Malwarebytes for Business

CASE STUDY

City of Vidalia gains a ransomware and vulnerability-free zone

1 week recovery

from ransomware attack

Peace of mind

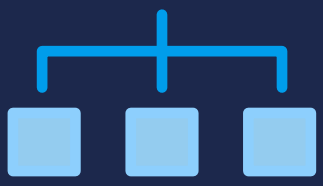
with powerful endpoint protection

Tackling vulnerabilities

with gained visibility

A municipality located on the west bank of the Mississippi River in Louisiana, the City of Vidalia has 120 endpoints to oversee the city's operations, including servers and workstations that run the full range of city departments, such as police, fire, and city hall. In addition, through a hydroelectric plant, the city operates utilities in house for its 4,000 citizens.

120 endpoints



Overview

Customer:
City of Vidalia
Industry:
Local government
Displaced Product:
Trend Micro
Solution:

- Malwarebytes Endpoint Detection and Response
- Malwarebytes Endpoint Detection and Response for Servers
- Malwarebytes Vulnerability Assessment

There are a lot of different, moving parts that go into our security ecosystem. Malwarebytes is probably our biggest and most important cog, and I would recommend it to all businesses.

- Andrew Jones, Senior IT Specialist
City of Vidalia

Challenges

Ransomware slips past endpoint protection

The city was using Trend Micro to safeguard its endpoints against ransomware, malware, and other threats. However, the product failed on its mission and allowed a ransomware attack to successfully encrypt the city's machines one Friday evening. Working into the weekend and long hours, the IT team initiated a rapid triage effort where several department operations pivoted to paper processes while the machines were restored.

"The ransomware created a nasty situation. We fought for a week to restore the endpoints. Luckily, we had some machines with Malwarebytes installed where the ransomware was stopped. That let us know we needed to move to Malwarebytes for endpoint protection," said Andrew Jones, Senior IT Specialist.

How Malwarebytes Solved the Problem

Security protection the city can count on

Since deploying Malwarebytes more than two years ago, the city has enjoyed effective endpoint protection. The solution's multi-layered security and anti-ransomware features, including ransomware rollback, give the city confidence in their endpoint security posture.

Malwarebytes also proved steadfast in its quality protection during the pandemic. As many employees moved to remote work, it meant their laptops didn't have the benefits of the city's perimeter defenses. "Having Malwarebytes protecting our remote machines gave us an extra security blanket knowing they had that level of protection. Malwarebytes did its job, and everything continued to run smoothly," said Jones.

> ***"Having Malwarebytes protecting our remote machines gave us an extra security blanket"***

Simple and accurate threat hunting for IOCs

As a government entity, the IT team must manage threat hunting responsibilities when a new indicator of compromise (IOC) is issued from the NSA, FBI, or Department of Homeland Security. With the Malwarebytes flight recorder feature, the team can proactively and efficiently search for cyberthreats to ensure that none are lurking on any endpoints.

"Flight recorder allows us to search event data that's captured from all our endpoints and look for attributes of an IOC like files, IPs, registry, processes, and networking activity. It's accurate with its data analysis, so when our search comes back clean with no indicators in our environment, I can confidently report that our endpoints are in good shape," said Jones.

Keeping the environment vulnerability-free

With the city's security ecosystem running smoothly, the IT team wanted to advance their security practices by adopting a vulnerability management program. With a range of operating systems and custom applications in use, the team needed visibility to understand if any software was out of date or if there were any vulnerability warnings. For this, they turned to Malwarebytes Vulnerability Assessment.

Vulnerability Assessment runs on the same Malwarebytes cloud-native platform the city uses for its endpoint protection, so enabling the module and launching the team's vulnerability program was as simple as a "flick of the switch."

"With the Vulnerability Assessment module, we have instant visibility into vulnerabilities in our applications and operating systems. We even get early warning alerts on new vulnerabilities before we hear about them in the news the next day. This gives us the advantage to remediate any issues before there's an exploit," said Jones.

Vulnerability Assessment also helps the city demonstrate that it's in alignment with compliance requirements. "Malwarebytes vulnerability scanning helps us with our PCI and CJIS compliance requirements for addressing vulnerabilities. We can print the reports on the identified vulnerabilities we've addressed and give them to our compliance officer, which gives us that helpful checklist for compliance reasons," concluded Jones.

Effective threat hunting

for new IOCs

Vulnerability program

that supports PCI, CJIS compliance

Learn more >

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes believes that when people and organizations are free from threats, they are free to thrive. Much more than malware remediations, the company provides cyberprotection, privacy, and prevention to tens of thousands of consumers and organizations every day. for more information, visit www.malwarebytes.com.