Malwarebytes

CASE STUDY

Southern Wesleyan University gains insight into threats

Malwarebytes delivers an unprecedented level of protection

Business profile

Southern Wesleyan University (SWU) was established in 1906 as the Wesleyan Methodist Bible Institute with a mission to develop Christian character in its students while providing thorough intellectual training. Today, SWU is a four-year, private, liberal arts college. After ransomware hit an administrative system, SWU deployed Malwarebytes to elevate its protection.

Business challenge

A search for robust protection

SWU's main campus covers 350 beautiful acres in Central, South Carolina. More than 1700+ students pursue studies in undergraduate, graduate, evening, or online programs. The IT team keeps it all running smoothly. They manage a highly virtualized server infrastructure, user services, the network, databases, data analysis, and security. They also manage and support faculty, administrative, and lab PCs.

Faculty members have administrative privileges on their systems to install software for classroom use, which makes systems more vulnerable to malware and other attacks. But administrative and lab systems with Internet access also experienced malware infections. When a machine was infected, the IT team ensured that its files were backed up and then re-imaged it.

"We had a robust backup policy but no endpoint protection against advanced malware or ransomware," said Brian Bartlett, Systems Administrator and Assistant Director of Information Technology at SWU. "Prior to Malwarebytes, we had a ransomware attack that infected an endpoint and encrypted files on a server. We restored it from backup and no data was lost, but the incident made university executives aware of just how serious advanced malware can be."

OVERVIEW

INDUSTRY

Education

BUSINESS CHALLENGE

Protect systems against ransomware and advanced malware

IT ENVIRONMENT

SafeNet antivirus, Microsoft antivirus, network access control, firewalls

SOLUTION

Malwarebytes Endpoint Security

RESULTS

Stopped ransomware and advanced malware infections

Blocked more than 1 billion threats

Gained threat insight for intelligent, efficient response

The solution

Malwarebytes Endpoint Security

The ransomware instance propelled SWU to find a better endpoint security solution. The IT team wanted a solution that not only stopped advanced malware and ransomware, but allowed them to manage everything centrally. They also wanted better visibility into threats that were targeting SWU. If users noticed that their PCs were slow or behaving differently, they didn't always notify IT. That meant threats could dwell on the system or move laterally across the network in attempts to steal information or other assets—and no one would know.

All of the IT team members had experience using Malwarebytes, and they were familiar with Malwarebytes powerful features and strong reputation. That made their decision easy. SWU deployed Malwarebytes Endpoint Security on PCs campus-wide from the Malwarebytes Management Console.

Knowledge is power

"Since Malwarebytes, we've had no more ransomware or advanced malware infections," said Bartlett. "Malwarebytes stopped high volumes of adware, Trojans, access to malicious websites, PUPs, and exploits—more than one billion threats to date."

Visibility into the threat landscape gives the IT team power to target investigations and proactively strengthen defenses. Before Malwarebytes, SWU didn't realize how much of a target it was. Discovering millions of threats was eye opening. But now the team knows exactly what's caught and takes appropriate action.

Malwarebytes reporting also identifies users who experience disproportionately high numbers of malware attacks. The IT team can target additional training to those users, helping increase their awareness of cyberthreats and promoting safer Internet browsing.

> SINCE MALWAREBYTES, WE'VE HAD NO MORE RANSOMWARE OR ADVANCED MALWARE INFECTIONS. MALWAREBYTES STOPPED HIGH VOLUMES OF ADWARE, TROJANS, ACCESS TO MALICIOUS WEBSITES, PUPS, AND EXPLOITS—MORE THAN ONE BILLION THREATS TO DATE.
>
> BRIAN BARTLETT, SYSTEMS ADMINISTRATOR, ASSISTANT DIRECTOR OF INFORMATION TECHNOLOGY, SOUTHERN WESLEYAN UNIVERSITY

Intelligent threat response

The user services team uses Malwarebytes reporting with email alerts to investigate individual threats. They can see the status of every system, easily hand off instructions to a technician, and ensure that all systems are up to date. Threat response is targeted and informed using Malwarebytes data. The data also provided the IT team with an accurate view of SWU's specific threat landscape so that they could increase security in other areas.

"The ransomware attack certainly raised the university's awareness of cybersecurity risk," said Bartlett. "Malwarebytes validated the size and extent of the risk. As a result, we received support for upgrading our security measures and policies, which benefits the entire university community.

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware and exploits that escape detection by traditional antivirus solutions. Malwarebytes completely replaces antivirus with artificial intelligence-powered technology that stops cyberattacks before they can compromise home computers and business endpoints. Learn more at www.malwarebytes.com.