



Service description document: Cortex XDR – Extended Detection and Response Platform

Cortex XDR – Extended Detection and Response Platform

Service overview

Cortex XDR is a cloud-delivered extended detection and response platform designed to prevent, detect, investigate, and respond to advanced cyber threats across endpoint, network, identity, and cloud environments.

The service unifies telemetry from multiple security sources into a single platform, using artificial intelligence and machine learning to identify malicious activity, reveal root cause, and automate response actions.

What the service provides

Cortex XDR provides a unified security analytics and response service that correlates endpoint, network, cloud, and identity data to detect sophisticated attacks that would otherwise evade siloed security tools.

The service enables security teams to:

- Prevent malware, exploits, and ransomware before execution
- Detect advanced threats using behavioural analytics
- Investigate incidents through automated root cause analysis
- Respond quickly using real-time containment and remediation actions
- Reduce alert fatigue by consolidating and prioritising signals

Cortex XDR is delivered as a fully managed Software-as-a-Service platform, eliminating the need for on-premise infrastructure.

Service features

Key technical features include:

- AI-driven analytics and threat detection
- Unified incident and alert engine
- Automated root cause analysis
- Identity Threat Detection and Response (ITDR)
- Multi-layer endpoint prevention
- Live terminal for real-time response
- Proactive threat hunting capabilities
- Managed threat hunting supported by Unit 42
- Network Traffic Analysis (NTA)
- Host Insights for vulnerability visibility

Service benefits

Cortex XDR enables organisations to:

- Dramatically reduce alert fatigue
- Lower mean time to resolution (MTTR)
- Improve prevention effectiveness against modern attacks
- Eliminate security blind spots across environments
- Reduce operational and tooling overhead
- Secure unmanaged and IoT devices
- Protect against credential theft and identity-based attacks
- Perform targeted response without business disruption

- Scale detection and response across hybrid estates
- Access expert threat intelligence and support

Service scope and dependencies

Cortex XDR is delivered as a public cloud Infrastructure Software as a Service (iSaaS) offering.

The service can operate as a standalone detection and response platform or integrate with other security services. It extends and enriches data from firewalls, secure access services, cloud workloads, and identity platforms, and integrates natively with orchestration platforms for automated response.

Deployment requires compatible endpoint agents and internet connectivity to enable telemetry ingestion and response actions.

Customisation and configuration

Cortex XDR can be configured to align with organisational security requirements. Customers can:

- Configure detection rules and policies
- Customise dashboards and reports
- Define automated response actions
- Manage access using role-based permissions
- Integrate additional data sources via APIs

Configuration is performed through a browser-based management console, with controls governed by assigned administrative roles.

Access and user experience

The service is accessed through a secure, browser-based interface designed for security operations teams. The interface consolidates alerts, investigations, and response actions into a single operational view.

Mobile access supports monitoring and response actions such as alert acknowledgement and host isolation. More complex investigation and configuration tasks are optimised for desktop use.

Accessibility is aligned with WCAG 2.1 Level AA, including keyboard navigation, screen-reader support, and appropriate colour contrast for security alerts and dashboards.

Support and service management

Vendor-backed support is available via online ticketing, phone, and web chat, depending on the selected support tier.

Support response targets include:

- **Platinum:**
 - Critical: under 15 minutes
 - High: under 30 minutes
 - Medium: under 2 hours
 - Low: under 4 hours

- **Premium:**
 - Critical: under 1 hour
 - High: under 2 hours
 - Medium: under 4 hours
 - Low: under 8 hours
- **Standard:**
 - Monday to Friday, 7am–6pm UK time, with response targets aligned to Premium during service hours

Technical account management and professional services are available as optional additions.

Availability and service levels

Cortex XDR is covered by a vendor Service Level Agreement that commits to 99.9% Monthly Uptime Availability.

Availability is calculated based on total minutes in a calendar month, excluding scheduled maintenance, emergency maintenance, scaling or high-availability events, customer environment issues, force majeure events, insufficient licensed capacity, beta or preview features, and security-driven service blocking. Delays in data ingestion are excluded from downtime calculations.

Where availability falls below the committed service level, eligible customers may claim service credits equivalent to 2% of the monthly subscription fee for qualifying incidents, subject to defined daily and monthly limits.

A public service status portal provides real-time availability information and optional alert subscriptions.

Security and data protection

Cortex XDR incorporates layered security controls across the service lifecycle, including:

- Encryption of data in transit and at rest
- Continuous monitoring and threat detection
- Regular vulnerability scanning and penetration testing
- Role-based access control and audit logging
- Secure data storage within approved regions

The service aligns with recognised security standards including ISO/IEC 27001, ISO 27017, ISO 27018, ISO 27701, SOC 2, and PCI where applicable.

Onboarding and offboarding

Onboarding is supported through documentation, online knowledge bases, training materials, video tutorials, and optional professional services.

At contract end, customers can export logs, reports, and investigation data in standard formats such as CSV, JSON, and PDF. Services cease in accordance with contractual terms, with support available for data retrieval and transition if required.

Commercial model

Cortex XDR is provided under a subscription-based licensing model.

The subscription includes access to the Cortex XDR platform and standard vendor support. Enhanced support tiers, technical account management, and professional services are available at additional cost. Fees for professional or managed services are excluded from SLA credit calculations.

Out of scope

The following are not included unless explicitly contracted:

- Managed security operations services
- Customer network connectivity
- End-user device management
- Custom software development beyond supported configurations
- Provisioning of on-premiss infrastructure

