CASE STUDY

Enhancing Automated Threat Protection Bolsters Defenses Against Zero-Day Attacks

Integrating McAfee® Advanced Threat Defense and the Bro open-source network security platform widens the scope of threat detection to include unmanaged devices

Multinational Software Company

Customer Profile
Large global software company

Industry
Technology

Environment
Fluid environment with up to 150,000 endpoints at any given time, many of them virtual, across 20 countries

Automated submission of threat information to McAfee Advanced Threat Defense and automated sharing of that information across the enterprise improves protection while saving security operations time and hassle.

Connect With Us

This large global software company with more than 20,000 employees in 20 countries has implemented an IT infrastructure that is highly virtual and fluid. Systems come and go daily on the company's network. For instance, in a recent week, 45,000 systems, including virtual machines, connected to the corporate network. However, during peak periods, up to 150,000 endpoints can be connected. For the company's senior manager of security engineering, who oversees the team responsible for deployment of all security tools across the global enterprise, this environment poses distinct challenges.

Challenge: Close Gaps to Block Zero-Day Attacks

Although the company employs the McAfee Complete Endpoint Threat Protection suite on all its high-risk physical and virtual endpoints, it also has many virtual endpoints connecting to its network that do not have a McAfee agent installed and are therefore not updated with the latest threat protection via the McAfee ePolicy Orchestrator (McAfee® ePO™) management console. The company's more important virtual machines host a McAfee agent but many "low-risk" systems do not. Until recently, if one of these unmanaged endpoints downloaded a malicious file, the McAfee ePO software-managed endpoints would be at risk because they had no way of knowing of the existence of that threat within the environment.

"Zero-day threats are our biggest concern," remarks the senior manager of security engineering. "If any of our endpoints—managed or unmanaged—downloads a zero-day threat, we want our whole environment to know about it, and we want to be able to react appropriately as fast as possible."

In addition, if a managed endpoint became infected, security analysts would receive an alert, but, because of the fluidity of systems coming on and off the network, by the time an analyst has logged in and has attempted to find the suspicious payload, the system could easily have moved offline, essentially removing the information needed to understand what had transpired. As a result, security operations center (SOC) engineers found that they had to spend extra time tracking down infected systems and remediating them.

Hunting and Blocking Zero-Day Threats with McAfee Advanced Threat Defense

Along with McAfee Complete Endpoint Threat Protection, the company had implemented the Data Exchange Layer (DXL) communication fabric and McAfee Threat Intelligence Exchange. DXL connects and optimizes security actions across multiple vendor products, as well as internally developed and open source solutions, and McAfee Threat Intelligence Exchange leverages DXL to bi-directionally share threat information across all DXL-connected systems. To this automated threat reputation-sharing framework, the company added McAfee Advanced Threat Defense for "zero-day hunting," as the senior manager of security engineering describes the appliance's main role.

Challenges

- Protect against zero-day threats across extended global enterprise
- Shrink detection to remediation gap

McAfee solution

- McAfee® Advanced Threat Defense
- McAfee® Complete Endpoint Threat Protection
- McAfee® ePolicy Orchestrator®
- McAfee® Threat Intelligence Exchange

Results

- Accelerates time to protection, thanks to automation
- Augments threat reputation information shared across McAfee ePO software-managed devices with information gleaned from incidents involving unmanaged devices
- Facilitates endpoint incident forensics and accelerates response
- Saves security operations time and hassle

"If an unknown or suspicious file comes across one of our endpoints protected by McAfee Endpoint Security, the file is automatically sent to McAfee Advanced Threat Defense for sophisticated static and dynamic behavioral analysis," explains the senior manager of security engineering. "If McAfee Advanced Threat Defense deems the file to be malicious, its reputation is then automatically broadcast via McAfee Threat Intelligence Exchange to all the endpoints connected to DXL. This automatic distribution of threat reputation information helps us block zero-day threats before they can harm our environment."

Enhancing Intrusion Detection with Bro

But what about threats entering the environment through the company's many unmanaged endpoints? To extend detection to these systems, the company turned to the open-source Bro network security monitoring platform. Bro ingests the company's network traffic off a span or inline tap and converts the traffic data into logs and metadata in binary format. In a typical week, Bro submits approximately 6,000 files to McAfee Advanced Threat Defense for analysis. Of those, approximately 10% to 20% end up in the McAfee Threat Intelligence Exchange threat reputation database and are subsequently shared throughout the enterprise.

"Bro gives us the ability to retain network traffic in a searchable format, which is extremely useful," the senior manager of security engineering explains. "For instance, using Bro, we can search for source or distributed IP so we can easily conduct lightweight investigations—discover who or what connected to a specific IP address, what the payload looks like, determine the packet size, and so on."

The information captured by Bro supplements the threat information delivered via the McAfee Global Threat Intelligence cloud and disseminated via McAfee Threat Intelligence Exchange. With the Bro script and advice provided by McAfee (now available as a deployment kit), the senior manager of security engineering's team integrated Bro with McAfee Advanced Threat Defense so that the Bro traffic data is automatically submitted to McAfee Advanced Threat Defense, just as suspicious files from McAfee Endpoint Security are automatically submitted through McAfee Threat Intelligence Exchange. Since the team was already very familiar with Bro, the integration was straightforward.

Automatic Immunization Against Threats that Hit Unmanaged Endpoints

"If one of our unmanaged endpoints downloads a malicious file, Bro will capture that event among the network traffic and submit it to McAfee Advanced Threat Defense for analysis," notes the senior manager of security engineering. "If McAfee Advanced Threat Defense determines the file is malicious, then that malicious reputation will be shared automatically with every McAfee ePO software-managed system in our entire enterprise—in other words, with all the systems we care about. Put another way, if one of our unmanaged virtual machines downloads a malicious file, all of our managed devices automatically receive an immune shot."

Facilitating and Accelerating Incident Response

With the McAfee Advanced Threat Defense/Bro integration and threat reputation information automatically disseminated across endpoints via McAfee Threat Intelligence Exchange, inoculation of endpoints happens much faster than it did before. Consequently, there is a much greater likelihood that a system will "receive the immune shot" before it goes offline. In addition, because the actual event and surrounding intelligence is captured by Bro, even if the system goes offline, McAfee Advanced Threat Defense, as well as security analysts, have a great deal more information to help determine appropriate action, and, if necessary, to remediate more quickly.

"With the McAfee automated threat framework and supporting intelligence from the Bro integration, plus automated remediation that we have also set up, our SOC very rarely needs to pay attention to endpoint incidents," points out the senior manager of security engineering. "The Bro integration and all that automation save a ton of time."

To fortify its defenses further, the company continues to build upon its DXL-based integrated security framework. For instance, the company is currently in the process of adding McAfee DLP Monitor to gather, track, and report on data in motion across its entire network and augment its McAfee DLP Endpoint host-based data protection. "The more we can integrate our systems and automate responses, the safer we will be," says the senior manager of security engineering.

> "Put another way, if one of our unmanaged virtual machines downloads a malicious file, all of our managed devices automatically receive an immune shot."
>
> —Senior Manager, Security Engineering, Large Software Company

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com