CASE STUDY

Federal Court System in Chile Benefits from Automation and Stronger Protection

New McAfee endpoint security technology helps combat ransomware, reduce manual intervention, increase visibility, and streamline management

Poder Judicial of Chile

Customer Profile
The Poder Judicial of Chile is one of the three branches of the nation's government and includes the Supreme Court, 17 appellate courts, and 465 lower courts.

Industry
Government

IT Environment
Multiple locations throughout Chile with approximately 6,550 endpoint nodes running Microsoft Windows XP, Windows 7, and Windows 10

The Poder Judicial (Judicial Authority) for the nation of Chile upgraded its existing McAfee solutions—including the management console and endpoint security—in order to ensure stronger and faster detection and prevention of ransomware attacks, do more with fewer resources, and gain visibility to threats and endpoint security posture.

Connect With Us

Matías Luengo is the system administrator supervising Poder Judicial's IT and security team, which includes a total of seven technicians whose main focus is on managing user requirements, making sure systems are up and running, applying security patches to endpoints in a timely fashion, and overseeing the McAfee® ePolicy Orchestrator® (McAfee ePO™) management console. Following stringent, self-imposed security requirements, team members make it a practice to regularly run security checks on applications used by employees and on data archives to ensure that they are free from infection that could compromise network operations.

Ransomware Attack Prompts an Upgrade to McAfee Endpoint Security

Recently, the government agency was hit with WannaCry ransomware, which had infected hundreds of thousands of Windows endpoints at commercial and government organizations in more than 100 countries worldwide. WannaCry spreads rapidly from machine to machine and locks up files with encryption so that they cannot be accessed. Perpetrators demand payment to unlock the files and threaten to delete the files if the ransom is not paid.

For the Poder Judicial, this was a serious security event that could have resulted in shutting down certain operations internally and reducing availability of services to court systems used by thousands of Chilean citizens every day.

Luengo and his team acted quickly to forestall the threat to the sensitive data housed on the organization's endpoints and spent a great deal of time and effort to manually block the outbreak and prevent it from spreading. Additionally, they created and applied new policies—and this also was done manually. At the time, the team was using an older version of the McAfee ePO, v. 5.3 management console and McAfee® VirusScan® Enterprise, v. 8.8.

This event prompted Luengo to seek greater efficiencies through automation. He made the decision to upgrade Poder Judicial's endpoint defenses to McAfee ePO, v. 5.9 software and McAfee Endpoint Security, v. 10.5. Partnering with McAfee sales engineers and technicians, he and his team migrated McAfee Endpoint Security to 6,550 Microsoft Windows-based nodes throughout the organization in less than a week's time.

Faster Incident Detection and More Effective Response Through Automation

Currently, Poder Judicial is running many of the collaborative defenses included in the solution—namely adaptive, advanced threat defense, web control, firewall, and Data Exchange Layer (DXL). This powerful combination of technologies automates actions and provides stronger and deeper insights into threat activity. All this helps Poder Judicial contain zero-day threats like ransomware, save patient zero, and prevent network infection. DXL makes it possible for multiple

Challenges

- Protect user endpoints against ransomware attacks
- Improve visibility to threats across the entire computing infrastructure
- Reduce time-consuming manual processes for creating and enforcing policies
- Ensure a secure user experience for employees
- Simplify and centralize security management

McAfee solutions

- McAfee Endpoint Security
- McAfee ePolicy Orchestrator (McAfee ePO) software

technologies to share threat intelligence, enabling Luengo and his team to gain insights and to pinpoint where infections are occurring so that they can act swiftly.

Luengo himself is at the helm of McAfee ePO software. This centralized single-pane-of-glass management tool enables him to monitor, investigate, and respond to threats. The updated version has vastly simplified security administration and provides complete visibility to endpoints across the entire Poder Judicial infrastructure. Luengo especially appreciates its user-friendly dashboard with its graphical interface. Now he can see the "top 10" threats responsible for the most frequent security violations and can easily produce monthly management reports. Thus far, based on metrics he obtained from the McAfee ePO console, he discovered that McAfee Endpoint Security has blocked and/or eliminated 232,000 threats at Poder Judicial.

"Ever since we made the upgrade to McAfee Endpoint Security, we no longer have to spend time manually blocking threats. The new tools detect advanced threats and automatically block, and, in some cases, completely eliminate them," points out Luengo.

Security Transformation Positively Impacts IT and End Users

He also pointed out that the new McAfee tools have resulted in other advantages. Prior to deployment, the security team experienced connectivity issues, but now, as Luengo notes, "Everything is running smoothly." Additionally, automation has significantly reduced the burden on his staff, allowing the team to spend time on more strategic projects.

"With the new, more agile tools, we're benefiting from many efficiencies. We've reduced the amount of time spent on configuration and deployment. Plus, threat detection is faster, easier, and more efficient, thanks to built-in automation features in McAfee Endpoint Security," reports Luengo.

Additionally, Luengo comments on how the human factor contributes to the proliferation of malware. In the past, users would routinely connect USB drives infected with Trojans or viruses to their computers, and these threats often went undetected. While users haven't changed their behavior, with the help of McAfee Endpoint Security and easy enforcement of new policies via McAfee ePO software, malware introduced by external drives is no longer an issue.

Results

- Fully integrated endpoint security with protection against potentially crippling ransomware attacks
- Automated blocking of threats before they do harm
- Simplified and comprehensive security management, reporting, and policy enforcement
- Visibility to endpoint security posture across the entire environment
- Less consumption of computational resources and less manual intervention
- Transparent user experience that maximizes productivity and minimizes disruptions

From an end-user standpoint, he finds that the solution operates quickly and transparently. "Previously, we had to contact the user in order to make updates and remotely take over their systems. That's no longer necessary, as it's all done internally. Users can continue to be productive and work without interruption," he emphasizes.

Deployment of Advanced Features on the Horizon

Luengo and his team look forward to the advanced features built into McAfee Endpoint Security. They have already initiated a proof-of-concept (PoC) for both Dynamic Application Containment (DAC) and Real Protect. DAC relies on automation to contain zero-day threats when malicious behaviors are detected and keeps them from infecting endpoints. Real Protect uses machine learning to classify threats and applies that knowledge to increase the efficacy of detection and remediation processes. They are also currently running a PoC for integration of DXL and McAfee Threat Intelligence, which will provide insights on the security reputation of files and content. DXL, a bi-directional communications fabric, enables sharing of this intelligence with other security components, enabling them to detect and prevent threats from spreading.

McAfee Simply Works

Luengo has enjoyed a long-term relationship with McAfee because, as he says, "McAfee always finds the threats. Why would I go anywhere else?" He even went so far as to run side-by-side comparative tests with a competitive product and found that, when serious incidents occurred, McAfee was far more effective.

He has no hesitation about recommending an upgrade to McAfee Endpoint Security to his colleagues at other government agencies, and, in fact, he has already spoken with a colleague at the National Registry of Chile about its many benefits.

> "With the new, more agile tools, we're benefiting from many efficiencies. We've reduced the amount of time spent on configuration and deployment. Plus, threat detection is faster, easier, and more efficient, thanks to built-in automation features in McAfee Endpoint Security."
>
> —Matías Luengo, System Administrator, Poder Judicial (Chile)

McAfee
Together is power.

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

3740_0218
FEBRUARY 2018