Malwarebytes

CASE STUDY

CSI Electrical Contractors powers up endpoint protection

Malwarebytes blocks, remediates, and reports threats

Business profile

CSI Electrical Contractors (CSI) is a full-service construction company headquartered in Los Angeles. Over the past 25 years, CSI has grown by combining consultancy expertise with top-notch engineering and project management capabilities. An important part of the company's success is delivering excellent service to its clients. When malware infections threatened to disrupt project work, CSI plugged into Malwarebytes.

Business challenge

Switching off threats

In addition to headquarters, CSI has offices in Palmdale and San Jose, California and a highly mobile workforce. Employees might be working at construction sites for anywhere from several days to a year or more before they—and their laptops—return to a main office and reconnect to the network.

"When I joined the company, Symantec Endpoint and Cynet 360 solutions were deployed to protect endpoints," said Angel Juarez, Network Administrator for CSI. "Both solutions were missing cyberthreats that infected mobile laptops and in-house systems."

To help prevent infected systems from spreading malware to the corporate network, the company did not enable VPN connections to the network from remote systems. As a result, it was impossible to ensure that mobile endpoints had the latest protection. The IT team received numerous calls from users saying that their browsers were slow or new icons had appeared. Juarez would have to initiate a web conferencing session to connect to the remote system, identify the threat, and remediate it if possible. If it couldn't be removed, he would have to re-image the user's system, which took

OVERVIEW

INDUSTRY
Construction

BUSINESS CHALLENGE
Prevent endpoint infections and disruptions due to malware

IT ENVIRONMENT
Windows Defender, layered enterprise security

SOLUTION
Malwarebytes Endpoint Protection

RESULTS
Stopped a wide range of threats that other solutions missed

Verified that all systems have the latest protection even when not connected to the corporate network

Avoided hours of user downtime and IT time spent remediating systems

> "WITH MALWAREBYTES, I KNOW OUR COMPUTERS AND MOBILE WORKFORCE ARE SECURE. INTEGRATED REMEDIATION FREES UP A LOT OF TIME.
>
> —ANGEL JUAREZ, NETWORK ADMINISTRATOR, CSI

several hours. The team saw an increasing amount of malware, trojans, viruses, ransomware, and bitcoin mining threats that were consuming computer-processing resources.

"Not only did each incident take several hours of IT time, the user was down too," said Juarez. "That disrupted project work, and in our industry, nobody can afford to be down."

The solution

Malwarebytes Endpoint Protection

Juarez had used Malwarebytes in the past and recommended it to the rest of the team. They evaluated cloud-based Malwarebytes Endpoint Protection for 30 days side by side with the existing solutions. Malwarebytes uses multiple technology layers to address advanced threats that leverage different attack vectors and techniques.

"During the trial, we watched Malwarebytes block malware, phishing emails, and access to malicious websites," said Juarez. "Malwarebytes was finding threats that our antivirus solution missed, so we replaced Symantec with Malwarebytes Endpoint Protection."

Using the deployment tool, the team rolled out Malwarebytes to all of its desktop and laptop systems, as well as to several VMware servers. Juarez said that the process was simple and they had all of the systems reporting in just a couple of days.

Validation through reporting

The Malwarebytes cloud console enables Juarez to ensure that all systems not connected to the corporate network have updated protection. Through the console, he also uses the asset management capability to validate software assets on the systems.

"The most important thing is to verify that all of our computers have the latest definitions and they're protected," said Juarez. "In the past, we didn't have that visibility. Being able to ensure that everyone is covered greatly reduces our attack surface."

Centralized control

Malwarebytes Endpoint Protection includes syslog support. The cloud console can automatically send malware detection information to syslog servers and SIEM solutions capable of receiving syslog messages. This enables the company to consolidate logs based on all events, endpoint registers, endpoints with scan infections, and histories. No added software is needed. When CSI deploys its new SIEM, the connection will be easy.

"The Malwarebytes syslog feature makes it easy to have one central repository for everything," said Juarez. "It will increase our control and allow us to retain logs for long periods of time to meet compliance requirements."

Free from worry

Malwarebytes finds the threats that the previous antivirus solutions routinely missed. It has blocked hundreds of malicious sites, network port scans, coin hive, and phishing email links that weren't recognized by other security measures. Even when remote users are not logged onto the CSI network, they are still protected.

When PUPs and extensions are installed in users' browsers, Malwarebytes removes them. If an infection does occur, the Malwarebytes Linking Engine completely remediates the system to a healthy state with minimal impact to the end user.

"With Malwarebytes, I know our computers and mobile workforce are secure," he said. "Integrated remediation frees up a lot of time. I don't have to spend several hours cleaning up a system. Malwarebytes handles it for me."

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

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.