CASE STUDY

McAfee
Together is power.

Security Transformation Begins with an Integrated and Automated Endpoint Defense

McAfee helps taxation bureau cut operational costs, speed incident response, and simplify management

South American Government Agency

Customer profile
This South American government agency collects sales tax, individual income tax, and corporate tax.

Industry
Government

IT environment
Multiple locations throughout the country with approximately 5,600 PCs and notebooks running Microsoft 10.5

This South American government taxation bureau revamped its entire security infrastructure with integrated McAfee solutions—from endpoint protection to advanced threat intelligence sharing—to proactively protect against advanced threats and ransomware, reduce administrative costs, and simplify security management while increasing visibility and speeding incident response.

With the high prevalence of advanced attacks and global ransomware attacks making headlines, the endpoint security engineer at a South American government taxation bureau, decided to launch a complete overhaul of the organization's endpoint security infrastructure. Although the taxation bureau had not suffered any notable major attacks, the endpoint security team believed they needed a stronger defense against today's sophisticated and ever-evolving threats.

Top of mind for the security team is ensuring full availability of the services that enable 14 million citizens to file tax returns online by the March deadline every year and to receive their refunds in a timely fashion. "If this operation is not carried out, the impact to our nation could be significant. It's imperative that these processes not be interrupted," said the endpoint security engineer.

Like other public and government entities in the country, the taxation bureau is required to comply with regulation ISO 27001 PMG, which clearly spells out stringent requirements for a comprehensive endpoint and data security strategy. For both network and endpoint security teams, best practices dictate security assessments of both internal and external systems to discover vulnerabilities and determine the level of risk associated with these.

Integrated Security Drives Transformation

The endpoint security engineer initiated his organization's security transformation by further expanding its security infrastructure to take full advantage of the integrated and connected approach offered by McAfee which detects, protects, and corrects across the entire threat defense lifecycle.

He and his team made the decision to migrate from McAfee® Endpoint Protection—Advanced to McAfee® Endpoint Security 10. They took this step because McAfee Endpoint Security provides additional defenses, such as advanced threat prevention, which he believed would fortify the organization's anti-malware and ransomware protection. Prior to McAfee Endpoint Security, the taxation bureau was using a competitive antivirus product that proved ineffective and required staff members to perform labor-intensive malware cleanup and remediation on each individual PC.

Out of the 11 people on the IT team, three are dedicated to overseeing endpoint security. With such a small team, the endpoint security engineer was looking for a way to reduce administrative overhead and simplify security management. Additionally, he wanted to gain better visibility into threat activity across the organization's geographically dispersed offices and to improve the speed and accuracy of detection.

Challenges

- Proactively defend endpoints against zero-day threats and ransomware
- Ensure continual availability of all services both internally to employees and externally to citizens
- Increase visibility to malicious activity across the entire endpoint environment
- Gain visibility to endpoint security posture across the entire organization
- Streamline security management through a single, customizable console
- Achieve an integrated security infrastructure where products communicate and coordinate with one another to improve incident response

McAfee Endpoint Security and Complementary Products Provide Integrated and Proactive Protection

After a proof of concept, the endpoint security engineer and his team deployed 5,600 licenses of McAfee Endpoint Security and McAfee Threat Intelligence Exchange on endpoints running Microsoft OS 10.5 earlier this year. They also deployed McAfee Advanced Threat Defense sandbox appliances, along with McAfee ePolicy Orchestrator (McAfee ePO) software to tie all the products together and provide single-pane-of-glass management. This fully integrated solution reduced the burden on the security staff, enabling them to spend less time and effort on manual processes and focus on strategic projects and initiatives. The endpoint security engineer and his colleagues were able to complete the deployment in just three weeks with the help of McAfee® Professional Services.

The endpoint security engineer feels confident about McAfee Endpoint Security's ability to automatically contain zero-day threats, ransomware, and other malware and to prevent infections from spreading throughout the network. It also monitors sensitive data that is copied onto removable USB devices and blocks the transfer of infected files, which, as he noted, can sometimes be a problem when employees violate policy. Finally, because the solution regularly scans for such policy violations, compliance has become easier to manage.

The endpoint security engineer wholeheartedly vouches for the effectiveness of McAfee Endpoint Security: "I am 100% sold on McAfee endpoint technology and would recommend it without hesitation—especially because of the low cost of administration, the ease of use of the management console, and the effective protection provided by this advanced tool."

The security team is exploring advanced features and has deployed Dynamic Application Containment (DAC) and Real Protect in a test environment with positive results. DAC automatically contains zero-day threats when malicious behaviors are detected and keeps them from infecting endpoints. Relying on machine learning, Real Protect investigates and classifies threats and applies those insights to detection and remediation activities.

Deployment of the endpoint solution was quickly followed with the rollout of McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense, which rounded out the security ecosystem. It was exactly what the security team had in mind. One of big benefits the taxation bureau has derived is proactive protection and remediation against ransomware and other zero-day threats.

McAfee Solutions

- McAfee® Endpoint Security
- McAfee® ePolicy Orchestrator® (McAfee ePO™) software
- McAfee® Threat Intelligence Exchange
- McAfee® Advanced Threat Defense
- McAfee® Business Support

Accurate Threat Detection and Accelerated Response Keeps System Malware-Free

The taxation bureau uses McAfee Advanced Threat Defense to detect and analyze all types of malware. It has proven its effectiveness by shielding the organization completely from the WannaCry and Petya ransomware attacks.

The endpoint security engineer is impressed with the superior detection of zero-day and unknown threats. Integration with the other McAfee products implemented at the taxation bureau was achieved via DXL, the bidirectional communication fabric that enables sharing of threat intelligence from multiple sources among McAfee and non-McAfee products. The endpoint security engineer finds that this is especially valuable, as many of their endpoints are located in distributed locations across the country. Systems from any location can send malware samples for analysis to the McAfee Advanced Threat Defense sandbox. The threat intelligence extracted from this process updates the reputation database, and this information is then shared among all the security tools across the entire organization.

"The McAfee Advanced Threat Defense appliance practically manages itself. The previous solution was ineffective against many viruses and Trojans, and my team spent many hours on system cleanup using yet another tool. The reports we've pulled from the McAfee appliance have shown us that it's been 100% effective at keeping our systems malware-free," explains the endpoint security engineer.

McAfee Threat Intelligence Exchange Separates the Good from the Malicious

The administrative team at the taxation bureau uses McAfee Threat Intelligence Exchange to distinguish known good files from known bad files and then to archive and share that data. The team currently uses the product in observation mode so that it learns about the files that circulate internally throughout the organization. McAfee Threat Intelligence Exchange works with McAfee Endpoint Security by providing extra verification as to whether a file is malicious.

"We just let McAfee Threat Intelligence Exchange do its job with minimal interaction on our part. If we discover that an internally developed application is not working properly or is blocked, we just make sure we whitelist it so that users can access it," says the endpoint security engineer.

It helps provides better visibility into endpoint threats overall, and the endpoint security engineer and his team can see a big difference in the level of protection they have now compared to solutions from their previous vendor.

Simplified Security Management Eases the Burden on IT

With a relatively small security department and a large internal and external user base, it was critical for the taxation bureau to have the ability to manage security and solve user issues from a central management console. McAfee ePO software has noticeably eased the administrative burden and has provided a level of

Results

- Unified and fully integrated endpoint security providing stronger, proactive protection against advanced threats and ransomware
- Improved visibility to security issues and malware across the entire infrastructure, including remote offices
- Reduced operational costs and administrative overhead due to automation plus simplified, single-console management
- Threat intelligence sharing enables faster detection and incident response

visibility that was not possible before. “McAfee ePO has a very intuitive and easy-to-use console. The dashboard allows me to see, at a glance and in real time, the security posture of any endpoint in our infrastructure,” asserts the endpoint security engineer.

According to the endpoint security engineer, the graphical user interface of the McAfee ePO console offers many advantages and capabilities that were not available to his team with their previous solution, namely, the ability to do network checks using metrics that are meaningful for their environment, real-time alerts, and both high-level and granular reporting.

As the endpoint security engineer points out, “McAfee ePO software has also helped us quickly remediate malware infections that are introduced when employees violate policy and use USB drives to transfer data. McAfee ePO reports show that, ever since we deployed our McAfee solutions, all viruses have been cleaned immediately, and no infections have been distributed across the network.”

Reliable and Consistent, McAfee Professional Services Streamlines Deployment and Maintenance

To ensure a smooth deployment process, the endpoint security engineer and his colleagues engaged the McAfee Professional Services team, who collaborated closely to enable the initial setup and configuration, delineate security processes, and develop policy. Post-deployment, the taxation bureau relies on McAfee Professional Services for preventative maintenance.

“The McAfee Professional Services team exceeded our expectations and provided us with consistently superior support. Along with helping us make the most of our McAfee solutions, they are quick to respond and take appropriate action when issues surface,” says the endpoint security engineer.

While the endpoint security engineer and his team have not signed up for formal McAfee product training, they feel that the knowledge transfer that occurred during the implementation and maintenance processes has prepared them fully to manage their McAfee solutions with confidence.

> “I am 100% sold on McAfee endpoint technology and would recommend it without hesitation—especially because of the low cost of administration, the ease of use of the management console, and the effective protection provided by this advanced tool.”
>
> —Endpoint Security Engineer, South American Government Taxation Bureau

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com