NEXT

Terms and Conditions

Extended Detection & Response (XDR) - Schedule CS-11

Effective Date: October 14, 2025 | Supersedes prior versions.

Service Summary

Service Provider shall provide Extended Detection & Response ("XDR") services to improve detection, containment, and response to cybersecurity threats across Client's environment, as selected in the Tiered Coverage Options below. XDR centralizes telemetry, applies detections, and initiates permitted containment actions. This Schedule enhances visibility and response but does not guarantee prevention of all breaches, nor does it include full incident response or forensics unless separately contracted.

Scope of Services

- Deploy and manage XDR platform components (agents, connectors, integrations) on Covered Systems selected for coverage.
- Continuously monitor supported telemetry for indicators of compromise (IOCs), suspicious behavior, and policy violations.
- Triage alerts, assign severity, and document recommended remediation steps.
- Execute automated or semi-automated containment actions where supported and authorized (e.g., isolate endpoint, disable user, revoke token).
- Escalate material events to Client's designated contacts and maintain case notes in Service Provider's ticketing system.
- Provide periodic reporting on notable events and trends.

Tiered Coverage Options (select one per Agreement)

Only the options expressly selected and executed by the Parties are included.

Tier A — Microsoft 365 Breach Prevention ("Mailbox-Only")

Covered Data Sources (illustrative): Microsoft 365 mail flow and account telemetry (e.g., risky sign-ins, suspicious inbox rules, impossible travel, anomalous OAuth grants), supported collaboration signals if available.
Included Actions: Alerting, triage, recommendations; optionally disable/suspend account, revoke sessions/tokens, and enforce password reset/conditional access if pre-authorized.
Not Included: Endpoint/Server agent coverage, host isolation, non-Microsoft workload coverage.

Tier B — XDR Agent (Standard)

Covered Data Sources (illustrative): Tier A, plus XDR endpoint/server agents on supported Windows/macOS/Linux systems; limited cloud or network integrations as available.
Included Actions: All Tier A actions plus host-level containment where supported (e.g., isolate endpoint, kill process, quarantine file), and push remediation guidance.
Not Included: Advanced/custom detections, bespoke playbooks, expanded cloud/network visibility beyond standard integrations, or extended data retention beyond standard policy.

Tier C — XDR Agent (Advanced)

Covered Data Sources (illustrative): Tiers A & B, plus enhanced or custom detections, expanded cloud/SaaS or network integrations where supported by the platform, and expanded analytics/telemetry as configured.
Included Actions: All Tier B actions plus custom response playbooks where supported, limited engineering for tailored detections/policies, and expanded reporting.
Not Included: Full incident response (IR), forensic investigation, e-discovery, legal/regulatory reporting, or business continuity services unless separately contracted.

Data Retention. Telemetry and alert retention are governed by Service Provider’s standard XDR policy, which may be updated with written notice to Client. As of the Effective Date, standard retention is as documented in Service Provider policy; expanded retention (if any) is available under Advanced tier or as an add-on.

Authorizations for Automated Actions

Client authorizes Service Provider to execute platform-supported containment actions defined in the selected Tier. Client will designate authorized approvers and notification paths. Absent pre-authorization, Service Provider will recommend actions and await Client direction.

Service Limitations

- XDR detections are limited to the telemetry provided by the platform, Covered Systems, and enabled integrations.
- Advanced threats (e.g., zero-day, APT, insider abuse), encrypted channels, or unsupported systems may evade detection.
- Automated actions may be constrained by platform capabilities, permissions, or policy.
- XDR does not include full IR/forensics, root-cause analysis, system rebuilds, regulatory notifications, or BCDR/RPO/RTO commitments (each available separately).

Exclusions

- Coverage of systems, users, tenants, or applications not expressly onboarded.
- Guaranteed prevention, total visibility, or 100% detection accuracy.
- Responsibility for actions not taken by Client after escalation/recommendation.
- Remediation of compromise beyond triage, guidance, and the authorized automated actions above.
- Unsupported/legacy platforms, shadow IT, or personal devices outside management.

Client Responsibilities

- Ensure deployment of XDR agents/connectors on all intended Covered Systems; maintain supported OS/versions.
- Provide and maintain least-privilege permissions needed for detections and response actions.
- Keep escalation contacts current; promptly review and act on alerts/recommendations.
- Approve and maintain conditional access, MFA, and other prerequisite controls required for containment.
- Notify Service Provider before material environment changes (new tenants, apps, networks, or major architecture shifts).

General Terms

- XDR is a detection/containment enhancement. It improves visibility and response but does not replace comprehensive IR, forensics, or BCDR planning.
- Client acknowledges XDR is one layer in a defense-in-depth strategy. No single control or combination of controls can guarantee complete protection; even advanced systems can be bypassed. Service Provider strongly recommends complementary safeguards (e.g., endpoint protection, MFA and conditional access in M365/Intune/Entra ID, DNS/email filtering, user training, vulnerability management).
- Response times for XDR-related service requests are governed by the Service Level Objectives in Schedule A of the Master Service Agreement (with/without Rapid Response as applicable); any separate IR agreement controls IR timelines.
- Fees. Billed per the Payment Terms of the Master Service Agreement. Required platform licensing is included in Service Provider’s standard service fees unless otherwise specified. Add-ons such as custom integrations, extended retention, or specialized response services may be billed separately.