

Ur & Penn refuses to give malware the time of day

Timepiece retailer uses Malwarebytes to prevent productivity disruption and reduce risk

INDUSTRY

Retail

BUSINESS CHALLENGE

Eliminate malware as a source of disruption, wasted resources, and risk

IT ENVIRONMENT

One data center; Microsoft Security Essentials antivirus; all network connectivity and security measures are provided by Ur & Penn's ISP

SOLUTION

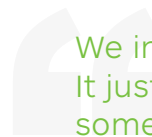
Malwarebytes Endpoint Security, which includes Anti-Malware, Anti-Exploit, and the Management Console

RESULTS

- Saved hours and days of IT time previously spent remediating endpoints
- Gained complete control over malware, eliminating thousands of threats
- Reduced risk associated with theft of credit card, financial, and other sensitive information

Business profile

Ur & Penn was established in 1943, and since then it has expanded to more than 100 stores in Scandinavia and the United States. The company designs its own watches and sells directly to customers, eliminating layers of intermediaries and cost. Ur & Penn also took a direct approach to securing its endpoints, using Malwarebytes to stop the clock on malware.



We instantly saw the value of Malwarebytes. It just runs. It updates itself. It tells us when something happens, and then it takes care of it. Simple.

—Emir Saffar, IT Specialist, Ur & Penn

Business challenge

Reduce risk and productivity disruption

Ur & Penn's employees are located in Sweden, Finland, and the United States. There are 60 computers and endpoints at headquarters in Sweden and approximately 190 computers deployed in the company's retail shops and other facilities. The IT team implemented Microsoft Security Essentials as its antivirus solution, but it wasn't catching rapidly multiplying malware.

"We had chronic problems with pop-ups, Potentially Unwanted Programs (PUPs), and Potentially Unwanted Modifications (PUMs)," said Emir Saffar, IT Specialist at Ur & Penn. "Our Google Chrome, Internet Explorer, and Firefox web browsers seemed to be the favorite targets."

Computers would slow to a crawl, users would call IT and complain, and IT would have to stop what it was doing to identify and clean up malware. Infections occurred several times each week at headquarters, and infected machines would have to be completely re-imaged if they were heavily infected.



Not only were malware infections disruptive, they increased the company's risk. As a retailer, Ur & Penn is responsible for credit card and financial data. Malware, such as Trojan-Bankers, and exploits could hijack sensitive data and steal personal information.

The solution

Malwarebytes Endpoint Security

The team looked at several malware solutions, but they were too computer-intensive or they didn't have centralized management capabilities. Without central management, they would have to install anti-malware on every endpoint across three countries and hope that the local staff could handle any problems. That wasn't a great solution.

"We chose Malwarebytes Endpoint Security as our extra layer of defense against malware because it solved both of those issues," said Saffar. "It gave us better protection that is simpler and more manageable."

Malwarebytes Endpoint Security provides a powerful multi-layered defense engineered to defeat the latest, most dangerous malware and exploits. It includes Malwarebytes Anti-Malware, Anti-Exploit, and the Management Console in one comprehensive solution.

No more wasted time

"We installed Malwarebytes ourselves—it was simple," said Saffar. "It took less than a day to deploy and begin using."

Active Directory integration made it easy to push out Malwarebytes software to all Ur & Penn endpoints. The team also installed Malwarebytes on a majority of their servers. Calls from users about malware-related issues quickly dropped to zero. In the past, it took four to five hours to re-image and reinstall just one machine. The IT team no longer loses time cleaning machines and users don't lose productivity—Malwarebytes just works in the background without any intervention from IT or users.

Works like...clockwork

Since it was deployed, Malwarebytes has removed almost 15,000 threats and blocked several exploits.

"We instantly saw the value of Malwarebytes," said Saffar. "It just runs. It updates itself. It tells us when something happens, and then it takes care of it. Simple."





Direct control gives peace of mind

Saffar also likes the ability to see and manage everything from the Management Console. With direct control over malware, the team is able to keep machines from infection, wherever they are located.

"Malwarebytes is a great product and a great company," he said. "Since deploying Malwarebytes Endpoint Security, we gained full control over malware and we no longer worry about it."

| 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