Frostburg State University stops malware at its front door

Malwarebytes helps IT team achieve auditing and user experience goals

INDUSTRY
Education

BUSINESS CHALLENGE
Find a more efficient and effective solution to fight malware and other advanced threats, such as ransomware

IT ENVIRONMENT
Commercial antivirus, next-generation firewalls, group security policies

SOLUTION
Malwarebytes Endpoint Security and Malwarebytes Breach Remediation for Mac

RESULTS
- Reduced malware-related help desk tickets by 80 percent
- Saved time for the small IT team, who could then focus on other projects
- Enabled team to meet audit requirements for malware detection and reporting
- Delivered high return on investment

Business profile

Frostburg State University, part of the University System of Maryland, offers classes from its campus in the mountains of Western Maryland, at remote sites, and online. It offers undergraduate and graduate programs in the sciences, education, business, arts, and humanities for more than 5,600 students. Technology is essential to teaching and learning, and Frostburg keeps its infrastructure current with new innovations. As cyberthreats evolved from junkware to malicious attacks, Frostburg added Malwarebytes and shut it down at the front door.

> Time savings was the top benefit of Malwarebytes for us. Time really is money, and that was very evident with the size of our team.
>
> —Harry Fike, Technical Support Manager, Office of Information Technology, Frostburg State University

Business challenge
Stop the flood of threats

Frostburg's Technology Services, a team of four, is responsible for all of the university-owned endpoints—desktop systems, laptops, tablets, smartphones, point-of-sale systems, and kiosks. Faculty and staff were seeing a rising tide of adware, toolbars, pop-ups, and Potentially Unwanted Programs (PUPs) on their machines.

"We want to maximize our users' uptime," said Harry Fike, Technical Support Manager in the Office of Information Technology at Frostburg State University. "They need to be able to do their jobs without having to work on a device weighed down with malware."

Fike and the Technical Services team were being inundated with malware reports and infected machines. As they put it, a user only needed a few seconds to click something that caused them three hours of work. As malware evolved, they began to see threats that took over browsers and connected out to malicious sites.

"Our traditional antivirus did nothing with malware," said Fike. "But our audit requirements demanded a malware solution, as well as detailed reports. To save my time and sanity, I proposed Malwarebytes and the university purchased it."

The solution

Malwarebytes Endpoint Security

Frostburg purchased Malwarebytes Endpoint Security for protection against malware, exploits, and ransomware. Now, Malwarebytes provides an extra layer of protection on the computers, as well as on the point-of-sale systems and standalone kiosks.

Fike's team rolled out Malwarebytes through the Malwarebytes Management Console to existing machines. As new faculty and staff machines come online, the network management system automatically installs Malwarebytes. Frostburg also deployed Malwarebytes Breach Remediation for Mac on its Mac systems.

"The built-in security systems in the macOS are not considered sufficient by our auditors," explained Fike. "Malwarebytes is a great single solution that meets our auditing requirements and works on both Mac and Windows platforms."

IT team gets an "A" for productivity

As soon as Malwarebytes was deployed, malware-related help desk tickets dropped by 80 percent, which greatly reduced technicians' workloads. The team uses the Management Console to automatically scan endpoints, install or update systems as needed, and clean up any malware that happens to get through.

"Time savings was definitely the top benefit of Malwarebytes for us," said Fike. "I began to have free time again to focus on other aspects of my job. I think that's something people don't realize—time really is money, and that was very evident with the size of our team."

Delivering a great user experience

Users access most of the university's systems through a web interface. When malware caused a browser to misbehave it seriously disrupted their work. Now users rarely have an issue because Malwarebytes stops malware and ransomware at the front door. If malware gets in, Malwarebytes detects it and cleans it up.

"Malwarebytes operates in the background, so users typically aren't aware that it's working," said Fike. "We rarely have to go look at anything. Malwarebytes allows our users to do their jobs, which means we've achieved our goal."

Satisfying audit requirements

Frostburg's IT team now has a detailed overview of its endpoint "fleet" through the Management Console's active reporting. At a glance, they can see the health of each endpoint, target the devices reporting threats, review logs, monitor uptime, and see update status. They routinely scan endpoints to keep them clean and can initiate a full scan from the console if Malwarebytes detects a threat. Fike has set policies to automate most of these activities.

"The management console has been a really valuable tool for us," said Fike. "It also lets us check off the 'active reporting' box during audits."

"Malwarebytes does the job that it was designed to do," said Fike. "Our time is valuable, and we can focus on other things now because we trust it. We definitely received a good return on our investment."