Regional Government Builds Adaptable Defense Against Tomorrow’s Threats

Stronger and lighter endpoint security in an integrated security framework to support fearless innovation

With an integrated security framework and McAfee Endpoint Security, the government of the French-speaking region of Belgium has dramatically increased its ability to protect against cyberthreats today as well as in the future. It has also created a culture in which security supports rather than hinders the pursuit of business objectives and continued innovation.
CASE STUDY

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 8,500 employees. As the head of Operational Security, Philippe Maquoi holds chief responsibility for monitoring critical security indicators and is one of the first persons be aware of potential cyberattacks.

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 P. 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, P. 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 P. Maquoi.

Powerful Central Console First Step to Easier Management

Seven 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 P. Maquoi. “It is so powerful. It lets us manage all our McAfee products with a single screen. For me, it is our most important security product.”

P. Maquoi trusts McAfee ePO software so much that he offered to beta test the latest release, version 5.10. “McAfee ePO software just keeps getting better,” he says. “For instance, I can now easily disable, temporarily or permanently, any of our delegated McAfee ePO software administrator accounts. The introduction of workflow to streamline the approval process for creation of policies and policy changes before they are put into production is also a fantastic addition.”

Migrating to McAfee Endpoint Security to Defend Against Future Threats Today

When P. 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 then migrated all 9,000 endpoints and 800 servers to McAfee Endpoint Security version 10.5, and, not long after that, to version...
10.6. “With each successive version, McAfee Endpoint Security has become more powerful and migration faster and easier.”

SPW 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 McAfee Advanced Threat Defense—across 800 servers, 9,000 endpoints, and 120 locations, in two days. Most of the systems were migrated in just four hours.

“What I like best about McAfee Endpoint Security is that it is both stronger and lighter,” says P. Maquoi. “By that I mean it has superior detection and prevention technology that protects us better against present and future threats, but, as a single modular product instead of multiple products, 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 before. “McAfee Endpoint Security is much more intelligent,” says P. Maquoi. “With its Real Protect behavioral detection capabilities and Dynamic Application Containment (DAC) 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 McAfee® Host Intrusion Prevention and McAfee® SiteAdvisor®, but with much stronger exploit prevention.”

“The Real Protect technology has improved our protection and reduced the number of alerts we receive, and DAC is a ‘must have’,” adds P. Maquoi. “While our McAfee Advanced Threat Defense sandbox is analyzing the unknown file, DAC keeps it quarantined so it can’t do harm. In other words, it shrinks the time to zero-day protection from up to five minutes to just seconds.”

For example, before installing McAfee Endpoint Security across all nodes, SPW was attacked by the Nemucod ransomware variant 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 McAfee Endpoint Security, the user’s action triggered a 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 JavaScript ransomware was prevented from executing and users continued working, business as usual. “That’s the type of example that justifies our move to McAfee Endpoint Security,” states P. Maquoi.

Time Savings, Reduced Operational Overhead, and Happier Users

As seen in the ransomware example above, 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.

Results

- Higher level of detection and exploit prevention, slashing time-to-zero-day protection from minutes to seconds
- Adaptable security infrastructure that supports fearless innovation
- Staff freed up to spend more time on strategic activities
- Easier security administration with reduced operational overhead
- Happier, more productive end users
“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 P. Maquoi. “Also, instead of having to push out and update multiple agents for various aspects of protection—a host intrusion prevention agent, a web content control agent, and so on—booting and rebooting each time, with McAfee Endpoint Security we have a stronger toolset, encompassed in one product with just one agent to deal with.”

Users also benefit from McAfee Endpoint Security. Before migrating to McAfee Endpoint Security, SPW users were always angry on the day when full anti-malware scans were run because the scans made their computers sluggish. Today, with McAfee Endpoint Security, malware scanning occurs only when the machine is idle so the user is never impacted. In addition, every time ransomware or other malware is stopped in its tracks, employees can 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**

In addition to McAfee Complete Endpoint Threat Protection to protect its physical endpoints, SPW deployed McAfee Threat Intelligence Exchange across all nodes as well as a McAfee Advanced Threat Defense sandboxing appliance. Leveraging the Data Exchange Layer (DXL) fabric, McAfee Threat Intelligence Exchange combines multiple threat information sources and instantly shares this data with all DXL-connected security solutions. Because SPW has deployed DXL 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 the organization’s endpoints can participate in the exchange of information with all other DXL-connected security systems in SPW’s environment.

With McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense part of the DXL-connected ecosystem, SPW endpoints can receive threat information from McAfee 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 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. Conversely, if McAfee Advanced Threat Defense learns of a malicious file on the network, it will automatically update McAfee 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 P. Maquoi. “The integrated McAfee ecosystem lets us automate our defenses a lot more.”

“What I like best about McAfee Endpoint Security 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 Operational Security, Service Public de Wallonie
Adaptable Security and a Culture that Supports 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,” says P. Maquoi. “In no case should security be a set of fortifications with unmovable walls.”

“With the bi-directional integration of our endpoint protection and sandbox and threat intelligence, and features like DAC and Real Protect, all working together to minimize risk, we have been able to give more freedom to departments 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 can now consider our imminent migration to the cloud without fear.”

“Preparing for the future is a key part of our job,” concludes P. Maquoi. “That’s why we need partners like McAfee.”