Malwarebytes

HOT Engineering turns up the temperature on malware

Malwarebytes protects endpoints at headquarters and in the field

Business profile

HOT Engineering & Construction Co. is one of the largest multidisciplinary engineering, construction, and maintenance companies in Kuwait. It builds infrastructure and superstructure projects, and it also provides heavy equipment rental and testing services. When HOT Engineering wanted to build stronger defenses against malware, it chose Malwarebytes.

Business challenge

Fighting back

Leading-edge solutions and outstanding customer service are pillars of HOT Engineering's business. As a result, the company has built lasting relationships with many leading companies in Kuwait and across the Middle East. HOT Engineering has three primary locations augmented by mobile engineering and construction teams who work on multiple remote projects. Maintaining high productivity is essential to meeting construction deadlines and customers' expectations.

In the past, HOT Engineering used Symantec Endpoint to protect users' systems against viruses and other threats. As malware and ransomware spread, the IT team increasingly was diverted from critical tasks to troubleshoot and clean PCs. Finding and cleaning or re-imaging machines in the main offices became extraordinarily time-consuming. Keeping up with infected PCs at active work sites was almost impossible.

"I had researched and used several different anti-malware solutions in the past," said Anas Ragai Tawfeek, Head of IT at HOT Engineering & Construction. "Some of those solutions destroyed files while cleaning PCs. Other solutions were disabled or destroyed by vicious malware. We needed a strong, effective solution to fight today's threats."

OVERVIEW

INDUSTRY
Construction

BUSINESS CHALLENGE
Prevent business disruptions due to malware-infected endpoints

IT ENVIRONMENT
Windows Defender, layered enterprise security

SOLUTION
Malwarebytes Endpoint Security

RESULTS
Halted calls about malware-infected systems

Prevented ransomware infections

Accelerated threat response through easy-to-use dashboard

Eliminated the need for periodic physical system checks, simplifying management

> "
> MALWAREBYTES DESTROYS MALWARE WITHOUT AFFECTING OUR ENDPOINTS OR FILES. DEPLOYMENT WAS EASY, AND NOW OUR ENDPOINTS ARE PROTECTED IN THE OFFICES AND IN THE FIELD.
>
> ANAS RAGAI TAWFEEK, HEAD OF IT, HOT ENGINEERING & CONSTRUCTION

The solution

Malwarebytes Endpoint Security

Anas drew on past experience using Malwarebytes to evaluate it for the company. He immediately saw that Malwarebytes caught threats that the existing antivirus product missed and delivered insight across all of the company's endpoints.

"We chose Malwarebytes Endpoint Security for its effectiveness," he said. "It destroys malware without affecting our endpoints or files. Deployment was easy, and now our endpoints are protected in the offices and in the field."

No calls, no downtime

Since Malwarebytes was rolled out, Anas hasn't received calls from users being attacked by malware. When Malwarebytes detects a threat, it quarantines the malware and notifies the system administrator. He can view the system through the Malwarebytes Management Console and determine how to respond.

"Malwarebytes protects us from high volumes—and the most vicious types—of malware," said Anas. "Employees use clean PCs without downtime, which makes them, our clients, and me very happy."

A global view and time savings

Through the central management console, Anas can see which systems are connected, threats that Malwarebytes has detected, how much malware was found during the last scan, and which systems are being attacked most frequently. This visibility gives him an at-a-glance overview of the company's endpoint security posture no matter where endpoints are being used.

"The dashboard saves time in responding to threats," he said, "and with Malwarebytes continuously handling malware, I no longer have to conduct periodic physical checks of every system."

When users realized that Anas' team could see when their systems are infected from Internet surfing at malicious websites, they became more careful about clicking on links and visiting questionable sites. This knowledge also reduced the number of malware infections.

Light and easy

Anas said that Malwarebytes has a light footprint on endpoints, which is a benefit for users who often work on large, complex files. Malwarebytes can scan in the background without interrupting users' work.

"Malwarebytes is easy to manage," he said. "I don't have to constantly maintain it, so it lightens my workload too. Everyone at HOT Engineering benefits from Malwarebytes."

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