Malwarebytes

CASE STUDY

Lipari Foods puts ransomware on ice

The company distributes Malwarebytes to its corporate and mobile endpoints to prevent zero-day and ransomware attacks

INDUSTRY
Food distribution

BUSINESS CHALLENGE
Prevent zero-day exploits and attacks such as ransomware

IT ENVIRONMENT
Data center with Trend Micro antivirus, firewalls, web filtering, and Intrusion Prevention Systems

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

RESULTS
- Stopped ransomware from successfully disrupting business
- Simplified anti-malware and anti-exploit management across corporate and mobile endpoints
- Helped increase user and help desk productivity by reducing the need to re-image machines

Business profile

Lipari Foods distributes more than 15,000 deli, bakery, dairy, meat, seafood, confection, and packaging products to grocers, supermarkets, convenience stores, and food services. Distribution is a subject that Lipari Foods knows well. So when distributed forms of malware began to show up on employees' computers, Lipari Foods shut them down with Malwarebytes.

> There have been no more Cryptolocker infections. Malwarebytes Endpoint Security is definitely one of the best tools around to fight the scary stuff trying to get in.
>
> —Alex Blondell, IT Help Desk Manager, Lipari Foods

Business challenge

Keep out malicious threats while simplifying management

"We started seeing a growing number of malware problems," said Alex Blondell, IT Help Desk Manager for Lipari Foods. "We got infected emails from customers. Internet browsing delivered malvertising, pop-ups, Potentially Unwanted Programs (PUPs), and redirects. When several users were hit by Cryptolocker, we knew we needed more protection."

Although Lipari Foods uses a signature-based Trend Micro antivirus product, it wasn't catching all zero-day malware or ransomware. Each time a user called the help desk to report suspicious emails or locked files, the help desk team had to quarantine the computer, scan it, and usually re-image it. Field salespeople lost use of their machines until they could be sent a clean computer. And that often meant they couldn't help customers as effectively, take orders, or access sales data.

Blondell and the help desk team wanted a way to stop exploits from delivering ransomware and other threats that infected their

machines, as well as a better way to manage protection across the company's endpoints. Already familiar with Malwarebytes, they chose Malwarebytes Endpoint Security.

The solution

Malwarebytes Endpoint Security

Malwarebytes Endpoint Security provides a powerful multi-layered defense engineered to defeat the latest, most dangerous malware, including ransomware. It includes Malwarebytes Anti-Malware for Business, Anti-Exploit for Business, and the Management Console in one comprehensive solution.

Ransomware such as Cryptolocker is typically distributed using phishing campaigns or compromised websites. By combining anti-exploit and anti-malware capabilities, Malwarebytes helps protect against zero-day malware threats, blocks exploits, and prevents malicious payloads from being delivered. Malwarebytes Anti-Malware for Business detects and eliminates zero-hour malware, Trojans, worms, rootkits, adware, and spyware in real time. Malwarebytes Anti-Exploit for Business adds four additional layers of protection.

Accelerating protection with easy installation

With about 250 endpoints used by salespeople on the road, the help desk team needed to deploy Malwarebytes on both mobile and in-house PCs. Once the solution was configured, the help desk team sent an email to mobile employees and provided a link to the Malwarebytes installer. With just a click, they were up, running, and protected. There hasn't been a single successful Cryptolocker attempt since.

Centralized, simplified visibility

Blondell uses the Malwarebytes Management Console to manage endpoints. From a single screen, he can update, monitor, and manage distributed Malwarebytes clients. Now the team can remotely scan a machine for suspected malware. If they uncover malware or ransomware, Malwarebytes automatically cleans it up. Blondell also reports that Malwarebytes works well with their traditional antivirus solution.

"Now we push updates and know that protection is deployed consistently," he said. "We know what's covered and that it's up to date."

Malwarebytes operates in the background, so users aren't affected by updates or scans. Users also can manually scan their computers themselves if they suspect suspicious behavior. It's easy, and they don't have to wait for a regular, policy-initiated scan to know that they're protected.

Peace of mind

In spite of other vendors' promises to be the only tool needed for fighting malware, Blondell believes that a layered approach is more effective. He has achieved much better results with Malwarebytes as another layer of protection, and it catches and cleans up malware that the other tools miss.

"Malwarebytes Endpoint Security gives us peace of mind," he said. "It's definitely one of the best tools available to fight the scary stuff that's trying to get in."

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