CASE STUDY

McAfee Endpoint Security and Upgrades Improve Speed and Safety of 175,000 Desktops

Advanced threat protection and enhanced performance and usability

Fairfax County Public Schools

Customer Profile
- Eleventh largest public school district in the U.S., in Fairfax County, Virginia

Industry
- K-12 Education

IT Environment
- 175,000 Windows desktops, 100 Macs, and 400 servers in 232 different locations

Public school districts everywhere face limited budgets for security. However, by relying on McAfee® Endpoint Security and keeping current with major upgrades, Fairfax County Public Schools has continued to update and fortify threat protection and improve desktop performance without breaking the bank. And, thanks to McAfee® ePolicy Orchestrator® (McAfee ePO™) software, one individual can manage desktop security even as the district's installed base has grown to more than 175,000 endpoints.

Connect With Us

For eight years, almost single handedly, Mehdi Harandi has been overseeing desktop security for the 175,000 desktops (and 400 servers that support desktop applications) across 232 schools and administrative offices in Fairfax County Public School District, the eleventh largest school district in the U.S. During his tenure as desktop management programmer, Harandi has witnessed exponential growth in the school district's installed base, data stored on users' PCs and laptops, and the number and type of cyberthreats faced.

Better Endpoint Protection that Still Requires Only Minimal Resources

Several years ago, the need for faster, more efficient scanning and more sophisticated malware protection drove the Fairfax County Public School District to replace its legacy endpoint protection—McAfee® VirusScan® Enterprise on desktops and another leading antivirus product on servers—with McAfee Endpoint Security and the McAfee ePO centralized console. "The newer McAfee antivirus software elevated our endpoint protection to a much higher level, while McAfee ePO [software] allowed us to continue managing endpoint protection for 175,000 desktops with just one person," says Harandi.

"With McAfee ePO [software], I can have a 50,000-foot view of all of our endpoints or deep dive for a 10-millimeter view," continues Harandi. "I can just click to push out a new policy or update and, within minutes, it is implemented on every single one of the tens of thousands of computers currently online—and to the others as they come online."

Upgrades Accelerate Scans and Enhance Usability

To benefit from continued improvements in performance and threat defense, Fairfax County Public Schools has continued to upgrade McAfee Endpoint Security. Just a few weeks before employees began working remotely in compliance with state COVID-19 shelter-in-place rules, the School District deployed McAfee Endpoint Security version 10.7 to take advantage of enhancements and prepare for a Microsoft Windows 10 rollout.

"Scan speed matters," says Harandi. "The faster the scan, the fewer complaints I receive. Faster scanning performance was the main reason we moved to McAfee Endpoint Security in the first place, and each upgrade has increased speed even more. Since full scans run in the background, our users are no longer aware that they are even happening. I can also set scans to use below normal percentage of the CPU."

"My phone used to ring off the hook on full scan day until we installed McAfee Endpoint Security," adds Harandi. "Now my phone is quiet."

McAfee Endpoint Security 10.7 also added usability and expert rules enhancements, enabling more fine tuning and granular rules. Harandi relies heavily on the endpoint security information built into the McAfee ePO dashboard.

Challenges

- Quick, full scans for malware without negatively impacting user experience
- Higher level of malware protection
- Desktop security management with one IT person
- Protection for 175,000 endpoints on limited budget

McAfee Solution

- McAfee Endpoint Security [with Advanced Threat Protection]
- McAfee ePolicy Orchestrator (McAfee ePO)

Results

- Dramatically improved virus scan performance and user experience
- More control over endpoint security management
- Reduced number of infections
- Better protection against fileless attacks
- Easy management of more than 175,000 endpoints by one IT person
- Fast full scans, eliminating calls from users

Adding Advanced Threat Defense Capabilities

Since implementing McAfee Endpoint Security, Harandi has seen a significant reduction in the number of infections at the endpoint. More than half of the 175,000 endpoints are laptops. Since most malware experienced by school district PCs enters from websites and more employees are working from home—even before the pandemic—McAfee Endpoint Security Web Control has greatly reduced the number of such infections substantially.

The McAfee Endpoint Security user interface also enables Harandi to more easily determine how the malware entered, so he can implement measures to prevent it from striking again. For instance, if a user clicks on a malware-infested URL, the McAfee Endpoint Security firewall module can be quickly and easily set to block that IP address or URL. In the past, finding the source of the malware took much more time and hassle. According to Harandi, with McAfee Endpoint Security 10.7, the already excellent firewall module is even better, with more granular options and better default settings.

With McAfee Endpoint Security version 10.7, Mehdi also appreciates that Fairfax County Public Schools gains access to some of the functionality of Advanced Threat Protection without the need to buy any additional products. "With McAfee Endpoint Security 10.7, for instance, we can take advantage of McAfee® Global Threat Intelligence to provide near real-time knowledge of known threats," says Harandi.

Increased Context with Story Graphs and Enhanced Protection Against Fileless Attacks

With the upgrade to McAfee Endpoint Security 10.7, Harandi uses the Story Graph feature to graphically visualize important contextual details, allowing him to more quickly and easily understand the events leading up to a detected threat. This information accelerates time to response. To protect against fileless, dual-use, and live-off-the-land attacks, he also set threat protection rules to automatically delete files commonly targeted by ransomware malware, disable critical operating system executables, and modify application compatibility shims.

Smarter, Modular Endpoint Protection That Saves Hours

Thanks to the modular design of McAfee Endpoint Security, Harandi can fine-tune control to a much higher degree. "The modular nature of McAfee Endpoint Security makes it much easier to manage," affirms Harandi. "You can tweak the areas you want to tweak and leave the others alone."

As an example of the value of modularity, Harandi notes that scanning was conflicting with an application on a user's desktop. "In the past, I had to disable antivirus protection completely and leave the desktop unprotected until the patch became available," he says. "But with McAfee Endpoint Security, I was able to find exactly which module was causing the issue, temporary disable just that module, and find the conflict within less than one hour. Finding such a conflict before could easily have taken eight to 20 hours."

Set It and Forget It—and Take Advantage of Updates

"Before McAfee Endpoint Security, I had to babysit our endpoint protection," says Harandi. "Now I have been able to forget it about 99% of the time. I can trust it is working. Management doesn't have to hear about endpoint security at all."

"McAfee also keeps improving their products, so upgrading to benefit from the improvements has made imminent sense, especially since doing so is so easy," adds Harandi. "With McAfee Endpoint Security, despite our budget limitations, we have endpoint protection that positions us well for the future."

Harandi offers this advice to those considering upgrading to McAfee Endpoint Security 10.7: "If you already have McAfee Endpoint Security, check to make sure that your current and future operating systems are supported. If they are, then go for it. If your endpoint security is still based on McAfee VirusScan, I highly recommend using the migration tool in McAfee ePO [software] to convert your policies and configurations, then fine-tune, deploy to test systems, and roll out. You won't regret it."

"The newer McAfee antivirus software elevated our endpoint protection to a much higher level, while McAfee ePO [software] allowed us to continue managing endpoint protection for 175,000 desktops with just one person."

—Mehdi Harandi, Desktop Management Programmer, Fairfax County Public Schools

McAfee

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, McAfee ePO, 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 © 2020 McAfee, LLC. 4510_0620
JUNE 2020