Malwarebytes

Rigaku Americas gains X-ray vision into ransomware and malware

Malwarebytes reveals, identifies, and eliminates malware and ransomware

INDUSTRY
Manufacturing

BUSINESS CHALLENGE
Protect against data loss and downtime due to malware and ransomware infections

IT ENVIRONMENT
AppRiver, Microsoft Endpoint Protection, perimeter security appliances

SOLUTION
Malwarebytes Endpoint Security

RESULTS
- Gained visibility into threats on endpoints that were otherwise undiscovered
- Enabled team to proactively block threats
- Prevented additional ransomware infections

Business profile

Nanotechnology researchers, structural protein scientists, materials science analysts, and life science researchers are just a few customers around the world who choose Rigaku's instrumentation solutions. Having an enhanced ability to uncover sub-microscopic particles and patterns is essential to their research. Malwarebytes enhanced Rigaku Americas' ability to uncover hidden malware and ransomware before they did damage.

> The demonstration swung us from deploying proactive remediation capabilities to choosing Malwarebytes Endpoint Security with anti-exploit, anti-ransomware, and monitoring features as well. When we saw how dynamic Malwarebytes is, we were convinced that it was worth the investment.
>
> —Scott Bendle, Chief Information Officer, Rigaku Americas Corporation

Business challenge
Preventing infections that can strike anytime

Rigaku innovation has resulted in tools that create better semiconductors, enable drug discovery, improve production line quality, and enable scientists to explore nanotechnology. With solutions based on X-ray, thermal, spectroscopy, and crystallography imaging techniques, Rigaku is a world leader in enabling people to see and analyze very, very small particles and structures. Rigaku Americas Corporation supports Rigaku activities outside of Japan, including protecting users and endpoints from cyberthreats.

In the past, Rigaku Americas' users experienced occasional virus and malware infections. When ransomware significantly ramped up, so did infection rates. The affected users were especially vulnerable because they were mobile and rarely at a main office location to receive the latest threat prevention updates.

"The first incident infected a user's laptop and spread to a network file server before it was caught," said Brandon Thorpe, Network

Engineer and System Administrator for Rigaku Americas. "We were able to recover the data from backup. But the two remote users who experienced infections on their laptops lost their data. It took several days to restore systems to a functional state."

The solution

Malwarebytes Endpoint Security

In the past, the IT team used Malwarebytes to clean up malware infections. With ransomware as a major threat, they once again turned to Malwarebytes for a solution.

"We trust Malwarebytes, and it is our top choice for cleaning up infections," said Thorpe. "It really made sense to see what else they could provide."

Rigaku Americas approached Malwarebytes for a demonstration of the proactive remediation capabilities. The team wanted to keep the solution as simple as possible. However, when they understood the power of Malwarebytes and the ability to have central visibility across their endpoints, they chose Malwarebytes Endpoint Security as their comprehensive solution.

"The demonstration swung us from deploying proactive remediation capabilities to choosing Malwarebytes Endpoint Security with anti-exploit, anti-ransomware, and monitoring features as well," said Scott Bendle, Chief Information Officer of Rigaku Americas. "When we saw how dynamic Malwarebytes is, we were convinced that it was worth the investment."

Malware and ransomware revealed

Thorpe deployed Malwarebytes, and right away he saw how much malware was actually present. At least one endpoint had 1,500 items ranging from toolbars, pop-ups, and Potentially Unwanted Programs (PUPs) to malicious software that had gone undiscovered. Without knowing it was present, the machine could have been used indefinitely until the user finally reported a problem.

"Having that visibility, and seeing what's going on is a top benefit," said Thorpe. "Of course, knowing that there is another layer of protection in place to keep malware and threats off the network is also a huge relief."

Proactive protection

The Rigaku Americas team scans endpoints regularly through the Malwarebytes Management Console. They also use the Management Console to push Malwarebytes to new machines that come onto the network and ensure that all are up to date. Real-time scanning has turned the tables on malware and ransomware, because now the team can proactively prevent and block threats instead of having to investigate and remediate machines.

Threat reports instantly tell Thorpe when threats try to infect endpoints, which threats have been quarantined, and which machines might have an issue that needs further attention. Malwarebytes automatically quarantines and cleans up malware and ransomware so that the Rigaku Americas team can focus on other issues.

"One of our users regularly travels to Asia, and in the past, he always came back with major infections on his machine," said Thorpe. "Since we implemented Malwarebytes, that hasn't happened. It does what it needs to do."

A lot less worry

The team plans to implement a package that will notify remote and mobile users of Malwarebytes updates and point them to the Internet for downloading the latest updates so that they stay protected.

"We support all users outside of Japan," said Bendle. "So we must provide support and protection 24 hours a day to users who go everywhere on the web. Having Malwarebytes, and knowing that we can rely on it to just work, is really valuable to us."

| About