Case Study

Detect & Response

How Techware stopped a breach in its tracks

Techware

Significant network breaches are becoming more commonplace as malicious threat actors develop increasingly sophisticated attacks. Regardless of size or reputation, it seems no business is immune from malicious activity online.

In this case study, we look at how a simple security check discovered multiple security breaches, and how the team at Techware developed a custom solution to ensure this manufacturing business could stay one step ahead of those who might seek to wreak havoc on their IT systems.

Techware

Learning from the mistakes of others – why prevention isn't enough

After learning about a massive ransomware attack and subsequent data breach within one of Australia's largest logistics companies, the manufacturing business recognised that although data breach prevention methods are essential to staying on top of cyber threats, these methods are not always fool proof.

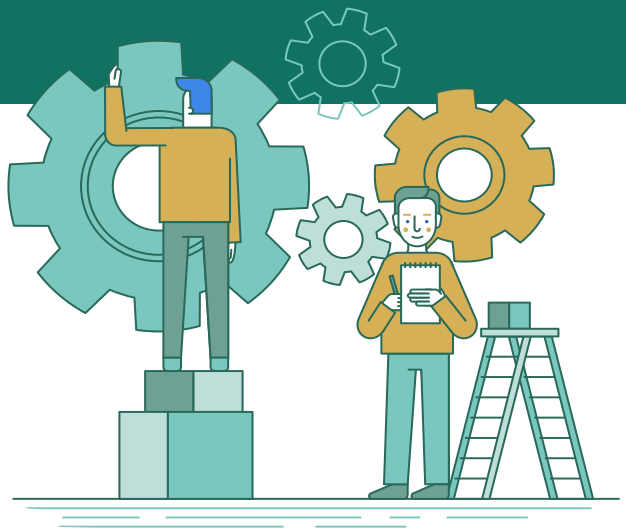
Concerned that their security controls were not up to the task of defending critical infrastructure against advanced malicious threats, the company's Head of IT sought help from a trusted partner and cyber security specialist to assist in implementing and managing a simple system vulnerability check.

Thanks to this proactive approach from the company's key IT figures, Techware were able to identify an existing breach, and so in-lieu of performing a detailed security assessment, moved forward by validating the breach and deploying a comprehensive endpoint detection and response solution.

The aim of this service?

To identify further threats, reduce risks of surface attacks and continue to support their existing working models with confidence in system security.

Being proactive is the first step towards better cyber defence



To deliver a robust and effective detection and response (DR) service, Techware adopted an end-to-end security operations process for finding and managing security threats across the entire lifecycle, using a standard, repeatable and proven DR implementation system characterised by the following:

Detection

Working alongside the customer's internal IT team, Techware implemented a combination of shared system software and a traffic analyser at the network endpoint. This powerful combo kept Techware informed of even the slightest of changes in the customer's regular activity.

The detection and response service eventually unearthed 21 breaches, all of which were progressing at various stages of an attack throughout the customer's system.

These breaches included:

- Intrusion attempts from malicious IP
- Exploit attempts against internal servers
- Malicious DNS requests
- User credentials found for sale on web
- Macro virus detection

Response

For this specific response strategy, the customer wanted immediate remediation for any breaches discovered. To ensure the most thorough response, threat analysis began from day one, continuing daily for 30 days. During this time, Techware verified, validated and remediated each breach instantly. This created a structured cycle of detection, response and monitoring without overwhelming the customer.

A company with a better understanding of its system vulnerabilities

As a result of identifying the 21 breaches, the company now has a clearer understanding of where their vulnerabilities lie and how to stay on top of any weak points in their cyber defence strategies.

With a trusted partner and cyber security specialist, the company can move forward confidently knowing that their critical information assets are now constantly monitored through a dedicated detection and response solution, offering the following benefits:

Peace of Mind

After deploying Techware's detect and response solution, the company has been on the front foot against any potential data breach. With consistent alerts and instant remediation, their network is now fully monitored against further malicious attacks.

Extra support for the team

With the internal IT team so focused on safeguarding their systems through prevention, the chance of an indetected data breach was quite high. The additional support from Techware provided another layer of protection and expertise, opening up time and resources for the internal team to strengthen their overall security posture and close the loop between preventing a breach and detecting a breach that has bypassed the prevention controls.

Stronger compliance with regulatory standards

With their information assets and network now constantly being monitored, this company can confidently meet all industry security standards, keeping their business and customers safe, while avoiding any fines or unwanted recovery expenses.

A boost in productivity

Even the most advanced IT systems can be brought to a halt by unwanted attacks or compromised networks. This company, its employees, and its customers can interact and work productively knowing that their IT environment and cyber security are in good hands thanks to Techware.

Cost management

The financial consequences of a compromised network can be disastrous. Thanks to Techware's managed detection and response solution, the company has been able to reduce risk and better position their company to respond to and recover from any potential losses.

Maintaining trust and reputation

Maintaining a high level of brand trust is crucial. For this business, they had words hard for years to establish a solid reputation wihin the manufacturing industry. By staying one step ahead of malicious threats, the company has ensured it will maintain its own high standards and that of its customers.

Plans for the future

As a number of Australian companies continue to come under scrutiny for their mishandling of significant data breaches, this manufacturing business has decided to do everything in its power to steer clear of similar results.

With an informed and proactive internal IT team now aided by Techware as their security partners, this customer will increase their knowledge and cyber defence through ongoing security training and enhanced IoT security. This ongoing partnership will give both Techware and our client a clearer understanding of what's going on with their systems, internally and externally, offering the chance to apply critical changes to their environment and further optimise our detect and response solution.

With quarterly reviews scheduled for the foreseeable future, the company is now more engaged than ever before. And as Techware continues to learn from past events and workshop new strategies that evolve to meet the customers security needs, the company is more confident than ever in their own network security posture.

Techware

Victoria
2/10 Duerdin St,
Clayton, VIC, 3168
T (03) 8542 7333

New South Wales
Level 49, 10 Darcy Street
Parramatta NSW 2150
T (02) 9816 9828

E sales@techware.com.au | help@techware.com.au
W techware.com.au