

# Home Hardware hammers exploits and malware

Desktop Support team regains hundreds of hours of productivity while improving security posture

## INDUSTRY

Retail

## BUSINESS CHALLENGE

Stop threats and reduce the number of alerts that require investigation

## IT ENVIRONMENT

McAfee antivirus and FireEye filtering solution

## SOLUTION


Malwarebytes Endpoint Security

## RESULTS

- Stopped threats at endpoints, dramatically reducing alerts
- Reduced the number of machines needing reimaging to zero
- Regained hundreds of hours of time for Desktop Support staff to focus on other tasks
- Gained protection with zero disruption to end users

## Business profile

Home Hardware Stores Limited is Canada's largest dealer-owned hardware, lumber, building materials, and furniture retailer with close to 1,100 stores and annual retail sales of more than \$5.8 billion. When its traditional antivirus solution failed to catch malware, and incident response consumed hundreds of hours, the corporate support team nailed exploits with Malwarebytes.



Malwarebytes has changed our response to malware for the better. It has saved us hours of work and given us a better comfort level.

—Phil Bousfield, Desktop Support Supervisor,  
Home Hardware Stores Limited

## Business challenge

Stop the bombardment

Home Hardware supports its Dealer-Owners from the corporate office and multiple distribution sites across Canada. With more than 1,200 computer endpoints, executives who travel frequently, and a rising tide of exploits, malware, and ransomware, the Desktop Support team found itself reacting to a rapidly increasing number of alerts.

“Our antivirus solution wasn’t catching threats like malware and exploits,” said Phil Bousfield, Desktop Support Supervisor for Home Hardware, “and scans were CPU-intensive. We got a lot of complaints from users during a scan.”

In an attempt to better fight threats, the Home Hardware network team deployed a FireEye solution. It dramatically increased visibility into network packets—and also started bombarding the Service Desk with alerts. Each time the solution detected an anomaly, it generated a support ticket. The details of those alerts were complex and not all support levels had access to the data. Therefore a zero-tolerance approach to malware and exploit threats was initiated. This meant that the Desktop Support team was responding to dozens of alerts, doing manual



remediation, system restores, and reimaging at least one machine a day. This involved significant support time and lost user productivity.

“Investigating alerts and reimaging machines was really disruptive to users,” said Bousfield. “A large number of FireEye alerts turned out to be false positives, mainly from legitimate website activity. This was seriously hindering user productivity and consuming hours of our time.”

It was time for Home Hardware to move from a reactive, firefighter mode to a proactive, prevention mode. The company’s managed security provider recommended scanning machines with a malware tool and suggested using Malwarebytes.

## The solution

### Malwarebytes Endpoint Security

Home Hardware chose Malwarebytes Endpoint Security, which provides a powerful multi-layered defense engineered to defeat the latest, most dangerous malware, including ransomware. Malwarebytes Endpoint Security also includes the Malwarebytes Management Console to simplify management and machine cleanup.

Using the Malwarebytes Quick Start service, Home Hardware worked closely with the Malwarebytes team to plan the deployment and set up the database for the Management Console.

“The Quick Start service made setup and installation go very smoothly,” said Bousfield. “The Malwarebytes team was with us on the phone when we installed it, and we had it done in about 45 minutes.”

### Better threat identification, less impact

Once Malwarebytes was deployed, it quickly identified many potential malware entry points, which if not addressed, could lead to malware infections and exploit attempts. Toolbars and Potentially Unwanted Programs (PUPs) are gateways for other malware to get into users’ systems. Now Malwarebytes quarantines malicious files

and blocks exploit attempts in real time. This makes it much easier to keep machines clean. Bousfield set up quick scans, and machines are scanned weekly with almost zero impact to users—and no complaints.

“Now we can have Malwarebytes on every machine and receive information back into the Management Console,” said Bousfield. “It’s fantastic.”

### Simpler remediation

With Malwarebytes on the scene, exploits and threats are blocked at the client level, which means that they don’t trigger FireEye alerts. Malwarebytes quarantines malicious items, blocks exploit attempts and then generates an email to notify the Home Hardware Support Desk. The support ticket is then forwarded to Desktop Support staff, who then check the machine in the Malwarebytes Management Console. The support ticket information provides a record of the event. Trends or similarities to other machines can be examined, the ticket is updated and a follow-up quick scan of the endpoint is remotely initiated. Then the Desktop Support staff members are free to move on to other tasks or duties.

“I’m very happy with the way that Malwarebytes works,” said Bousfield. “It remediates, and we do a follow-up scan. If it scans clean, we’re done. We haven’t had to reimage a machine since we put Malwarebytes in place.”


### Time savings with a high comfort level

Because support operates 24 hours a day, Malwarebytes also helps the night shift. Before, if a firewall event occurred overnight, an operator was paged and had to investigate and remove the system from the network. Now, if a malware ticket is generated, the team knows that Malwarebytes has already remediated the threat, so that they can wait and look at it the next morning.

“Malwarebytes has changed our response to malware for the better,” said Bousfield. “It has saved us hours of work and given us a better comfort level.”

## | 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