Case Study

Regional Government Prepares to Defend Against Tomorrow's Threats

Service public de Wallonie

Customer profile
Government of the French-speaking region of Belgium.

Industry
Government.

IT environment
9,000 workstations and 1,300 servers.

Challenges
- Be ready to combat tomorrow's cyber threats.
- Simplify security management.

Intel Security solutions
- McAfee Advanced Threat Defense
- McAfee Complete Endpoint Threat Protection
- McAfee Endpoint Security
- McAfee Security for Microsoft Exchange
- McAfee Threat Intelligence Exchange

Results
- Staff able to spend more time on strategic activities.
- Easier security administration with reduced operational overhead.
- Higher level of detection and exploit prevention.
- Adaptable security infrastructure for the future.
- Happier end users.

With an integrated security framework and McAfee® Endpoint Security, the government of Wallonia, Belgium has dramatically increased its ability to protect against cyber threats today as well as in the future.

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 9,000 desktops, 1,300 servers, and 1,000 major applications used by more than 10,000 employees. As head of the SPW Endpoint and Server Security team, Philippe Maquoi holds chief responsibility for monitoring critical security indicators, making him the first person to be aware of potential cyberattacks.

Wanted: Easier Security That Protects Against Tomorrow's Threats

"In today's ever-morphing threat landscape, of course I want the most robust protection I can get," says Maquoi. "But 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. I want security that learns and adapts so it can successfully combat future threats."

In addition, Maquoi and the others in SPW security operations strive to reduce time spent reacting to security incidents or working on tasks that are not strategic. "We are always looking for ways to make our jobs easier so that we can have more time to focus on proactive, strategic activities," explains Maquoi.

Powerful Central Console First Step to Easier Management

Six years ago, SPW deployed the McAfee Complete Endpoint Threat Protection suite after McAfee won a public tender, thanks in large part to its central management console, McAfee ePolicy Orchestrator® (McAfee ePO™) software. McAfee ePO software provides easy-to-use, at-a-glance dashboards as well as the ability to drill down for greater detail and create out-of-the-box and customized reports. "We absolutely love McAfee ePO software," says Maquoi. "It is so powerful. It lets us manage all of our McAfee products with a single screen. For me, it is our most important security product."

In addition to McAfee Complete Endpoint Threat Protection to protect its physical endpoints, SPW deployed McAfee Security for Microsoft Exchange to protect its email servers as well as McAfee Threat Intelligence Exchange across all nodes. Leveraging the McAfee Data Exchange Layer (DXL) fabric, Threat Intelligence Exchange combines multiple threat information sources and instantly shares this data with all DXL-connected security solutions.

Migrating to McAfee Endpoint Security to Defend Against Future Threats Today

When Maquoi heard about McAfee Endpoint Security, a new endpoint protection framework that provides a more intelligent, collaborative defense against new and emerging threats, he immediately signed up to became one of its first beta testers. "I had been looking for a product like McAfee Endpoint Security for some time," he says, "and I had confidence that McAfee, with its experience and market leadership, was capable of giving me such a product."

After initially migrating 1,000 computers to McAfee Endpoint Security version 10.2, SPW plans to migrate all 9,000 endpoints to Endpoint Security version 10.5 imminently. "With the latest version of Endpoint Security, we are looking forward to taking advantage of the Real Protect machine learning and behavioral detection functionality to further enhance our ability to prevent exploits."

intel Security

"What I like best about McAfee Endpoint Security so far is that it is both stronger and lighter. By that I mean it has superior detection and prevention technology that protects us better against present and future threats, but it is also easier to manage. Both aspects are equally important."

—Philippe Maquoi, Head of Endpoint and Server Security, Service public de Wallonie

"What I like best about McAfee Endpoint Security so far is that it 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, but it is also easier to manage. Both aspects are equally important."

Superior Detection and Exploit Prevention

With McAfee Endpoint Security, SPW endpoints can detect and block a much broader range of malware and zero-day threats than they could previously. "McAfee Endpoint Security is much more intelligent," says Maquoi. "With its behavioral detection capabilities and Dynamic Application Containment feature, an unknown file or even a known file with 'not bad' reputation can be limited in its actions or blocked entirely if it acts suspiciously. It's the best of a host intrusion prevention solution (HIPS) and McAfee SiteAdvisor® software but with much stronger exploit prevention."

For example, before installing McAfee Endpoint Security across all nodes, SPW was recently attacked by Nemucod ransomware that originated within Belgium. A handful of users—both on desktops with and without McAfee Endpoint Security—clicked on a button within a phishing email. On the desktops not-yet migrated to Endpoint Security, the user's action triggered a JavaScript that downloaded the ransomware. This resulted in two days of work restoring corrupted administrative shares. But on the desktops already protected by Endpoint Security, the JavaScript was prevented from executing and users continued working, business as usual. "That's the type of example that justifies our move to Endpoint Security," states Maquoi.

Time Savings and Reduced Operational Overhead

As seen in this ransomware example, superior detection and blocking of malware results in significant time savings for SPW security operations simply by avoiding time spent remediating after attacks. In addition, SPW security operations save time thanks to reduced operational overhead associated with McAfee Endpoint Security.

"McAfee Endpoint Security is smart enough to stop threats without us having to manually create a bunch of rules like 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—a HIPS agent, a web content control agent, and so on, booting and rebooting each time—with Endpoint Security, we have a stronger toolset, encompassed in one product, with just one agent to deal with."

Eliminating Scan Impact on Users

According to Maquoi, security administrators aren't the only ones benefiting from McAfee Endpoint Security; users benefit just as much. Before migrating to Endpoint Security, SPW users were always angry on the day full anti-malware scans were run because the scans made their computers sluggish. Today, with Endpoint Security, malware scanning occurs only when the machine is idle so the user is never impacted. "Users with Endpoint Security on their machines are much happier now," says Maquoi.

Government operations also benefit every time ransomware or other malware is stopped in its tracks because work is not disrupted. Employees stay productive instead of having to make do without their computers while the devices are offline being purged of malware.

Increasing Level of Automated Protection with Integration

Because SPW has deployed the Data Exchange Layer fabric across all nodes, McAfee Threat Intelligence Exchange can receive and share near real-time local and global threat information across all nodes. And because McAfee Endpoint Security framework communicates using DXL, all of the organization's endpoints can participate in the exchange of information with all other DXL-connected security systems in SPW's environment.

In the near future, SPW plans to implement McAfee Advanced Threat Defense for In-depth sandbox analysis of all unknown files. With Threat Intelligence Exchange and Advanced Threat Defense part of the DXL-connected ecosystem, SPW endpoints will be able to receive threat information from Advanced Threat Defense and vice versa, creating even stronger threat detection capabilities and enabling even faster response. For example, if a questionable file attempts to execute on an endpoint, it will be immediately quarantined at the endpoint and sent securely to Advanced Threat Defense for immediate inspection. If Advanced Threat Defense determines the file is malicious, it will convey that information via Threat Intelligence Exchange to all SPW endpoints. Conversely, if Advanced Threat Defense learns of a malicious file on the network, it will automatically update Threat Intelligence Exchange and inform the endpoints.

"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," declares Maquoi. "The integrated McAfee ecosystem lets us automate our defenses a lot more."

Preparing for the Future

Furthermore, with collaborative McAfee endpoint protection and integrated security architecture, security operations for the Wallonia regional government now have in place the foundation for an adaptable, sustainable threat defense lifecycle.

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

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