



Optus Managed Threat Monitoring Service

It starts with yes

yes OPTUS

Threats don't sleep – that's why you need 24/7 security monitoring to protect your environment and preserve customer trust

As threats become more automated and industrialised, the ability to identify, alert and respond swiftly has never been more important. Threat monitoring not only protects your assets, but also helps you ensure compliance, maintain business continuity and preserve the trust of your customers.

But many teams are challenged by time, skills shortages, budget and mature security processes – all vital in a fast-changing landscape.

Be confident in your defences with automated, intelligent threat monitoring that protects you around the clock

The Optus Managed Threat Monitoring Service provides a cost-effective and sophisticated solution that works continuously in the background on your behalf, identifying known threats, anomalous behaviour and suspicious activity – and giving you instant visibility into what's happening.

As part of our expert 24x7 managed service, we'll proactively detect and respond to threats in your environment, managing threat data at any scale. Incident, change and escalation notifications are visible via a single pane of glass with Optus Secure Managed Network Services (SMNS). Delivered through our Australia based integrated NOC and SOC analysts, Optus Threat Monitoring Service provides swift service response and recovery.

An Australian-first offering, already proved globally

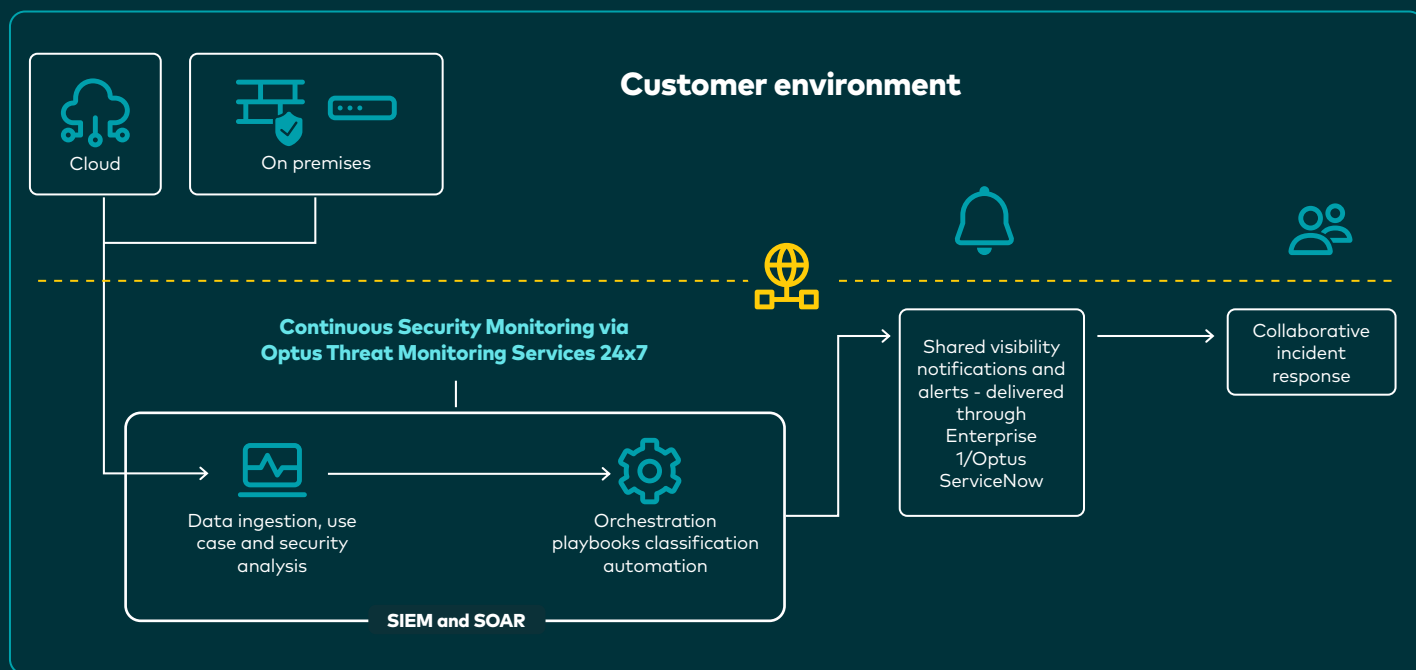
The Optus Managed Threat Monitoring Service collects machine data generated by traditional sources and business applications to enable sophisticated analytics.

It's based on the Devo technology platform, which is rated as 'Visionary' in the Gartner Magic Quadrant and scores highly on a large number of criteria described in the well-regarded GigaOm Radar¹ report.

Built-in applications, dashboards and alerts give you real-time insights into what's happening with your business apps, infrastructure and systems. The platform also provides your security, IT and data professionals with the tools they need to extract valuable and actionable intelligence from petabytes of data.

¹ Source: GigaOm Radar for Autonomous Security Operations Center (SOC)v2.0

How it works



Optus collects the data from your environment – whether in the cloud or on-prem – and analyses it through our Australian-based SIEM and SOAR.

Continuous Security Monitoring via Optus Threat Monitoring Services 24x7: once the data is ingested, threat notifications are delivered to you and our security analysts via email or SMS, based on the threat level SLA.

The Devo platform is visible to you (read only) and our security analysts for detailed information.

Based on whether your assets are managed* or unmanaged#, Optus security analysts will either respond to the threat or advise you on the next steps.

* Managed Assets – these assets are under a valid Optus Managed Service contract and are defined by the customer contract.
#Un-Managed Assets – these assets are not under a managed services contract but Optus Threat Monitoring will receive logs.

The Optus Threat Monitoring service has validated integrations for the following:

- Cisco Meraki
- Cisco ISE (Network Access Control)
- Cisco Firewall
- Cisco Routers
- Cisco SSE – Umbrella
- Palo Alto Firewalls
- Windows AD
- Zscaler SSE ZIA



Key features



24x7 security monitoring



Ability to effectively prioritise and triage security incident alerts



Access to highly trained and certified security specialists



Flexible, cloud-native SaaS Security monitoring platform hosted locally in AWS Sydney



Integrated SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response) & UEBA (User & Entity Behaviour Analytics)



Single pane of glass for incident, change & escalation notifications through our Optus Secure Managed Network Services (SMNS)



Correlation and analysis of logs to create security alerts and incidents



Monthly automated email reports and quarterly meetings



Playbook and use case management



400 days of hot data with the option to add cold storage into a customer-owned S3 bucket



Predefined and customisable* dashboards via the Devo tenant



Enterprise-grade SLAs



Flexible pricing based on ingestion

Need more help?

You can also opt for the services of a dedicated Information Security Manager who'll provide expert advice and help you ensure security governance and compliance.

*This will attract an additional fee.

Key benefits



Australian based security team of experts: The Optus Managed Threat Monitoring Service is delivered through our Australia-based integrated Security Managed Networks Services (SMNS) for swift service response and recovery



Robust network security helps protect your data and network assets from cyber threats, ensuring a secure and reliable network environment



Removes complexity thanks to:

- Optus' mature workflow and processes
- The Devo platform's ability to triage and prioritise alerts and incidents



Excellent value: high scalability, low operating costs, limited data management requirements and minimised infrastructure



Frees your team to focus on core business activities

Want a solution with even more impact?

Talk to us about how Optus can help you with internet carriage, Optus Managed Firewalls, Optus Managed SSE, Optus Managed Meraki, Optus Managed NAC, or Optus Managed Cisco Routers

Find out more

Trusted by many of Australia's largest organisations, Optus is uniquely positioned as a network service provider to help organisations protect themselves from security risks and deliver the level of resilience needed today. Together with exceptional expertise and service, we offer a world-class network and best-in-breed partner solutions.

Interested in Optus Threat Monitoring?

Request a call back at
optus.com.au/enterprise/contact-us

Follow us

