Statement of Services

Supra ITS Managed Detection and Response (MDR)

Purpose of this Document

This document represents the scope of included services of Supra ITS (Provider) Managed Detection and Response and the respective deliverables and unique features of the included services.

Managed Detection and Response (MDR)

Scope: Provider delivers a turn-key Managed Detection and Response service, including licensing for an industry-leading Endpoint Detection and Response (EDR) platform, deployed across Client/Customer's (Client) specified endpoints. Provider's Security Operations Center (SOC) provides 24/7 monitoring, detection, prevention, and response to threats, leveraging Machine Learning (ML), Artificial Intelligence (AI), behavior-based Indicators of Attack (IOAs), exploit blocking, and threat intelligence. The service includes proactive threat hunting, full endpoint visibility with raw event recording, and attack lifecycle context to enhance situational awareness. MDR also offers Incident Support, providing expert guidance and coordination during security incidents to minimize impact and expedite recovery.

Deliverables:

- Real-time alert notifications to Client.
- Proactive threat prevention and response actions by the SOC, including host isolation, threat containment, exploit blocking, and remediation steps as feasible within Client's environment.
- Investigation and response to detected threats, enriched with threat intelligence and attack lifecycle visibility.
- Incident Support, including real-time consultation during active incidents and post-incident summaries with recommended next steps.
- Monthly reports delivered by email or Account Manager detailing incidents, response actions, threat trends, and organizational threat level insights, supported by full endpoint activity data for proactive threat hunting.

Unique Features:

- Usage and Counts: Based on total number of Endpoints

On-Boarding Services

On-Boarding Services are required services that fast-track value by installing agents, tuning detections and handing your team clear policies and training materials.

General Provisions for All Services:

- **Service Level Objective (SLO) Response Times:** Provider will respond to incidents or inquiries based on the following priority levels, measured from detection or notification:

Priority Level	Example	Response Time

Priority 1 (Critical)	Active malware outbreak, data breach in progress, etc.	15 minutes
Priority 2 (High)	Suspicious activity, critical system alerts, etc.	30 minutes
Priority 3 (Standard)	Routine inquiries, low-risk alerts, etc.	4 hours

- **Service Availability:** Services are provided 24x7x365 with a target uptime of 99.9%, excluding scheduled maintenance.
- **Reporting:** Delivered monthly, via email, performance reports will be provided for all active services, detailing key metrics as outlined per service.
- **Escalation:** For incidents requiring Client input or approval, Provider will escalate to Client within 1 hour of identification by the SOC,
- **Client Communication:** All monthly reports will be delivered via email or via an Account Manager.

Client and SupraITS Responsibilities

- **SupraITS Responsibilities:**
    - Deploy, configure, maintain, and manage selected services as outlined in the Service Description.
    - Monitor and respond to incidents per the SLO Response Times in the General Provisions.
    - Deliver reports and notifications as specified per service.
- **Client Responsibilities:**
    - Provide all required system access, permissions, and initial asset/user lists within 5 business days of, as applicable, order or SOW execution, unless otherwise specified.
    - Respond to escalations from Provider for incidents requiring Client input or approval, unless otherwise agreed within a timeframe in accordance with our onboarding checklist, to facilitate timely decision-making and resolution.
    - Client shall maintain any installed agent, hardware, or software as part of any service in an active, unaltered state throughout the term and to promptly notify Provider of any issues affecting its functionality. Failure to comply may result in suspension of affected services up to and including termination of the contracted service.
    - Provider shall not be liable for any service failure, delay, or resulting damages to the extent caused by Client's negligence, including but not limited to failure to fulfill the responsibilities outlined herein (e.g., delayed access, unauthorized modifications to systems, or untimely responses to escalations), as further detailed by the parties where applicable.
    - Provide a designated point of contact for all services.

Covered Items

This Statement of Services applies to the following SupraITS MDR Services

7489C006 - SupraITS - Managed Detection and Response (Management Only) - Min 50 Endpoints - #010101004001
7489C007 - SupraITS - Managed Detection and Response (Inc. Premium Next-Gen AV & EDR Licensing) - Min 50 Endpoints - #010100201002

Any product, service, or deliverable not expressly set forth in the foregoing is out of scope of this Service.

About Supra ITS

Supra ITS, a Canon IT Managed Services partner, is based in Canada, established in 1999 and blends deep enterprise know-how with a "customer-first" mindset to deliver everything-as-a-service for growing organizations. Supra ITS has offices in the US, UK, India and Canada. More than 200 certified professionals operate four tier-3

data centers and run tightly integrated 24 × 7 SOC and NOC teams, so clients get prompt, around-the-clock support. The company’s portfolio spans managed IT and cloud, cyber-security, business-process outsourcing, and custom application development, all backed by top-tier credentials and strategic alliances. This combination of scale, pedigree, and nimble execution lets Supra ITS safeguard critical workloads, speed digital transformation, and simplify compliance.

Canon U.S.A., Inc.