

AvMed gets insured against malware and ransomware

Health insurance company proactively blocks the latest exploits and malware with Malwarebytes

INDUSTRY
Healthcare

BUSINESS CHALLENGE
Stop nuisance-ware and cyber threats from robbing IT and user productivity

IT ENVIRONMENT
Check Point antivirus, McAfee on servers, Proofpoint Email Protection, network firewalls, web filtering, and URL filtering


SOLUTION
Malwarebytes Endpoint Security, which includes Anti-Malware for Business, Anti-Exploit for Business, and the Management Console

RESULTS

- Achieved visibility into the extent and types of threats targeting users' machines
- Dramatically reduced IT time spent cleaning and re-imaging machines
- Gained ongoing, proactive protection

Business profile

AvMed offers affordable health insurance solutions for businesses and individuals in Florida. More than 340,000 members count on AvMed for their health insurance coverage. When malicious exploits began sneaking in, AvMed chose Malwarebytes for better protection and greater visibility.



Malwarebytes is proactive protection. We see it block malware and ransomware every day. It works perfectly for us.

—Juan Forero, Lead Info Security Engineer, AvMed

Business challenge

Stop the exploits

Like many organizations, AvMed began seeing a growing volume of threats in the past two years. Employees frequently called IT with complaints about poor computer performance, and the team would scan the machine, looking for malware. Initially, the majority of malware that they found was nuisance-ware, such as toolbars and Potentially Unwanted Programs (PUPs). However, increasingly they found that users had clicked on malicious URLs, or that exploits had successfully gained access undetected by firewalls or antivirus. Because AvMed is responsible for protecting policyholders' health and financial information, exploits and threats like ransomware represent a dangerous risk.

"We were cleaning or re-imaging machines several times a week," said Juan Forero, Lead Info Security Engineer at AvMed. "And those were just the machines we knew about. Without visibility into all of our users' machines, it was hard to know just how widespread the infections were."



The solution

Malwarebytes Endpoint Security

AvMed had deployed a McAfee antivirus solution on its servers, but they didn't want to put it on users' computers because it significantly slowed performance. Forero and other members of his team had prior experience with Malwarebytes, and they knew that it worked almost invisibly in the background. They chose Malwarebytes Endpoint Security to gain a powerful multi-layered defense against the latest, most dangerous malware, including ransomware.

The team initially deployed Malwarebytes to users in the smallest departments with Microsoft System Center. It worked so well that they rolled out the solution globally. Because Malwarebytes has a small system footprint, users aren't disrupted by the security protection it delivers. They now work without even being aware of malware scans occurring in the background.

"One thing that's really helpful is support for Macs," said Forero. "Some of our users have Macs, and now we can deploy Malwarebytes to protect them too."

Better visibility for stronger defense

Almost immediately, the team saw how much malware existed on users' machines, and they were able to quickly clean infections and install protection. Using the Malwarebytes Management Console, they also initiated policies for scheduled scanning of endpoints to keep machines clean and maintain a high level of protection.

Comprehensive reporting identifies vulnerable endpoints and aggregates reporting to show the status of users' machines at a glance. The team receives alerts, they can ensure that all machines are up to date, and they can see exactly what's going on if a user clicks on an infected link.

"We schedule scans, updates—everything," said Forero. "If a user's machine is becoming infected because something slipped by the firewall and the user clicks on it, we see it in Malwarebytes and can take action right away. It's been great."

Proactive protection

Since AvMed deployed Malwarebytes, it has dramatically reduced malware activity on users' machines. PUPs, toolbars, and exploits are blocked, resulting in far fewer infections.

"Malwarebytes is proactive protection," said Forero. "It effectively blocks incoming threats—even catching those that the firewalls or antivirus missed. Malwarebytes saves us lots of time and worry about what might be getting in."





Effective ongoing defense

The AvMed team knows that new threats arise every day. But they appreciate the fact that Malwarebytes threat data is continuously updated and even the latest threats are quarantined or blocked effectively.

"Malwarebytes updates its database faster than anybody else," said Forero. "By the time something slips by a traditional antivirus tool, the damage is already done. We see Malwarebytes block malware and ransomware every day. It works perfectly for us."

| About

Malwarebytes provides anti-malware and anti-exploit software designed to protect businesses and consumers against zero-day threats that consistently escape detection by traditional anti-virus solutions. Malwarebytes Anti-Malware earned an "Outstanding" rating by CNET editors, is a PCMag.com Editor's Choice, and was the only security software to earn a perfect malware remediation score from AV-TEST.org. That's why more than 38,000 SMBs and Enterprise businesses worldwide trust Malwarebytes to protect their data. Founded in 2008, Malwarebytes is headquartered in California, operates offices in Europe, and employs a global team of researchers and experts.

-  Santa Clara, CA
-  malwarebytes.com
-  corporate-sales@malwarebytes.com
-  1.800.520.2796