Malwarebytes

CASE STUDY

Alamo Colleges District eradicates malware from endpoints

Malwarebytes keeps academic systems protected and open

INDUSTRY
Education

BUSINESS CHALLENGE
Increase endpoint protection while preserving academic openness

IT ENVIRONMENT
Symantec antivirus, firewalls, enterprise layers of security

SOLUTION
Malwarebytes Endpoint Security

RESULTS
- Minimized malware infections
- Freed IT support teams for other tasks and priorities by eliminating time spent on re-imaging machines due to malware
- Automated malware cleanup

Business profile

The Alamo Colleges District in San Antonio, Texas, helps students successfully acquire the knowledge and skills needed in today's world. Five colleges—San Antonio, St. Philip's, Palo Alto, Northeast Lakeview, and Northwest Vista—offer associate degrees, certificates and licensures in occupational programs, as well as arts and science courses that transfer to four-year colleges and universities. When malware began infecting systems, Alamo Colleges chose Malwarebytes to proactively defend systems against it and other cyberthreats, such as ransomware.

> Since deploying Malwarebytes, we've seen a dramatic reduction in malware infections. Malwarebytes gives our teams time to focus their efforts on other strategic priorities.
>
> —Oscar T. Salazar, IT Risk and Security Manager, Alamo Colleges District

Business challenge

Implementing the right amount of protection

Each of the district's five colleges has an IT team, and all teams collaborate with each other and staff at the district office. Together, they're committed to providing an open environment that encourages academic exploration while protecting the colleges' information. The IT teams are responsible for faculty and administrative PCs. Students own their systems, and that traffic is confined to a separate protected VLAN.

The district had deployed Symantec antivirus software on its endpoints, but more and more instances of malware were not being detected by the antivirus, firewalls, or Internet protections. IT system administrators received a growing number of calls from faculty and staff that their systems behaved in unusual ways, or performance slowed dramatically. Each college's IT team was spending unproductive time investigating issues or re-imaging affected systems.

"It was clear that our antivirus solution was not enough," said Oscar T. Salazar, IT Risk and Security Manager for Alamo Colleges District. "It needed assistance. We decided to look at adding another layer of endpoint protection."

Salazar and the colleges' IT teams began investigating options. As the teams talked with vendors and colleagues at other institutions, Malwarebytes kept coming to the top of the list.

The solution

Malwarebytes Endpoint Security

The team approached Malwarebytes with questions. How well would Malwarebytes work with the toolsets in place? Would it work with the antivirus solution? Could they use it on servers and on virtual machines? How far could they extend it? A proof of concept test answered all of their questions.

"The proof of concept was great," said Salazar. "Malwarebytes met our requirements and integrated well with our current security solutions. There were no conflicts or performance impacts, so we created a deployment plan and then rolled it out."

The team created a baseline policy for all systems and customized policies for systems in labs or other unique circumstances. They excluded specific URLs to block users from known malicious sites, and whitelisted other locations. When they installed Malwarebytes on systems, they did it "silently" so users were not disrupted and never knew that Malwarebytes was now protecting their systems. The team also deployed Malwarebytes on some critical servers.

Confidence in defenses

Malwarebytes now catches threats that previously slipped through the antivirus, giving the team confidence that endpoints are well protected. It has eliminated the need to re-image systems, because Malwarebytes is preventing malware and cleanup is automatic.

"Since deploying Malwarebytes, we've seen a dramatic reduction in malware infections," said Salazar. Malwarebytes frees up time so that our team can focus their efforts on more strategic priorities."

Visibility across everything

Malwarebytes gives each team new visibility into its college's systems, and Salazar's team at the district office can view the entire enterprise deployment from the Malwarebytes Management Console. For the first time, they can see at a glance if there are unprotected systems. Centralized visibility delivers insight that they never had before. Salazar's team pushes Malwarebytes logs to their SIEM system so that they can correlate data and perform more in-depth investigations.

"Our goal is to make sure that data is always accessible but protected," said Salazar. "As institutions of higher education, we can't lock down systems like private industry can. Malwarebytes enables us to be open—but secure—so that academic freedom can flourish."

About

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

Santa Clara, CA

malwarebytes.com

corporate-sales@malwarebytes.com

1.800.520.2796