CASE STUDY

Regional Government Builds Adaptable, Proactive Defense Against Tomorrow's Cyberthreats

Proactive insights, stronger and lighter endpoint security, and an integrated security framework support fearless innovation

Service public de Wallonie

Customer Profile
Government of the French-speaking region of Belgium

Industry
Government

IT Environment
10,000 workstations and 1,300 servers across 200 locations

With an integrated security infrastructure that includes products such as McAfee® Endpoint Security and McAfee® MVISION™ Insights, the government of Wallonia, Belgium has dramatically increased its ability to protect against cyberthreats, from device to cloud, today and in the future. It has also created a culture where security supports rather than hinders the pursuit of business objectives and continued transformation and innovation.

Connect With Us

Service public de Wallonie (SPW) is the public administration arm of the regional government of Wallonia, the French-speaking region of Belgium. At SPW, the endpoint security team oversees information security for the 10,000 desktops, 1,300 servers, and 1,000 major applications used by more than 8,000 employees. As the leader of the SPW Endpoint Security team, Philippe Maquoi holds chief responsibility for monitoring critical security indicators and is therefore the first person aware of potential cyberattacks.

Searching for Easier Security that Protects Against Tomorrow's Threats

"In today's ever-morphing threat landscape, I don't just want to be protected against dangerous threats today; I want protection against the threats that will exist in six months or a year," says Maquoi. "I want security that learns and adapts so it can successfully combat future threats."

In addition, SPW security operations strives to reduce time spent reacting to security incidents or working on non-strategic tasks. "We are always looking for ways to make our jobs easier and more proactive so that we can have more time to focus on strategic activities," explains Maquoi.

Predictive Intelligence Empowers Proactive Stance

SPW's most recent step toward greater proactivity was to implement McAfee MVISION Insights, which helps security staff identify potential threats outside SPW's perimeter. Using data gathered from one billion sensors globally that has been distilled and analyzed by artificial intelligence and experts, MVISION Insights provides comprehensive risk intelligence to help prioritize which threats and campaigns are most likely to target a given organization. SPW security staff use the solution every day to quickly filter for variables like geography and industry to see which threats might be of concern.

"MVISION Insights is invaluable for proactive threat hunting," says Macquoi. "All the important information is distilled for me and easily filtered. For example, in the past, it took me two to three hours skimming various security sites, lab reports, and news articles to fully understand one specific COVID-19-related threat campaign. After installing MVISION Insights, I had the same result within five minutes. Often the information I need is available in seconds."

"Once we know which threats to watch, we use the predictive assessment information in MVISION Insights to very quickly decide what to do and how to do it, as well as to prioritize our actions," continues Macquoi. "If we have any concern about a threat that might be headed our way, we import the indicators of compromise (IoCs) provided by MVISION Insights into McAfee® Threat Intelligence Exchange to share the information across the enterprise."

SPW is also in the process of rolling out McAfee® MVISION EDR, which, when integrated with MVISION Insights, will further enhance the organization's ability

Challenges

- Be ready to combat tomorrow's cyberthreats
- Simplify security management
- Unify policies for the entire environment—on premises, at home, and in the cloud

McAfee Solution

- McAfee® Advanced Threat Defense
- McAfee® Complete Endpoint Threat Protection
- Data Layer Exchange (DXL)
- McAfee® Endpoint Security
- McAfee MVISION™ EDR
- McAfee® ePolicy Orchestrator® (McAfee® ePO™)
- McAfee® MVISION™ Cloud for Shadow IT
- McAfee MVISION Insights
- McAfee® Security for Microsoft Exchange
- McAfee Threat Intelligence Exchange
- McAfee® Web Gateway
- McAfee® Web Gateway Cloud Service

to conduct deep-dive investigations into threats—in real time as well as historically. Campaign artifacts can be loaded into MVISION EDR to determine if related attacks exist and must be prioritized where further investigation is required.

A Powerful Console: The First Step to Easier Management

SPW's journey toward easier security administration began six years ago when they deployed the McAfee Complete Endpoint Threat Protection suite. McAfee had won the public tender in large part because of its central management console, McAfee ePolicy Orchestrator (McAfee ePO) software. "We absolutely love McAfee ePO [software]," says Maquoi. "It is so powerful. It lets us manage so much security functionality with a single screen. For me, it is our most important security product."

To provide a higher level of detection and protection, SPW used McAfee ePO software to migrate its endpoint protection suite to McAfee Endpoint Security a few years later. The organization completed a full "big bang" migration—including modules for Web Control, Advanced Threat Protection, and Firewall, as well as agents for McAfee Threat Intelligence Exchange and a McAfee Advanced Threat Defense sandbox appliance—across 800 servers, 9,000 endpoints, and 200 locations—in just two days. Most of the systems were migrated in just four hours.

"Stronger and Lighter" Endpoint Security With Superior Threat Detection and Exploit Prevention

"McAfee Endpoint Security is both stronger and lighter," says Maquoi. "By that I mean it has superior detection and prevention technology that protects us better against present and future threats, and, as a single modular product instead of multiple products, it is also easier to manage."

SPW endpoints can detect and block a much broader range of malware and zero-day threats than they could before. "The behavioral detection technology in McAfee Endpoint Security has significantly improved protection and reduced the number of alerts we receive, but the Dynamic Application Containment (DAC) functionality is a 'must have'," continues Maquoi. "While our McAfee Advanced Threat Defense sandbox is analyzing the unknown file, DAC quarantines it so it can't do harm. In other words, it can shrink the time to zero-day protection from minutes to just seconds."

For example, before installing McAfee Endpoint Security across all nodes, SPW was attacked by Nemucod ransomware after a handful of users clicked on a button within a phishing email. On the desktops not yet migrated to McAfee Endpoint Security, the user's action triggered JavaScript that downloaded the ransomware, which kept the computers out of commission for two days. On the desktops already protected by McAfee Endpoint Security, on the other hand, the malware was blocked from executing and users continued working, business as usual.

Results

- Higher level of detection and exploit prevention, slashing time-to-zero-day protection from minutes to seconds
- Intelligence on potential threats and potential impact garnered in minutes rather than hours
- More proactive security posture
- Faster threat investigations
- Adaptable, fully integrated security infrastructure that supports fearless innovation
- Support for cloud transformation journey
- Staff freed up to spend more time on strategic activities
- Easier security administration with reduced operational overhead
- Happier, more productive users

Time Savings and Reduced Operational Overhead

Besides saving significant time by eliminating the need to perform remediation after attacks, SPW security operations spends less time on manual tasks, reducing operational overhead. "McAfee Endpoint Security is smart enough to stop threats without us having to manually create a bunch of rules, as we had to do in the past," notes Maquoi. "Also, instead of having to push out and update multiple agents for various aspects of protection, booting and rebooting each time, we have a stronger tool set, encompassed in one product with just one agent to deal with."

Integration Increases Automated Protection

In addition to McAfee Endpoint Security, SPW deployed a McAfee Advanced Threat Defense sandboxing appliance, a McAfee Web Gateway appliance, and McAfee Web Gateway Cloud Service. To share threat information bi-directionally between endpoints and all these systems, the organization deployed McAfee Threat Intelligence Exchange across all nodes. McAfee Threat Intelligence Exchange maintains a threat reputation database and uses the Data Exchange Layer (DXL) to receive and share near real-time local and global threat information across the entire enterprise for even faster response to threats.

Thus, if a questionable file attempts to execute on an SPW endpoint, while DAC quarantines it at the endpoint, it will be sent securely to McAfee Advanced Threat Defense for immediate inspection. If McAfee Advanced Threat Defense determines the file is malicious, it will convey that information via McAfee Threat Intelligence Exchange to all SPW endpoints. Likewise, if the McAfee hybrid web protection detects a malicious file, that information is shared instantly to endpoints throughout SPW, whether on premises or at home.

"The integrated McAfee ecosystem lets us automate our defenses a lot more," says Maquoi, who also plans to integrate SPW's McAfee infrastructure with other tools in their environment, such as Rapid7 and BeyondTrust. "If we can do anything automatically with the same level of effectiveness or better, then we want to do it, so we can concentrate human energy where it can add the most value."

Adaptable Security that Supports Cloud Transformation and Innovation

"We have come to believe that cybersecurity ought to support rather than hinder the introduction of new applications, new ways of doing things, and innovation in general," states Maquoi. "In no case should security be a set of fortifications with unmovable walls."

"With a device-to-cloud ecosystem of products all working together to minimize risk, we have been able to grant more freedom to test and implement new applications," he continues. "The McAfee integrated security platform allows us to keep adapting to meet business needs, to focus on objectives rather than worrying too much about security, in an ever-evolving IT landscape. For example, we are now migrating to the cloud without fear."

> "The McAfee integrated security platform allows us to keep adapting to meet business needs, to focus on objectives rather than worrying too much about security, in an ever-evolving IT landscape. For example, we are now migrating to the cloud without fear."
>
> —Philippe Maquoi, Head of Endpoint Security, Service Public de Wallonie

As a first step in its cloud transformation, SPW is using McAfee MVISION Cloud for Shadow IT to monitor use of cloud applications and implement policies to control access to unauthorized cloud services. SPW also plans to implement McAfee MVISION Unified Cloud Edge to protect data from device to cloud and prevent cloud-native breach attempts that are invisible to the corporate network.

"Preparing for the future is a key part of our job," concludes Maquoi. "That's why we need partners like McAfee."

> "The integrated McAfee ecosystem lets us automate our defenses a lot more... If we can do anything automatically with the same level of effectiveness or better, then we want to do it, so we can concentrate human energy where it can add the most value."
>
> —Philippe Maquoi, Head of Endpoint Security, Service Public de Wallonie

McAfee™

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