Malwarebytes

CASE STUDY

San José Unified School District cleans up Mac malware

Malwarebytes protects sensitive data on teachers' MacBook laptops

INDUSTRY
Education

BUSINESS CHALLENGE
Protect student data from threats posed by malware on teachers' MacBook laptops

IT ENVIRONMENT
Avast antivirus, enterprise network security layers

SOLUTION
Malwarebytes Incident Response

RESULTS
- Removed PUPs and malware from hundreds of Mac systems in just minutes
- Delivered instant visibility into connected systems and quarantined malware
- Reduced risk with ability to proactively detect and remediate threats

Business profile

San José Unified is an innovative, urban school district in Silicon Valley. The district prepares more than 30,000 of today's students to be the thinkers, leaders, and creators of tomorrow. When malware began to increasingly attack teachers' Macs, the district chose Malwarebytes for advanced threat detection and proactive remediation.

> Malwarebytes Incident Response is one of the best tools we have on our tool belt. It's easy to deploy, use, and understand, and gives us great insight.
>
> —Patrick Scanlan, Supervisor Technology & Data Services, San José Unified School District

Business challenge

Get one step ahead

San José Unified is Silicon Valley's largest and most diverse school system, operating 41 schools ranging from kindergarten through high school. Supporting the district's technology is a staff of 30 who purchase, manage, and maintain more than 10,000 devices. Teachers receive reliable, easy-to-use MacBook laptops for teaching and home use. In the past two years, the IT team began seeing a significant rise in malware infections. Soon, the team was scanning Macs for almost every teacher needing tech support and finding that a large number of the systems had malware. Sometimes the malware had been on the system for months without the user knowing it.

"Teachers often have student data, parent contact information, email addresses, and other data that must be kept private," said Patrick Scanlan, Supervisor Technology & Data Services for the San José Unified School District. "They didn't realize they had malware on their systems or that downloads to their systems could be trying to trick them into divulging sensitive information."

Fake Adobe Flash installations were the most common culprit. High volumes of phishing attacks also made users vulnerable to fake emails and malicious links. Phishing was so rampant that the district once was blacklisted for 30 days and blocked from sending emails to other organizations.

"We knew that the longer malware is on a system, the higher the risk to the district," said Scanlan. "We wanted to remove malware as quickly as possible and proactively protect users' systems from having malware-related problems."

The solution

Malwarebytes Incident Response

The team chose Malwarebytes Incident Response for their Macs and never looked back. Initially they deployed Malwarebytes to thousands of teacher laptops through the district's mobile device management system. Today, they automatically install Malwarebytes on every new teacher computer and use the web-based dashboard to manage everything.

"The fact that we can deploy Malwarebytes through our mobile device management system is fantastic," said Scanlan. "It's really fast and easy to push out."

Fast, simple and worry-free

Before Malwarebytes, finding and removing malware meant manually reviewing mobile device management log files to get the most basic information. In just the first few weeks, Malwarebytes Incident Response automatically identified and removed large amounts of malware from teachers' systems. The IT team also found Potentially Unwanted Programs (PUPs) such as Genieo, IronCore, Mindspark, MacCleaner, and fake antivirus products.

"Having a web-based dashboard is great," said Scanlan. "We can immediately see how many clients are currently connected, view the quarantine and all of the discovered malware, run weekly scans, and do everything without affecting users. When Malwarebytes finds malware, it cleans up the Mac system in about a minute from start to finish."

Nonstop protection

Protection keeps working even after teachers leave school. Once the systems are outside of the district's environment, they are vulnerable to malware coming from the Internet on a home connection or hidden on a home network. Scanlan says that was always a concern in the past. With Malwarebytes, the system can still be scanned and proactively prevent malware from infecting the machine.

"Malwarebytes Incident Response is one of the best tools we have on our tool belt," said Scanlan. "It's easy to deploy, use, and understand and gives us great insight."

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