CASE STUDY

Oil and Gas Leader Gains Visibility and Boosts Endpoint Defenses

McAfee® endpoint and EDR solutions help resolve threats faster for the company's critical infrastructure and for its remote workers

Oil and Gas Infrastructure Company

Customer Profile
This leading North American oil and gas infrastructure company owns or operates more than 90,000 miles of pipelines and 200 terminals.

Industry
Oil and gas

IT Environment
16,000 endpoints

This leading North American oil and gas company, with offices throughout the U.S., sought to boost its overall endpoint security with a comprehensive next-generation solution set that included advanced Endpoint Detection and Response (EDR) functionality. With 16,000 endpoints, the company augmented its on-premises McAfee endpoint protection with cloud-based MVISION products.

Connect With Us

For nearly a decade, this oil and gas company relied on McAfee endpoint and data protection to safeguard its more than 10,000 employees, 16,000 endpoints, and factory operations. In 2019, it made a decision to upgrade and further fortify its defenses remotely and on premises. For a company of its size, it has a relatively small security team.

According to the IT security manager, the volume and sophistication of threats was rapidly escalating. The company was experiencing multiple challenges. A top priority was to better secure and stabilize the company's critical infrastructure, which was, in his words, "constantly on the threat firing line." Additionally, existing on-premises web tools could not provide visibility into the security of endpoints used by employees working remotely. The security team also decided to beef up protection for its mission-critical servers.

Responding to Security Priorities That Changed on a Dime

In 2019, the IT security team launched an initiative to modernize and strengthen its security infrastructure. As a starting point, the IT security manager renewed the company's McAfee endpoint protection. He and his team realized that the best route to take was a multilayered solution that provided the breadth and depth of coverage they were lacking. He upgraded to McAfee® Complete Endpoint Protection, a fully integrated solution with a single-agent architecture and advanced technologies: machine learning analysis, containment, and endpoint detection and response (EDR).

This powerful and comprehensive suite replaced legacy McAfee endpoint technologies that the oil and gas company had used in the past. McAfee Complete Endpoint Protection suite includes Threat Prevention with advanced malware scanning features to defend against emerging and targeted attacks. This combined with exploit prevention mitigates against fileless attacks, ransomware, and zero-day attacks. The solution's Web Security component keeps the company's users safe from accessing malicious or unauthorized websites. Finally, the built-in Firewall feature blocks suspicious inbound and outbound network traffic.

McAfee Complete Endpoint Protection was the right choice because it provides a platform where additional integrated defenses can be easily added with the advantages of the single, centralized management McAfee® ePolicy Orchestrator® (McAfee ePO™) console.

"We don't want shelfware. Rather, we try to implement all the features of the products and solutions we deploy," said the IT security manager. "We've had outstanding results with McAfee."

Challenges

- Provide a more robust defense for the critical infrastructure, which was under continual attack
- Improve time to detect, investigate, and remediate threats
- Provide visibility and better protection for all systems used by the remote workforce, along with on-premises endpoints and servers
- Streamline and centralize security management
- Minimize infrastructure complexity and cost in a hybrid environment

McAfee solutions

- McAfee® Complete Endpoint Protection
- McAfee® MVISION Endpoint
- McAfee® MVISION EDR
- McAfee® Application Control for Servers

"We've done several successful investigations with MVISION EDR on some pretty nasty threats. The product has been invaluable in helping us quickly identify issues and block attacks. Putting in MVISION EDR gives us the visibility we needed to systems that connect to malicious sites, so we can block or quarantine them."

—IT Security Manager, Oil and Gas Company

Expanded Visibility and Accelerated Detection, Investigation, and Remediation

When he learned about the device-to-cloud protection delivered by McAfee® MVISION Endpoint, the IT security manager worked closely with McAfee to launch several proofs-of-concept (PoCs). The product was put to the test against two competing vendors.

McAfee® MVISION EDR was a hands-down winner, due to its integration capabilities, attractive pricing, and lack of dependency upon a complex and costly infrastructure. The IT security manager was so impressed that he began the rollout effort in October 2019.

When the pandemic hit in March of 2020 and employees were forced to work remotely, there was a heightened sense of urgency to complete the deployment. The security team undertook an aggressive push to implement MVISION EDR. Even though they were under a tight timeline, they completed the task in just two weeks. Thanks to the help and collaboration of the McAfee technical support experts, the process was smooth and efficient.

Now, with most of the company's staff working at home, MVISION EDR enables the IT security manager and his team to expand visibility into threats across all endpoints and to prioritize alerts. They are able to leverage artificial intelligence-guided investigations and automation to improve threat analysis and threat-hunting, thereby speeding up time to response.

"Where other products have failed, McAfee has succeeded. I am a big fan," asserted the IT security manager.

Results

- An integrated device-to-cloud platform that covers all endpoints—on premises and remote
- Improved visibility and efficiency with centralized, single-pane-of-glass management
- Alert prioritization and more productive investigations leading to faster, more accurate detection and remediation
- Single-vendor approach, with lower total cost of ownership
- Reduced infrastructure requirements
- Accurate inventory control and licensing tracking for computing resources

Stopping Attacks Before They Do Harm

Since the onset of the remote work environment, the company has experienced a much higher volume of campaigns by sophisticated threat actors. In each of these cases the visibility provided by MVISION EDR has helped the IT security manager and his team identify patient zero and follow the trajectory of the attack to get an indication of the potential impact. MVISION EDR has helped them determine every lateral movement that took place and allowed them to analyze endpoints to see if they were affected.

"We've done several successful investigations with MVISION EDR on some pretty nasty threats," explained the IT security manager. "The product has been invaluable in helping us quickly identify issues and block attacks. Putting in MVISION EDR gives us the visibility we needed into systems that connect to malicious sites, so we can block or quarantine them."

Continuing their intent on not having "shelfware," the IT security manager and his team also found a novel use for MVISION EDR outside the realm of traditional security: inventory tracking. They can easily check registry settings to monitor system licensing and can also ensure proper configurations. When they roll out new tools in the factory environment, for example, they use MVISION EDR to make sure systems are working properly and communicating the way they should.

During and after implementation, the IT security manager and his team have leaned heavily on McAfee for ongoing support. "I cannot say enough good things about McAfee and the support that their team have provided. We've always had access to the right people when we've needed them. We've enjoyed a great relationship with McAfee," he remarked.

McAfee

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com