CASE STUDY

Convenience Store Retailer Centralizes Security for Easier Management and Enhanced Endpoint Protection

McAfee integrated security platform helps small security team safeguard data across stores, headquarters, and remote workforce

Convenience Store Chain

Customer Profile
Major American convenience store chain

Industry
Retail

IT Environment
20,000 IT and IoT endpoints across more than 700 locations

By consolidating seven endpoint security tools and six consoles into one McAfee integrated security platform with a central management console, this American chain of hundreds of convenience stores reaped many benefits. In addition to increasing the efficiency and effectiveness of its small security team, the company improved its overall security posture and gained granular visibility across all of its endpoints.

Connect With Us

When M.T., an information security analyst, joined this American retailer, its small security team used multiple tools and consoles to protect its 20,000 endpoints—16,000 store point-of-sale devices, 2,000 servers, and 2,000 employee PCs with multiple versions of Windows, MacOS, and Linux operating systems. "Just keeping all the tools up to date was a challenge, and some tools, like EDR, were largely ignored because of the additional steps required to use them" recalls M.T. "We also had no way to grasp the larger picture."

In addition, if there was an incident, the security team had to jump from one console to the next trying to gather the information needed to understand what had happened and respond appropriately. They also wanted to apply policies to specific types of devices—such as only to point-of-sale machines—or to exclude specific machines from policies, but either lacked the flexibility or the time needed to do so.

Consolidating Management for More Effective and Efficient Endpoint Protection

After exploring options to lessen the burden of managing endpoint protection, the company's security team chose to implement the McAfee Endpoint Security suite and other McAfee endpoint security and data loss prevention (DLP) solutions. "We chose McAfee not for one particular product but for the entire integrated platform," notes M.T. "Going with McAfee let us consolidate a lot of solutions and manage a wide range of security functionality across multiple environments, all through one interface. With McAfee, we are way more efficient and effective than we were before."

Dramatically Reducing Management Burden for Small IT Team with Limited Resources

The company implemented a wide range of endpoint and data protection functionality from McAfee—antivirus, endpoint encryption, endpoint threat detection and response (EDR), network and host DLP, and dynamic sandboxing, among others. All of this functionality is managed by the McAfee MVISION ePolicy Orchestrator (McAfee ePO) centralized management console.

"In our environment, the McAfee integrated ecosystem replaced seven different security tools and six vendors' management consoles," says M.T. "The difference in ease of management was night versus day."

The security team deployed all four McAfee Endpoint Security (ENS) modules: Threat Prevention, Web Control, Firewall, and Adaptive Threat Protection—all of which improve protection and consolidate security functionality. With the Threat Prevention module, for instance, they gained superior ability to protect, detect, and correct security issues as well as replaced a device control tool. The Firewall module replaced a host intrusion prevention tool. And Adaptive Threat Protection introduced machine learning behavioral analysis, dynamic application containment to quarantine unknown files and real-time scanning driven by cloud-based analytics.

The Web Control module of McAfee ENS replaced a web filtering tool and enabled the security team to enforce safe Internet use for its remote workforce. When a

Challenges

- Reduce the management burden for small security team
- Safeguard PII and comply with PCI regulations
- Build a strong defense across retail stores and corporate offices against sophisticated attacks, including ransomware and advanced malware

Solutions

- McAfee® Active Response
- McAfee® Advanced Threat Defense
- McAfee® Application Control
- McAfee® DLP Discover
- McAfee® DLP Endpoint
- McAfee® Drive Encryption
- McAfee® Endpoint Security
- McAfee® File and Removable Media Protection
- McAfee® File Integrity Monitor
- McAfee® MVISION™ ePolicy Orchestrator® (McAfee MVISION ePO™)
- McAfee® Threat Intelligence Exchange

company-owned PC is not at corporate or connected via VPN, Internet access is blocked. Since remote users must connect via VPN anytime they want Internet access, whether for business or personal use, they connect more often, which provides the security team better visibility into the remote workforce as well as allows for more frequent updating and patching of their devices.

Saving Time, Improving Visibility, and Accelerating Incident Response

"Having antivirus, encryption, EDR, device control, host intrusion prevention, and other protection all accessed from the same interface is more than just helpful," states M.T. "It saves us significant time and hassle. Not having to jump between tools to deploy new software, update existing software, or investigate incidents is also huge timesaver."

"In addition, McAfee ePO gives us a big picture view that helps us manage security posture and speed incident response," adds M.T. "The main dashboard gives a high-level view of all the McAfee tools, but we can also drill down for highly granular details from each component. For instance, if an incident occurs, I can immediately assess the security posture of an affected device, then click to view the entire event timeline, pre-event to post-event…What triggered the event? Was there a registry change or DLL injection, for example? An unknown app running? An AV signature triggered? A HIPS alert? All the information is available in one place."

Proactive Protection through Integration and Bidirectional Threat Intelligence

The information security analyst points to McAfee Threat Intelligence Exchange (TIE) as one of his favorite aspects of the integrated security platform. Threat Intelligence Exchange aggregates global and local threat information in a threat reputation database and shares that information in near real time throughout the enterprise using the Data Exchange Layer (DXL) client software and broker.

For instance, malware encountered on an endpoint by McAfee Endpoint Security provides critical insights that are immediately shared via Threat Intelligence Exchange with all other endpoints as well as McAfee EDR for faster threat hunting and remediation. If an endpoint encounters an unknown file, that file can be automatically quarantined while the company's McAfee Advanced Threat Defense (McAfee ATD) sandbox appliance analyzes it. If McAfee ATD determines the file is malicious, then that information is immediately conveyed across the enterprise.

"With Adaptive Threat Protection, it's also quick and easy to proactively protect our endpoints when we learn of new IoCs for ransomware or whatever the latest threat is," says M.T. "Even if we don't yet have a DAT, we can throw in a hash or filename and deploy it with a couple clicks to all nodes within five minutes or let it deploy automatically within an hour."

Results

- Reduced administrative burden of small information security team
- Replaced six separate management consoles with one for easier, more efficient management
- Gained big picture view of security posture in addition to granular visibility
- Faster incident investigation and response
- Superior protection with greater flexibility for policy enforcement and remediation

Flexibility to Deploy and Enforce Highly Granular Policies in Multiple Ways

Before deploying McAfee ePO and McAfee Endpoint Security, the retailer's security team was limited in the policies it could enforce. "With McAfee, we can build highly granular policies using the system tree or by tagging devices based on IP, custom properties set up during installation, or base attributes such as device type or operating system," notes M.T. "We use tagging all the time—for example to exclude specific devices for an update or update only specific devices."

Since switching to McAfee, the security team has been able to deploy and customize many more policies to block potential bad actors than they could before. For instance, using the Access Protection and Exploit Prevention functionality of McAfee Endpoint Security, they can quickly and easily implement policies to block known malicious files from being downloaded or restrict users' access to applications that are unnecessary or known to be vulnerable to bad actors. They also have multiple ways to implement such policies—such as by hash, filename, or program file path. In the past, they either couldn't create and enforce such policies or lacked the time and effort to do so.

Protecting PCI and PII Data

To safeguard consumers' credit cards and other personally identifiable information (PII), the security team deployed McAfee DLP Endpoint host-based protection and a McAfee Network DLP Discover appliance. They took the McAfee DLP solution's built-in PCI and PII default profiles and added additional key terms specific to its business. For store devices, McAfee DLP blocks all unauthorized USB device access. For other endpoints, McAfee DLP monitors data at rest and in motion, automatically blocking any unauthorized attempts at exfiltration, such as through websites or external media. Alerts from both DLP solutions appear in the McAfee ePO dashboard.

Defending Against Tomorrow's Threats

Always working to improve security to defend against future threats, the retailer's security team is in the process of testing McAfee Application Control to lock down payment servers and eliminate yet another tool and management console. They are also testing McAfee MVISION Insights to identify global and local threat campaigns, prioritize risk level, and respond proactively.

"Having the McAfee integrated security platform as our foundation lets us manage cybersecurity with a small team," says M.T. "We haven't needed to add headcount as we adapt to meet the changing threat landscape."

> "In our environment, the McAfee integrated ecosystem replaced seven different security tools and six vendors' management consoles. The difference in ease of management was night versus day."
>
> —M.T., Information Systems Analyst, American Convenience Store Chain

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

McAfee, the McAfee logo, MVISION, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2021 McAfee, LLC. 4704_0221
FEBRUARY 2021