Malwarebytes

Yaskawa Motoman puts malware in its place

Malwarebytes delivers visibility to reduce risk and enhance productivity

INDUSTRY
Automation and robotics manufacturing

BUSINESS CHALLENGE
Stop malware and ransomware infections without restricting users' access to Internet resources

IT ENVIRONMENT
Kaspersky antivirus, Morphisec anti-exploit, enterprise perimeter security measures
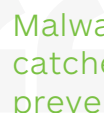
SOLUTION
Malwarebytes Endpoint Security

RESULTS
- Reliably stopped more than 90 percent of malware
- Gained visibility into client machines to ensure total coverage
- Reduced risk associated with endpoint infections
- Increased IT team productivity by eliminating the need to re-image malware-infected machines and address slow PC performance due to malware

Business profile

Yaskawa America Inc., Motoman Robotics Division (Yaskawa Motoman) is a leading industrial robotics company in the Americas. With over 360,000 Motoman® robots installed globally, Yaskawa provides automation products and solutions for virtually every industry and robotic application; including arc and spot welding, assembly, coating, dispensing, material handling, material cutting, material removal, packaging, and more.

> Malwarebytes covers all of the bases for us. It catches more than 90 percent of malware and prevents users from going to malicious sites. We gained the endpoint protection we needed without having to restrict users' access to anything. Malwarebytes has performed above our expectations.
>
> —Jeff Magnuson, Senior IT Architect, Yaskawa Motoman

Business challenge

Blocking ransomware and malware instead of Internet access

Yaskawa maintains sites across the United States, Canada, Mexico, and Brazil. More than 90 percent of users are engineers, scientists, and software developers, and all have administrator access privileges on their PCs. They load applications that they want to use and often download software or utilities from the Internet. Unfortunately for the IT team, some downloaded software came with malware attached. After the company migrated from an on-premises email service to Office 365, the IT team saw a huge influx of malware, ransomware, Trojans, and malicious emails.

"We were seeing much more malware than viruses," said Jeff Magnuson, Senior IT Architect at Yaskawa Motoman. "Our Kaspersky antivirus didn't catch malware, so I pushed to place malware protection on all of our endpoints."

Magnuson proposed restricting access to known malicious Internet sites, but users objected. By now, the team was cleaning up multiple infections every week, which quickly added up to hundreds of cases over a few months. As Magnuson began looking for an endpoint solution, he wanted one that used minimal CPU resources and ran in real time so that he wouldn't have to rely on end users to interact with the application. It also had to be easy to manage. Finally, he wanted a centralized console that provided visibility into all clients.

The solution

Malwarebytes Endpoint Security

Magnuson had documented the high volume of help desk calls, hours spent remediating infected machines, and numbers of systems that had to be reimaged. It was instantly apparent to the executive team that large amounts of time and money were being spent simply to clean up malware. Magnuson got the go-ahead to find a solution that best fit the company's environment.

"I reviewed a lot of different solutions but it was easy to see that Malwarebytes was the product of choice for us," said Magnuson. "We tested it and chose Malwarebytes Endpoint Security for its effectiveness, manageability, and ease of use."

Greatly reduces risk

"Right off the bat, Malwarebytes greatly reduced risk from endpoint infections," said Magnuson. "It catches more than 90 percent of malware and prevents users from going to malicious sites via links."

Magnuson also says that Malwarebytes does a great job of blocking and cleaning up threats coming in through email. Recently, a user received an email with a PDF attachment that included a URL link. The user clicked on the link, but Malwarebytes blocked access to the site because it contained malware.

Visibility increases productivity

"Malwarebytes has significantly increased our daily productivity," he said. "End users aren't calling with complaints about slow machines, and my team isn't having to continually clean up malware messes."

Magnuson regularly reviews reports from Malwarebytes to make sure that all of the company's endpoints are protected and up to date. It also finds endpoints on the network that would otherwise go undetected. For example, the software development or engineering groups will often add PCs to the network for specific projects. Magnuson periodically performs Active Directory scans and IP scans on the network using the Malwarebytes Management Console, and it finds new endpoints that have been added. When he sees any that aren't protected, he simply pushes Malwarebytes to them.

"Malwarebytes covers all of the bases for us," he said. "We gained the endpoint protection we need without having to restrict users' access to anything. I'm very glad that we chose Malwarebytes, because it has performed above our expectations."