Case Study

Thwarting Ransomware and Easing Security Administration by Migrating to McAfee Endpoint Security

Norrköpings Kommun

Customer profile
Municipality in Östergötland County in Sweden.

Industry
Government.

IT environment
14,000 endpoints across the administration and schools in the municipality.

Challenges
- Prevent ransomware and other malware.
- Mitigate risk of disrupting services for citizens.
- Secure environment with very limited staff and budget.

McAfee solution
- McAfee Complete Endpoint Threat Protection
- McAfee Endpoint Security
- McAfee ePolicy Orchestrator Software

Results
- Detection and blocking of ransomware before any damage inflicted.
- Easier security administration.
- Reduced operational burden for small security staff.

The small IT team for this Swedish town of 140,000 has reduced its security administration burden with more robust protection and more streamlined management, thanks to McAfee® Endpoint Security and McAfee ePolicy Orchestrator® (McAfee ePO®) software.

As head of security, Jens Lindström oversees security operations for Norrköpings Kommun, a municipality of 140,000 inhabitants in Östergötland County, Sweden. Besides political governance, the municipality's services include water and waste management, construction and other permits, public transportation, libraries, parks and recreation, and schools.

Ransomware and Other Firefighting Not Acceptable for Small Security Team

Like so many of today's for-profit and non-profit organizations, Norrköpings faced an ever-increasing volume of ransomware attacks. "We provide our local population with many services, some of them absolutely critical, and disruption of services because of ransomware or anything else is simply not acceptable," says Lindström. "The impact can be enormous."

Furthermore, the Swedish municipality cannot afford to tie up its very small IT team remediating ransomware. To stay on top of security administration, it must avoid firefighting and simplify and streamline security wherever possible.

Ease of Management with McAfee ePO Software

Norrköpings Municipality first implemented McAfee Endpoint Protection several years ago when its trusted security provider Advania strongly recommended McAfee and praised its McAfee ePO software, the central management console built into many McAfee products that enables management of multiple security solutions from one screen.

"Upon license renewal, we looked at other security vendors but no one else could match the broad portfolio of security products that McAfee offers, or its ease of management thanks to McAfee ePO software," says Lindström. "We have been very happy with McAfee."

The Municipality initially implemented McAfee Endpoint Protection Advanced. When the license for this software expired, the organization upgraded to the McAfee Complete Endpoint Threat Protection suite to gain additional protection functionality such as Real Protect and Dynamic Application Containment functionality. Real Protect uses machine learning rather than manual intervention or signatures to stop difficult-to-detect malware, including ransomware, and reduces manual intervention by automatically unmasking, analyzing, and remediating hidden threats. Dynamic Application Containment quarantines suspicious, but not convicted, files in memory and stops potentially malicious changes from executing on the endpoint while the file can be analyzed.

Quick, Straightforward Migration to McAfee Endpoint Security

Not long after McAfee Endpoint Security version 10.2 became available, Lindström decided to migrate the McAfee VirusScan® Enterprise engine, McAfee Host Intrusion Prevention, and McAfee SiteAdvisor® functionality of its McAfee Complete Threat Protection suite to McAfee Endpoint Security to further bolster endpoint protection. By migrating to Endpoint Security,

intel Security

"Our single biggest driver for migrating to McAfee Endpoint Security and our biggest benefit thus far has been better protection. Since implementing Endpoint Security, we have seen a dramatic reduction in infected systems and ransomware attacks."

—Jens Lindström, Head of Security, Norrköpings Municipality

the municipality also consolidated each of these solutions to an integrated, single-agent approach.

"Migrating all 14,000 nodes took only a few hours each day for about a week," explains Lindström. "With the help of our partner Advania and the McAfee migration tool, it was extremely straightforward and not complicated at all. First, we rolled it out to all of our schools, then we moved on to the administrative networks."

Not long after rolling out McAfee Endpoint Security version 10.2, the organization upgraded to Endpoint Security version 10.5 to take advantage of Real Protect technology and even greater performance improvements. Upgrading took just a few days using McAfee ePO software.

Ransomware Slashed with Improved Endpoint Protection

"Our single biggest driver for migrating to McAfee Endpoint Security and our biggest benefit thus far has been better protection," notes Lindström. "Since implementing Endpoint Security, we have seen a dramatic reduction in infected systems and ransomware attacks."

Before implementing Endpoint Security, a ransomware attack on one PC could easily consume an entire day in clean up, creating a new desktop image, and restoring the system's data. "With the increasing pace of ransomware attacks, I was beginning to imagine a day in the not-too-far-off future when all my time would be dedicated to dealing with ransomware attacks," muses Lindström. "Thankfully, we implemented McAfee Endpoint Security before that could happen."

Much of the improvement in endpoint protection that Norrköpings Municipality is experiencing with McAfee Endpoint Security is due to the new endpoint protection framework's Dynamic Application Containment and Real Protect technologies. Dynamic Application Containment loads suspicious, but not convicted, files in memory and stops the potentially malicious from executing on "patient zero," essentially quarantining the questionable files so they can be analyzed. Real Protect uses machine learning to automatically match attributes and behaviors of unknown files to threat models to effectively convict zero-day malware, including ransomware.

In the future, Lindström would also like to add McAfee Endpoint Threat Defense and Response to automatically prioritize suspicious activity and provide live and historical threat data to determine the full scope of an attack before using one-click correction across the entire organization.

Day-To-Day Security Management Eased

"The improved graphical user interface in McAfee Endpoint Security has helped me a lot in my role as the day-to-day security administrator," adds Lindström. "Dealing with endpoint security has become much easier and more streamlined since we migrated. I can quickly see what tasks require action and more easily do many of those tasks, such as push updates across the enterprise."

intel Security

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