Malwarebytes

CASE STUDY

American National finishes the job on malware removal

Malwarebytes leaves no malware remnants behind

INDUSTRY
Financial services

BUSINESS CHALLENGE
Ensure that machines are completely free of malware

IT ENVIRONMENT
Cisco Advanced Malware Protection (AMP), Cylance, layered enterprise security model

SOLUTION
Malwarebytes Breach Remediation

RESULTS
- Removed remnants of malware that other solutions missed
- Simplified remediation for help desk staff
- Freed time for advanced security training and projects

Business profile

American National offers a wide range of life and property/casualty insurance products for more than 5,000 individuals, agribusiness, and commercial policyholders. Headquartered in Galveston, Texas, American National employs 3,000 people, and is represented by agents in all 50 states and Puerto Rico. When the IT team needed a lightweight—but highly effective—remediation solution, it turned to Malwarebytes.

> Malwarebytes Breach Remediation does a great job. In some cases, Cisco AMP or Cylance removed portions of malware but left remnants behind. Malwarebytes completely cleans things up.
>
> —Fran Moniz, Network Security Architect, American National

Business challenge

Malware is inevitable

When Fran Moniz arrived at American National as its Network Security Architect, one of his first tasks was to streamline security platforms. He replaced McAfee and Symantec antivirus solutions with a Sophos product and augmented it with Cisco Advanced Malware Protection (AMP). A year later, he added Cylance threat prevention to the infrastructure.

"Unfortunately, the antivirus solution interfered with both Cisco AMP and Cylance," said Moniz. "When we ran them together, we experienced malware infections. I removed the antivirus and now rely on the other tools to protect us."

Cisco AMP runs on the company's IronPort email gateways, and Moniz uses Cylance on company servers. When a malicious email or suspicious item evades detection at the gateway, the network-monitoring tool alerts the team, but it doesn't actively block potential threats. Threats are becoming more specialized, and

American National saw new forms of malware get through its other solutions unrecognized. That's why they needed a fast, efficient remediation solution.

The solution

Malwarebytes Breach Remediation

Moniz had used Malwarebytes in the past and turned to Malwarebytes again for Breach Remediation. When the team receives an alert about potential malware on a machine, they scan the machine with Malwarebytes Breach Remediation.

"Malwarebytes Breach Remediation does a great job," said Moniz. "In some cases, Cisco AMP or Cylance removed portions of malware but left remnants behind. Malwarebytes completely cleans things up, especially browser plug-ins, Potentially Unwanted Programs (PUPs), and toolbars."

Help for the help desks

American National has two help desk teams. With Malwarebytes deployed internally, the internal help desk staff might receive a request for scanning a machine only once or twice a month. However, independent agents located across the country own their machines and usually don't have an IT team to make sure that they have adequate, updated malware protection. A second help desk team supports agents, using Malwarebytes Breach Remediation several times a week to scan an agent's machine. Because Malwarebytes is lightweight and efficient, help desk staff can scan and remediate machines remotely without disrupting the agent's work.

Moving toward real-time response

Fewer malware incidents to worry about and fast, easy remediation with Malwarebytes freed Moniz's team for more proactive, strategic projects. For example, they now have time for advanced security training. They also are focusing more on anomalies that could signal the presence of an advanced persistent threat (APT) or other serious attack.

"We're more proactive and aiming to shorten response times to as close to real-time as possible," said Moniz. "Malwarebytes Breach Remediation is a great solution for helping us make sure that machines are as clean as they can be."

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