

At United Bank, there is no payoff for ransomware

Bank uses Malwarebytes to prevent malware and exploits from cashing in

INDUSTRY

Financial Services

BUSINESS CHALLENGE

Prevent malware and ransomware attacks

IT ENVIRONMENT

Data center with firewalls, network monitoring, VIPRE antivirus

SOLUTION

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

RESULTS

- Successfully identified threats and blocked serious exploits
- Minimized risk of disruption associated with malware or ransomware
- Gained peace of mind

Business profile

United Bank's focus is providing quality customer service and offering innovative, yet practical financial solutions for its customers in the communities where it does business. With 17 locations near metropolitan Atlanta, the bank is just as practical when it comes to preventing malware and ransomware.

The threat environment is just going to get worse and the bad actors continuously get more clever. That's just the kind of risk we won't take. Malwarebytes makes sure we don't.

—Russell Heelan, Network Administrator, United Bank

Business challenge

Prevent attacks from the start

United Bank's IT team had used and then discarded many different antivirus solutions over time. Solutions either were too "bloated" with features the bank didn't need, they were too costly, or they were just ineffective. Most recently, the bank used the VIPRE antivirus to combat viruses and malware. However, the solution required a lot of computing overhead on each user's PC. If a user encountered a malicious website or piece of malware, performance slowed dramatically. And malware kept getting through. For example, users commonly found rogue security software, such as fake antiviruses, popping up on their screens.

"It was only a matter of time before ransomware or extortionware showed up," said Russell Heelan, Network Administrator, United Bank. "We weren't going to wait for that to happen."

The solution

Malwarebytes Endpoint Security

Heelan began looking for a solution to replace the existing antivirus and add additional protection against malware. His previous experience with Malwarebytes had impressed him, and he chose to take an aggressive stance against malware and ransomware with Malwarebytes Endpoint Security.



“Malwarebytes always has been proactive in staying ahead of threats,” said Heelan. “We thought it best to just use it from the start.”

Endpoint Security provides a powerful multi-layered defense engineered to defeat the latest, most dangerous malware, including ransomware. It includes Malwarebytes Anti-Malware, Anti-Exploit, and the Management Console in one comprehensive solution. Malwarebytes Anti-Malware detects and eliminates zero-hour malware, Trojans, worms, rootkits, adware, and spyware in real time. It stops threats in their tracks, eliminating the need for United Bank to manually remove malware from endpoints. Malwarebytes Anti-Exploit adds four additional layers of protection to block exploits and prevent malicious payloads from being delivered.

Nowhere to hide

Heelan deployed the software using the Malwarebytes Management Console to push software to 400 endpoints. According to Heelan it was straightforward and completed in less than a week.

“The Management Console shows us everything—reports, the number and types of threats, and threat sources,” he said. “In-depth analysis shows us exactly what’s coming in and how Malwarebytes handles it. The reports definitely help us see what is happening so that we can be even more proactive.”

Malwarebytes quickly identified Potentially Unwanted Programs (PUPs) and blocked malicious sites. It also blocked four different exploits, any of which could have seriously affected user productivity or bank operations.

Proactive protection and better performance




“The threat environment is just going to get worse and the bad actors continuously get more clever,” said Heelan. “That’s just the kind of risk we won’t take. Malwarebytes makes sure we don’t.”

Malwarebytes’ small footprint on user PCs also ensures that users’ productivity isn’t disrupted. Heelan performs a quick scan across the network every day and then conducts a full scan twice a week. That way, he’s sure that everything stays clean.

“Thankfully, we’ve had no issues since deploying Malwarebytes,” he said. “I can’t say enough about what a great solution it is. We feel so much better with Malwarebytes in place.”

| 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