CASE STUDY

University Fortifies Protection with Integrated Threat Defense

McAfee helps block ransomware and zero-day malware while reducing complexity

Utrecht University

Customer Profile
University in the Netherlands with more than 30,000 students

Industry
Higher education

IT Environment
Approximately 10,000 endpoints across seven sub-campuses

With tightly integrated McAfee® Endpoint Security, McAfee Advanced Threat Defense, and McAfee Threat Intelligence Exchange, this European university enhanced zero-day threat protection, shrank time from encounter to containment, and simplified security operations.

Utrecht University, in the city of Utrecht in the Netherlands, serves more than 30.000 students annually and is ranked 47 on the Academic Ranking of World Universities. With extensive experience managing endpoint security, Utrecht University's IT Administrator Andreas Van Dijk oversees endpoint infrastructure decisions and implementation. Van Dijk is always looking to improve protection as well as reduce costs and improve efficiency within the university's infrastructure.

Challenges: Blocking Ransomware and Keeping Endpoint Protection Current

The need to abate the ongoing threat of ransomware and reduce the risk of damage from zero-day and other malware attacks drove Utrecht University to look for better endpoint protection. "Ransomware is not just a problem for companies," says Van Dijk. "We also wanted to upgrade from yesterday's technology to more current technology that incorporates more than signature-based malware detection."

Time for Stronger Endpoint Protection

The university had relied on McAfee® endpoint protection since 2007, primarily because of its easy-to-use central management console, McAfee® ePolicy Orchestrator® (McAfee ePO™) software, which enables management of multiple McAfee security solutions from a common interface. "It is incredibly helpful to have everything in one place, to be able to manage your endpoint environment from a single screen," says Van Dijk.

So when McAfee introduced McAfee Endpoint Security, it sounded logical to Van Dijk and his colleagues at Utrecht University to upgrade their McAfee Complete Endpoint Threat Protection suite to take advantage of the improved detection and protection technology. "Our goal is better protection and less time spent on remediation," explains Van Dijk. "We were especially interested in the McAfee Endpoint Security's behavioral detection technology that goes beyond .DAT signatures and Dynamic Application Containment (DAC) functionality as a safeguard to keep potential threats quarantined while they are being analyzed."

Smooth Migration to McAfee Endpoint Security

Utrecht University migrated to McAfee Endpoint Security, version 10.5 not long after it became available. The Threat Prevention module was implemented first across the university's IT department. That deployment went extremely smoothly as desktops were migrated in waves of 500 until all 10,000 endpoints were completed.

"Before migration, we were concerned, since each of the university's faculty groups had its own specialized applications that could potentially be blocked," recalls Van Dijk. "However, we had only a few minor incidents of blocked applications that we were able to rectify quickly. Within three weeks all our endpoints were protected by McAfee Endpoint Security. We were very satisfied with the entire migration.

Challenges

- Protect against ransomware and zero-day cyberattacks
- Provide stable environment that enables users to be as productive as possible
- Minimize administrative overhead for information security

McAfee Solution

- McAfee Advanced Threat Defense
- McAfee Complete Endpoint Threat Protection
- McAfee Endpoint Security
- McAfee Threat Intelligence Exchange

Results

- Improved protection against advanced and zero-day threats
- Blocked ransomware within environment
- Reduced time from encounter to containment
- Easier security administration with central console

More Robust Protection from the Start

Van Dijk and the infrastructure team noted the dramatic improvement in detection and prevention provided by McAfee Endpoint Security from day one. "As soon as McAfee Endpoint Security was deployed, it began detecting and blocking files that were already on workstations but should not have been," states Van Dijk. "During the migration rollout, this happened almost every day. McAfee Endpoint Security improved our detection capabilities right from the start."

"McAfee Endpoint Security also works very well against ransomware," adds Van Dijk. "We used to see ransomware in waves—weeks with nothing and then a week with several occurrences. Since deploying McAfee Endpoint Security, we haven't had a single incident."

In addition, Utrecht University is taking advantage of the DAC functionality, which is part of the Adaptive Threat Prevention Module in McAfee Endpoint Security, to immediately quarantine suspicious files as soon as they are encountered, before they can infect patient zero or its neighbors. "DAC was one of the main reasons we went with McAfee Endpoint Security," claims Van Dijk. "We see DAC containing sketchy files and, when necessary, sending them to our McAfee Advanced Threat Defense sandbox appliance for analysis."

Faster Time to Protection, Thanks to Integration and McAfee Advanced Threat Defense

Utrecht University has also implemented McAfee Data Exchange Layer an open-source platform that connects security components for automated, real-time data exchange, and McAfee Threat Intelligence Exchange, which gathers and transmits local and global threat information to all security systems connected to the DXL framework. By adding McAfee Endpoint Security, which is built to leverage McAfee Data Exchange Layer, the university can protect itself faster when threats enter its environment.

For instance, if a McAfee Endpoint Security-protected endpoint encounters a known malicious file stored in the McAfee Threat Intelligence Exchange database, the file will immediately be blocked from executing, not only on patient zero, but across all endpoints and all McAfee Data Exchange Layer-connected devices in the company's environment. If the file is unknown, it will be sent via McAfee Threat Intelligence Exchange to the McAfee Data Exchange Layer-connected McAfee Advanced Threat Defense appliance for in-depth analysis. Once analyzed, the file's reputation will be shared throughout the environment.

Van Dijk credits McAfee Advanced Threat Defense as an imported tool in the university's security arsenal. It meets the top security challenge—namely, increasing protection against zero-day and advanced attacks. McAfee Advanced Threat Defense combines in-depth static code and dynamic analysis (malware sandboxing) to detect such threats, especially those that use sandbox evasion techniques. "McAfee Advanced Threat Defense acts like a virtual machine that extracts the suspicious file, examines what happens when it executes, and analyzes it while shielding our environment from adverse risk. It's really outstanding," says Van Dijk.

> "As soon as McAfee Endpoint Security was deployed, it began detecting and blocking files that were already on workstations but should not have been. During the migration rollout, this happened almost every day. McAfee Endpoint Security improved our detection capabilities right from the start."
>
> —Andreas Van Dijk, IT Administrator, Utrecht University

Van Dijk was surprised, however, that McAfee Advanced Threat Defense isn't catching even more malware. "We realized that McAfee Advanced Threat Defense catches less malware than we expected because McAfee Endpoint Security blocks a lot as well, which reduces the number of files that McAfee Advanced Threat Defense sees," explains Van Dijk. "McAfee Advanced Threat Defense has caught some advanced malware, though, so we are very happy with it."

Allowing End Users to Stay Productive

With the protection provided by McAfee Endpoint Security, the university's IT department now spends less time remediating security incidents than before. More importantly, however, business users aren't interrupted; they can stay productive rather than having to wait for their infected computers to be fixed.

Furthermore, users are not even aware when anti-malware scanning occurs because it has been set to occur when their machines are idle. During the McAfee Endpoint Security migration, Van Dijk recounts, an application that a user wanted was blocked, so, at the user's insistence, a security engineer uninstalled McAfee Endpoint Security from the user's PC. Unbeknownst to the user, however, the engineer reinstalled McAfee Endpoint Security remotely the next day. The oblivious user never realized McAfee Endpoint Security was back in place, transparently protecting his desktop. "Clearly, McAfee Endpoint Security was not the problem," says Van Dijk.

Easier Security Administration and Reduced Complexity

With McAfee Endpoint Security, McAfee Threat Intelligence Exchange, and McAfee Advanced Threat Protection, Utrecht University has bolstered its protection against the most dangerous threats to a considerable degree and spends much less time on remediation. What Van Dijk appreciates most about the integrated threat defense, though, is that it acts as one united solution. "The tight integration of McAfee products and the ability to manage diverse aspects of security from one console makes administration so much easier," he says. "McAfee reduces complexity, which is always a good thing."

McAfee
Together is power.

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