Malwarebytes

CASE STUDY

CLEVNET eliminates malware across members' systems

Malwarebytes delivers protection with huge time savings

Business profile

CLEVNET is a consortium of 45 library systems located in 12 counties across Northern Ohio. It enables member libraries and their patrons to access the vast collections of every participating library. When cleaning up malware began to consume extraordinary amounts of time, CLEVNET chose Malwarebytes to reclaim technicians' time.

Business challenge

Fighting waves of cyber threats
The Cleveland Public Library originally launched CLEVNET in 1982, with a vision of automating processes and connecting libraries to share their collections. Today, CLEVNET makes 12 million items accessible to 1 million customers in Northern Ohio. Headquartered at the Cleveland Public Library, CLEVNET provides networking, catalog, and security services to consortium members. If one member library's systems become infected with malware, it can affect the entire network.

Prior to Malwarebytes, consortium members used a variety of antivirus and security measures. As malware and cyberattacks became more frequent and widespread, libraries' technicians were spending more and more time cleaning up browser hijacks and nuisance-ware. Attacks then escalated to automated phishing and malware attacks. Each time an infection occurred, a technician would have to travel to the location of the infected system to remediate it.

"In one case, cybercriminals directly targeted financial officers of all CLEVNET libraries," said Larry Finnegan, Director of IT for Cleveland Public Library. "Using spoofed emails, they tried to convince financial officers to authorize wire transfers and even knew their banking contacts. We had to fight back."

OVERVIEW

INDUSTRY
Nonprofit

BUSINESS CHALLENGE
Protect network and endpoints from threats that disrupt member libraries' operations

IT ENVIRONMENT
Palo Alto Networks Traps, layered security

SOLUTION
Malwarebytes Endpoint Security

RESULTS
Saved hundreds of hours of time for CLEVNET members' technicians

Eliminated browser hijacks, popups, and viruses

Stopped threats that evaded Palo Alto Networks Traps

> BROWSER HIJACKS, VIRUSES, AND POPUPS HAVE DISAPPEARED. MALWAREBYTES HAS IDENTIFIED AND REMOVED EXPLOITS ON SYSTEMS WITHOUT TRIGGERING ANY CALLS FROM USERS. IT ALSO GIVES THE IT TEAM EXTRA CONFIDENCE.
>
> LARRY FINNEGAN, DIRECTOR OF IT, CLEVELAND PUBLIC LIBRARY

The solution

Malwarebytes Endpoint Security
CLEVNET members have varying levels of onsite tech support. However, all technicians were familiar with Malwarebytes. As their go-to cleanup tool, Malwarebytes had high credibility with all members. When threats got through, the team could quickly remediate them without having to spend extensive amounts of time trying to identify them.

"We chose Malwarebytes Endpoint Security for proactive protection," said Finnegan. "It gives us an extra layer of defense."

Granular visibility
The Malwarebytes console gives the CLEVNET team visibility across all of the consortium's endpoints. It also made it easy to allow each library's team to see and manage its own systems.

"We set Malwarebytes management policy in sync with our Active Directory domains," said Chris Wisniewski, Solutions Architect for the Cleveland Public Library. "Each library can see its own systems and manage them, but they can't see the systems at any of the other libraries. We can see all systems, so small libraries without their own techs are managed by us."

Time savings
Malwarebytes has saved hundreds of hours of time for CLEVNET members. When malware evades other controls and gets through, Malwarebytes alerts the team and cleans up the threat. Staff members no longer have to travel across Northern Ohio to re-image systems. With Malwarebytes already on the systems, techs can handle any incident—from remote scanning to troubleshooting—from a central console.

"Malwarebytes delivers huge time savings for member libraries," said Finnegan. "Library systems with multiple locations can eliminate staff travel time to clean up machines. Small libraries can be equally protected even without having technicians on staff."

Hijacks and popups disappear
Malwarebytes scans system hard drives and files, which other endpoint solutions don't. Those capabilities have delivered an extra layer of protection to member libraries' systems.

"Browser hijacks, viruses, and popups have disappeared," said Finnegan. "Malwarebytes has identified and removed exploits on systems without triggering any calls from users. It also fills a gap, giving the IT team extra confidence."

Threats come from everywhere. CLEVNET is considering Malwarebytes Endpoint Protection cloud-based security to protect mobile devices and cell phones while they are off the CLEVNET network.

"Exploits and spoofing attempts can attack through home networks or public WiFi connections," said Wisniewski. "We want to make sure that all devices are protected—wherever they are."