Malwarebytes

CASE STUDY

City of Memphis gives malware the blues

Malwarebytes puts distance between advanced threats and city endpoints

INDUSTRY
Government

BUSINESS CHALLENGE
Add a layer of protection with deeper insight into threats

IT ENVIRONMENT
Data center with firewalls, Symantec Enterprise Management antivirus, BeyondTrust vulnerability management, Aruba wireless controller security

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

RESULTS
- Gained deep visibility into threats and used insight to improve security training and fine-tune other security measures
- Reduced the time and cost associated with cleaning endpoints from malware
- Caught threats that evaded other tools and assured a "deeper clean"

Business profile

Memphis, Tennessee, is known as the Home of the Blues. Its rich history helps make it a unique place to live and visit. To keep things rockin' and rollin', the City of Memphis deployed Malwarebytes to defend against malware threats.

> Malwarebytes saves time, which equals money. Whether it's saving us a resource cost or reducing downtime for a user, Malwarebytes helps minimize impact to the city. That's good for everyone.
>
> —Brent Nair LSSBB, PMP, CISSP, MS, Chief Information Officer, City of Memphis

Business challenge

Add protection with deeper insight

Music, smoky barbecue, soul food, and paddlewheel steamboat cruises on the Mississippi River make Memphis one of America's top domestic travel destinations. However, cities like Memphis are also targets for less desirable visitors, like ransomware and other forms of malware.

Brent Nair, Chief Information Officer and Chief Security Officer for the city, is responsible for securing its IT assets. That includes 5,600 desktops and laptops installed across the city—from public libraries, fire stations, and public works offices to individual employee systems.

"We experience the same threats that attack all corporate and public sector environments," he said. "The most common ones are malicious file attachments, Potentially Unwanted Programs (PUPs), malicious URLs, unwanted tracking cookies, and command-and-control nuisance-ware."

The IT team received daily infection reports from its antivirus program, which quarantined the threats it found. To investigate, a technician had to drive to the machine's location. If a machine had a deeper level of infection, he would run another scan with the antivirus tool until the machine was clean. However, the antivirus didn't always find nuisance-ware and command-and-control malware. If the team thought that malware persisted, they sent their findings to the antivirus vendor or re-imaged the machine.

"We needed another layer of defense in our arsenal," said Nair. "I wanted a tool that was effective against zero-day attacks and exploits with central management capabilities and the ability to do a deep clean on nuisance-ware."

The solution: Malwarebytes Endpoint Security

The team researched potential solutions and chose Malwarebytes because it met all of their requirements. It could be deployed on mobile endpoints. It could be installed on a USB drive for cleaning machines on location. And it provided the Malwarebytes Management Console for configuring and managing endpoints centrally.

"Malwarebytes is a great product, which is why we moved forward with it," said Nair. "Since we deployed it, we're able to clean up exploits and malware faster and more easily than ever before."

The City of Memphis chose Malwarebytes Endpoint Security, which 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. Anti-Malware for Business detects and eliminates zero-hour malware, Trojans, worms, rootkits, adware, and spyware in real time. Anti-Exploit for Business adds four additional layers of protection. 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 threats and prevents malicious payloads from being delivered.

Visibility into endpoint health

Now the City of Memphis has much more visibility into its endpoints and their health status. When exploits or ransomware show up, they have nowhere to hide.

"It's not a matter of 'if' these threats show up," said Nair. "It's 'when.' Malwarebytes gives us empirical data that's useful in a lot of ways."

Deep visibility and data from Malwarebytes helps enhance the city's information security training program. For example, the team now can see what happens when users click on a specific URL. With that insight, they can tailor security tweets and other employee messages to provide specific information. They also can fine-tune other security devices that limit users' abilities to go certain websites.

Getting deep-down protection

Even though the city is a public entity and the majority of its information is public, certain assets—such as employee data—are not. When threats evaded the antivirus solution, there was only so much the team could do remotely to remediate. With Malwarebytes, they have another tool to get more detail and protect assets more strategically.

"Malwarebytes is an integral part of our tool kit," said Nair. "It helps clean up some of those things that still slip through—the Internet dirt that other tools can't reach."

Saving time, reducing cost

With the Management Console, the IT team now has the reach to view and manage Malwarebytes on endpoints

across the city. They have organized endpoints by groups and areas for greater efficiency. They receive alerts and notifications so that they can proactively address potential infections. They can push updates remotely to endpoints and remove threats, saving time and eliminating unnecessary trips around the city.

“Malwarebytes saves time, which equals money,” said Nair. “Whether it’s saving us a resource cost or reducing downtime for a user, Malwarebytes helps minimize impact to the city. That’s good for everyone.”

Expanding the benefit

Nair plans to extend Malwarebytes deployment to portions of the city’s server infrastructure and continue to fine-tune use of the product’s capabilities. As the City of Memphis moves toward a software-as-a-service environment, he plans to continue to leverage Malwarebytes’ capabilities.

“Everyone from Malwarebytes that we’ve worked with has been great,” said Nair, “and professionally I’m impressed with the Malwarebytes product. It’s a good, solid product.”

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