A full-stack observability platform unifying security, performance, costs, and SLAs into real-time actionable insights.

Today's Australian businesses face more than just cybersecurity threats – they're navigating a complex resilience challenge that touches performance, costs, customer experience, and strict regulatory demands.

Enter Haylix OBSERVE | The See Clearly Suite completes and brings together siloed observability tools into a unified, intelligent platform – empowering businesses with a holistic view, smarter automation, and AI-driven transformation that unlocks new efficiencies and insights.

The Australian Signals Directorate (ASD) urges organisations to adopt a "when, not if" mindset for cyber incidents. It's no longer enough to react – you must be prepared. That means proactive response planning, end-to-end visibility, and operational readiness.

Cybersecurity and compliance visibility are essential – but they're just one piece of the puzzle.

To truly lead with confidence, businesses need a holistic view. Haylix OBSERVE brings together every part of your digital and IT landscape into a unified, cloud-powered, always-on platform – delivering real-time, actionable insights that drive smarter decisions.

For executives facing the pressures of governance, resilience, and performance, Haylix OBSERVE is your strategic edge – giving you the clarity, intelligence, and foresight to stay ahead of risks, earn stakeholder trust, and fuel sustainable growth.

HAYLIX OBSERVE

Cyber Security & Compliance
Performance & Availability
User Experience
Commercials
Applications, Databases & Services

HAYLIX
SECURE
AZURE SOC + SIEM

An integrated SOC + SIEM solution combining human expertise and AI-driven tools for end-to-end cyber resilience.

Cyber security is no longer a choice between people or technology — it demands the combined strength of both, working in concert to deliver a resilient and intelligent defence.

The Australian Signals Directorate (ASD) has reaffirmed a stark reality: cyber breaches are no longer a matter of if, but when. In the 2023-24 financial year, over 87,000 cybercrime reports were lodged with the Australian Cyber Security Centre (ACSC), averaging one every six minutes . Despite this persistent threat, many organisations continue to operate in silos—deploying Security Information and Event Management (SIEM) tools without dedicated Security Operations Centre (SOC) oversight, leaving threats unactioned. Conversely, SOC teams lacking integrated SIEM solutions often miss the visibility needed to detect and respond swiftly. This fragmented approach underscores the necessity for cohesive cybersecurity strategies that combine robust monitoring with comprehensive threat detection and response capabilities.

Haylix SECURE | Azure SOC + SIEM unifies both. Our Azure-native solution delivers Microsoft-verified MXDR protection, combining expert-led operations with the AI-powered capabilities of Microsoft Sentinel. Integrated with ASD's Cyber Threat Intelligence Sharing (CTIS) program, we provide enriched, contextual intelligence tuned to Australia's unique threat landscape.

From continuous threat hunting to real-time incident response, our expert team manages the complete detection and response lifecycle — delivering not just strong protection, but executive-level assurance.

With mandatory reporting now required under the new Cyber Security Act, increased penalties under the Privacy Act (up to $50 million), and mounting compliance pressures from APRA and the Essential Eight, Haylix SECURE doesn't just protect your organisation, customers and employees — it builds confidence.

AZURE SOC + SIEM SOLUTION

chorus Microsoft Sentinel

- Fully integrated SOC + SIEM service for end-to-end coverage
- Microsoft-verified MXDR platform with Sentinel and Defender XDR
- Supports new Cyber Security Act reporting, Privacy Act penalties, and governance obligations
- Real-time threat intelligence enriched with local (ASD) and global feeds
- Rapid incident response combining automation and human expertise
- Tailored onboarding, custom rulesets, and security playbook design

HAYLIX
SECURE
SOCaaS

Expert-led 24/7 security operations delivering rapid threat detection, response, and compliance alignment.

Australia's increasingly hostile cyber threat environment puts small and medium-sized enterprises — which make up 97% of all businesses — squarely in the crosshairs. Yet many lack the internal expertise or resources for round-the-clock cyber defence.

According to the Australian Industry Group, a significant majority of organisations continue to rely on external providers to support their security posture. This dependency often lacks continuous oversight, leaving critical vulnerabilities exposed. In the first quarter of 2025, ransomware attacks surged, with reports indicating a record-breaking number of incidents, marking a 45% increase compared to the same period in 2024 . Phishing and insider threats remain persistent risks, underscoring the need for comprehensive cybersecurity strategies.

Haylix SECURE | SOCaaS, powered by Chorus, delivers a fully managed, 24x7x365 Security Operations Centre built on Microsoft Defender XDR and Microsoft Sentinel. Leveraging AI-enhanced analytics and automation, our SOC analysts ensure fast, reliable response — with a mean time to acknowledge (MTTA) under five minutes, and mean time to contain (MTTC) under twenty minutes.

This expert-led, human-in-the-loop model enables precision response that automation alone cannot achieve — helping Australian businesses stay one step ahead of cyber attackers while meeting compliance obligations under the Privacy Act, APRA CPS 234, the Essential Eight, and the 2024 Cyber Security Act.

By adopting Haylix SECURE | SOCaaS, organisations reduce risk exposure, strengthen business continuity, and equip executives to meet rising governance expectations under Australia's evolving regulatory regime.

SOCaaS SOLUTION

chorus

- 24/7/365 expert-led Cyber Security Operations Centre (CSOC)
- Mean Time to Acknowledge (MTTA) under 5 minutes
- Microsoft-verified MXDR service with Defender XDR integration
- Proactive threat hunting and tailored security recommendations
- Automated and analyst-led incident containment
- Supports compliance with Privacy Act, CPS 234, and Essential Eight

Microsoft chorus DICKER DATA

HAYLIX SECURE
AZURE SENTINEL SIEM

Why Microsoft Sentinel Should Be the SIEM of Choice for Australian Businesses.

As the cyber threat landscape intensifies in Australia, organisations must adopt intelligent and compliant security solutions. Microsoft Sentinel, a cloud-native Security Information and Event Management (SIEM) platform, offers a strategic advantage in cyber defence, particularly for Microsoft-centric environments. Key reasons to consider Microsoft Sentinel include:

Integration with the Microsoft Ecosystem: Fully integrated with Microsoft 365, Azure, Defender for Endpoint/XDR, and Entra ID, it reduces complexity, accelerates deployment, and ensures cohesive security coverage. It maximises value from existing investments.

Cloud-Native Architecture & Cost Efficiency: Being fully cloud-native via Microsoft Azure eliminates the infrastructure burden. Elastic scalability accommodates growth without capital expenditure, along with a consumption-based pricing model for transparency and cost control.

Data Residency & Sovereignty Compliance: Hosted within the Microsoft Azure Australia Central and East regions, it supports compliance with the Australian Privacy Principles (APPS) and local data sovereignty mandates. Integration with the Australian Signals Directorate's CTIS enhances the relevance of local threat intelligence.

AI-Powered Threat Detection & Automation: It leverages over 65 trillion daily threat signals from global telemetry, incorporating machine learning and anomaly detection. This reduces Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) by up to 80%.

Robust SOAR Capabilities: Security Orchestration, Automation & Response automates 70-80% of manual security operations tasks with custom playbooks, enabling consistent and rapid incident response, thereby enhancing analyst productivity and reducing lag.

Compliance Alignment with Australian Regulations: It supports compliance with APRA CPS 234, The Essential Eight (ACSC), the Privacy Act 1988 (as amended), and the 2024 Cyber Security Act, enabling consistent governance reporting and incident auditability.

Unified Visibility Across the Hybrid Enterprise: Provides centralised visibility across on-premises, cloud, and multi-cloud infrastructure, making it ideal for remote workforces or hybrid transitions.

Executive-Ready Reporting & Governance Insight: Real-time dashboards provide key metrics, including threat counts, response times, and compliance scores, offering board-level visibility into cyber posture and risk, thereby supporting strategic risk management and governance obligations.

Globally Recognised Platform Backed by Microsoft: Microsoft is recognised as a Leader in Gartner's Magic Quadrant for SIEM (2025). Benefits from ongoing Microsoft R&D, global threat insights, and 24x7 support capability.

Rapid Deployment with Local Expertise: Supported by Australian partners (e.g. Haylix) for managed SOC + SIEM delivery, with a full rollout typically achievable within 30-45 days and ongoing support.

AZURE SIEM SOLUTION

Microsoft Sentinel

METRIC	MICROSOFT SENTINEL	TRADITIONAL SIEMS
Mean Time to Detect	<5 min. (with AI & automation)	30+ min.
Mean Time to Respond	<20 min.	1-2 hrs.
Time to Deploy	30-45 days	90+ days
Cost Structure	Consumption-based	Fixed licensing or infrastructure cost
Compliance Coverage	CPS 234, Privacy Act, Essential Eight, Cyber Security Act	Varies