

MITCON stops ransomware and improves clients' experience

Malwarebytes reduces management overhead and client downtime

INDUSTRY
Technology

BUSINESS CHALLENGE
Stop ransomware while improving endpoint security manageability


IT ENVIRONMENT
Windows Defender, layered enterprise-level security infrastructure

SOLUTION
Malwarebytes Endpoint Security

- RESULTS
- Stopped ransomware incidents
 - Reduced overall incidents and time spent remediating endpoints and servers
 - Increased clients' uptime by eliminating disruptive scans
 - Deployed complete endpoint protection in a small footprint

Business profile

Midland Information Technology Consortium (MITCON) provides end-to-end IT services for nonprofit organizations and foundations in Michigan's Great Lakes Bay region, which includes Midland, Saginaw, Bay, Clare, and Isabella counties. Thanks to MITCON, member organizations can spend less on IT and more on serving their constituencies. Keeping overhead to a minimum while delivering great service is key—for both MITCON's lean IT team and its member organizations. That's why MITCON chose Malwarebytes.



Keeping clients' endpoints and data safe are priorities for us. Malwarebytes is an integral piece of our security infrastructure to help us achieve that mission.

—Dawn Wright, Program Manager, MITCON

Business challenge

Stopping ransomware while improving manageability
Client organizations connect to MITCON over a countywide network, much like branch offices would connect to their headquarters. Direct connection enables MITCON to manage client workstations and provide help desk and end user support. Antivirus protection has always been part of MITCON's service offering for its clients. In the past, users commonly were afflicted with adware and nuisanceware, such as pop-up advertising, toolbars, and browser hijacks. But recently, ransomware had become a major concern.

"We never had a solution that would proactively stop ransomware," said Matt Space, Network Engineer at MITCON. "By the time we'd find a ransomware infection, the damage was done."

Oftentimes, the first indication of a ransomware infection was a user calling to say that they couldn't open files on a server. When the MITCON team delved into the issue and determined that the user's files were indeed encrypted, they immediately located and isolated the machine—patient zero. Then a team member would drive to the client's location, physically pick up the machine, and bring it back to the office for reimaging. MITCON's longstanding policy was that it was faster and more cost-effective to simply reimage and restore it from the previous day's backups. Even though the remediation process went smoothly, it still took a lot of time and effort to restore



everything to normal and left the end-user in limbo until the process was completed.

MITCON's previous antivirus solution wasn't helping matters. Software bugs and functionality issues caused client and server hard drives to fill up with temporary files, bringing them to a halt. When computers stopped working and servers also came to a crawl, it was simply unacceptable.

"We went back to the drawing board and re-evaluated potential antivirus and anti-malware solutions," said Dawn Wright, Program Manager for MITCON. "We'd tried numerous other offerings in the past but they wouldn't alert us to ransomware until the infection had already occurred. We needed a complete endpoint solution—one that worked while being manageable and cost-effective."

The solution

Malwarebytes Endpoint Security

MITCON tested Malwarebytes Endpoint Security on a few machines and it immediately set off alerts when it detected exploits that the team had no idea were on the machines. After seeing how easy it was to manage the decision to move forward was easy, so they purchased it and began deploying it. Deployment was straightforward. Malwarebytes scanned machine addresses and detected the computers. With a click it was installed, and clients began reporting back with status reports.

Benefits in black and white

MITCON's IT team used their own computers as the initial deployment machines. They weren't quite prepared for what they found.

"We all have good computer and online habits and don't open things we're not supposed to," said Rocky King, Technical Network Manager for MITCON. "Talk about surprising IT folks—it was almost a contest to see which one of us was the most infected. Malwarebytes caught all of the things that our previous antivirus software missed. That's one of the things we really liked about it."

Malwarebytes intelligence detects anomalies in how a threat behaves. Even if the malware isn't known, Malwarebytes can quarantine anything that is acting suspiciously and prevent it from reaching the desktop. Since deploying Malwarebytes, MITCON has not had any ransomware incidents.

"We knew that the previous product wasn't working," said Space. "But when we deployed Malwarebytes, it was like a slap in the face to actually see the other product's deficiencies in black and white."

The strong, silent solution

One of the most attractive Malwarebytes features, besides its effectiveness, is its ability to run in the background without affecting the user's experience. In the past, the team had to schedule full scans at night because it slowed users' machines to a crawl. Now, Malwarebytes can do a full scan of the C drive in the background, and users don't even know it's running. MITCON also hasn't experienced any conflicts between Malwarebytes and other software.

"I can't tell you how excited we were to have software with a proven track record," said Wright. "We finally had a solution that we could deploy to the consortium and have confidence that it worked silently in the background."

Staying safe and healthy

MITCON's responsibility to its clients is making sure that they have healthy, functioning computers. The Malwarebytes Management Console surpassed MITCON's requirement for ensuring client machine health while reducing overhead. The team of six is responsible for all IT operations and does not have a dedicated security team. Now, they can centrally track the health of hundreds of client endpoints located all over the region and make sure that they have a handle on threat issues.

"The number one thing for us is being able to gauge the overall health of our nodes on our network," said King. "We need to know if something's emerging. If a machine alerts us to a threat, we can automatically scan and remove it. If we start getting alerts from multiple groups and identify a trend, we can quickly and actively resolve it."

Besides ensuring healthy computers, MITCON also takes responsibility for protecting clients' data. That means protecting its servers and other infrastructure as well.


"Keeping clients' endpoints and data safe are priorities for us," said Wright. "Malwarebytes is an integral piece of our security infrastructure to help us achieve that mission."


| 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