Malwarebytes

At PAPSTAR GmbH, malware no longer crashes the party

Leading European distributor of party and catering products uses Malwarebytes to avoid downtime and revenue loss

INDUSTRY
Distribution

BUSINESS CHALLENGE
Eliminate revenue loss and downtime due to ransomware

IT ENVIRONMENT
Data center with corporate network firewall, Microsoft System Center, Trend Micro OfficeScan antivirus

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

RESULTS
- Stopped ransomware from affecting operations
- Avoid revenue loss associated with ransomware-induced downtime
- Regained valuable staff time by eliminating need to re-image endpoints
- Gained visibility into endpoints and threat status

Business profile

As a leading European packaging distributor, PAPSTAR GmbH delivers more than 7,000 beautiful, premium-quality table and party decorations, disposable tableware, and food packaging items to retailers and professional caterers. When ransomware struck, PAPSTAR used Malwarebytes to show it to the door.

> Malwarebytes completes our endpoint protection strategy with real-time scanning and notification. The added protection we receive from Malwarebytes has made malware and ransomware things of the past.
>
> —Marcus Rodermond, Manager, Data Center and IT Services, PAPSTAR GmbH

Business challenge
Avoid ordering and shipping disruption

PAPSTAR's data center and IT services team looks after 200 endpoints across German headquarters and subsidiaries in seven countries, as well as 34 terminal servers that host the company's extensive product catalog and ERP system functions. Until recently, the company's antivirus solution had sufficiently handled viruses.

Suddenly, users noticed that they couldn't access product images of the product database. This effectively halted customer service, sales, and shipping operations, since the product catalog is a primary sales channel. As the team discovered, a ransomware attack had targeted PAPSTAR's ERP product image library.

Then it happened twice more, each time with a slightly different twist. For example, one time ransomware encrypted product photographs. Another time it tried to encrypt network applications.

"Each time, we were able to recognize what was happening and immediately cut off access from the infected client," said Achim Hilger, System Engineer at PAPSTAR GmbH. "We restored applications from backup, but it resulted in about four hours of downtime for some functions of our core application. In addition, it took one to two hours to re-image the endpoints affected."

The solution

Malwarebytes Endpoint Security

The company's antivirus vendor and external IT partner couldn't offer a solution for ransomware, so the PAPSTAR team conducted research online to find a solution. They found Malwarebytes.

"Malwarebytes works differently than antivirus solutions," said Marcus Rodermond, Manager Data Center and IT Services at PAPSTAR GmbH. "Instead of relying on known patterns, it analyzes how the malware or exploit works. It's much faster, because we don't have to wait for new patterns to download."

Malwarebytes Endpoint Security provides a powerful multi-layered defense engineered to defeat the latest, most dangerous malware, including ransomware. It includes Malwarebytes Anti-Malware, Anti-Exploit, and the Management Console in one comprehensive solution. Malwarebytes Anti-Malware detects and eliminates zero-hour malware, Trojans, worms, rootkits, adware, and spyware in real time. It stops threats in their tracks, eliminating the need for PAPSTAR to manually remove malware from endpoints. Malwarebytes Anti-Exploit adds four additional layers of protection to block exploits and prevent malicious payloads from being delivered.

Comprehensive protection with rapid deployment

PAPSTAR deployed Malwarebytes in January 2016, needing only two weeks to roll it out to all endpoints.

They also deployed Malwarebytes on their terminal servers with the help of Malwarebytes support.

"Support is excellent," said Achim Hilger. "The Malwarebytes support team helped us work out a detail with one of our existing applications that triggered a false positive. Now we have excellent coverage with separate policies for endpoints and terminal servers."

Email alerts enable fast response

"We wanted the Malwarebytes Management Console for centralized control," said Marcus Rodermond. "We really like the email reporting feature. The moment an exploit is found, we know. We know the type, which user, and the location of the endpoint so we can react quickly and appropriately."

Since deploying Malwarebytes, PAPSTAR has identified spam emails, Potentially Unwanted Programs (PUPs), malicious attachments, fake invoices, and other threats. Malwarebytes directly quarantines the malware without intervention from the team, and they can clean or re-image a machine if needed.

Saving time and revenue

"Since we deployed Malwarebytes, we have had no impact from ransomware," said Achim Hilger. "Malwarebytes successfully blocks malware and has saved significant time because we no longer have to re-image machines."

At the same time, PAPSTAR has avoided malware-related downtime and revenue loss. The product catalog stays available to customers, and shipments go out on time.

"Malwarebytes completes our endpoint protection strategy with real-time scanning and notification," said Marcus Rodermond. "The added protection we receive from Malwarebytes has made malware and ransomware things of the past."