

Cheshire Constabulary closes the case on threats

Prevents ransomware from affecting emergency services

INDUSTRY

Local government

BUSINESS CHALLENGE

Prevent ransomware from affecting operations

IT ENVIRONMENT

Endpoint protection antivirus, firewalls, IPS, web filtering, email filtering

SOLUTION

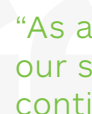
Malwarebytes Endpoint Security

RESULTS

- Prevented ransomware and zero-day exploits from affecting operations
- Simplified protection with rules-based policy
- Gained visibility into machines across installed base
- Allowed uninterrupted user experience without compromising security

Business profile

Cheshire Constabulary serves more than one million citizens in the UK North West, providing critical emergency services through 999, as well as a range of non-emergency provisions. When zero-day exploits began to show up and ransomware attacked, the Constabulary dialed Malwarebytes for help.



“As an emergency services organization, our systems have to run optimally and continuously. And we want to protect sensitive information with a robust, layered (defense-in-depth) approach. Malwarebytes helps us do both.

—Stuart Rogers, IT Security and Technical Architecture Manager,
Cheshire Constabulary Langdale Industries

Business challenge

Prevent ransomware and zero-day exploits

The Constabulary's IT team oversees the infrastructure and security for all of Cheshire, including 4,500 users, 4,200 Windows laptops and desktops, and Microsoft Surface mobile devices. Although multiple layers of security protect the network and desktop systems, ransomware got through and infected a computer.

“Fortunately, we stopped it quickly and prevented it from spreading,” said Stuart Rogers, IT Security and Technical Architecture Manager for Cheshire Constabulary. “Although our other security measures, using multiple vendor products, look for various types of malware, they didn't stop this particular type of ransomware from coming in the front door.”

The episode shook the team's confidence in traditional, signature-based malware protection. Without being able to see across their systems or into each system, there was no way to be sure that malware wasn't also on other machines. At the same time, the department was rolling out 1,700 new Microsoft Surface mobile devices. The tablets have multiple connectivity options—3G,



LTE, and Wi-Fi—which increased the attack surface. The team wanted something to deal specifically with zero-day exploits and ransomware, and they wanted it fast.

The solution

Malwarebytes Endpoint Security

“I’d used Malwarebytes previously with great results,” said Rogers. “It was an obvious choice. It’s cost-effective, and we could deploy it quickly with minimal delay and disruption as part of our mobile initiative.”

“Once it finds malware, it quarantines it, and we scan machines regularly to keep them clean,” Rogers said.

“Malwarebytes complements our existing security products and gives us the layer of protection we needed against zero-day threats. Since going live with Malwarebytes, it has detected and stopped malware that other products failed to catch.”

Rules deliver better protection

Rogers likes Malwarebytes’ rule- and policy-based approach to detecting malware for two reasons. First, zero-day exploits are everywhere, but the team can be sure that Malwarebytes catches them without waiting on updated signatures and then deploying the updates.

Second, Malwarebytes rule-based protection delivers another unique advantage. With 4,200 machines to manage, implementing software updates and patches is time-consuming. Sometimes, machines will be running an older version of Adobe or an older version of Java. With Malwarebytes, the Help Desk can tailor rules to build a “shield” around these software versions to immediately help prevent threats from exploiting any vulnerability prior to patches and updates being applied. Endpoints stay protected.

Low overhead, high assurance



“In our environment, Malwarebytes just runs in the background without slowing the machine or disrupting productivity,” Rogers said. “When it finds malware, it alerts the user and our staff. We can review what it finds, make sure that the device is updated, and fine-tune policy if necessary.”

Rogers expects threats to evolve, and he plans to expand the use of Malwarebytes as needed. He also plans to export Malwarebytes log data to the agency’s SIEM to enhance security visibility.

“As an emergency services organization, our systems have to run optimally and continuously,” said Rogers. “And we want to protect sensitive information with a robust, layered (defense-in-depth) approach. Malwarebytes helps us do both.”

| 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