CASE STUDY

Migration to McAfee Endpoint Security Lets Small Security Staff Provide More Robust Protection, More Easily

By migrating to McAfee® Endpoint Security, this provider of customer payment services has improved endpoint protection while making security administration easier.

Accarda provides customer loyalty cards, gift cards, mobile payments, and other payment-related services to companies throughout Switzerland. Although the company's services are used by more than two million end customers, it runs a fairly lean business with just 220 employees, only 21 of them in information technology operations.

Security Must Be Easy

"With our limited information security staff, a security tool must be easy to use or we won't even consider it," says Norbert Marx, a senior security engineer responsible for technical security decisions and troubleshooting. "It also has to do what it is supposed to do. We simply don't have time to deal with extremely complicated systems or firefighting."

The ease of use of McAfee ePolicy Orchestrator® (McAfee ePO™) software—the central management console that enables management of many solutions from a single screen—led Accarda to deploy a McAfee antivirus endpoint protection seven or eight years ago. In addition to ease of use, the integrated McAfee security ecosystem motivated the company to renew McAfee endpoint protection and add solutions such as McAfee Web Gateway and the McAfee security information and event management (SIEM) solution, McAfee Enterprise Security Manager.

"The integration of all the McAfee products gives McAfee a huge advantage," says Marx. "Our McAfee solutions can share information with each other in ways that other vendors' solutions just can't. When I talk with other security professionals, they agree that McAfee has the best integration around."

Accarda

Customer profile
Swiss provider of customer card programs.

Industry
Financial.

IT environment
Complex physical and virtual environment with 300 desktops and 500 servers.

Challenges

- Protect environment from advanced threats with limited technical security staff.
- Provide stable, nonintrusive security environment that does not hinder business users.

McAfee solution

- McAfee Endpoint Threat Protection
- McAfee Enterprise Security Manager
- McAfee Threat Intelligence Exchange
- McAfee Web Gateway
- McAfee ePolicy Orchestrator Software
- McAfee Endpoint Security

Results

- Easier security management that saves staff time.
- Better protection thanks to integrated security.
- Happier users who no longer complain about performance during full antivirus scans.

Exponential Improvement in Endpoint Security with Migration to McAfee Endpoint Security

"Over the years, Accarda did look at other endpoint vendors when renewals neared, but the other products could never match the integration and ease of use of our McAfee endpoint protection," explains Marx. "Then McAfee introduced Endpoint Security 10, which made us even happier with McAfee. McAfee Endpoint Security is no small improvement in endpoint protection; it's an exponential improvement."

Accarda migrated to McAfee Endpoint Security version 10.1 as soon as it became available. "We were so excited by the new architecture that we wanted to take advantage of it right away," says Marx. "Instead of multiple agents, McAfee Endpoint Security is one product with greater intelligence built in."

Using the McAfee migration tool inside McAfee ePO software, Accarda migrated all the company's endpoints in one day from the McAfee VirusScan® Enterprise antivirus engine and McAfee SiteAdvisor application in its McAfee Endpoint Threat Protection suite to the Threat Prevention and Web Control modules in McAfee Endpoint Security. As new versions of Endpoint Security have been released, Accarda has upgraded to them. Marx notes that each version has offered improvements over previous versions and that Endpoint Security version 10.5 is the best yet.

Accarda also implemented Dynamic Application Containment functionality when it rolled out Endpoint Security 10.5. "With the added reputation and behavior-based capabilities of Endpoint Security, we can identify malware and zero-day threats more quickly and effectively," says Marx, "and with Dynamic Application Containment, we can contain them before they can cause harm."

Saving Time and Easing Management with McAfee ePO Software and McAfee Endpoint Security

The ability to manage multiple McAfee solutions via the McAfee ePO central management console saves Accarda security operations as well as others a significant amount of time and hassle each week. Four or five people use McAfee ePO console regularly. Each of them has his own dashboard for instant viewing of the information most important to them. For instance, one dashboard is strictly used by IT operations, another by the people who oversees PCs, another by a server administrator, and another by Marx for an overall view of security and troubleshooting. "Without McAfee ePO console, my job would be many times more difficult," claims Marx.

> ***"What are you waiting for? McAfee Endpoint Security protects better, is easier to use, and saves time. It is better in every way than its predecessor. It's like two different worlds. It's like moving from a Volkswagen bug to an Aston Martin."***
>
> —Norbert Marx, Senior Security Engineer, Accarda

With McAfee Endpoint Security, Accarda has consolidated endpoint protection into a single agent instead of multiple agents, which saves time when pushing out updates and simplifies management overall. The improved graphical user interface of Endpoint Security also facilitates endpoint security management. According to Marx, the Endpoint Security interface within McAfee ePO software is notably easier to use, with very helpful and understandable graphical displays and alerts. In addition, it provides more insights into the origins, attempted actions, and targets of attacks to help with decision making and hardening of policies and defensive actions. The Endpoint Security interface also allows much more customization than the company's legacy endpoint protection.

Integration Fortifies Defenses and Enables Faster Response

Another reason Accarda migrated to McAfee Endpoint Security is because Endpoint Security is built to leverage the McAfee Data Exchange Layer (DXL), an open-source platform that connects security components to automate integration and real-time data exchange. Accarda has implemented DXL throughout its enterprise and benefits from

McAfee Threat Intelligence Exchange, which combines multiple internal and external threat information sources and instantly shares this data with all DXL-connected security solutions, including McAfee Web Gateway and McAfee Enterprise Security Manager, which logs events for all devices managed by McAfee ePO software.

"With McAfee Threat Intelligence Exchange, if we see an activity in our environment that is potentially malicious or against corporate policy, we can tag it and instantly blacklist it throughout our entire infrastructure," explains Marx. "For instance, if an application is violating our security policy or causes suspicious activity that is detected by McAfee Endpoint Security, we can immediately tag the file as potentially malicious, thus preventing its execution anywhere in the enterprise. And with the relevant data now contained in the Threat Intelligence Exchange database, if the anyone else attempts to go to that website, Web Gateway won't allow it."

Happier End Users and Security Team Thanks to Improved Performance

In the past, before implementing McAfee Endpoint Security, end users complained every time their computers underwent full antivirus scans because of the resulting sluggishness of their systems. "Now we don't hear a single complaint about virus scanning," says Marx. "Scans occur completely in the background when the computers are idle so users aren't even aware of them. Our users are a lot happier. And the security team is happier because we can trust that Endpoint Security is working."

"What Are You Waiting For?"

When Marx meets other security professionals whose companies have not yet migrated to Endpoint Security, he invariably asks them, "What are you waiting for? McAfee Endpoint Security protects better, is easier to use, and saves time. It is better in every way than its predecessor. It's like two different worlds. It's like moving from a Volkswagen bug to an Aston Martin."

McAfee and the McAfee logo, ePolicy Orchestrator, McAfee ePO, SiteAdvisor, and VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.
Copyright © 2017 McAfee, LLC. 3133_0517
MAY 2017

McAfee™
Together is power.

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