Case Study

Easily Managed, Advanced Endpoint Security Results in 125,000 Safer Desktops and Happier Users

With migration to McAfee® Endpoint Security, this desktop security manager can single-handedly manage security for more than 125,000 endpoints as well as provide better protection and, thanks to improved performance, a much better experience for end users.

Fairfax County Public Schools

Customer profile
11th largest public school district in the US, in Fairfax County, Virginia.

Industry
K-12 Education.

IT environment
125,000 desktops and 400 servers in 232 different locations.

Challenges
- Time-consuming virus scans impacting user experience.
- Need for higher level of malware protection.
- Need to be able to manage desktop security with one IT person.
- Protect environment on limited budget.

Intel® Security solutions
- McAfee® Endpoint Security
- McAfee Endpoint Threat Protection

Results
- Dramatically improved virus scan performance and end user experience.
- More control over endpoint security management.
- Easy management of 125,000+ nodes by one IT person.
- No more calls on mandatory full scan day from upset users.

For five years, almost single handedly, Mehdi Harandi has been overseeing desktop security for the 125,000 desktops—and the 400 servers that support desktop applications—across 232 schools and administrative offices in Fairfax County Public School District, the 11th largest school district in the US. During his tenure as desktop security manager, Harandi has seen a lot of changes that affect desktop security, including the exponential growth in data stored on PCs and laptops.

Growth in Data Stored on PCs Straining Legacy Endpoint Protection

Harandi likens the impact of the tremendous growth in data volume on malware scanning to moving into a new home. "When you move from a tiny apartment, it doesn't take long and you can use a Honda Civic," says Harandi. "But when you try to move from a five-bedroom house, it takes a lot more time and the Civic just won't cut it anymore; you need an 18-wheeler."

"Our legacy endpoint protection was great when users had only 20 gigabytes on their hard drives, but now the operating system alone takes 20 GB," continues Harandi. "The volume of data and files on our 125,000 desktops has grown exponentially and, until recently, endpoint protection just hasn't kept pace."

For example, antivirus scans on some of the School District's data-heavy PCs didn't have enough time to finish before greatly impacting the end user's experience. "We knew we could use a higher level of anti-malware protection," notes Harandi, "but what drove us to act was the need for faster, more efficient scanning."

Easy Management of 100,000+ Nodes

Fairfax County Public Schools had a leading antivirus product protecting the servers that ran its desktop applications and McAfee Endpoint Threat Protection protecting its desktops. After a few years, however, the School District replaced the server protection with McAfee endpoint protection because all of its endpoints—desktops and servers, both growing in number—could be managed many times more easily using the single McAfee ePolicy Orchestrator® (McAfee ePO™) central console.

"In terms of IT, size matters," states Harandi. "What's good for protecting 500 nodes might not work well for 50,000 nodes, let alone our 125,000 nodes. We have access to 'free' malware software, but the amount of time needed to manage it would more than remove any initial cost benefit. With McAfee ePO software, I can click to push out a new DAT or policy and within 10 to 20 minutes it will be implemented on every single one of the 60,000 to 80,000 computers currently online." (Aside: Harandi purposefully sets the process to take 10 to 20 minutes so as not to overload the network, otherwise the information could be pushed out even faster.)

Accelerating Upgrade to Superior McAfee Endpoint Security

After hearing about the dramatic improvements in performance and better threat defense enabled by McAfee Endpoint Security, the School District decided to migrate the McAfee VirusScan® Enterprise, McAfee SiteAdvisor® software, and host intrusion prevention functionality of its previous endpoint suite to McAfee Endpoint Security.

"With McAfee Endpoint Security, I set it up once and then have been able to forget about 99% of the time. I can trust it is working. And neither I nor my bosses receive calls on scan days. Management doesn't have to hear about endpoint security at all."

—Mehdi Harandi, Desktop Security Manager, Fairfax County Public Schools

First Harandi ran a pilot of McAfee Endpoint Security on a handful of test PCs, then extended the test to five heavily used desktops with large hard drives. Once he was assured that there were no conflicts between McAfee Endpoint Security and desktop applications, he extended the migration to one administrative building, then to three school buildings (one high school, one middle school, and one elementary school), and, finally, to all remaining schools and administrative offices.

With McAfee Endpoint Security version 10.2, all of Harandi's requirements were met, so he pushed it out to half the School District. Since McAfee Endpoint Security 10.5 had become available after the rollout began, he then upgraded the desktops with McAfee Endpoint Security 10.2 to 10.5. The remaining desktops he migrated directly to McAfee Endpoint Security 10.5.

For the initial migrations to McAfee Endpoint Security 10.2 and the migrations directly from McAfee VirusScan Enterprise to McAfee Endpoint Security 10.5, Harandi used the migration assistant tool available through McAfee ePO software to transfer security policies and configurations to the new endpoint platform. (He did not need to use the tool again in the upgrade from 10.2 to 10.5.) "Some of our security policies apply to the McAfee Endpoint Security Threat Prevention module, some to its Firewall module, and some to its Web Control module, so the McAfee Endpoint Security migration tool helped immensely in translating from old platform to new," explains Harandi. "It did an excellent job."

Using the migration tool also helped educate Harandi on McAfee Endpoint Security. "The migration tool not only walks you through the migration steps, it helps you understand how the old and new compare, what's the same but perhaps done differently, and what's new," he notes. "It brings you up to speed quickly and fast forwards the migration process. It easily saved me a month if not more."

Smarter, Modular, More Granular Endpoint Protection That Saves Hours

With McAfee Endpoint Security, Harandi can now fine tune control to a much higher degree and employ "many more bells and whistles." For example, with McAfee VirusScan Enterprise, when Harandi ran a full scan every Tuesday, he couldn't use a scan cache, but with McAfee Endpoint Security, he can. Before, when a desktop was in presentation mode, nothing could be done to prevent the user from being impacted during the scan; she simply had to wait until the scan finished before being able to use her computer. With McAfee Endpoint Security, however, the scan occurs when the system is idle and not in presentation mode. In addition, now Harandi can easily set conditions for when to block or allow certain files, whereas before doing so was much more difficult if not impossible.

One of the biggest changes between the legacy endpoint protection and Endpoint Security is its modular design. "I am a big fan of modularity," states Harandi. "The modular nature of McAfee Endpoint Security makes it much easier to manage. You can tweak the areas you want to tweak and leave the others alone."

As an example of the value of modularity, Harandi shares that recently antivirus scans were 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, using a modular trouble-shooting approach, I was able to find exactly which module was causing the issue, temporarily 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."

"The migration tool not only walks you through the migration steps ... It brings you up to speed quickly and fast forwards the migration process. It easily saved me a month if not more."

—Mehdi Harandi, Desktop Security Manager, Fairfax County Public Schools

Better Endpoint Defense and Forensics

Faster troubleshooting and increased granularity and control is worth nothing, however, if it doesn't result in better protection. Since implementing McAfee Endpoint Security, Harandi has seen a significant reduction in the number of infections at the endpoint. He notes that most of the malware he sees enters the environment through websites. More than half of the 125,000 endpoints are laptops. Malware infections frequently arise from users surfing the web at home. McAfee Endpoint Security Web Control has 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 firewall 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. Harandi also claims that he finds the Web Control module in McAfee Endpoint Security much faster and more efficient compared to the previous McAfee SiteAdvisor software included in the School District's previous endpoint protection suite.

Goodbye Scan Day Phone Calls from Irritated Users

When asked about the performance of McAfee Endpoint Security, Harandi points to the lack of calls from grumpy or irate end users on Tuesdays—mandatory full scan day—as his metric for success. "My phone used to ring off the hook on Tuesdays and now it doesn't," he replies. Gone also are the never-ending scans that seriously impacted user experience.

According to Harandi, another reason for his quiet phone is that when the previous endpoint protection scanned a desktop's memory, the user was always impacted, but now the user hardly notices. "Desktops used to have two gigabytes of RAM; now they have 8, 16, or even 32 GB," explains Harandi. "Previous scans of memory could leave our users sitting idle, unable to use their computers for five or ten minutes—or what seemed 'forever' to them. With McAfee Endpoint Security, a desktop with 12 GB of RAM is only tied up for 20-40 seconds while memory is scanned."

Set It and Forget It

"In the past, I had to babysit our endpoint protection," says Harandi. "With McAfee Endpoint Security, I set it up once and then can forget about 99% of the time. I can trust it is working. And neither I nor my bosses receive calls on scan days. Management doesn't have to hear about endpoint security at all."

In short, concludes Harandi, "With McAfee Endpoint Security, we now have endpoint protection that positions us well for the future."

Thanks to the modular design of McAfee Endpoint Security, it will also be easy for Fairfax County Public Schools to add new Endpoint Security modules and functionality as McAfee introduces them. In addition, since McAfee Endpoint Security can communicate via the McAfee Data Exchange Layer (DXL) fabric, it can easily be integrated with McAfee Threat Intelligence Exchange and other security solutions to continue strengthening the School District's ability to maintain a robust threat defense lifecycle.

intel Security

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