



# Air Academy Federal Credit Union

## Ahead of the Cyber Security Curve with FireEye



### FACTS AT A GLANCE

#### INDUSTRY



Finance

### CUSTOMER PROFILE

The Air Academy Federal Credit Union (AAFCU) was founded in 1955 to serve cadets and staff of the nearby United States Air Force Academy at Lowry Air Force Base, located in Denver, Colorado. At its launch it only had 27 members, one location and just over \$4,000 in assets. Today, AAFCU's assets total in excess of \$500 million with eight branches and almost 50,000 active accounts.

Having experienced more than 60 years of growth and change, the four pillars of AAFCU's foundation have remained solid: A commitment to service, quality, community, and integrity for its account holders. By extension, because of setting such high standards for itself, AAFCU has a strong focus on cyber security and protecting the integrity of its customers' information.



### Challenge

The threat landscape is continuously evolving, with increasingly sophisticated malware being discovered every day. Jeremy Taylor, network manager for AAFCU, reflected, "Our mindset has changed over the years from the premise that a secure perimeter should be sufficient to stop malicious attacks, to assuming that at some point the outer defenses will be breached. This has fueled the need to implement a robust, multi-level security strategy that identifies and mitigates any threats that do make it into our infrastructure."

With a centralized team of IT professionals covering all eight branches of its business, AAFCU focuses on operating as effectively and efficiently as possible. "We've always implemented best-in-class security solutions, and we try to lock down the environment as much as possible," Taylor noted, "but there's always the possibility of someone finding a way through; the potential for compromise is always there."

### Solution

When a high-profile breach of a nationally known retail chain occurred, AAFCU decided it was time to further enhance its defenses. "Industry publications highlighted that FireEye had been called on to assist in the containment and clean-up of the breach. This put the company on our radar and after a thorough

## “FireEye is keeping us out of the news, and this is a really good thing!”

— **Jeremy Taylor**, network manager, Air Academy Federal Credit Union

investigation of viable options, we decided that FireEye would be the ideal partner to meet our needs,” recalled Taylor. “It was clear that FireEye was capable of detecting threats that other solutions just weren’t catching.”

The credit union selected FireEye® Network Security (NX Series) — incorporating the signature-less FireEye® Multi-Vector Virtual Execution (MVX) engine — for protection against known and zero-day advanced attacks; FireEye® Email Security (EX Series) to block targeted email spear phishing — by far the most common vector for attacks; and FireEye® Central Management (CM Series) for central control of and correlation across devices in the network.

“We tested the FireEye solutions and confirmed that they were picking up malware that was getting past some of the other defenses. The ability to expose malware in a wide range of encrypted traffic was impressive.” Taylor stated. “The solutions are affordable too. I could not have asked for a better scenario.”

### Results

With the implementation of Email Security, Taylor’s team immediately started seeing spear phishing attempts being halted. “Every day AAFCU receives around 6,400 emails — of which half are junk or spam — the bad guys are sending us messages with malicious attachments, frequently encrypted via TLS [Transport Layer Security] to avoid detection by our firewall,” Taylor explained. “FireEye Email Security validates every message that contains links and attachments. Over the past year it has blocked about 100 malicious email-based attacks, including ransomware and multiple cryptolocker-type threats, which would otherwise have made it through.”

FireEye blends technology and robust intelligence to protect against sophisticated persistent cyber attacks, many of which are being employed for the delivery of ransomware. By being deployed inline, the FireEye solutions can detect and block threats in real time, preventing any damage from being done.

“FireEye Network Security serves as our ‘canary in a coal mine’ just in case something gets past our other defenses,”

described Taylor. “AAFCU has very stringent security policies; any potentially malicious activity to a specific location is automatically blocked so that all phases of the attack lifecycle are not only identified but prevented before any significant damage is inflicted.”

FireEye Central Management enables Taylor and his team to monitor network-wide traffic for malware in real time and to correlate data from different vectors. Being able to initiate simultaneous upgrades across all Network and Email Security appliances allows the AAFCU team to maximize use of its operational resources. Moreover, having visibility into region- and industry-based threat trends enables the credit union’s defenses to be tuned using the most up-to-date information. “FireEye is keeping us out of the news, and this is a really good thing!” stated Taylor.

With a security solutions provider that matches its four pillars of service, quality, community and integrity, AAFCU is confident that FireEye will help protect its account holders’ information from even the most advanced cyber-security attacks. Furthermore, FireEye provides increasing value to the organization by saving the IT team time. “The cyber attacks that hit institutions like health organizations, department stores, and so on really spurred us to purchase FireEye solutions,” Taylor reflected. “They are able to instantly block these advanced malware attacks.

“When I talk to other IT organizations that aren’t using FireEye, I’m astonished they experience so many spurious alerts. When they ask, ‘How much time do you spend investigating false positives?’ I sometimes feel bad when I tell them, ‘It doesn’t happen with FireEye!’”

Taylor concluded, “Bad guys have done their research; they’ve uncovered the positions and roles that staff have in the credit union, and they’ve tried to target these employees through spear-phishing campaigns. However, their attempts do not get past FireEye.

“Our employees are highly protected and never see malignant emails; we have FireEye to thank for that.”

To learn more about FireEye, visit: [www.FireEye.com](http://www.FireEye.com)

### FireEye, Inc.

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

© 2018 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.AAFCU.US-EN-062018

### 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 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

