Malwarebytes

CASE STUDY

Vocus Group NZ dials up defense with Malwarebytes

Solid protection against ransomware

INDUSTRY
Telecommunications

BUSINESS CHALLENGE
Deploy additional endpoint protection against ransomware

IT ENVIRONMENT
Antivirus, firewalls, email gateway

SOLUTION
Malwarebytes Endpoint Security

RESULTS
- Stops ransomware
- Integrates with existing security infrastructure
- Operates without disruption to users

Business profile

Vocus Group operates a range of ISP and telco businesses in New Zealand. Its national network spans more than 4,200km of fibre optic connectivity, enabling customers to easily connect multiple locations. Vocus Group NZ delivers IP WAN, internet connectivity, data center, cloud, voice, backup, firewall, and DDOS services to its customers, configured to meet their specific needs. To give its own endpoints additional protection against advanced threats like ransomware, Vocus Group NZ implemented Malwarebytes.

> We deployed Malwarebytes quickly with minimal overhead. It gives us protection that is highly complementary to our existing security infrastructure.
>
> —Ivan Reutskiy, Security Manager, Vocus Group NZ

Business challenge

Add a lightweight layer of protection to endpoints

Vocus Group New Zealand operates a diverse range of computing environments—from high-end technical engineering installations to office and follow-the-script call centers. Most of the company's PC workstations are located in its main offices in Auckland, New Zealand. With ransomware increasingly targeting enterprises, the Vocus security team wanted to add more protection to the endpoints.

"We had seen isolated instances of ransomware, which raised executives' concerns," said Ivan Reutskiy, Security Manager at Vocus Group New Zealand. "They came in through web drive-by attacks on users' browsers—which the antivirus missed."

The company's security technologies and processes caught and contained the incidents, enabling the team to quickly restore network access for the affected users. But each incident created extra work for the security team. They had to ensure that the ransomware was correctly isolated, conduct an investigation, and

analyze the forensic data. Each instance took at least a day and a half for two people to resolve. Reutskiy and the network team wanted stronger endpoint protection that was easy to manage and cost effective. They chose Malwarebytes Endpoint Security.

The solution

Malwarebytes Endpoint Security

The network team deployed Malwarebytes specifically for endpoints on the main office LAN. They created a group policy and pushed the software to the workstations, and they made Malwarebytes part of a standard configuration build for workstations. They also integrated Malwarebytes with the SIEM to deliver additional data for aggregation and correlation. Since the deployment, Malwarebytes runs quietly on users' systems in the background, protecting the workstations every day.

"We deployed Malwarebytes quickly with minimal overhead," said Reutskiy. "It gives us protection that is highly complementary to our existing security infrastructure. My IT guys like it, and they can spend time on other network tasks. It makes everyone happy."

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