Telstra Managed Security Services

Telstra's Managed Security Services represent a leap forward in the way we help businesses navigate security and manage risk across their cyber, electronic & IoT ecosystems.

They are underpinned by a powerful big data security and analytics platform leveraging our Security Operations Centres in the Sydney and Melbourne CBDs – centres that have been purpose-built for our customers to provide the visibility, expertise, intelligence and tools needed to help secure their business in an evolving threat environment.

24/7 security services to assist business and government

In Australia and around the world, there has been a seemingly endless wave of high-profile cyber security incidents which have managed to compromise corporations and government agencies. According to Telstra's 2018 Security Report, 60 per cent of the Australian organisations surveyed faced business interruption due to a security breach at least once over the past year.

The reality is that most businesses find it challenging to implement and maintain the extensive security controls needed to safeguard their systems, customer data and ultimately, their reputation.

Recognising the unique role we can play in security convergence and our history in protecting our own network, Telstra has made two significant announcements that provide 24/7 security services to assist business and government:

- The launch of two customer-dedicated, CBD located, state of the art Telstra Security Operations Centres (TSOCs) built to the ASIO T4 security standard – meaning that they are highly secure facilities, both physically and data-wise.
- The implementation of a big data security and analytics platform which combines event data, analysis and discovery tools with experts across multiple domains. The result is a real-time coordinated security response that helps protect clients against a broad swathe of threats, both cyber and electronic.

Importantly, you don't need to be an existing Telstra customer to use our Managed Security Services.

Telstra's unique way of delivering better security

Our big data security and analytics platform, the backbone of Telstra's suite of managed security services gives clients:

Visibility and insight
The platform examines data 24/7 from a wide range of sources. This can include server logs, storage logs, video logs, branch security logs, IoT logs – even drone logs. Analytics enables this information to be correlated with the latest local and global threat intelligence in the context of your business environment. This allows us to provide an extensive view of vulnerabilities across your IT and digital assets, maintained in an asset database so you're able to gain a better understanding of your risk profile and get the actionable intelligence needed to address it.

Transparency
The security services you subscribe to are completely transparent. Using the Security Monitoring portal allows you to see what our security analysts see.

High performance
It is based on Apache Metron – a big data security and analysis platform – and additional software built by Telstra. Apache Metron runs on the Hortonworks Hadoop stack, which provides the scalability and search capabilities required to support web-scale quantities of security event data.

Affordable
The use of open source eliminates the high cost of proprietary technology. The services are typically more affordable than taking on the cost of an additional security resource.

Accessibility
The Security Operations Centres are based in multiple CBD locations so they are readily accessible, allowing clients to work closely with our experts to tailor their security service.

Collaboration and expertise
A team of skilled security analysts, business analysts and data scientists work with operations people as a single team. Since development teams work hand in hand with operations, we can develop, deploy and validate solutions in one integrated process and can quickly counter threats.

Co-creation
Telstra has a philosophy of co-creation with our customers, allowing for unique requirements to be catered for and developed either in concert with you or on your behalf.

Machine learning and big data
Our advanced security analytics utilises big data tools in conjunction with purpose-built machine learning algorithms to examine anomalies in near real time, while building baseline, trending and outlier analysis. The result is identification of "unknown unknowns" to reduce risk and highlight malicious activity on the client's network.

ASIO T4 security standard
The Security Operations Centres are built to ASIO T4 standards, a requirement in protecting government agency data.

A single focal point
The Security Operations Centres deliver a single focal point for customer engagement. The team you deal with know your environment, your site and your people, the result being a quick, individual response.

Continual improvement
Development of the platform is a live and ongoing project, with new features regularly added to help ensure the services evolve to meet the changing threat landscape. A recent example is the Threat Intelligence dashboard showing the total and new threat indicators per day, the number of threat indicator matches per day, and the number of incidents per day with threat indicator matches – the end result helping you make targeted threat mitigation plans.

Managed locally
Telstra doesn't adopt a 'follow the sun' model – your security is managed 24/7 in Australia using local expertise. As Australia transitions to a knowledge economy, Telstra is investing heavily both in its people and its technology.

Industry recognition

Telstra has made a strong commitment to improving security for organisations, both Australian and internationally.

- In December 2017, Telstra won the Frost and Sullivan Australia Managed Security Services Provider of the Year award.
- Earlier in the year Telstra was awarded AISA's Information Security Project of the Year.

Cyber Security services

The following services are delivered out of Telstra's platform. Flexibility is key and new services are regularly added.
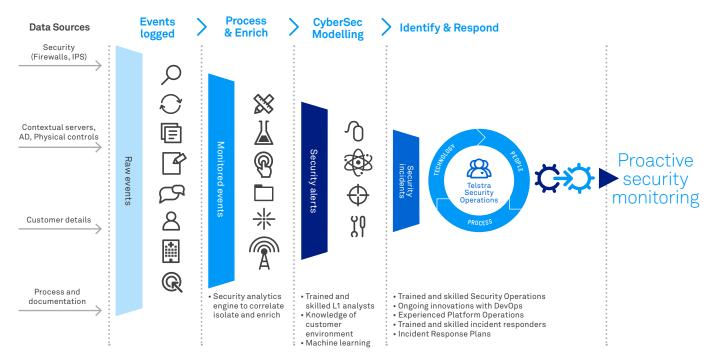
Security Monitoring

Telstra's Security Monitoring service provides visibility through detection and notification of security incidents, allowing the customer to respond in a timely manner to that incident.

It does this by ingesting data from the customer's event log data from multiple data sources – core, contextual and threat indicator feeds. These include, but are not limited to, network (including SD-WAN) and satellite feeds, end points devices, IoT devices and more.

With 24/7 visibility and actionable reports in plain English, clients can gain deeper understanding of their risk status and clearer paths for mitigation.
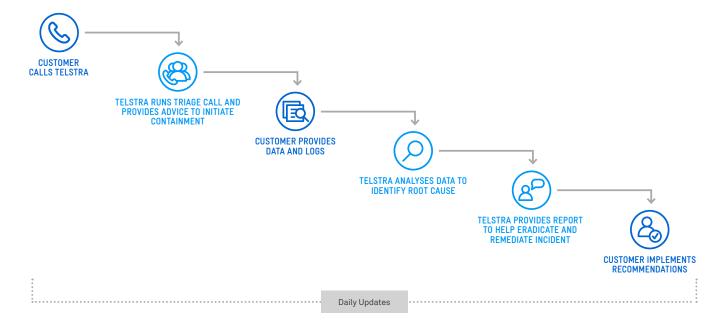
How does it work?

- The Security Monitoring service feeds event data from multiple sources across both your on-premises and cloud infrastructure.
- Telstra stores the log and event data received, performing correlation, enrichment modelling and machine learning to identify anomalies and threats.
- Suspicious incidents and activity are identified and responded to based on the predefined and agreed process with the customer.
- Importantly, this service is open to any organisation regardless of whether they are an existing Telstra customer or not.

Incident Response

Incident Response is a single use product, purchased in advance, to have Telstra on retainer in the event of a major security incident. The Incident Response retainer provides a quick response and expert advice to deal with threats including unauthorised or compromised system access, data loss or theft, intentional or accidental introduction of a virus, unauthorised money transfers and more.

How does it work?

CUSTOMER CALLS TELSTRA

TELSTRA RUNS TRIAGE CALL AND PROVIDES ADVICE TO INITIATE CONTAINMENT

CUSTOMER PROVIDES DATA AND LOGS

TELSTRA ANALYSES DATA TO IDENTIFY ROOT CAUSE

TELSTRA PROVIDES REPORT TO HELP ERADICATE AND REMEDIATE INCIDENT

CUSTOMER IMPLEMENTS RECOMMENDATIONS

Daily Updates

- As soon as you suspect that your business has suffered a cyber-attack, simply pick up the phone and call the dedicated Telstra phone number. Our team of security specialists will usually arrange a triage call within an hour to quickly commence the IR process. They will commence analysis as soon as you provide the required data, then investigate and provide advice to contain the threat.

- If you also have our Security Monitoring service we can respond faster as we'll already have access to your logs and an understanding of your ICT environment. You'll also receive a written report with recommendations to help you put measures in place in an effort to prevent the incident from recurring.

- You will receive daily updates throughout this process.

- If the retainer service is unused, it can be redeemed for five days' worth of Security Consulting and Professional services.

⌂ contact your Telstra account executive

☎ 1300 835 787

🔗 telstra.com/enterprisesecurity