

orro®

SentinelOne®



Managed XDR

(Extended Detection & Response)

Enterprise-level cyber protection for every business



Securely Connected Everything™

Secure together, succeed together

In Australia's fight against cyber threats, we're all in this together. That's why we believe robust cybersecurity should be accessible to all businesses. Orro's Managed XDR service champions this cause, providing end-to-end cyber protection that adapts to your business, whether you're scaling up or dialling down.

Our service is powered by our expertly staffed Security Operations Centre (SOC) and bolstered by SentinelOne's Singularity Data Lake, a sophisticated platform that consolidates data from your endpoints and scoped security controls for AI-assisted monitoring, investigation and response.

Both cost-effective and comprehensive, our Managed XDR service has the added benefit of keeping your data exclusively within the borders of Australia, locked safely in a Sydney-based data centre to uphold data residency. Additionally, the SentinelOne Singularity Platform has been assessed to operate at the 'Protected' level status under IRAP and the Australian ISM.

This innovative alliance means you have a team of security experts that harnesses the most advanced technology in the market to:

- Provide visibility of potential entry points into your environment
- Keep your security posture up to date
- Proactively hunt for hidden threats
- Deliver actionable intelligence as soon as a threat has been detected
- Automate responses to known threat activities
- Maintain your compliance with evolving security standards and regulations
- Offer a unified, panoramic real-time view of your IT environment
- Unravel and investigate threat patterns to pre-empt future attacks
- Get your business back on its feet swiftly after an incident
- Provide one click rollback from adverse attack scenarios
- Provide expert advice around the clock

How XDR addresses critical challenges in cybersecurity

> Escalating threats

- 24x7 continuous monitoring
- Real-time threat detection and investigation
- Adaptive response to new and emerging threats

> Costly data breaches

- Rapid incident response
- Less disruption to operations
- Reduced damage to IT assets and reputation

> Integrated security solutions

- Consolidation of multiple security tools
- Unified data for decisive action
- Coordinated defences across endpoints and Security controls

> Changing regulations

- Compliments the delivery of robust security frameworks
- Ability to manage a diversified workforce
- Covers on-prem, cloud and container workloads

> Skills shortage

- Access to experts around the clock
- Automation of various security tasks
- Redefine cyber budgets

Secure more, save more:

The smart economics of Managed XDR

✔ Save on your security setup

Multiple security capabilities are brought into one place, eliminating your need to invest in additional hardware and software.

✔ Cut recovery time, cut costs

By accelerating threat detection and response, you are minimising the costs associated with downtime, data loss, and system restoration.

✔ Elite expertise, without the expense

Top-tier security experts are brought directly to you, saving you the resources typically required to manage sophisticated security systems.

Key capabilities to keep you protected

Base services: Covering the fundamentals

> Endpoint protection

A sophisticated platform is implemented to ensure comprehensive prevention, detection, and response across your attack surface, from servers, containers and desktops to mobile devices.

> Policy creation & enforcement

Custom security policies are crafted, defining protocols for everyday and emergency scenarios, and are regularly updated to protect against new and emerging threats.

> Threat intelligence

Real-time, AI-enhanced threat intelligence from external and internal data sources allow our SOC experts to pinpoint current and future threats targeting you and speed up investigations.

> 24x7 monitoring & alert triage

SOC experts continuously monitor your IT environment, quickly discerning real threats from false alarms to ensure efforts are focused where needed most.

> Threat containment & removal

During a security breach via our Incident Response capabilities, your compromised systems are isolated to prevent further infiltration, and access obtained as part of the breach is removed.

> Automated response actions

Remediation actions such as network quarantine and password resets can be automated to accelerate incident resolution. These are automated based on agreed response playbooks.

> Rollback capability

SentinelOne offers a one click rollback on Windows devices, allowing your operations to be up and running again. This reduces the impact of ransomware and account misuse.

Forward-thinking businesses see XDR as the path to cyber resilience.

Auxiliary services: Taking your security up a notch

> IR & recovery planning

An Incident Response management plan and response playbooks are created and maintained, encompassing data protection technology, data sharing policies, backups, archiving, restoration, and compliance.

> Threat hunting

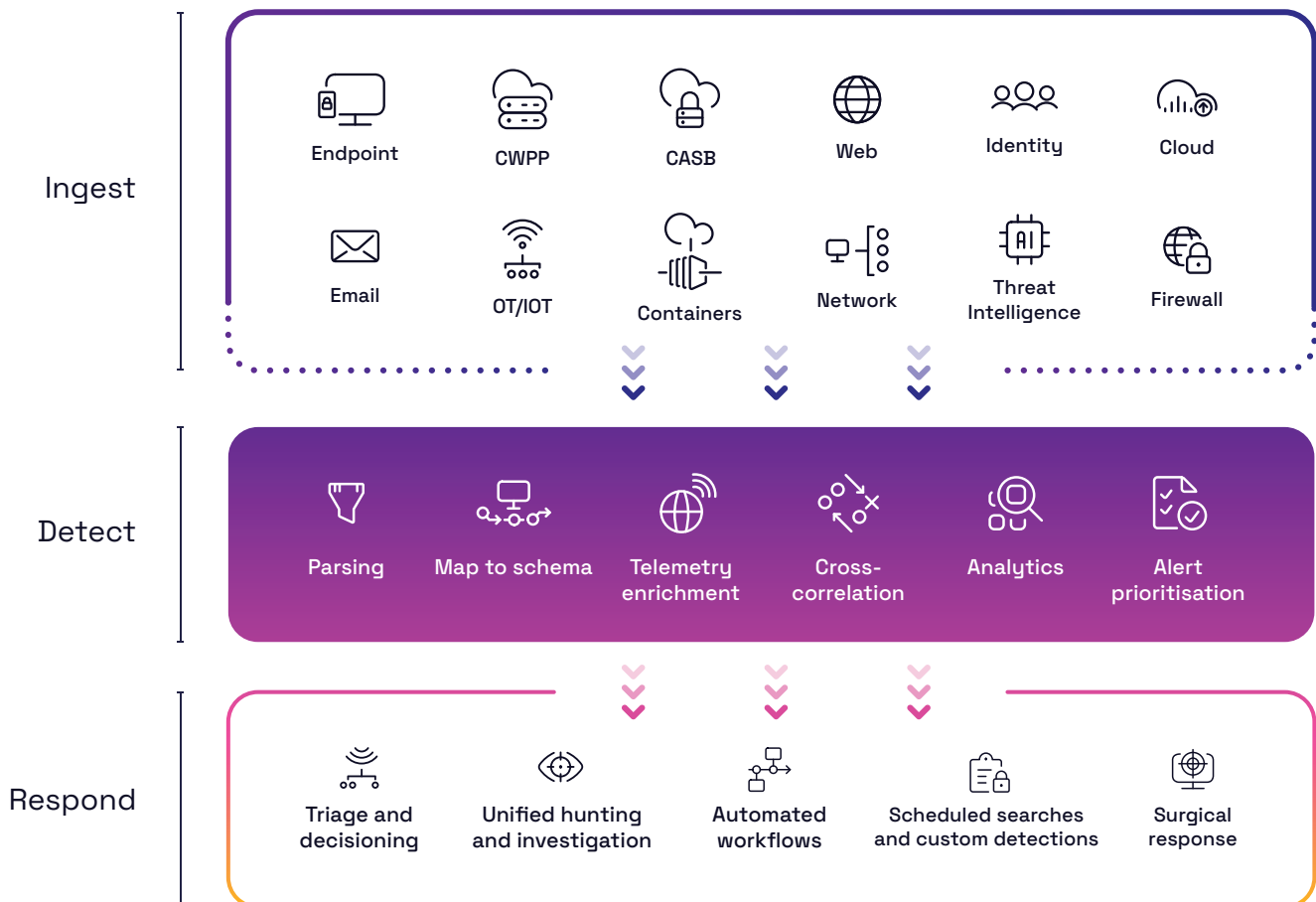
With the addition of SentinelOne Watchtower Threat Intelligence our security experts can pro-actively scour your systems to find and neutralise threats that may have flown under the radar.

> Cybersecurity risk assessment

Experts analyse everything from your network devices and cloud configurations to security policies and practices, then deliver a report with recommendations.

> Incident analysis

Via our Incident Response service, security experts investigate the breach to determine its cause, close the hackers out, and identify any potential data leaks, then deliver findings and remediation recommendations in a report.



The future feels like this.®

We are a multi-disciplinary technology powerhouse, committed to keeping our customers secure and connected. We partner with our customers to boldly embrace the challenges of tomorrow, ignite innovation, and facilitate growth.

> **Trusted Partner**

Our customers don't just trust us to keep them productive and secure today, but to prepare them for what's next, to grow with them over time and to collaboratively shape their future.

> **Strategic Advisor**

With deep expertise in multiple facets of technology, our customers rely on us to provide them with strategic advice and guidance, helping them make smart moves towards a secure future.

> **Solution Provider**

Our versatile suite of skills enables us to tackle complex challenges for our customers, providing them with complete business solutions that draw from our vast pool of expertise and resources.

Stay connected and protected with Orro®.

Discover how we can help your business and your people with Securely Connected Everything™.

Reach out to the team at Orro today.

1300 900 000
sales.enquiries@orro.group

Sydney | Melbourne | Brisbane | Perth | NZ | UK | Philippines