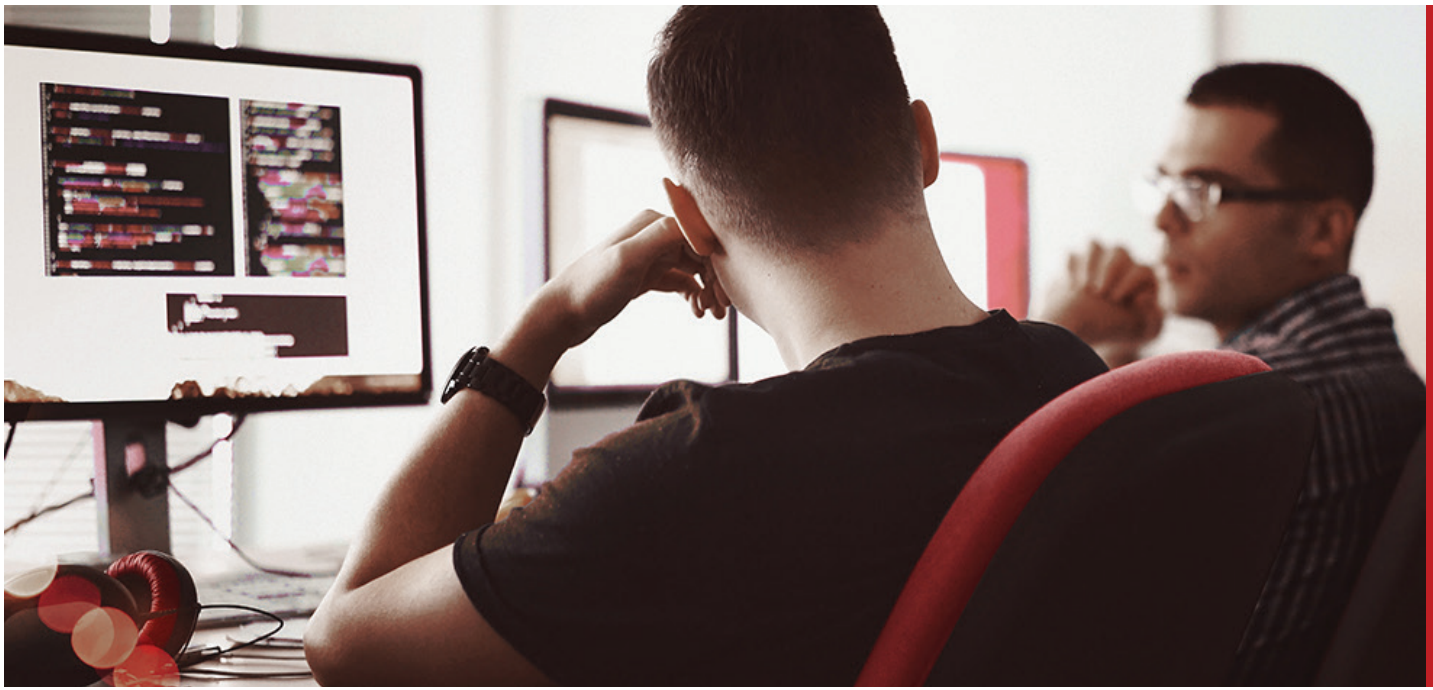
CASE STUDY

Petroleum Refiner Overhauls Security Infrastructure

Small team strengthens security posture and responds faster to threats



HollyFrontier

Customer Profile
Fortune 500 independent petroleum refiner and distributor

Industry
Oil and gas

IT Environment
4,000 endpoints in US, 800 in Canada, China, and the UK

By replacing critical components of its security infrastructure with integrated McAfee solutions, this small security team transformed its ability to defend against cyberthreats. The result: easier management, stronger protection, and faster detection and correction.

HollyFrontier is a Fortune 500 independent refiner and distributor of petroleum products. The company operates six refineries—five in the middle of the US and one in Ontario, Canada. The company employs 3,500 people across 43 sites in the US, 16 in Canada, and a handful of locations in China and the United Kingdom.

Search for Better Endpoint Protection Leads to Revamped Security Architecture

As part of an endpoint security review, HollyFrontier invited six leading vendors to make presentations in competition for the business. McAfee stood out from the other vendors with its integrated security strategy and attainable vision of a threat defense lifecycle that learns and adapts to meet changing requirements.

"We agreed wholeheartedly with the McAfee® approach," says Cybersecurity Engineer Phillip Fort, the main person responsible for HollyFrontier's day-to-day security posture. "With the integrated McAfee ecosystem, our limited security team can automate a lot of security tasks. We can essentially do a lot more to protect our company a lot faster, without adding staff."

In addition to McAfee endpoint protection and its bundled McAfee ePolicy Orchestrator (McAfee ePO) central console, in just a few weeks, HollyFrontier deployed:

- McAfee Network Security Platform intrusion prevention system (IPS) appliances.
- McAfee Data Exchange Layer, the open-source fabric that connects security components to automate integration and real-time data exchange.
- McAfee Threat Intelligence Exchange, which aggregates threat intelligence from local and global sources and shares file reputation information across McAfee Data Exchange Layer-connected systems.
- McAfee Enterprise Security Manager and other components of the McAfee SIEM solution set.
- McAfee Advanced Threat Defense sandboxing appliance.

Within a year, the company also began deploying McAfee Endpoint Threat Defense and Response and McAfee Web Gateway.

Infection Rate and Ransomware Reduced Dramatically

HollyFrontier initially deployed the McAfee Complete Endpoint Threat Protection suite. However, because of "all the ransomware going around," HollyFrontier was anxious to install McAfee Endpoint Security and its Dynamic Application Containment (DAC) functionality. When DAC encounters a file that does not have a trusted reputation or is unknown, it immediately quarantines the file before it can infect "patient zero." Consequently, as soon as McAfee Endpoint Security became available, the company migrated the McAfee VirusScan® Enterprise portion of its endpoint protection suite to the McAfee Endpoint Security Threat Prevention module, first rolling out version 10.1, then upgrading to version 10.2, and upgrading again to version 10.5.

Although DAC initially blocked a few legacy applications that are still used, Fort was able to quickly create exclusions for those applications. "The McAfee Endpoint

Challenges

- Manage security effectively with limited staff.
- Increase visibility across extended enterprise.
- Minimize time from detection of threats to protection.

McAfee Solution

- McAfee Active Response
- McAfee Advanced Threat Defense
- McAfee Complete Endpoint Threat Protection
- McAfee Endpoint Security
- McAfee Endpoint Threat Defense and Response
- McAfee ePolicy Orchestrator® (McAfee ePO™)
- McAfee Network Security Platform
- McAfee SIEM: McAfee Advanced Correlation Engine, McAfee Enterprise Log Manager, McAfee Enterprise Security Manager, McAfee Event Receiver, McAfee Global Threat Intelligence for SIEM
- McAfee Threat Intelligence Exchange

Security graphical user interface is very easy to use," he notes. "Once I created the first couple exclusions, the rest were easy."

It didn't take long for the biggest impact of the new endpoint protection framework to became evident. "After implementing McAfee Endpoint Security and DAC, our malware infection rate plummeted," states Fort. "We used to have ransomware attacks each month, but we have had none since migrating to McAfee Endpoint Security and integrating it with McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense … Truthfully, I don't have to deal with McAfee Endpoint Security very much—and that's a good thing."

Results of Sandbox Analysis Automatically Shared Throughout Enterprise

As Fort contemplated the benefits of an integrated security platform prior to its implementation, the integration he was most excited about was that of the endpoint and other security components with the McAfee Advanced Threat Defense.

"McAfee Advanced Threat Defense does as much or more than other sandboxes, but its integration with other McAfee solutions is what makes it so incredibly powerful," says Fort. "It immediately detects and contains a potentially malicious file on the endpoint, IPS, or gateway.

First it sends the file automatically to McAfee Advanced Threat Defense for analysis, and, if found malicious, the file is then automatically removed across the entire enterprise. That is truly transformative for our small security team," states Fort. "It augments our own abilities and saves us a lot of time."

Every day a security analyst checks McAfee Advanced Threat Defense to review the list of files that the appliance has convicted as malicious. "Once an administrative assistant clicked on a phishing email," explains Fort. "The IPS, McAfee Network Security Platform, blocked the suspicious file and sent it to McAfee Advanced Threat Defense, which determined that it was bad. The file appeared in the day's list of convicted files, and we confirmed that it was indeed blocked and automatically entered in the McAfee Threat Intelligence Exchange reputation database shared throughout the enterprise."

Periodically, the HollyFrontier security team runs assessments in which sample malware is put on a machine. "We then watch to make sure the malware shows up in McAfee Advanced Threat Defense and is removed from the host machine and blacklisted throughout the enterprise," clarifies Fort. "It works every time—just as it's supposed to."

Increasing Visibility and Facilitating Reporting with McAfee SIEM

The desire for better visibility across the enterprise drove HollyFrontier to replace its aging SIEM with the McAfee SIEM technology. According to Fort, McAfee SIEM technology provides a much more complete security picture and widespread visibility across the network, which helps in countless ways. To cite just one example, a considerable number of users were becoming locked

- McAfee Web Gateway
- McAfee Platinum Support

Results

- Malware infection rate slashed.
- Vulnerabilities eliminated much faster.
- Time-to-protection reduced significantly across environment.
- Reduced operational overhead and easier management.

out as they tried to reset their passwords because they had failed to log off other machines. A security analyst simply entered the user ID in the McAfee SIEM system, and immediately could see exactly which machines a user was logged into, whether or not he was locked out, and whether he should have access—and then could reset passwords as necessary. "In that case and many more, McAfee Enterprise Security Manager technology saves us a lot of investigative time," says Fort.

The HollyFrontier security team also uses many out-of-the-box rules and alerts, as well as custom ones within the McAfee SIEM solution. "Even if we haven't developed a custom rule, if I have just a little information on a security event, it is easy to drill down and do a search based on single or multiple variables to find as much additional information as I need," explains Fort.

The McAfee Enterprise Security Manager solution also makes reporting easier. For example, to produce a quarterly security review to upper management, Fort simply runs out-of-the-box executive reports created by the McAfee SIEM solution and McAfee Advanced Threat Defense from within McAfee ePO software.

Rapid Searching Saves Time, Eliminates Vulnerabilities Faster

According to Fort, before learning about the McAfee integrated security platform, he had "fallen in love" with an endpoint detection and response (EDR) product from another vendor. "When we looked at McAfee Endpoint Threat Defense and Response, however, we realized it did everything that other solution did," he recalls. "It gives us all the information we ever wanted to know—really, really fast."

With the McAfee EDR software, the HollyFrontier security team can eradicate vulnerabilities much faster. If Fort learns of a vulnerability in a specific version of an application—for instance, in Microsoft Office 2013—he can use the McAfee Active Response search functionality to quickly and easily find out exactly how many desktops have that version or create a list of all endpoints with that version. It took less than a minute for one of Fort's colleagues to find all versions of Adobe Acrobat in the enterprise recently and just a few more minutes to determine which endpoints required updating. After pushing out the update, he clicked to rerun the search to confirm that all the updates were successful.

"The rapid searching we can do using McAfee Active Response saves us a tremendous amount of time," says Fort. "We used to manually maintain inventory spreadsheets of all the various applications and systems. Now we can run real-time reports in seconds, and everyone is confident they are correct."

Adding Hybrid Web Protection

At a McAfee user conference, while Fort was singing the praises of McAfee Network Security Platform and McAfee Advanced Threat Defense to other attendees. Many of the participants were raving about McAfee Web Gateway, claiming it was their favorite McAfee product, prompting Fort to investigate. He quickly became convinced that McAfee Web Gateway was worth the investment, even though the company had an adequate

"The rapid searching we can do using McAfee Active Response saves us a tremendous amount of time. We used to manually maintain inventory spreadsheets of all the various applications and systems. Now we can run real-time reports in seconds, and everyone is confident they are correct."

—Phillip Fort, Cybersecurity Engineer, HollyFrontier

web gateway solution. In addition to being able to share threat information in near real time with the other McAfee Data Exchange Layer-connected security solutions, McAfee Web Gateway offers more granular control and the ability to deploy a hybrid environment managed from the same console.

As a result, HollyFrontier is in the process of deploying its first McAfee Web Gateway appliance and McAfee Web Gateway Cloud Service. HollyFrontier employees working from home or on the road will be protected by the same corporate web security policies as users at corporate locations. In addition, any malware detected by McAfee Web Gateway is sent immediately to McAfee Advanced Threat Defense, and its information is shared throughout the enterprise.

Integration and Increased Protection Ease Security Administration

"With the McAfee integrated security infrastructure and McAfee ePO software, I can manage just about everything through one pane of glass," says Fort. "That alone makes administration so much easier, but so does increased protection. If there is an infection somewhere else in the world, thanks to McAfee Threat Intelligence Exchange, my network knows about it and is protected before the infection even reaches us. If, on the other hand, the malware is detected within our environment, it is immediately sent to McAfee Advanced Threat Defense for analysis, and the rest of the environment is automatically informed. We have reduced operational overhead dramatically while improving our security posture."

Fort has not only been impressed with McAfee products and their integration with one another, but also with McAfee personnel. "Any time I need anything, I just call or email my McAfee Security Engineer, and he responds right away," he notes. "McAfee Platinum Support is also extremely responsive. I can usually get the help I need within a couple of minutes. We learned early on that McAfee is a strategic security partner as well as a dependable one."

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

3458_0817
AUGUST 2017