

Service description document: Managed security services

About eir business

eir Business is a leading provider of secure connectivity, cloud, and managed IT services, supporting public and private sector organisations across the UK and Ireland for almost 30 years. We design, deliver, and manage technology services that underpin critical public services, national infrastructure, and complex enterprise environments.

Our approach is built on understanding the operational realities of the organisations we support. We work closely with customers to align technology services to business outcomes, regulatory obligations, and risk profiles, delivering solutions that are practical, resilient, and sustainable over the long term.

eir Business provides end-to-end capability across network connectivity, cloud platforms, cyber security, digital workplace, data centre services, automation, and service integration. Our services are delivered by experienced engineers, security specialists, and service managers, supported by 24×7 operational centres and structured governance frameworks aligned to ITIL and ISO best practice.

Our role is to give customers confidence that their technology services are secure, available, and professionally managed — enabling them to focus on delivering essential services and organisational objectives.

Introduction to our managed security services

The services described in this document are designed to help organisations prevent, detect, investigate and respond to cyber threats across modern IT environments, including endpoints, identities, cloud workloads, SaaS applications, data, and extended connected devices.

Each service can be purchased individually or combined to create a layered security capability aligned to organisational risk, maturity, and operational requirements. The services are delivered using cloud-native security platforms and advanced analytics to provide continuous visibility, prioritised risk insight, and rapid response without the need for customers to manage complex security infrastructure. The services focus on security outcomes such as endpoint protection, identity security, cloud security, exposure management, threat intelligence, managed detection and response, and security operations enablement. While the services operate on a common underlying technology foundation, the platform itself is not sold as a standalone service; customers can procure only the specific security services they require.

All services are provided under subscription-based commercial models and are supported by defined service levels, availability targets, and escalation processes. Platform availability and core service level commitments are governed by the underlying technology providers, with eir Business acting as the primary commercial and service interface for customers, coordinating onboarding, support, escalation, and ongoing service management.

1. AI-Enabled SOC Analyst Service

Service overview

This service provides an AI-enabled Security Operations Centre (SOC) analyst capability designed to accelerate threat detection, investigation, and response across complex digital environments.

The service uses advanced analytics and generative AI to assist security teams by analysing security telemetry, surfacing high-risk activity, summarising incidents, and supporting investigation workflows through natural-language interaction. It integrates across endpoint, identity, cloud workload, and vulnerability data sources to provide unified visibility and prioritised security insights.

The service is intended to augment internal security teams, improving response speed, consistency, and operational efficiency without replacing human decision-making. Analysts remain in control of all response actions.

Service levels and support

The service is delivered as a cloud-based, highly available security platform with an availability target of 99.9% monthly uptime, calculated on a calendar-month basis. Availability is measured excluding scheduled maintenance and defined exclusions such as customer-side connectivity failures.

Support is provided via online ticketing and phone channels, with defined severity-based response targets. Critical security incidents are prioritised for rapid triage and investigation, supported by automated workflows and predefined response playbooks.

Incident escalation follows structured procedures, with access to advanced security specialists where required. Service level commitments, including uptime targets and service credits, are defined by the underlying technology provider, with credits applied in line with documented service level agreements.

Commercial model

The service is purchased as a subscription-based cloud security service, typically licensed on an annual term. Licensing is structured around the scope and scale of protected assets or data sources, with minimum commitment levels applicable.

Optional components may be added to extend functionality, integrate additional data sources, or enhance automation and response capabilities. Professional services, onboarding support, and advanced assistance are available separately where required.

Commercial terms, licensing units, minimum quantities, renewal options, and contract duration are defined at call-off.

2. Cloud Security (Unified Cloud Security Platform)

Service overview

This service provides a unified cloud security capability designed to protect public, private and hybrid cloud environments across infrastructure, workloads, applications, data and identities.

The service delivers continuous visibility of cloud assets, configurations and runtime activity, enabling organisations to identify misconfigurations, vulnerabilities and active threats across their entire cloud estate. Security controls are applied consistently across environments, helping organisations reduce risk, prioritise remediation and respond rapidly to incidents. The service supports both proactive cloud security posture management and real-time cloud detection and response, allowing organisations to improve security maturity while maintaining operational agility in dynamic cloud environments.

Service levels and support

The underlying cloud security platform is delivered with a service availability target of 99.9% monthly uptime, measured across the service management plane and core security functions. Support services are provided in defined tiers, typically including:

- 24×7 access to technical support via portal and phone
- Severity-based response targets for incidents
- Escalation to senior engineering teams for critical issues
- Access to security advisories and service status notifications

Service level commitments for platform availability and core service performance are defined by the technology provider. Where the service is delivered through a managed or reseller model, customer support, escalation and coordination are provided by the supplier, with vendor SLAs flowing through to the customer contract.

Commercial model

The service is purchased as a subscription-based cloud service.

Licensing is typically based on cloud resource consumption, such as the number of cloud accounts, workloads, hosts, containers or services monitored and protected. Licences are provided on a per-term basis, with standard contract terms of one, two or three years.

Optional service components may include:

- Enhanced detection and response capabilities
- Managed threat hunting or monitoring services
- Advanced analytics and reporting modules
- Integration with third-party security and IT service management platforms

Professional services, onboarding assistance and optimisation support can be purchased separately where required.

3. Data Protection Service

Service overview

This service provides cloud-delivered data protection capabilities designed to prevent unauthorised access, movement, and exfiltration of sensitive information across endpoints, users, and data flows. It delivers real-time visibility of data in use, in motion, and at rest, enabling organisations to detect, monitor, and prevent data loss events without relying on complex, agent-heavy architectures.

The service uses contextual analysis to understand how sensitive data is created, accessed, transformed, and transferred, allowing accurate enforcement of policies while minimising false positives and user disruption. It supports modern working practices, including cloud services, remote users, and emerging productivity tools, while maintaining compliance and data governance requirements

Service levels and support

The service is delivered as a resilient, cloud-hosted platform with a target availability of 99.9% or higher, calculated on a monthly basis. Availability excludes scheduled maintenance and events outside the provider's reasonable control.

Support is provided through tiered service levels, offering 24x7 incident handling for critical issues and defined response targets aligned to incident severity. Escalation paths are clearly defined, with access to senior engineering resources for high-impact events.

Platform-level SLAs, including uptime commitments and service credits, are provided by the underlying technology provider. Operational support, escalation management, and customer engagement are delivered by the reseller, ensuring a single commercial and support interface for buyers

Commercial model

The service is purchased as a subscription-based cloud service, licensed annually or on a multi-year term. Licensing is typically based on measurable units such as protected endpoints, users, or data scope, depending on deployment requirements.

Minimum subscription thresholds may apply to ensure effective service delivery. Optional components can be added to extend coverage, enable advanced policy controls, or integrate with broader security operations capabilities.

The subscription includes access to the core platform, standard updates, and baseline support. Professional services, onboarding assistance, advanced support tiers, and integration services are available as optional add-ons.

4. Endpoint Detection and Protection Service

Service overview

This service provides cloud-delivered endpoint protection, detection and response across user devices and servers. It uses a lightweight endpoint sensor combined with a centralised security platform to continuously monitor activity, identify malicious behaviour, and support rapid investigation and response to cyber threats.

The service protects against malware, ransomware, fileless attacks, credential misuse and adversary behaviour by analysing endpoint activity in real time and correlating it with threat intelligence. It supports both prevention and post-incident investigation, enabling organisations to reduce dwell time, contain incidents quickly, and maintain operational resilience across their endpoint estate.

Service levels and support

The underlying cloud platform is designed for high availability using a multi-region, resilient architecture. The service targets 99.9% or higher monthly availability, excluding planned maintenance and customer-side connectivity issues.

Support is provided on a 24x7 basis for critical security incidents, with severity-based response targets. Standard support includes access to an online support portal and incident management workflow. Enhanced support options may be available, including faster response targets and named technical resources.

Security incidents are prioritised by severity. Escalation paths are defined for high-impact events to ensure timely investigation and containment. Platform-level SLAs are provided by the technology provider, with reseller support wrapping commercial engagement, coordination, and customer communication.

Commercial model

The service is purchased as a subscription-based cloud service, licensed per protected endpoint. An endpoint typically represents a workstation, laptop, virtual machine, or server instance.

Licensing is calculated based on the number of endpoints onboarded to the platform. Different endpoint types (for example user devices versus servers) may be licensed separately depending on scope and use case.

Optional add-on capabilities may be available, including advanced threat hunting, extended detection and response, or managed security services. These are procured separately and layered onto the core endpoint protection service.

Professional services are purchased separately and delivered on a call-off or day-rate basis.

The service can be contracted on a 12, 24 or 36-month subscription term, aligned to public sector procurement requirements. Renewal, expansion, or reduction of scope is managed through the Call-Off Contract.

5. Exposure Management Service

Service overview

The Exposure Management service provides continuous visibility and prioritisation of an organisation's internal and external cyber exposure. It identifies known and unknown assets, assesses vulnerabilities and misconfigurations, and correlates these with real-world threat intelligence to highlight the exposures most likely to be exploited.

The service enables security teams to move beyond periodic vulnerability scanning by maintaining an always-current view of attack surface risk across endpoints, cloud workloads, identities, and internet-facing assets. This allows organisations to focus remediation efforts on the small number of exposures that present genuine business risk, rather than managing large volumes of low-value findings.

The Exposure Management service includes:

- Continuous discovery of internal and external assets, including unmanaged and unknown resources
- Identification of vulnerabilities, misconfigurations, and exposed services
- Correlation of exposure data with active threat intelligence and adversary behaviour
- Risk-based prioritisation to highlight exposures most likely to be exploited
- Consolidated visibility across endpoint, cloud, identity, and third-party assets
- Dashboards and reporting to support remediation planning and risk governance
- Integration with security operations, incident response, and IT service management workflows

The service is delivered as a cloud-hosted security capability and does not require disruptive network scanning or manual asset inventories.

Service levels and support

The Exposure Management service is supported through tiered support options aligned to incident severity.

Support includes:

- Access to a service desk via ticketing portal and phone
- Incident logging, triage, investigation, and escalation
- Platform availability monitoring and operational support
- Incident communications and service reporting

The underlying platform is designed for high availability, with a monthly uptime target of 99.9% or higher, excluding planned maintenance.

Response times are based on incident priority, for example:

- **Critical incidents**: rapid response, typically within minutes
- **High priority incidents**: response within one hour
- **Medium priority incidents**: response within standard business hours
- **Low priority incidents**: response aligned to agreed service windows

Escalation paths and service credits are governed by the underlying platform service level agreement, with reseller-provided support managing customer engagement and coordination.

Commercial model

The Exposure Management service is purchased as a subscription-based cloud security service.

Licensing model

- Licences are typically based on measurable units such as assets, endpoints, identities, or cloud resources under management
- Subscriptions are purchased for a defined contract term, usually annual or multi-year
- Minimum licence quantities may apply depending on deployment size

What is included

- Access to the Exposure Management platform
- Continuous exposure discovery and risk prioritisation
- Standard platform updates and enhancements
- Access to standard support services

Optional components

- Enhanced support tiers with faster response times
- Professional services for onboarding, configuration, or optimisation
- Integration support with third-party security or IT management tools

6. Identity Security Service

Service overview

The Identity Security service provides continuous protection against identity-based threats across hybrid identity environments. It focuses on detecting, preventing, and responding to attacks that exploit user identities, credentials, privileges, and authentication pathways rather than traditional malware-based techniques.

The service delivers visibility across on-premises directory services, cloud identity providers, and connected SaaS applications, identifying misconfigurations, excessive privileges, and risky authentication behaviours. Advanced analytics and behavioural baselining are used to detect anomalous activity such as credential misuse, lateral movement, and privilege escalation in near real time. Identity Security is designed to integrate with endpoint and workload security controls to provide a unified view of identity-driven attack paths, enabling faster investigation and response. The service supports risk-based enforcement, including conditional access and adaptive authentication controls, to prevent unauthorised access while minimising disruption to legitimate users.

Service levels and support

The underlying platform is delivered as a highly available, cloud-based service with resilience designed into the core architecture. Availability targets are defined by the technology provider and are typically aligned to enterprise-grade SaaS service levels.

Support is provided through a combination of platform support and reseller-led service management:

- Availability targets are governed by the platform service level agreement.
- Incident response and fault resolution follow defined severity-based response times.
- Escalation paths are available for critical incidents impacting service availability or security posture.
- Service credits, where applicable, are defined at the platform level and flow through the reseller in line with contractual terms.

The reseller acts as the primary commercial and service interface for the buyer, coordinating support requests, escalation, and vendor engagement as required. Optional enhanced support tiers and managed services may be available under separate agreement.

Commercial model

The Identity Security service is purchased as a subscription-based service, licensed annually or multi-year depending on buyer requirements.

Licensing is typically based on measurable identity-related units, such as:

- Number of protected identities or directory objects
- Connected identity providers or environments
- Enabled security capabilities or modules

The service may be purchased as:

- A standalone identity security capability, or
- An add-on integrated with wider security and monitoring services

Minimum subscription terms and unit thresholds may apply depending on the scope of deployment. Optional components, such as advanced analytics, extended identity coverage, or enhanced response capabilities, can be added to tailor the service to organisational needs.

7. IT Automation and Operations Orchestration Service

Service overview

This service provides cloud-delivered IT automation and operations orchestration capabilities designed to give organisations real-time visibility of their IT estate and the ability to automate operational and security response actions at scale.

The service enables IT and security teams to maintain a continuously updated inventory of endpoints, workloads and systems, enrich incidents with deep asset context, and execute automated workflows for remediation, configuration changes and operational tasks. It is delivered as a software-as-a-service (SaaS) platform and integrates with existing IT service management (ITSM), security operations and workflow tools.

The service is typically used to improve asset visibility, reduce manual operational effort, accelerate incident response, and support IT and security convergence through a single operational control plane.

Service levels and support

The service is delivered via a globally distributed, cloud-native platform designed for high availability and resilience. The underlying platform operates across multiple geographically separate data centres with redundancy, failover and continuous replication.

The service targets **99.9% or higher monthly availability**, excluding planned maintenance and events outside the provider's reasonable control. Availability commitments and service credits are governed by the underlying vendor service level agreement (SLA).

Support is provided on a tiered basis, with response times aligned to incident severity. Support services are available via an online support portal and, where applicable, telephone support.

Typical response targets include:

- **Critical incidents:** response within minutes to one hour
- **High severity incidents:** response within one to two hours
- **Medium severity incidents:** response within several hours
- **Low severity incidents:** response within standard business hours

Escalation paths, incident management processes and service restoration procedures are defined within the vendor SLA and support policy. Optional enhanced support levels may include faster response times, named support contacts or service delivery management.

eir Business provides first-line service coordination, contract management and escalation to the underlying software vendor where required.

Commercial model

The service is purchased on a subscription licensing model and delivered as a managed SaaS platform. Licensing is typically based on measurable units such as:

- Number of protected endpoints or systems
- Number of monitored assets or workloads
- Enabled automation or orchestration modules

Subscriptions are usually contracted on annual or multi-year terms, with the option to scale licence quantities up or down at renewal or during the contract term, subject to minimum commitments. The base subscription typically includes:

- Access to the core IT automation and asset visibility platform
- Use of automation workflows and operational response actions
- Standard support and access to documentation and updates

Optional additions include:

- Enhanced or premium support tiers
- Advanced automation modules or integrations
- Professional services for onboarding, configuration, integration or optimisation

Professional services are purchased separately and delivered on a call-off or day-rate basis.

8. Managed Detection and Response (MDR) Service

Service overview

This service provides fully managed, 24x7 detection, investigation and response across endpoint, identity, cloud workload and third-party telemetry sources. It combines continuous monitoring, advanced threat intelligence, proactive threat hunting and hands-on incident response to rapidly detect and contain security threats. The service operates as an extension of the customer's security team, delivering end-to-end incident management from initial alert through to remediation and recovery.

Service levels and support

The service is delivered on a 24x7 basis by a dedicated security operations team. Pre-defined response playbooks are used for common threat scenarios including malware, ransomware, credential compromise and lateral movement. Availability targets are aligned to a cloud-native, globally distributed security platform with a target availability of 99.9% or higher.

Support response times are severity-based:

- **Critical incidents:** response within minutes
- **High severity incidents:** response within tens of minutes
- **Medium severity incidents:** response within hours
- **Low severity incidents:** response within agreed business hours

Escalation is handled through defined incident workflows, with customers receiving incident notifications, investigation summaries and post-incident reports. Platform availability SLAs are provided by the underlying software provider, while service delivery SLAs and response commitments are managed by the reseller as part of the managed service.

Commercial model

The service is purchased as a subscription-based managed security service, typically aligned to a fixed contract term. Licensing is consumption-based and commonly measured per protected asset (such as endpoint, identity or workload), with minimum quantities applying depending on scope.

The service includes core managed detection and response capabilities as standard, with optional components available to extend coverage (for example identity protection, cloud workload protection, device control or third-party data ingestion). Professional services such as onboarding, integration and configuration are typically included or offered as optional add-ons depending on customer requirements.

Commercially, the service is provided under a reseller-managed contract, with licensing and platform access supplied by the technology vendor and wrapped with managed service delivery, support and governance by the reseller.

9. Next-Generation SIEM (Cloud-Delivered)

Service overview

This service provides a cloud-delivered, next-generation Security Information and Event Management (SIEM) capability designed for modern security operations. It ingests, correlates and analyses large volumes of security telemetry from across endpoints, cloud workloads, identities, applications and third-party sources to detect, investigate and respond to security incidents at speed.

The service replaces traditional, infrastructure-heavy SIEM tools with a scalable, AI-assisted platform that enables near real-time threat detection, rapid investigation and automated response through a single, unified interface.

The service is suitable for organisations seeking to modernise their Security Operations Centre (SOC), improve detection accuracy, reduce incident response times, and gain full visibility across their security data without managing on-premise SIEM infrastructure.

Service levels and support

The underlying platform is designed as a cloud-native, multi-region service with built-in redundancy, fault tolerance and automatic failover. Availability is measured on a monthly basis and targets 99.9% uptime, excluding agreed maintenance windows and defined service exclusions.

The service provider publishes a live service status dashboard and provides automated outage notifications via the management portal and email alerts. Regional availability and operational status information is available at all times to customers.

Support is delivered through a combination of the platform provider's global support capability and the reseller's managed support services. Support includes incident logging, investigation, escalation and resolution.

Support is available 24×7×365, with response targets aligned to incident severity:

- **Critical incidents** – rapid initial response and continuous engagement until service restoration
- **High and medium incidents** – prioritised investigation and resolution
- **Low-priority requests** – handled through standard service queues

Escalation paths are clearly defined, and service credits may apply where availability commitments are not met, in line with the platform Service Level Agreement. Professional services and managed SOC services are not included unless explicitly purchased.

Commercial model

The service is purchased as a subscription-based, cloud-delivered service. Licensing is typically based on one or more of the following units, depending on deployment scope:

- Volume of data ingested or retained
- Number of protected assets, users or workloads
- Enabled functional modules or capabilities

Licences are purchased for a fixed contract term (for example, 12, 24 or 36 months). The subscription includes access to the SIEM platform, core analytics, detection logic and platform updates.

Customers may optionally purchase:

- Extended data retention periods
- Advanced analytics or automation capabilities
- Integrations with additional third-party data sources
- Professional services for onboarding, tuning or migration
- Managed detection and response or SOC augmentation services

10. SaaS Security Posture Management Service

Service introduction

This service provides continuous security posture management for Software-as-a-Service (SaaS) applications used across an organisation. It enables public sector organisations to gain visibility of their SaaS estate, identify security misconfigurations, excessive permissions, data exposure risks, and identity-based threats, and prioritise remediation actions based on risk.

The service continuously monitors SaaS applications for configuration drift, insecure access settings, unmanaged integrations, and risky user behaviour. It is designed to support organisations operating large and diverse SaaS environments, helping security and IT teams maintain control as SaaS usage grows. The service is delivered as a cloud-hosted security platform and integrates with common enterprise SaaS applications to provide a unified view of SaaS risk and security posture. The service includes:

- Continuous discovery of SaaS applications and connected services
- Monitoring of SaaS security configurations and permissions
- Identification of excessive privileges and risky identities
- Detection of publicly shared or exposed SaaS data
- Risk-based prioritisation of findings
- Guided remediation workflows and recommended actions
- Compliance mapping against recognised security frameworks
- Centralised dashboards and reporting

Service levels and support

The SaaS platform is operated on a highly resilient, cloud-native architecture designed for continuous availability. The underlying vendor platform targets 99.9% or higher monthly service availability, measured on a monthly basis, excluding scheduled maintenance and agreed exclusions.

Support is provided through tiered service levels, which may include:

- 24×7×365 access to technical support
- Incident logging via secure support portals
- Defined response targets based on incident severity
- Escalation to senior engineers and security specialists for critical incidents

Availability commitments and service credits, where applicable, are defined within the underlying vendor Service Level Agreement. Service credits relate to the SaaS platform only and exclude optional professional or managed services.

eir Business provides service management, customer coordination, and escalation management, acting as the primary point of contact for customers.

Commercial model

This service is purchased as a subscription-based SaaS security service.

The commercial model typically includes:

- Subscription licensing based on the number of SaaS applications, users, or monitored identities
- Annual or multi-year subscription terms
- Optional add-on modules for advanced capabilities
- Optional professional services for onboarding, integration, and optimisation

Licensing is scalable, allowing organisations to start with a subset of SaaS applications and expand coverage over time. Minimum subscription commitments may apply depending on the service configuration selected.

Professional services, onboarding support, and advisory services are available as optional additions and are purchased separately from the core subscription.

11. Threat Intelligence and Proactive Threat Hunting Service

Service overview

This service provides continuous threat intelligence and proactive threat hunting to help organisations identify, understand, and respond to cyber threats targeting their environments. It delivers insight into adversary behaviour, emerging attack techniques, and active campaigns, enabling security teams to anticipate attacks rather than react after compromise.

The service combines global threat intelligence, adversary tracking, and human-led threat hunting to identify malicious activity across endpoints, identities, cloud workloads, and external infrastructure. It supports security teams by enriching alerts, prioritising real risk, and providing context-driven intelligence to inform response and remediation decisions.

The service is suitable for public sector organisations seeking enhanced visibility of external threats, advanced detection of stealthy adversaries, and intelligence-led security operations.

Service levels and support

The service is delivered as a cloud-based subscription with defined support tiers aligned to operational criticality.

Availability targets are aligned to a 99.9% monthly service availability objective, excluding planned maintenance and defined service exclusions.

Support is provided through tiered service levels, which may include:

- **Standard / Express support** for organisations with lower operational complexity
- **Enhanced or Essential support** for larger or higher-risk environments
- **Elite support** for organisations requiring advanced assistance and strategic engagement

Support services include access to technical support engineers, threat intelligence specialists, and escalation paths for high-severity incidents. Higher support tiers include faster response times and may include access to a named technical account manager.

Incident response, service availability, and support commitments are governed by the underlying software service level agreement. Where applicable, service credits may apply if availability targets are not met, in line with the vendor SLA.

eir Business acts as the primary service interface for customers, managing escalation, coordination, and ongoing service engagement.

Commercial model

The service is purchased as a subscription-based cloud service and is typically licensed on a per-endpoint basis. Licensing units represent protected assets within the customer environment and scale according to organisational size and coverage requirements.

Subscription terms are normally multi-year, with standard minimum commitment thresholds. Volume-based scaling is supported, allowing organisations to increase coverage as requirements evolve.

Optional service components may include:

- Advanced threat intelligence modules
- Proactive threat hunting capabilities
- Intelligence-led investigations and reporting
- Enhanced support or premium service tiers

Support services are charged as a percentage of the annual subscription value, with minimum commitments applicable at higher service tiers. Premium support options may include strategic advisory services and dedicated technical resources.

All commercial terms, licensing structures, support entitlements, and service commitments are defined contractually at the point of purchase.

12. XIoT Security Service

Service overview

The XIoT Security Service provides visibility, threat detection, and response capabilities for extended Internet of Things (XIoT) environments, including IoT, OT, IoMT, and industrial control system (ICS) assets. The service is designed to identify, monitor, and protect connected devices that traditionally sit outside standard IT security controls and are often difficult or impossible to patch.

The service enables organisations to discover managed and unmanaged XIoT assets, understand their exposure and risk, and detect malicious activity targeting operational and cyber-physical environments. It supports environments where availability, safety, and continuity of operations are critical, such as healthcare, utilities, manufacturing, and critical national infrastructure.

The service operates using cloud-based analytics and lightweight data collection methods to minimise operational disruption while providing near-real-time visibility and protection across converged IT and OT environments.

Service levels and support

The underlying platform supporting the XIoT Security Service is delivered as a cloud service and is designed for high availability and resilience. Platform availability targets are defined in the vendor service level agreement, with a typical monthly availability target of 99.9% or higher, excluding planned maintenance and agreed exclusions.

Service availability is monitored continuously, and platform status is made available via an online status portal. Where applicable, service credits for availability breaches are governed by the vendor SLA and flow through the reseller in accordance with the call-off contract.

The service includes access to technical support aligned to defined support tiers. Support is provided via online ticketing and, where applicable, telephone support.

Typical support response targets are aligned to incident severity, for example:

- **Critical incidents (service unavailable or active threat):** initial response within minutes
- **High severity incidents:** response within hours
- **Medium and low severity incidents:** response within standard business or extended support hours, depending on support tier

Escalation paths are defined within the support framework, with access to senior engineering and threat specialists for complex or high-impact incidents.

Security incidents affecting XIoT assets are triaged and investigated using enriched telemetry, threat intelligence, and asset context. Where response actions are supported, containment and

mitigation actions may be executed in a controlled manner to minimise operational impact.

Service level commitments related to response times, escalation, and incident handling are governed by the vendor SLA, with the reseller responsible for contract management, service coordination, and customer communication.

Commercial model

The XIoT Security Service is delivered on a subscription basis. Subscriptions are typically aligned to a defined contract term (for example, one, three, or five years) and are renewable at the end of the agreed term.

The service is purchased through the reseller under the applicable framework call-off contract. The reseller acts as the contracting party, providing commercial management, invoicing, and first-line service coordination.

Licensing is typically based on measurable units relevant to XIoT environments, such as:

- Number of XIoT assets or devices monitored
- Asset classes or environment scope (e.g. IoT, OT, IoMT)
- Enabled capabilities (e.g. asset discovery, threat detection, response functionality)

Minimum licensing thresholds may apply depending on deployment size and service scope. Licensing units are defined at contract award and documented in the order form or service schedule.

Optional components may be added to enhance the core service, including:

- Advanced threat detection and response capabilities for XIoT assets
- Integration with third-party OT security, monitoring, or asset management platforms
- Automation and orchestration features to support response workflows
- Professional services for onboarding, configuration, or operational integration

Optional components are purchased as part of the subscription or as separately scoped additions, subject to contract terms.

The service is contracted for a fixed term, with options to scale asset coverage up or down in line with contractual provisions. Changes to scope, licensing units, or enabled capabilities are managed through formal contract variation.


business
secure, managed solutions for all.