Wunderlich invests in ransomware protection

Malwarebytes helps proactively protect company and customer data

INDUSTRY
Financial services

BUSINESS CHALLENGE
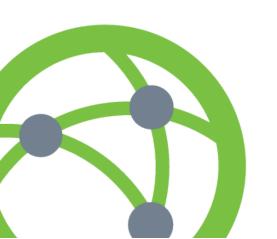Protect data against ransomware and exploits entering through endpoints

IT ENVIRONMENT
Data center with Symantec Endpoint Protection antivirus, firewall, IPS, IDS, IronPort appliances, Dell SecureWorks Information Security service

SOLUTION
Malwarebytes Endpoint Security

RESULTS
• Stopped ransomware at the door
• Delivered a highly accurate view of actual threats that Symantec missed
• Saved at least eight hours per week in tracking down alerts
• Achieved better alignment with FINRA compliance requirements

Business profile

Wunderlich is a full-service investment firm in Memphis, Tennessee. It provides a range of wealth management, investment banking, and advisory services to individuals, corporations, and institutional clients. Because ransomware threats and phishing attacks have dramatically increased against financial services organizations, Wunderlich invested in another layer of protection.

> Malwarebytes has been like having another staff member on our team. It's really beneficial and a big win for our department and company.
>
> —Aaron Goodwin, Chief Information Officer, Wunderlich

Business challenge

Protect company and customer data from being held hostage

Aaron Goodwin, Chief Information Officer at Wunderlich, is focused on securing Wunderlich's assets, which include endpoints for 450 employees in 26 offices across 17 states. As Internet and email threats have increased over the past few years, his team has seen almost everything—from viruses, adware, Trojans, and browser redirects to active phishing campaigns and ransomware.

"We're laser-focused on security for our company and for our customers," he said, "and we continually look for ways to improve protection. Cyber terrorism and cybercrime are real threats that we worry about daily. The cost of a breach is not only financially costly, the loss of reputation and client trust can be devastating."

Wunderlich financial advisors, accounting staff, and corporate officers had begun to experience a high volume of phishing attacks, with emails spoofed to look like they came from executives requesting financial disbursements. Although the team worked with a partner to improve the effectiveness of the company's IronPort appliances, the spoofing problems remained. User training helped make employees more aware of potential threats, but the security team still was overwhelmed with high numbers of false alerts.

The solution

Malwarebytes Endpoint Security

The company's Symantec antivirus solution wasn't helping much. It frequently missed malware and issued false alerts. The team spent hours tracking down potential problems with no visibility into what—or where—they might be.

"We knew that we didn't have a full endpoint protection solution," said Goodwin. "We needed better malware protection, as well as an anti-exploit capability, because Symantec just isn't picking up these threats."

Goodwin and his team deployed a proof-of-concept trial with Malwarebytes Endpoint Security on 100 machines. Malwarebytes was easy to use. After whitelisting one specialized investment-related application file, it worked with no false positives. The team built the endpoint configuration in the Malwarebytes Management Console and pushed it to users' machines with Dell KACE.

Stopped ransomware at the door

As soon as Malwarebytes was deployed, it found 20,000 pieces of malware and began cleaning it off systems. Once the systems were clean, the number of malware pieces dropped to approximately 50. Shortly after deployment, Wunderlich experienced a ransomware attack. Malwarebytes caught it, notified the team, and they were able to stop it from infecting 12 targeted machines before any damage was done.

"Malwarebytes takes away threats before they reach my end users," said Goodwin. "It's a huge relief, and it stops issues from propagating through the network to cause major problems."

Delivers an accurate view

Goodwin uses the Malwarebytes Management Console daily, and it saves him from "chasing ghosts" on users' machines. He checks for the latest updates and views the top threats. He says that the alerts give his team much richer detail about the threats they're looking for.

"Malwarebytes saves us from chasing down false threats that might be out there," said Goodwin. "It gives us an accurate real view of an event, and leads us to the precise location of the problem. It's a huge time-saver."

In the past, the team typically spent 10 or more hours per week chasing down antivirus and Dell SecureWorks alerts and re-imaging machines. With Malwarebytes running on machines in the background, team members might spend two hours a week focused on actual threats and stopping potentially serious situations from developing.

Cybersecurity confidence

Malwarebytes also gives Wunderlich better alignment with the Financial Industry Regulatory Authority (FINRA) cybersecurity list of recommended measures. When similar financial services companies are audited for FINRA compliance, many don't have a malware protection engine. With FINRA's intensified focus on cybersecurity, Wunderlich's Malwarebytes deployment was a plus.

"We love the products," said Goodwin. "Malwarebytes has been like having another staff member on our small team. It's really beneficial and a big win for our department."

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