**, Cyber Security Defense Center manager, City and County of San Francisco

FireEye Network Security detects and stops attacks that traditional security products miss and allows organizations to rapidly respond to threats. The FireEye patented, signature-less Multi-Vector Virtual Execution (MVX) engine and Intelligence-Driven Analysis (IDA) technology are at the heart of FireEye Network Security, identifying and blocking both known and zero-day threats. The actionable intelligence from FireEye Network Security gives context to security staff so they can promptly prioritize and respond to alerts.

Sinclair’s department concluded that FireEye Network Security would be a valuable investment and subsequently deployed it inline, where threats are immediately blocked and investigated. “It’s to the point now that I’m actually afraid of removing FireEye Network Security because I see everything that it catches,” declared Sinclair. “It finds things on local computers that the anti-virus program misses. I’ll send a report to the department and if needed they will then re-image the offending machine. We don’t have any other security components that cover what FireEye Network Security does: It’s pretty amazing in what it catches!”

Adding FireEye Email Security

Based on its success with FireEye Network Security, Sinclair’s department added FireEye Email Security (available as FireEye Government Email Threat Prevention (ETP) Service in the FedRAMP Marketplace). The service meets the FedRAMP security requirements and has been granted an Authority to Operate (ATO) by the U.S. Department of the Interior (DOI). It enables government entities to save time and money as they add email security for cloud services such as Microsoft® Office 365 or Google® Mail.

Sinclair has been impressed by his experience with FireEye Email Security. He noted, “We are a Microsoft Office 365 shop and while the in-built security is not bad, it can’t

catch everything. We like that FireEye Email Security can tie into FireEye Network Security to help us more thoroughly identify threats.”

Bringing in Endpoint Security

Most recently the City and County of San Francisco purchased FireEye Endpoint Security to protect, detect, and respond to threats across a wide variety of laptop and desktop devices both on or off the managed network. It provides protection from the most common malware, advanced behavioral analytics to detect and block the advanced threats and frontline intelligence to help security analyst rapidly understand attack activity and respond accordingly.

“City departments have been looking to us for direction around endpoint security,” Sinclair shared. “We’re excited that when we put FireEye Endpoint Security on a laptop, it has the ability to gather threat intelligence – even when the user is not in the office – and then correlates all of the logs with FireEye Network Security when it is reconnected so instant action can be taken if it has been infected with malware.”

Service and Simplicity

Sinclair is delighted with the support he gets from FireEye. He emphasized, “When I need guidance from an expert, they’re there, and that’s huge for me! I don’t want to have to wait on the phone for hours; it’s nice to know that when I call they’ll immediately answer and ask how they can help.”

The ease of use of the FireEye solutions also means a lot to Sinclair. “I look at FireEye Network Security as a ‘black box.’ After plugging it in and providing a basic configuration, we just leave it alone. That’s it. I can literally walk away and know that it’s doing its job,” observed Sinclair.

He concluded, “I really like the direction that FireEye is going. I like that it doesn’t just look at one aspect of security; everything is looked at as a whole.”

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

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. CS-EXT-CS-US-EN-000135-01

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.

