CASE STUDY

Telecom Company Shrinks Time to Detect and Respond to Cyberthreats

Cloud-based EDR and a McAfee® integrated security platform streamline investigations and enable proactive threat hunting

European Telecom Company

Customer Profile
Large European mobile and fixed telephony provider

Industry
Telecommunications

IT Environment
8,000 endpoints

To bolster its security posture and reduce the gap from detection to remediation, this large European mobile and fixed telephony company added McAfee® MVISION™ Endpoint Threat Detection and Response along with McAfee® Advanced Threat Defense sandboxing and other solutions to its integrated security infrastructure. As a result, the security operations team caught more malware, improved workflows, shaved days off incident investigations, and became proactive threat hunters without needing additional headcount or expertise.

Connect With Us

This large telecom provider, which provides millions of phone lines to customers in Eastern Europe, has relied on McAfee solutions for many years to protect its 8,000 endpoints. Despite several strong competitors, it has grown rapidly and become a major mobile operator brand. With such a competitive environment, the company continually faces pressure to keep prices—and therefore costs—low and cybercriminals at bay in order to protect customers' personally identifiable information (PII) as well as the company's reputation.

A Smarter, More Efficient Security Ecosystem

The telecom company's information security architect joined the company several years ago—in large part because the company relied on McAfee as a foundation for its security infrastructure. "I had worked previously with McAfee solutions and experienced how well they worked together," says the security architect. "I like the McAfee strategy of creating a security ecosystem in which systems share relevant threat information among themselves, making every tool smarter and the whole environment more secure."

An integrated security system with a central management console also helps streamline operations, reducing the security operations team's burden. The security architect and other administrators use McAfee® ePolicy Orchestrator® (McAfee® ePO™) software as a single pane of glass to manage not only a wide range of McAfee endpoint and data protection solutions but Microsoft Defender as well.

Concerned about ransomware and other advanced threats, the company decided to enhance its existing McAfee infrastructure by upgrading its on-premises endpoint protection to cloud-based McAfee® Endpoint Security, adding McAfee® MVISION™ Endpoint Threat Detection and Response (MVISION® EDR), and implementing two McAfee Advanced Threat Defense appliances for dynamic and static sandboxing. As with the company's other McAfee solutions, the company deployed them and manages them using McAfee ePO software.

Simplifying Endpoint Protection and Improving Threat Detection and Prevention

By implementing McAfee Endpoint Security, the security operations team simplified endpoint protection, reducing multiple technologies—including Threat Protection, Firewall, Web Control, and Adaptive Threat Prevention—to a single agent. Unlike traditional antivirus software, McAfee Endpoint Security also leverages connections between local endpoints and McAfee® Global Threat Intelligence in the cloud to detect zero-day threats in near real time. As soon as a threat has been identified on any endpoint, that information is shared with all the other endpoints. And if one of the company's endpoints encounters an unknown or suspicious file, the file is dynamically quarantined until it can be analyzed, whether via MVISION EDR or by a McAfee Advanced Threat Defense sandbox.

Challenges

- Provide a more robust, proactive defense to safeguard customers' personal information
- Accelerate time to detect, investigate, and remediate cyberthreats
- Reduce operational burden of the security operations team

McAfee Solution

- McAfee® Advanced Threat Defense
- McAfee® Endpoint Data Loss Prevention
- McAfee® Endpoint Security
- McAfee® ePolicy Orchestrator® (McAfee® ePO™)
- McAfee® File and Removable Media Protection
- McAfee® MVISION™ Endpoint Threat Detection and Response
- McAfee® Native Encryption
- McAfee® Network Data Loss Prevention

> “The volume of malware we have to deal with has definitely shrunk since implementing McAfee Endpoint Security. But adding MVISION EDR as well has made an even bigger impact on security posture. When our endpoints do encounter malware, we can now respond many times faster and more effectively than ever before.”
>
> —Information Security Architect, Large European Telecom Company

“The volume of malware we have to deal with has definitely shrunk since implementing McAfee Endpoint Security,” notes the security architect. “But the addition of MVISION EDR has made an even bigger impact on security posture. When our endpoints do encounter malware, we can now respond many times faster and more effectively than ever before.”

Faster, Easier Investigation and Time to Remediation

Before implementing MVISION EDR, the operations team had only tedious, manual methods to try to investigate suspicious files or incidents. “A typical threat investigation used to take multiple days or a week or was even ignored because we just didn’t have that amount of time to spend,” explains the security architect. “Now there is no reason to ignore anything. From first detection of a malicious file to the start of remediation is typically 10 to 15 minutes, rather than days.”

Since the McAfee Advanced Threat Defense appliances and MVISION EDR are integrated with the company’s McAfee® SIEM solutions and McAfee ePO software, when a suspicious file or behavior is detected at the endpoint, the company’s SIEM automatically triggers an investigation in MVISION EDR. McAfee ePO software alerts can also trigger an investigation. Within MVISION EDR, advanced analytics and artificial intelligence (AI) help administrators understand the alert, fully investigate, and quickly respond.

“MVISION EDR does all the investigative preparation for us, collecting all the relevant details automatically—IP addresses, device information, users, and so on—and reducing thousands of artifacts to the 100 or so that are relevant,” continues the security analyst. “Then graphic visualizations show how the various artifacts relate to one another, and AI-guided investigations help us quickly understand what’s happening. Best of all, we don’t have to be experts to use it, so more staff can perform investigations.”

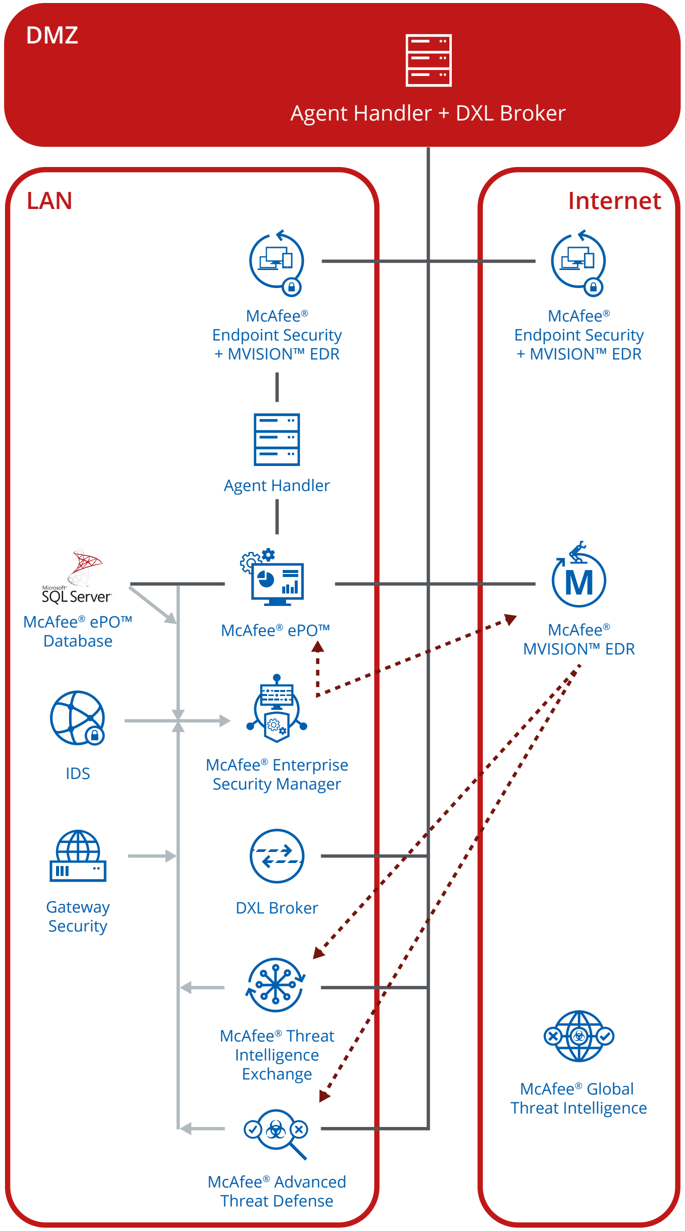
In addition, the security operations team uses MVISION EDR to run real-time queries to determine if anything similar has occurred anywhere else in the environment. They also conduct historical searches. MVISION EDR takes a snapshot of a device or devices at a given point in time, allowing the security team to investigate an incident later in greater depth.

McAfee Solutions (continued)

- McAfee® SIEM solutions: McAfee® Enterprise System Manager, McAfee® Log Manager, McAfee® Event Receiver, McAfee® Advanced Correlation Engine, McAfee® Global Threat Intelligence for McAfee® Enterprise Security Manager
- McAfee® Threat Intelligence Exchange

Results

- Time to investigate threats slashed from days to minutes
- Ability to investigate real-time and historic incidents with existing staff and skill sets
- Simpler but more effective endpoint protection
- More proactive defense from threat information sharing and automatic actions
- More efficient security operations and easier administration thanks to central console and integrated security platform
- Reduced hassle and expense due to a single-vendor approach


DMZ
Agent Handler + DXL Broker
LAN
Internet
McAfee® Endpoint Security + MVISION™ EDR
McAfee® Endpoint Security + MVISION™ EDR
Agent Handler
Microsoft SQL Server
McAfee® ePO™ Database
McAfee® ePO™
McAfee® MVISION™ EDR
IDS
McAfee® Enterprise Security Manager
Gateway Security
DXL Broker
McAfee® Threat Intelligence Exchange
McAfee® Global Threat Intelligence
McAfee® Advanced Threat Defense

A More Proactive Security Posture

Now that McAfee MVISION EDR is continuously monitoring and gathering data to provide the visibility and context needed to detect and respond to threats, the company can also maintain a much more proactive defense than ever before. “Proactive threat hunting is one of the biggest benefits for us,” claims the information security architect, who also praises the solution’s detailed reporting functionality and customization capabilities.

The company also improved its proactive stance by implementing an integrated security infrastructure that shares threat information bidirectionally throughout the enterprise via the Data Exchange Layer (DXL). For instance, when a malicious file has been detected at an endpoint, whether blocked by McAfee Endpoint Security immediately or quarantined and determined malicious by investigation or sandbox analysis, that information is automatically added to the McAfee Threat Intelligence Exchange threat reputation database and shared with all DXL-connected systems connected—which today includes all the company’s endpoints, its McAfee SIEM, McAfee Advanced Threat Defense sandboxes, and MVISION EDR software, as well as its Cisco pxGrid infrastructure. The company plans to integrate more third-party tools with the DXL in the future.

Preparing for the Future

Like many organizations, this telecom company is beginning its move to the cloud, starting with Microsoft Office 365 and Microsoft Azure. In the near term, it plans to keep the McAfee ePO management console on premises but intends to soon transition management of endpoint protection for Internet-only users to the cloud-based McAfee® MVISION ePO™.

"Taking measured steps to augment our security infrastructure has helped us succeed at keeping our company and customers secure," concludes the company's security architect. "It's nice to know that McAfee can support us wherever we are in our journey and can extend our integrated security infrastructure from device to cloud when we're ready."

> "A typical threat investigation used to take multiple days or a week, or was even ignored… Now there is no reason to ignore anything. From first detection of a malicious file to the start of remediation is typically 10 to 15 minutes, rather than days."
>
> —Information Security Architect, Large European Telecom Company

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