Malwarebytes

Jo Mercer gives ransomware the boot

Malwarebytes simplifies protection from the cloud

INDUSTRY
Retail

BUSINESS CHALLENGE
Maintain business continuity to avoid production downtime

IT ENVIRONMENT
Windows Defender antivirus

SOLUTION
Malwarebytes Endpoint Protection

RESULTS
- Accelerated protection with one-day rollout and "easability"
- Replaced Symantec and stopped malware and ransomware infections
- Simplified operations, freeing the team for other priorities

Business profile

Australian women who want on-trend footwear with exceptional craftsmanship look to Jo Mercer for the season's newest looks. Based in South Yarra, Victoria, Jo Mercer prides itself on a diverse range of contemporary footwear inspired by global trends. However, ransomware was a global trend that the brand wanted to avoid. It gave ransomware the boot with Malwarebytes Endpoint Protection.

> ❝ It took one day to roll Malwarebytes out across the company. Malwarebytes detects and manages threats without human interference. It lets us move forward on technology and other priorities because we always know what's going on.
>
> — William Buhl, IT Support, Jo Mercer

Business challenge

Kicking ransomware out

There are 40 Jo Mercer sites across Australia, including retail stores, regional managers, and a Support Office. William Buhl, of Jo Mercer's IT Support team, manages IT and security for all of the locations. Australia's size makes it infeasible to visit remote sites for support. Many employees work on the road and others travel globally, so Jo Mercer had moved much of its IT infrastructure to the cloud to simplify operations for its four-person IT team.

When the company was hit by a vicious ransomware attack, the team realized that their Symantec solution wasn't effective against it. In just three minutes, ransomware paralyzed a portion of the business and tried to destroy all of its data and backups.

"We stopped it before it jumped from corporate systems to our stores," said Buhl. "But our mobile employees couldn't access data or systems for a couple of days. It was pretty crazy."

Infected machines were immediately disconnected from the network and re-imaged three times, just to be sure that they were clean. Then the team reinstalled and tested systems again before

reconnecting to the network. Buhl's team also locked down the company's Internet connection, only enabling access to a handful of legitimate websites and the Office 365 email system.

The solution

Malwarebytes Endpoint Protection

"After we recovered, we Googled 'ransomware defense systems' and Malwarebytes was at the top of the list," said Buhl. "We read reviews, downloaded a trial version, and evaluated Malwarebytes Endpoint Protection. It was really successful, so we were up and running."

Jo Mercer replaced its Symantec solution with Malwarebytes, deploying it from the cloud on endpoint systems and servers. Besides delivering protection against ransomware, Malwarebytes was more efficient on users' systems. Its small footprint takes up little space and runs almost invisibly in the background compared to the intrusive Symantec solution.

Flexible deployment

Now the team simply deploys Malwarebytes on new systems from the cloud console. They can add an endpoint and bring up the whole network to view status. They also can log in through Active Directory and do the same thing. Either way, they silently push Malwarebytes and install it in the background.

"It took me one day to roll Malwarebytes out across the company," said Buhl. "We're always flat out, and Malwarebytes was pretty much plug and play. The network discovery tool made it simple to push out—that was fantastic. We saved a lot of time."

"Easability" of everything

Buhl allocates policies according to different groups of users. He can separate the support office from regional sites, individual stores, and servers and deploy specific policies for each.

"Malwarebytes is so easy to use," said Buhl. "Because it's in the cloud, we can log in from anywhere. If I receive an email alert while I'm at a conference, I can check to see what's going on, which computer is infected, and contact the end user before taking action."

Giving the boot to infections

Jo Mercer hasn't had a single malware or ransomware infection since deploying Malwarebytes. In addition, Malwarebytes blocks malicious websites, which significantly reduces risk to the company.

"We haven't found another solution that successfully blocks malicious sites like Malwarebytes," said Buhl. "If an incident occurs during off hours, it would take me 45 minutes to get to the office to see what happened before I could do anything, and in 45 minutes, anything can happen."

Getting real-time protection

The team can see exactly what's happening at any moment through the Malwarebytes real-time protection tab. It delivers an overview at a glance of how many computers are online or offline, threats that have been detected, what was cleaned up, and other data. Live updates keep the team informed—even when they aren't logged into the console.

"Malwarebytes detects and manages threats without human intervention," said Buhl. "It lets us move forward on technology projects and other priorities because we always know what's going on. It's fantastic for us."