

City calls 911 on ransomware

Deploys Malwarebytes as strong line of defense against ransomware

INDUSTRY

Government

BUSINESS CHALLENGE

Prevent ransomware

IT ENVIRONMENT

Two data centers, one of which hosts emergency services infrastructure; McAfee antivirus, firewalls, web filtering, email scanning

SOLUTION

Malwarebytes Endpoint Security

RESULTS

- Reduced risk of ransomware getting into systems
- Detected threats and cleaned up infected machines automatically
- Enabled the team to avoid constantly re-imaging machines, saving hours of time
- Delivered peace of mind

Business profile

Bedford, Texas, is a suburb of Fort Worth with 48,000 citizens. The city's IT infrastructure supports all city services, including police, fire, and Emergency Medical Services (EMS). As the amount of malware—and the potential for ransomware attacks—grew, Bedford wanted another layer of defense on its endpoints. With Malwarebytes, the city received the additional protection it wanted, as well as serious peace of mind.



Malwarebytes gives us the endpoint protection we need. If the antivirus or web filtering miss something, we don't have to worry. Malwarebytes gives us serious peace of mind.

—Gary Clopton, IT Manager, City of Bedford, Texas

Business challenge

Prevent ransomware

The city of Bedford has two data centers: one at City Hall and the other at its law enforcement headquarters, which includes additional emergency services infrastructure. Gary Clopton, IT Manager for the city, had already deployed a layered approach to security with McAfee antivirus on endpoints and enterprise-class security measures in both data centers. However, the McAfee antivirus wasn't effective against zero-day threats, such as browser redirects, toolbars, Potentially Unwanted Programs (PUPs), and others. As threats began getting through more frequently, they slowed PC performance, which was especially a potential problem for EMS machines.

"All we could do was react," said Clopton. "We usually had to re-image the machine, which was time-consuming. Worse, we could never be 100 percent sure that there wasn't malware on other machines that we just hadn't found yet."

Clopton wanted to adopt a proactive stance and prevent malware—or something worse. In early 2016, the Bedford City Manager learned about the successful ransomware attack on California's



Hollywood Presbyterian Medical Center and met with Clopton to plan the city's defense. They first deployed a layer of web content filtering, which reduced the amount of employee web surfing. But malware still infected machines occasionally. Although they hadn't experienced a ransomware attack, Clopton had heightened concerns about ransomware. He began looking for an effective tool to prevent it.

The solution

Malwarebytes Endpoint Security

"I'd had previous experience with Malwarebytes, and I knew it worked well," he said. "Malwarebytes Endpoint Security with the Management Console was appealing to us because it gave us broad visibility across our devices and deep visibility into client devices, which we didn't have. It was cost effective and worked well with our antivirus and McAfee ePolicy Orchestrator solutions."

Easier cleanup

"We knew we'd see a lot of activity when we first deployed Malwarebytes," said Billy Mason, Lead IT Specialist for Bedford. "We had some cleanup to do, but we didn't have to re-image any machines. That was a relief. The Management Console is very intuitive and easy to use."

The IT team scans machines daily and hasn't seen false positives or conflicts with other security solutions. When Malwarebytes detects a threat, it alerts the team via email. Mason said that usually by the time a staff member goes to check the machine, Malwarebytes has already cleaned up the problem.

"If you're using unlicensed software and just doing single installs, you don't have granular control over the situation," said Clopton. "Now the 'make work' is gone. We no longer have to constantly re-image computers. We can focus on more important things without being derailed by malware."

Efficient and invisible




Users didn't realize that Malwarebytes was deployed and running. The software runs quietly in the background and scans don't affect machine performance. This is especially critical for EMS users, because when someone calls for help, they can't be waiting on a slow machine for information. And most importantly, ransomware has not gotten in.

Serious peace of mind

"Malwarebytes gives us the endpoint protection we need," said Clopton. "If the antivirus or web filtering miss something, we don't have to worry. Malwarebytes gives us serious peace of mind."

| 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