Malwarebytes

CASE STUDY

H.T. Hackney cancels ransomware delivery

Company uses Malwarebytes to defend endpoints while improving user productivity

INDUSTRY
Wholesale distribution

BUSINESS CHALLENGE
Gain effective protection against ransomware and zero-day threats

IT ENVIRONMENT
Data center with Kaspersky antivirus, Windows Active Directory, IBM servers, IBM SmartCloud, Proofpoint Email Protection, Dell KACE console, Cisco Adaptive Security Appliances

SOLUTION
Malwarebytes Endpoint Security

RESULTS
- Reduced threats by 96% in first three weeks
- Stopped ransomware immediately
- Eliminated user complaints about slow computer performance
- Significantly simplified endpoint management with better visibility

Business profile

H.T. Hackney provides everything that its grocery and convenience store customers need to be successful—from food service products to food-handling equipment. The company also owns five subsidiary companies. When ransomware and other malware started to bypass the company's antivirus solution, H.T. Hackney turned to Malwarebytes to stop it cold.

> When we first deployed Malwarebytes, it reported 108,000 threats, and within three weeks, that was reduced by 96%. When Cryptolocker attacked the company, Malwarebytes stopped it in its tracks with no impact to the machines or files.
>
> —Weston Waggoner, IT Administrator, H.T. Hackney

Business challenge

Prevent ransomware from getting in without compromising productivity

Headquartered in Knoxville, Tennessee, H.T. Hackney operates from 24 locations ranging north to Michigan and south to Florida. Until recently, the company had been protecting its endpoints with a Kaspersky antivirus solution—and it wasn't doing the job.

"Not only wasn't it doing the job, it was creating a lot of user complaints," said Weston Waggoner, IT Administrator for H.T. Hackney. "With more than 750 endpoints and only three of us managing IT, complaints about slow computers and problems with malware were taking up a lot of valuable time and affecting our users' productivity."

Waggoner and his team needed a better solution, so they evaluated Cylance, Carbon Black, and others. These products were not only cumbersome, they had a big inherent risk. The products needed to run for up to three weeks to inventory and whitelist everything on the company's network. However, Waggoner knew that undetected threats, such as ransomware, were still on the company's network. So these products actually whitelisted the malware and ransomware with everything else, effectively setting it up to be accidentally activated and undetectable—opening a huge security hole.

The solution

Malwarebytes Endpoint Security

"Once we saw a demonstration of Malwarebytes, it was a no-brainer," said Waggoner. "We could actually see the threats, stop them, and clean them off our systems."

H.T. Hackney initially deployed Malwarebytes on 750 endpoints. Using the Malwarebytes Management Console, the team built their installation package and pushed the software out to its endpoints through Dell KACE.

Stopped ransomware cold

When the team first deployed Malwarebytes, it reported 108,000 threats. Within three weeks, Malwarebytes reported 5,000—down by 96%. When Cryptolocker attacked the company and attempted to infect machines, Malwarebytes stopped it in its tracks with no impact to the machines or files.

"We see all kinds of malware—from ASK toolbars and Potentially Unwanted Programs (PUPs) to ransomware and exploits," said Waggoner. "If a threat has been hiding dormant on an endpoint and then tries to execute, Malwarebytes stops it. Malwarebytes also prevents users from re-installing toolbars that it removes."

No more calls

Once Malwarebytes was deployed, complaints from users about slow machines stopped. They no longer have problems because Malwarebytes has a minimal footprint on computers and requires far fewer computing resources than the traditional antivirus solution did.

"Their computers are faster," said Waggoner. "Malwarebytes gives us peace of mind knowing that not only are we protecting the company from zero-day malware and ransomware, we are helping our users be more productive and happier."

Continually testing effectiveness

Waggoner continually tests Malwarebytes on his own system by throwing the nastiest malware he can find at it. As a member of Virus Total, he can download viruses and malware to test the effectiveness of the company's security measures.

"I've downloaded viruses and fired them off on my computer," he said. "Malwarebytes takes care of every bit of it. When zero-day threats came through our traditional antivirus, it might clean them up, but the bad actors just change the hashtag and do it again. Malwarebytes actually cleans it up and prevents it from coming back in once and for all—which is what I love about it."

Life is much easier

Malwarebytes is set to scan H.T. Hackney machines weekly, sending any alerts directly to Waggoner. He uses the Malwarebytes Management Console to investigate, track the types of malware attempting to gain access, assess the extent of any impact, and know exactly where to remediate if necessary.

"Malwarebytes and the Management Console are tremendous, and they're making our life a lot easier," he said. "Malwarebytes is handling 90% of the threats coming into users' endpoints. In fact, the Kaspersky antivirus tool doesn't send us alerts anymore. I think it's given up."

Regardless of how much the company locks down its endpoints, Waggoner knows that threats will still find a way in. But knowing that Malwarebytes has their back is a huge relief, and being able to see exactly what is happening through the Management Console gives them more visibility than they ever had before.

"We're stopping threats that get in and try to move laterally," he said. "We've seen that. Malwarebytes does a great job of cleaning that stuff up and keeping it off the network. It's doing what it's supposed to."

Next steps

The IT team is planning to extend Malwarebytes protection to other H.T. Hackney subsidiaries. "My goal is to have every PC that is part of H.T. Hackney have Malwarebytes on it. We're extremely happy—it really is an amazing product."

About

Malwarebytes provides anti-malware and anti-exploit software designed to protect businesses and consumers against zero-day threats that consistently escape detection by traditional anti-virus solutions.

Santa Clara, CA

corporate-sales@malwarebytes.com

malwarebytes.com

1.800.520.2796