Malwarebytes

Agnico Eagle Mines Ltd. strikes gold with Malwarebytes

Malwarebytes proactively blocks exploits from entering and digging in

INDUSTRY
Mining

BUSINESS CHALLENGE
Block advanced threats that escape traditional antivirus tools

IT ENVIRONMENT
Trend Micro antivirus, data center with firewalls, SSL certificate authority

SOLUTION
Malwarebytes Endpoint Security, which includes Anti-Malware for Business, Anti-Exploit for Business, and the Management Console; Malwarebytes Quick Start Service

RESULTS
- Stopped ransomware and malware and blocked malicious sites and sources of exploits
- Deployed consistent protection across the organization in North America, Central America, and Europe
- Gained deeper visibility into potential threats and attackers

Business profile

Agnico Eagle Mines Limited has produced precious metals since 1957. Headquartered in Toronto, it explores, develops, and operates mines in Canada, the United States, Mexico, Finland, and Sweden. To prevent malware from digging in, Agnico Eagle Mines deployed Malwarebytes.

> Malwarebytes picked up so many things that our traditional antivirus tool was missing. Malwarebytes absolutely works and is totally worth it.
>
> —Augusto Juarrero, Analyst of Information Technology, Agnico Eagle Mines Limited

Business challenge
Continuously build defenses against security threats

Gold-mining operations generate the majority of Agnico Eagle Mines' revenue, although the company also mines silver, zinc, and copper. And where there's gold, there are people who want it. Cybersecurity has recently become a huge issue for energy and mining companies as hackers increasingly target them.

Even before hackers started focusing on mining and energy companies, the Agnico Eagle Mines IT teams had taken a proactive stance against threats. They'd deployed a Trend Micro antivirus solution for the company's endpoints, but a growing number of advanced threats, like exploits and ransomware, were still getting through. Browsing-related issues also increased. Site-to-site tracking and nuisance-ware affected users' machines.

"Security can always be breached," said Augusto Juarrero, Analyst of Information Technology at Agnico Mines Limited. "We do everything we can to add layers of security. We needed to add a layer that complemented our antivirus without affecting PC performance."

The solution
Malwarebytes Endpoint Security

The IT teams from Mexico, Finland, and Canada met to discuss their options. All had previous experience with Malwarebytes, and all agreed that it was the best solution for Agnico Eagle Mines. They chose Malwarebytes Endpoint Security to combat malware and exploits.

Malwarebytes Endpoint Security provides a powerful multi-layered defense engineered to defeat the latest, most dangerous malware, including ransomware. It includes Malwarebytes Anti-Malware for Business, Anti-Exploit for Business, and the Management Console in one comprehensive solution. Anti-Malware for Business detects and eliminates zero-hour malware, Trojans, worms, rootkits, adware, and spyware in real time. Anti-Exploit for Business adds four additional layers of protection. Ransomware, such as Cryptolocker, is typically distributed using phishing campaigns or compromised websites. By combining anti-exploit and anti-malware capabilities, Malwarebytes helps protect against threats and prevents malicious payloads from being delivered.

Agnico Eagle Mines also chose the Malwarebytes Quick Start Service to help deploy and configure its Malwarebytes solution. Quick Start provides assistance with project management, knowledge transfer, and deployment planning.

"Our Malwarebytes Technical Account Manager walked us through the Management Console in a videoconference meeting," said Juarrero. "He also helped us roll it out—from scheduling to doing the installations. He was always available to us."

Agnico Eagle Mines deployed Malwarebytes on approximately 3,500 endpoints. They also deployed the Management Console in Canada, Mexico, and Finland, giving each local IT team visibility into their machines.

It works

Immediately after installing Malwarebytes on machines in Mexico, the team found ransomware, Trojans, and a wide range of other malware. All of it had slipped by the traditional antivirus tool.

"That was the proof of concept right there," said Juarrero. "Malwarebytes picked up so many things that our traditional antivirus tool was missing. Malwarebytes absolutely works and is totally worth it."

Zero disruption to users

Malwarebytes has almost zero impact on users. The teams can deploy it on new endpoints, update it, or scan users' machines—and users never notice. The Malwarebytes database is small, and it can update machines either directly from the server or over the Internet. This feature is ideal for Agnico Eagle Mines, because many of the company's sites are located in remote areas with only satellite connectivity. Satellite bandwidth is highly constrained by its cost, so a small update footprint is essential for delivery over satellite communications.

Visibility for stronger policy

"In the past three years, 70% of malware findings have been exploits from bad sites," said Juarrero. "Malwarebytes Anti-Exploit for Business blocks malicious sites. I can see which sites are blocked, and I can use that insight to better educate users and continuously improve policies for machines under management."

Worth recommending

Juarrero said that the support Agnico Eagle Mines received from Malwarebytes was outstanding. As they continue to add as many layers as needed to their security architecture, he appreciates Malwarebytes' support.

"The help we received was great," said Juarrero, "and I felt safe and comfortable every step of the way. Malwarebytes is a great product, it's reliable, and I highly recommend it to anyone."