Malwarebytes

CASE STUDY

Danforth Center deploys sustainable defense against malware and ransomware

Malwarebytes delivers trusted, real-time protection in a dynamic environment

Business profile

Founded in 1998, the Donald Danforth Plant Science Center is a not-for-profit independent institute that conducts research, education, and outreach to improve agriculture productivity and sustainability. Based in St. Louis, the center attracts scientists from all over the world who contribute to developing improved crops and agricultural technologies. An open research environment is also a target for cyberthreats. When ransomware hit, the center hit back with Malwarebytes.

Business challenge

Finding the balance
By 2050, providing food and fuel for nearly 10 billion people will require that the world increase agriculture productivity by at least 50% and achieve a major shift toward clean, renewable sources of energy. Interdisciplinary teams of scientists at Danforth Center focus on developing solutions to these challenges daily. The Danforth employee scientists representing more than 20 countries and trainees who stay anywhere from several weeks to several years. For the IT security team, a constantly changing user base and the open, collaborative nature of research creates unique challenges.

“We always must balance openness with security,” said Jeremy Tate, Information Technology Security Manager at the Danforth Center. “Researchers communicate with colleagues, rely on scientific websites around the world, and connect with their home organizations. We can’t lock everything down, but we still need to defend against cyberthreats that can come from anywhere, at any time, and in any form.”

The center’s defense-in-depth strategy applies multiple layers of security to the organization’s infrastructure, applications, and data. However, it only took one click in a malicious email message for ransomware to infect

OVERVIEW

INDUSTRY
Nonprofit

BUSINESS CHALLENGE
Protect endpoints against malware and ransomware in a dynamic open environment

IT ENVIRONMENT
Symantec Endpoint Protection, layered enterprise security solutions

SOLUTION
Malwarebytes Endpoint Security

RESULTS
Prevented future ransomware infections

Stopped and removed malware, as well as blocked attempts to connect from malicious websites that other security layers missed

Saved at least a day per month that previously was needed to remediate infections

Enabled team to become proactive in preventing infections

> “
>
> MALWAREBYTES IS FANTASTIC. IF THERE’S AN ISSUE, MALWAREBYTES BLOCKS IT, DELETES IT, REBOOTS THE MACHINE IF NECESSARY, AND THEN SENDS ME AN ALERT.
>
> JEREMY TATE, INFORMATION TECHNOLOGY SECURITY MANAGER, DONALD DANFORTH PLANT SCIENCE CENTER

a user's machine and network share and encrypt more than a terabyte of data. After eight hours, Tate's team successfully restored the data and had everything back up and running, but the incident was a significant disruption for everyone.

The solution

Malwarebytes Endpoint Security

After the ransomware infection, Tate and his team began looking for a solution that would protect against malware, ransomware, and other advanced threats. Their additional layer of protection had to complement the center's existing antivirus product and come from a trusted name in security. Members of Tate's team had previous experience with Malwarebytes and trusted it. They conducted a short trial, deploying it on a handful of systems, and it became an easy decision.

"Malwarebytes gave us the protection we wanted from a trusted name," said Tate. "After a bit of testing, it was one of those no-brainer choices for us."

The team deployed Malwarebytes Endpoint Security using its Dell KACE endpoint management platform. Today, all endpoints and the center's servers are protected.

Trusted real-time protection

With real-time protection on each endpoint, any malicious plug-in or drive-by download that manages to reach an endpoint is handled. Malwarebytes instantly alerts the IT security team when it detects malware, scans a machine, or removes a threat automatically.

"Malwarebytes is fantastic," said Tate. "If there's an issue, Malwarebytes blocks it, deletes it, reboots the machine if necessary, and then sends me an alert."

Malwarebytes also has blocked requests coming to the center's web server from suspicious websites. Once or twice a month, Tate will receive an alert that Malwarebytes blocked an attempt to connect by an untrusted site. At first, he thought the alerts were false positives.

"When I went to check the sites that were blocked, every time it was an IP address with a poor reputation," said Tate. "Kudos to Malwarebytes for picking up things that other solutions missed."

The ability to be proactive

Before Malwarebytes, the center's security team could only respond when malware or ransomware showed up. The Malwarebytes Management Console delivers a daily summary to Tate that enables the team to be proactive. They can immediately see which clients are online and which are offline, which endpoints had malware, the types of malware targeting the center, and more.

"The Malwarebytes interface provides an easy color-coded system to visually see everything," said Tate. "It also integrates with Active Directory, so I don't have to manually add anything. If a new system is added without Malwarebytes, I see it. I'm not missing anything, and I can remedy any situation quickly."

A day per month saved

Tate said that the center's help desk team had recovered hours of time since Malwarebytes was deployed. They no longer have to drop everything to go to a machine and deal with a problem. Malwarebytes handles it.

"Malwarebytes has given us back at least a day per month," he said. "If someone downloads a malicious file or something makes it through our layers to an endpoint, Malwarebytes lights up like a Christmas tree and stops it. The threat goes no further."

A best practice

Even though the center's dynamic, open environment prevents Tate and his team from limiting Internet access or taking other restrictive measures that would be considered a best practice in other environments, he's not worried.

"Malwarebytes prevent infections that would otherwise occur in our environment because of our open policy," said Tate. "It fills that gap and keeps us—and our auditors—happy."

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.