

# Spellman deals ransomware a major shock

Facing global cyberthreats with confidence

## INDUSTRY

Electronics

## BUSINESS CHALLENGE

Stop ransomware and malware before they affect the company's global users

## IT ENVIRONMENT

Multi-tiered approach to security software and hardware

## SOLUTION

Malwarebytes Endpoint Security

## RESULTS

- Accelerated threat response and increased endpoint performance
- Increased visibility into threats
- Enhanced overall security posture with added threat intelligence

## Business profile

Spellman High Voltage is the world's leading independent supplier of precision, DC high-voltage power supplies, X-Ray generators, and Monoblock X-Ray sources. Its products power applications that advance medical care, industrial processes, quality control, scientific research, security, and telecommunications. When the company needed better protection against ransomware and zero-day threats, it came to Malwarebytes.



With responsibility for global locations, I'm really concerned about ransomware. I'm confident that Malwarebytes technology defends against advanced threats to help keep our employees and data safe.

—Michael Butler, Director Network Operations and Information Security, Spellman High Voltage

## Business challenge

Stop ransomware before it affects global users

Spellman's operations span North America, Europe, and Asia, creating exposure to cyberthreats worldwide. It uses an endpoint security solution to help protect its devices and users.

With cyberthreats advancing and ransomware becoming more common, the IT team has had to become much more aggressive in protecting users and data. If ransomware finds a way in, it can potentially infect systems across the company. Several ransomware incidents affected a manufacturing location, and although the team was able to quickly pull infected machines off the network and reimaged them, the threat was especially worrying.

"With responsibility for global locations, I'm really concerned about ransomware," said Michael Butler, Director of Network Operations and Information Security for Spellman High Voltage. "If it gets a foothold, it will spread through the environment. That's what keeps me up at night."



As malware and ransomware increasingly began to reach users' machines, it was clear that the conventional antivirus wasn't detecting enough. The Spellman team wanted an extra layer of protection against advanced threats.

## The solution

### Malwarebytes Endpoint Security

"We needed a better way to prevent ransomware and deal with the tremendous amount of garbage coming in," said Butler.

"Many of us were already aware of Malwarebytes and had experience using it. When we investigated it further, we found that it could give us much better visibility and central management capabilities in a global enterprise environment."

Malwarebytes Endpoint Security with the Malwarebytes Management Console centralizes deployment, updates, monitoring, and information gathering in one place. The Spellman team field-tested Malwarebytes extensively before deciding to deploy it worldwide.

"The Management Console is key," said Butler. "It's great for us and it works well with our antivirus tools. We have a policy that automatically installs Malwarebytes or updates as soon as an endpoint checks into the network. It doesn't affect the user, and it's really quick."

### Performance increases for everyone

The first thing the team noticed was that machine performance increased for users. Simply removing the adware, Potentially Unwanted Programs (PUPs), and other malware made machines run better. It also eliminated confusing pop-ups that distracted users. Malwarebytes real-time email notifications alerted the IT team when anything suspicious was detected.

"Anytime we get a Malwarebytes email, we immediately check it out," said Mark Balcerak, Information Security Supervisor at Spellman High Voltage. "Regardless of what it might be—we know that it's potentially serious. We can quickly pull the machine off the network and deal with it. It's a huge benefit for us."

### Visibility and better intelligence

Daily and weekly scans increase the team's visibility. Thanks to Malwarebytes, the team has removed tens of thousands of Ask toolbars, instances of peer-to-peer software, ChinAd and Dropper Trojans, PUPS, and zero-day threats. Spellman also has more intelligence for monitoring its overall security strategy. Malwarebytes integrates with the company's SIEM, which aggregates and correlates Malwarebytes alerts with other data to investigate any anomalies occurring in the network.

"We print out a weekly threat report to share with our CIO," said Balcerak. "We weren't surprised that the threats were there—but we were a little taken aback by the sheer volume."

### Support in the fight

The Spellman team said that their Malwarebytes representative has been invaluable to their efforts. He has kept them informed, been available to brainstorm, answer questions, and direct the team to the help they need when they need it.


"I'm confident that Malwarebytes technology defends against advanced threats to help keep our employees and data safe," said Butler.


## | About

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

 Santa Clara, CA

 malwarebytes.com

 corporate-sales@malwarebytes.com

 1.800.520.2796