CASE STUDY

Malwarebytes

Building supply company becomes an endpoint security superhero with Malwarebytes

> Large US building supply company overcomes cyberthreats by establishing endpoint resiliency with Malwarebytes Endpoint Protection and Response.

Achieving growth through lasting relationships

It's rare to find a company with a strong history of growth and profits that is focused on lasting relationships and positive community impact. Many partners, contractors, and homeowners rely on the company's unwavering commitment to innovation, quality, and building trusted relationships for their materials needs.

With hundreds of employees across several, US-based office locations, the building supplies company contends with many remote endpoints and an IT staff of two who are tasked with keeping the business operations running. With the continued advances in cybercrime, the company knew one successful breach would threaten their valued relationships and put their growth at risk.

BEFORE MALWAREBYTES

REMEDIATIONS

20 manual remediations per month

REMEDIATION TIME

Several days

REMEDIATION EFFORT:

- IT ships new computer to employee
- IT helps employee set up new computer
- Employee ships infected computer to HQ
- IT spends hours attempting to remediate infected computer

REMEDIATION IMPACT:

- Employee time interrupted
- Extensive IT time consumption

WITH MALWAREBYTES

REMEDIATIONS

3 automated remediations per month

REMEDIATION TIME

Minutes to an hour

REMEDIATION EFFORT:

- IT checks dashboard for suspicious activity
- Malwarebytes EPR automatically isolates the endpoint for high-severity threats
- Malwarebytes EPR automatically runs a deep scan and restores the endpoint

REMEDIATION IMPACT:

- No employee downtime
- Freed up hours of IT time each week

Time-consuming response severely impacted business

With a focus on quality that extends to the company's security posture, as well as employees' ability to work without interruption, relying on unmanaged freeware and consumer security products for endpoint protection was taking its toll on the IT team. Its two employees were starting to experience alert fatigue, and they worried about exposing the company to undue cybersecurity risks.

"Our consumer freeware security approach was unmanageable. We didn't know what threats were in our environment across our endpoints, which was scary and created an unacceptable level of risk to our company's operations," said the IT Project Manager.

The IT team needed to regularly replace a lot of employee machines because they were running slow or had malware and ransomware infections. Up to 20 successful attacks infected employee endpoints each month, limiting their productivity and ability to service customers. Of equal concern: Every infection was taking several days to fully remediate. "Our response process was time consuming and left the impacted employee without a working computer for a good part of the effort," said the IT Project Manager.

For each response, the IT team needed to set up a new machine, ship it to the employee, and help the employee get up and running. Then, the employee needed to ship the infected endpoint back to corporate headquarters, where IT would expend hours of valuable time investigating the threat, attempting to recover lost files, and re-imaging the machine.

"You can imagine the amount of time we spent on responding to attacks. The end-to-end process for each remediation took days to complete," the IT Project Manager explained. "With 15 to 20 remediations each month, that's valuable time our IT team couldn't spend on other things."

Modernizing endpoint security and response to achieve scale

The company knew it needed to pivot from reactive remediation to a proactive approach to endpoint protection and response. Setting out to modernize the company's endpoint security, the IT Project Manager began a multi-vendor evaluation effort. With two IT staff members remotely supporting the company's locations, a cloud-based solution was one of the team's top requirements. In addition, the solution needed to have automated endpoint protection, isolation, and remediation capabilities to ensure business resiliency.

After an evaluation of several solutions, the team selected Malwarebytes Endpoint Protection and Response (Malwarebytes EPR). "Malwarebytes EPR stood out in our evaluation. The product's cloud-based management, along with its intuitive user interface, lightweight agent, and powerful agentless remediation capabilities put it at the top of our vendor list," said the IT Project Manager.

The company engaged with Malwarebytes Quick Start Services for their roll out. "Having professional services as a resource was a huge help," said the IT Project Manager. "They were incredibly knowledgeable and ensured everything went smoothly. With their help, our complete installation took only three to four weeks.

Tackling malware like superheroes

Since installation, Malwarebytes EPR has detected and remediated over 30,000 threats, including ransomware, malware, unwanted programs, exploits, and others. "I log in to Malwarebytes each morning and check for any suspicious activity. With one click, I can either set all the endpoints for immediate remediation or further investigate resolution for more complicated attacks. Remediation is so fast that we get more time back than even imagined. What used to take days, is now done from minutes to an hour without impacting our employees," said the IT Project Manager.

Malwarebytes EPR has also streamlined the IT team's response workflow. Threat cases can be closed with a single click. And the team can easily add safe activity to the exclusion list to ensure it is not flagged as suspicious moving forward. "Having a robust exclusion type list allows us to have readable dashboard data that only shows suspicious activity requiring our attention, which is a game changer for us," said the IT Project Manager.

Malwarebytes EPR helped IT move from putting out fires to being proactive with security. The team has a better understanding of the company's security posture and receives instant alerts when there's a high severity endpoint issue. The company's monthly volume of remediations has plummeted from 20 to three, which are now seamlessly handled by Malwarebytes EPR.

"Malwarebytes EPR gives our stretched-thin IT team the ability to tackle malware and viruses like superheroes. And, the solution gives our employees back their time, which is invaluable," said the IT Project Manager.

Malwarebytes pays for entire endpoint fleet — twice over

Malwarebytes EPR reporting provides the IT team with the important metrics they need to present to executive leadership. "Malwarebytes reporting is robust and it's easy to run reports with a click of a button. Our CFO can easily log in to the cloud console and run a report on the status of our endpoints to confirm the resiliency of our IT environment to our CEO," said the IT Project Manager. "The reports give us the metrics we need to validate that what we're doing for security is paying off."

Malwarebytes has empowered the IT team to optimize endpoint security operations and achieve a strong return on investment. Before Malwarebytes, the building supplies company couldn't find an infection until it was too late. Now, the mean time to response is merely seconds. As soon as Malwarebytes EPR detects a threat, IT is alerted, infections are isolated, and remediation is managed automatically.

"The increased protection and time Malwarebytes has given back to our employees and IT team has paid for our entire fleet of endpoints twice over," said the IT Project Manager.

> "Malwarebytes EPR gives our stretched-thin IT team the ability to tackle malware and viruses like superheroes. And, the solution gives our employees back their time, which is invaluable."
>
> IT project manager
> building supplies 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.