Malwarebytes

CASE STUDY

All Saints Grammar turns the tables on persistent malware

Malwarebytes finds hidden threats and restores IT confidence

Business profile

Located in Sydney, Australia, All Saints Grammar is a co-educational school for students from pre-kindergarten to Year 12. A rich curriculum and host of tailored programs help ensure that students have every opportunity to grow with confidence and make the most of their individual gifts and talents. However, zero-day malware attacks increasingly threatened school systems. All Saints Grammar chose Malwarebytes to turn the tables.

Business challenge

Fighting persistent attackers

All Saints Grammar provides computer endpoints for teachers, administrators, and staff and has recently moved toward a complete Bring Your Own Technology (BYOT) environment for students. The IT team is responsible for everything from infrastructure, security, and servers to applications and classroom technology. The team also provides support to students with their systems when a computer problem interferes with learning.

"We stipulate that students take charge of their personal device's health with antivirus and antimalware solutions," said Andre Tomlinson, Network Administrator/IT Manager at All Saints Grammar. "My primary concern is keeping cyber threats from entering our network via endpoints."

When Andre noticed a growing number of "weird" misbehaving systems, he initially discovered that the school's Sophos antivirus updates were failing. He sandboxed one severely infected computer and contacted Sophos for assistance.

"For several months, this threat constantly mutated on the sandboxed machine," said Andre. "Sophos' products couldn't detect or clean it. Hours were spent with numerous support staff via remote sessions, sending logs and virus samples, and trialing utilities and other third-party tools. Each time the machine was re-infected with a variant strain and the whole support process

OVERVIEW

INDUSTRY
Education

BUSINESS CHALLENGE
Protect endpoints from rapidly evolving malware and system compromise

IT ENVIRONMENT
Windows Defender, Sophos email filtering, other layers of enterprise security

SOLUTION
Malwarebytes Endpoint Protection

RESULTS
Detected high volumes of dangerous malware and threats that the Sophos antivirus had missed

Identified potential vulnerabilities and blocked access to compromised websites

Increased browser performance for users

Restored trust in endpoint protection

> MALWAREBYTES IS A HUGE SUCCESS. IT KEEPS TEACHERS TEACHING, STUDENTS SAFER, AND ALLOWS ME TO FOCUS ON MORE STRATEGIC IT ISSUES. IT DELIVERS CONFIDENCE, WHICH ENABLES ME TO SLEEP AT NIGHT—SOPHOS DID NOT.
>
> ANDRE TOMLINSON, NETWORK ADMINISTRATOR/IT MANAGER, ALL SAINTS GRAMMAR

began again. They didn't seem interested in analyzing the system in depth, and they finally told us to re-image the system. I lost all faith in their solution."

The final blow came when the payroll administrator's system became infected. Bank logon details were harvested, and the school was notified that two personal bank accounts had been frozen due to suspicious logon activity. The school worked with Sophos and the banks to try and remedy the problem with software tools but failed. Again, the only solution was to re-image the system to be absolutely sure.

"When you can't trust your machine, you can't do your job," said Andre. "We needed a solution—and a vendor—that took malware seriously."

The solution

Malwarebytes Endpoint Protection

The All Saints Grammar IT team began searching IT forums for suggestions, and Malwarebytes repeatedly came up as a recommendation. After contacting Malwarebytes, All Saints Grammar conducted a trial and chose it to replace Sophos.

"Malwarebytes Endpoint Protection was the best product for us," said Andre. "It's quick, it's easy, and it doesn't require onsite resources. After some short tutorials, we installed it on 20 machines to test and then began to roll it out."

He said previously, Sophos had been difficult to install and manage on Mac systems. Malwarebytes installed easily on Macs, and these systems were integrated seamlessly in the centralized cloud console. The team simultaneously removed Sophos and deployed Malwarebytes across Macs, PCs, and virtual servers.

Nothing can hide

Immediately, Malwarebytes identified a wide range of malware on a large number of endpoints. It detected malware hiding in the "known trusted image" that the team used to restore systems. It detected Trojans, cryptomining, and other advanced malware. It even found persistent malware on the payroll system—after it had been reimaged. Frame extensions, browser hooks, and other latent malware had been embedded in a roaming profile and had followed the user from system to system. Malwarebytes also identified suspicious vulnerabilities in several Active Directory Group Policy settings, which the team was able to easily exclude from future scans.

"The cloud management interface is clean, fast and intuitive," said Andre. "It presented information about our systems in a concise way that allowed a quick response to threats."

He also said that Malwarebytes' ability to block infected websites is one of its biggest benefits. Malwarebytes has blocked sites that staff trust and use daily, preventing access to previously unknown threats. Recently, when the team began installing an Open Source FTP application, Malwarebytes detected and blocked numerous outbound connections to third-party marketing websites.

"It's great to have a solution that precisely tells you what it finds," said Andre. "Malwarebytes found tons of malware and vulnerabilities that we weren't previously aware of. Malicious website blocking and system cleaning has significantly increased browser performance."

Restored trust

Malwarebytes restored the IT team's trust in its endpoint protection. It proactively detects and blocks attempts to compromise application vulnerabilities and remotely execute code on the endpoint. Malwarebytes machine learning and payload analysis keep the school ahead of emerging threats without relying on signatures that quickly mutate. Updates are automatic, so that Andre and his technician don't have to take systems offline to distribute updates.

"Malwarebytes is a huge success," said Andre. "It keeps teachers teaching, students safer, and allows me to focus on more strategic IT issues. It delivers confidence, which enables me to sleep at night—Sophos did not."