



Service description document: Cortex Xpanse

Introduction to eir Business

eir Business is a leading provider of advanced network, cloud, and IT managed services, supporting public and private sector organisations across the UK and Ireland for almost 30 years. We design, implement, and manage next-generation solutions that strengthen resilience, enhance security, and enable organisations to work seamlessly and securely from anywhere.

Every engagement starts with listening, understanding your environment, your priorities, and the outcomes you need to achieve. From there, we shape solutions that deliver genuine value, long-term performance, and measurable operational impact.

As a trusted managed service provider, we bring together specialist engineering, proactive service management, and a 24x7 operations capability. Our tightly integrated teams work across the full IT and network landscape, including cloud, cybersecurity, WAN/LAN, connectivity, digital workplace, AI and automation, data centre services, and unified communications.

Our managed services are built on industry best practice and underpinned by ITIL principles, ensuring consistency, accountability, and continual improvement. We combine rigorous processes with real human engagement: our service managers, engineers, and analysts work side-by-side with customers to anticipate needs, resolve issues quickly, and identify opportunities for ongoing optimisation.

Service Introduction

Cortex Xpanse is an External Attack Surface Management (EASM) service that continuously discovers, maps and monitors an organisation's internet-facing assets. The service identifies unknown, unmanaged and forgotten assets across cloud, on-premises and third-party environments, helping organisations understand their true external exposure.

Delivered as a cloud-based service, Cortex Xpanse provides continuous visibility of external risks, prioritises exploitable exposures, and supports remediation workflows to reduce the likelihood of external attack.

eir Business delivers Cortex Xpanse as a managed SaaS capability, enabling customers to gain an attacker's-eye view of their environment and strengthen their external security posture.

Key Service Features

Active Discovery

Continuously identifies internet-facing assets across global infrastructure.

Shadow IT and Cloud Asset Detection

Detects unmanaged and unauthorised cloud and internet-exposed services.

Automated Asset Attribution

Maps assets to business units, applications and ownership context.

Risk-Based Prioritisation

Focuses attention on exposures that present real, exploitable risk.

Zero-Day and CVE Exposure Detection

Identifies vulnerabilities and misconfigurations exposed to the internet.

Supply Chain and Third-Party Risk Monitoring

Tracks exposures introduced by partners, vendors and shared infrastructure.

Active Response and Remediation Support

Validates fixes and confirms risk reduction through follow-up scans.

Mergers and Acquisitions Due Diligence

Rapidly assesses external exposure during M&A and organisational change.

Compliance Monitoring

Supports regulatory and security assurance activities through visibility and evidence.

Agentless Operation

Requires no agents or network changes to begin discovering assets.

Key Service Benefits

Eliminate Shadow IT Risk

Identifies unknown and unmanaged assets before attackers do.

Prevent Zero-Day Exploitation

Highlights exposed vulnerabilities that could be actively targeted.

Prioritise True Risk

Reduces alert noise by focusing on exposures that matter most.

Accelerate Incident Response

Improves mean time to respond by providing clear external context.

Improve M&A Security

Supports faster, safer integration during mergers and acquisitions.

Reduce Compliance Penalties

Improves visibility and control for audit and regulatory purposes.

Secure the Supply Chain

Detects exposure introduced through third parties and dependencies.

Adopt an Attacker's Perspective

Shows what adversaries can see from outside the organisation.

Quantify External Risk

Provides measurable insight into external exposure trends over time.

Zero Deployment Effort

Rapid time to value without agents, sensors or infrastructure changes.

Service Scope*Included*

- SaaS access to the Cortex Xpanse External Attack Surface Management platform
- Continuous discovery and monitoring of internet-facing assets
- Risk scoring and prioritisation of external exposures
- Dashboards, analytics and reporting
- Integration with security and IT workflows (for example Cortex XSOAR, ServiceNow, Splunk)
- Support aligned to the selected support tier

Optional Add-ons

- Professional services for onboarding, tuning and operational integration
- Incident response workflow automation
- Advanced reporting and operational use-case development
- Technical account management services

Not Included

- Internal vulnerability scanning or endpoint protection
- Network connectivity or infrastructure services
- Remediation execution within customer-owned systems
- User training beyond standard documentation unless purchased separately

Onboarding

eir Business supports onboarding using a structured, low-impact approach. Deployment typically involves confirming organisational scope, enabling discovery, validating asset attribution, and integrating with operational workflows. The service is agentless and cloud-based, allowing rapid onboarding with minimal customer-side effort. Documentation, guidance and optional professional services are available to support adoption and operational maturity.

Support

Support is provided through email or online ticketing, with optional phone and web chat support depending on the selected support tier.

Indicative response targets include:

- **Platinum:** S1 <15 minutes, S2 <30 minutes, S3 <2 hours, S4 <4 hours
- **Premium:** S1 <1 hour, S2 <2 hours, S3 <4 hours, S4 <8 hours
- **Standard:** Monday to Friday 7am to 6pm (UK time), aligned to Premium response targets within support hours

Support includes incident handling, fault investigation, service reporting and escalation where required.

Dependencies

- Internet connectivity for access to the SaaS platform
- Customer engagement to confirm asset ownership and business context
- Optional integration with existing security or IT management platforms

Service Constraints

- Asset discovery depends on publicly observable data sources
- Some findings may require customer validation for attribution accuracy
- Planned maintenance windows may apply
- Feature availability may vary by licence tier

10. Pricing

Cortex Xpanse is provided on a subscription basis, priced according to scope and organisational size. Optional professional services and enhanced support are available at additional cost. Full pricing details are provided in the applicable G-Cloud pricing document.

11. Exit and Offboarding

At contract end, access to the service is ceased or transitioned in line with renewal or exit plans. Customers can export reports, logs and asset data in standard formats such as CSV, JSON and PDF. Where required, eir Business can support transition activities as a professional services engagement.

