Malwarebytes

Vermeer deploys industrial-strength anti-malware detection

The security team uses Malwarebytes Endpoint Security to remediate and prevent new malware infections while simplifying remote monitoring and scanning

INDUSTRY
Manufacturing

BUSINESS CHALLENGE
Formalize the enterprise security plan and add a new layer of endpoint protection

IT ENVIRONMENT
Data center with enterprise security solutions, including firewalls, perimeter security, web filtering, email and spam filtering, and antivirus software

SOLUTION
Malwarebytes Endpoint Security, which includes Anti-Exploit, Anti-Malware, and the Management Console

RESULTS
- Received scan results 50 percent faster than previously
- Achieved proactive malware detection, blocking, and removal
- Removed malware and improved endpoint performance
- Significantly improved management efficiency

Business profile

Vermeer provides agricultural and industrial equipment that is built tough, built to perform, built for value, and backed by caring customer service provided by its global dealer network. So when the company went to formalize its security policies and add anti-malware and anti-exploit protection, it looked for a product that matched the strength of the products it manufactures.

> I know that Malwarebytes saves time and that our users' machines perform better. Vermeer has taken the right steps and put best practices in place to protect our endpoint users.
>
> —Michael Kraft, IT Security Engineer, Vermeer

Business challenge
Deploy enterprise-class endpoint security with sole proprietor ease of management

Vermeer is a global company headquartered in Pella, Iowa, with subsidiaries in South Dakota, China, Singapore, the Netherlands, and Brazil. The IT team supports Vermeer employees worldwide, and Michael Kraft, IT Security Engineer for Vermeer, is responsible for protecting the organization against cyber threats—including malware.

As part of an initiative to upgrade and formalize the company's security plan, Kraft knew that an extra layer of endpoint security is a best practice. The previous antivirus software chosen by Vermeer handled viruses effectively, but some malware got through anyway. The company's perimeter network security product would alert the team when that happened.

"We got what I call 'nuisance' malware on a weekly basis," said Kraft. "We had toolbars, adware, PUPs, and occasionally a malicious file that was inadvertently downloaded by an employee. I could remediate problems, but we needed a solution that could detect and prevent infections in the first place."

Kraft had tried another endpoint solution that focused on malware, but it was maddeningly slow and lacked robust remote management features. When Kraft received an alert, he wanted to be able to triage and clean up a problem quickly from wherever he happened to be. He was familiar with Malwarebytes from past experience but evaluated several other potential enterprise-class solutions to find the right one.

As a former penetration tester, Kraft conducted a proof-of-concept and put Malwarebytes Endpoint Security through its paces. After testing systems, he selected Malwarebytes Endpoint Security for Vermeer.

"I originally planned to use Malwarebytes just for remediation," he said, "but when I saw the Management Console, it accelerated and simplified management. In addition, if I needed to view a machine, scan, or remediate a system while traveling, I could do it quickly and easily."

The solution
Malwarebytes Endpoint Security
Malwarebytes Endpoint Security includes Anti-Malware for Business, Anti-Exploit for Business, and the Management Console. Malwarebytes Anti-Malware for Business reduces vulnerability to zero-hour malware with powerful detection and remediation. Malwarebytes Anti-Exploit for Business protects endpoints with a layered defense engineered to defeat the latest and most dangerous malware, including ransomware.

Higher visibility
"Malwarebytes confirmed my suspicions about the amount of malware that was actually lurking undetected below the surface," said Kraft. "When we first deployed Malwarebytes, we found lots of stuff on our endpoints that was slowing performance. And none of it had triggered alerts."

After implementing daily and weekly scans, Kraft's list of threats is much, much shorter. Malwarebytes is preventing almost all malware from gaining a foothold and making it much easier to clean up if a user unknowingly downloads a malicious file.

Proactive detecting and blocking
As a proactive anti-malware scanning engine, Malwarebytes blocks malicious websites and detects and remediates malware threats before they can launch serious infections. Proactive detection and blocking saves time for Kraft and quickly points him to potential issues that require intervention. Malwarebytes also quarantines or removes discovered malware, depending on the policy deployed.

"We generated several reports for our quarterly meeting, and the Malwarebytes reports provided comprehensive data," he said. "They were great because they visually demonstrated how effectively we've been able to attack and prevent malware with Malwarebytes."

Fast, easy remote management
"I have the Malwarebytes Management Console up on my screen all day and it just runs," said Kraft. "I don't have to be glued to the monitor, but I can see at a glance what I need to know."

With the Malwarebytes Management Console, Kraft can quickly and easily administer Malwarebytes software on clients while assessing the overall security of the company's endpoints—all from one screen. He can sort by "Last Threats Seen" and quickly identify any anomalies. He knows right away when a scan is running and estimates that he gets scan results about 50 percent faster than with previous antivirus solutions.

"I know that Malwarebytes saves time and that our users' machines perform better," said Kraft. "Vermeer has taken the right steps and put best practices in place to protect our endpoint users."