Malwarebytes

CASE STUDY

Entrust Datacard scores win against disruptive malware

Malwarebytes finds and remediates threats without affecting end-user productivity

Manual remediation consuming an hour of employee time per incident

SOC team saves hours per week by eliminating manual threat remediation

Thorough remediation finds and cleans 14,000 PUPs and secondary artifacts

Business profile

Entrust Datacard is a leading provider of trusted identity and secure transaction technology solutions for financial, corporate, government, education, healthcare, retail, transit and other industries. Solutions include everything from physical financial cards, passports, and ID cards to digital authentication, certificates and secure communications. Entrust Datacard needed a way to remediate malware and unwanted software on users' endpoints without interrupting their workflow. The company turned to Malwarebytes.

Business challenge

Seeking reliable, anywhere-anytime threat remediation

Consumers, citizens, and employees increasingly expect anywhere-anytime experiences whether they are making purchases, crossing borders, accessing e-government services, or logging onto corporate networks. Entrust Datacard solutions make those experiences reliable and secure. The company is headquartered in Minneapolis with more than 2,200 employees in 34 worldwide locations.

"Our team uses automated solutions to monitor the corporate infrastructure for malware and other malicious software," said Brian Withrow, senior manager of the security operations center at Entrust Datacard. "That includes everything from desktops, laptops, and mobile phones on our guest wireless network to servers. When we receive an alert, we serve as the first line of remediation."

Withrow's team receives alerts from the company's Symantec antivirus solution when it detects suspicious or malicious software that it cannot resolve. Until the team could manually remediate the system, suspicious items represented a risk that could result in damage. When the team received an alert, they would call the end user and the conversation usually went like this: "File abc.exe is in such-and-such a file path or directory. Can you click

OVERVIEW

INDUSTRY
Technology

BUSINESS CHALLENGE
Reduce the impact of malware on enterprise resources

IT ENVIRONMENT
Layered security solutions, Malwarebytes providing thorough endpoint remediation

SOLUTION
Malwarebytes Incident Response

Entrust Datacard™

> For every malware alert we recieve, we clean it up with Malwarebytes without affecting the end user. It's a win for us, the SOC team, and for the company.
>
> Brian Withrow, Senior Manager of Security Operations Center
> Entrust Datacard

start? Now click Run. Can you type in the file path? Is it searching for the file? Did it find the file? Fine—you can delete it. Now we'll clear your browser cache." Then the security team member would walk the user through the process of clearing the browser cache as well.

"This created a tremendous impact on our users," said Withrow. "A sales or marketing employee doesn't need someone calling and taking an hour out of their day to fix a suspicious item on their system. We needed a faster, less intrusive way to remediate systems."

The solution

Malwarebytes Incident Response
Withrow had evaluated Malwarebytes Incident Response at a previous company to solve a similar problem. Malwarebytes Incident Response provides threat detection and remediation from a highly scalable, cloud-based management platform. Entrust Datacard conducted a proof of concept on 250 systems and quickly recognized the value Malwarebytes delivered.

"The cloud-based architecture made Malwarebytes Incident Response a no-brainer for us," said Withrow. "It enhanced our layers of defense and was an easy sell."

The SOC team pre-deployed Malwarebytes Incident Response on Windows and Mac endpoints, enabling advanced threat detection and remediation at the click of a button. Malwarebytes resides invisibly on endpoints, ready to instantly remediate suspicious or malicious files without impact to users.

Time savings are cost savings
Malwarebytes Incident Response has saved time for everyone—the SOC team and end users. When the SOC receives an alert, the team simply enters a command on the cloud console and Malwarebytes scans the endpoint, finds the malicious software, and remediates the system. No interaction with the end user is needed.

"Malwarebytes Incident Response is very affordable to start with," said Withrow. "The amount of time it saves us in cleaning up malware makes it highly cost-effective, and that doesn't even take into consideration the cost to the company if we were breached."

Removing the unknown
Before Malwarebytes Incident Response, the SOC team focused on removing the item that triggered the alert. However, there might be other malicious or unwanted software on the system that remained undiscovered. Threat actors can use undetected malware dwelling in the network for malicious purposes later. Now when Malwarebytes scans systems to find a suspicious file and finds other malware lurking on the system, it remediates it at the same time.

"We love the thoroughness of Malwarebytes Incident Response," said Withrow. "In just the past 90 days it cleaned up 14,000 PUPs. It not only fixes what we have identified as a threat, it also remediates secondary and tertiary infections and artifacts."

A winning scorecard
Withrow finds Malwarebytes reports invaluable for keeping the Chief Information Security Officer (CISO) informed. He simply schedules a report and exports it as a plain-text file, which he adds to overall SOC metrics.

"I bundle all of that data into a scorecard for our CISO, so he can see the value that Malwarebytes delivers," said Withrow. "For every malware alert we receive, we clean it up with Malwarebytes without affecting the end user. It's a win for us, the SOC team, and for the company."

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.