



Service description document: Cortex Cloud – Unified Cloud Security Platform

Cortex Cloud – Unified Cloud Security Platform

Service overview

Cortex Cloud is a cloud-native security platform designed to deliver unified visibility, protection, and response across modern cloud environments. It provides real-time security across code, infrastructure, identities, and runtime workloads by combining cloud native application protection with autonomous security operations.

The service enables organisations to continuously detect, prioritise, and remediate risks across multi-cloud and hybrid deployments using artificial intelligence and automation, without the need for on-premises infrastructure.

What the service provides

Cortex Cloud delivers a single, unified cloud security platform that spans the full cloud lifecycle from development to runtime and security operations. It centralises telemetry from cloud services, applications, identities, and infrastructure into a common platform where risks are identified, correlated, and remediated.

The service provides:

- Centralised cloud security command centre
- Continuous monitoring of cloud workloads and infrastructure
- Autonomous AI agents for detection and response

- Application Security Posture Management
- Cloud Detection and Response across workloads and identities
- Runtime protection for cloud workloads
- Infrastructure as Code scanning
- Cloud Infrastructure Entitlement Management
- Data Security Posture Management
- AI posture management for cloud-based AI services

Cortex Cloud supports both proactive prevention and real-time threat response across the full cloud attack surface.

Service features

Key technical features include:

- Unified cloud command centre
- Autonomous AI agents
- Application Security Posture Management
- Cloud Detection and Response
- Runtime workload protection
- Infrastructure as Code scanning
- Cloud entitlement risk management
- Data security posture management
- AI security posture management
- Precision AI threat prevention

Service benefits

Cortex Cloud enables organisations to:

- Dramatically reduce mean time to respond
- Resolve security issues autonomously
- Shift security left into development workflows
- Consolidate multiple cloud security tools
- Eliminate cloud security blind spots
- Optimise cloud performance while securing workloads
- Achieve precision AI-driven security outcomes
- Automate compliance and governance controls
- Enable developer-friendly security workflows
- Maintain unified visibility from code to cloud to SOC

Service scope and dependencies

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

The service can operate as a standalone platform or extend existing deployments by integrating with other Cortex services. It merges cloud native application protection capabilities with Cloud Detection and Response and integrates with endpoint telemetry and security operations platforms for end-to-end visibility.

The service requires deployment of compatible agents where applicable and relies on internet connectivity to deliver real-time monitoring and response.

Customisation and configuration

Customers can customise Cortex Cloud to align with their cloud architecture and security model. Configuration options include:

- Defining security policies and risk thresholds
- Customising dashboards and analytics
- Configuring automated remediation workflows
- Integrating third-party scanners and data sources
- Controlling access through granular role-based permissions

Customisation is performed through a browser-based management interface and APIs, with permissions controlled by role-based access control.

Access and user experience

Cortex Cloud is accessed via a web-based management console that provides a unified operational view of cloud security posture, threats, and remediation actions.

The interface is optimised for security teams and supports accessibility standards aligned with WCAG 2.1 Level AA. Features include keyboard-only navigation, screen-reader compatibility using ARIA labels, and appropriate visual contrast for alerts and dashboards. Mobile access supports monitoring and response actions, with complex configuration optimised for desktop use.

Support and service management

Vendor-backed support is provided 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 enhanced support services are available as optional professional services.

Availability and service levels

Cortex Cloud is covered by a vendor Service Level Agreement providing a 99.9% Monthly Uptime Availability commitment.

Availability is calculated based on total minutes in a calendar month, excluding defined events such as scheduled or emergency maintenance, customer environment issues, force majeure events, insufficient licensed capacity, beta features, high availability or scaling events, and security-driven traffic blocking. Delays in data ingestion are not considered downtime.

If availability falls below the committed service level, eligible customers may claim service credits equivalent to 2% of the monthly fee for the affected product for qualifying incidents, subject to daily and monthly caps as defined in the SLA.

Service status and regional availability are published via a public status portal with optional alert subscriptions.

Security and data protection

Cortex Cloud is designed with security embedded across all layers of the service. Protections include:

- Encryption for data in transit and at rest
- Segmentation, firewalls, and threat detection within the service
- Continuous vulnerability scanning and penetration testing
- Rapid patching of critical vulnerabilities

- Centralised logging and audit trails within the Cortex data lake

Data is stored and processed within the UK, EEA, and other approved locations, with compliance to 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, knowledge bases, online help, video tutorials, training resources, and optional professional services.

At contract end, customers can export logs, reports, and data in standard formats including CSV, JSON, and PDF. Services cease in line with contractual terms, and customers may retrieve required data or transition to an alternative solution with vendor assistance if required.

Commercial model

Cortex Cloud is provided under a subscription-based commercial model, with pricing based on licensed capacity and enabled capabilities.

The subscription includes access to the Cortex Cloud platform and standard vendor support. Enhanced support tiers, technical account management, and professional services are available at

additional cost. Fees for additional 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 support
- Custom software development beyond documented capabilities
- On-premises infrastructure provisioning

