Malwarebytes

CASE STUDY

# **Federation Council** increases cyberthreat protection and management simplicity

Malwarebytes finds and removes junkware and unexecuted ransomware

## Business profile

The Federation Council of New South Wales (NSW), Australia, provides a range of services to the region. From community and economic development, roads and transport, and environmental services to promoting tourism, the Federation Council seeks to create a safe and healthy living, working, and recreational environment. A healthy environment includes administrative systems that are free from cyberthreats. When it was time to renew its antivirus product, the Federation Council opted for a better solution and chose Malwarebytes.

## Business challenge

**Stepping up protection**

The Corowa region of New South Wales is located on the border of New South Wales and Victoria and is one of the most productive wool, grain, lamb, and beef-cattle areas of Australia. Federation Council's operations span two primary offices, public libraries in outlying towns, and multiple water and sewer plants. User endpoints had a Trend Micro antivirus product installed, but when renewal time came, the IT team wanted stronger protection against advanced malware attacks than Trend Micro provided.

"Prior to joining the Federation Council, I'd faced almost everything that the Internet could throw at me," said Simon Allen, IT Systems Administrator for the Federation Council. "I had used Malwarebytes in previous roles to clean up systems after other antivirus products dropped the ball. I recommended that we replace Trend Micro with Malwarebytes, and our management agreed."

## OVERVIEW

**INDUSTRY**
Government

**BUSINESS CHALLENGE**
Improve detection of cyberthreats and enhance the ability to protect users

**IT ENVIRONMENT**
Layered enterprise security measures

**SOLUTION**
Malwarebytes Endpoint Protection

**RESULTS**
Detected and removed thousands of pieces of malware, junkware, ransomware, and related artifacts that the traditional antivirus missed

Simplified endpoint security management across a large area with remote systems

Reclaimed bandwidth from excess web traffic generated by adware and command-and-control malware

> MALWAREBYTES IS ABSOLUTELY DOING ITS JOB. MALWAREBYTES IS NOT ONLY PROTECTING US, IT'S SAVING MANAGEMENT TIME, FREEING BANDWIDTH, AND DELIVERING OUTSTANDING VALUE.
>
> SIMON ALLEN, IT SYSTEMS ADMINISTRATOR, FEDERATION COUNCIL NSW

## The solution

**Malwarebytes Endpoint Protection**
The Federation Council chose Malwarebytes Endpoint Protection for its advanced malware detection and remediation capabilities. Web protection, application hardening, exploit mitigation, payload analysis, behavior monitoring, and other features provide the Federation Council with multi-vector protection against all kinds of threats.

Based in the cloud, Malwarebytes Endpoint Protection made it easy for Allen and his team to protect systems in remote offices across 500 square kilometers. A microwave network with 100 Mbps bandwidth links all Federation Council facilities, and each location has Internet connectivity. With bandwidth at a premium, cloud-based management enables the team to manage each location's computers over its own Internet link without having to send updates across the microwave connections.

"Malwarebytes deployment was effortless," said Allen. "I used the deployment tool from the cloud console. We deployed the vast majority of endpoints in a day, and caught up with remote, offline endpoints when they reconnected with the network."

**Simplicity with effectiveness**
Malwarebytes immediately detected 30,000 instances of junkware, malware, system anomalies—even unexecuted ransomware that had been ignored by the Trend Micro solution for two years.

"Malwarebytes' simplicity is outstanding," said Allen. "Deployment was fantastic and management is simple. For example, when I whitelisted a proprietary government application on the cloud console it automatically worked for everyone. It is so easy."

Allen said that in addition to detecting malicious files, Malwarebytes finds and removes the onslaught and buildup of PUPs, toolbars, adware, and PUMs, most of which the Trend Micro product had missed. Currently Malwarebytes is blocking dozens of cryptojacking websites—legitimate websites that are compromised by malware that uses the endpoint's CPU power to mine cryptocurrency.

**Protection with performance**
Removing the buildup of junkware on systems improves their performance. Malwarebytes also protects users from landing in places on the Internet that they don't want to be. For example, Allen says that when someone uses a "dodgy" search tool and clicks on paid ad results, they can end up with a malicious search agent installed in their Chrome browser. From there, users can easily end up on malicious or even criminal websites.

"For me, the real-time web blocking is phenomenal," said Allen. "Trying to stay on top of site blacklists is a never-ending and impossible mountain to climb. I trust Malwarebytes to handle that for me and keep our users safe."

**Reclaiming valuable bandwidth**
High levels of adware and PUPs generated extra web traffic through plugins and command-and-control scripts. That unwanted traffic wasted valuable bandwidth that the Federation Council must pay for. With more than 100 users on a 9 Mbps ADSL Internet connection, the cost adds up quickly. Malwarebytes removes everything that gets in the way, enabling the Federation Council to reclaim the bandwidth that is crucial to deliver resident, business, and tourism services efficiently.

"Malwarebytes is absolutely doing its job," said Allen. "Malwarebytes is not only protecting us, it's saving management time, freeing bandwidth, and delivering outstanding value."

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.

Copyright © 2018, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.