SURELOCK TECHNOLOGY SOCaaS

Service Guide — Essential, Enhanced, Premium Tiers & Add-On Services

Contents

Overview 2
In Scope / Out of Scope Services 2
Customer Requirements 2
Services Description 3
Support 5
SOCaaS Roles & Responsibilities Matrix 6
Service Level Objectives (Essential) 8
Service Level Objectives (SL Enhanced & SL Premium) 8
Containment Authorization (SL Premium) 8
Remediation, Recovery & Evidence 8
Service Limitations & Dependencies 9
Service Implementation & Delivery 9
On Boarding Outline 10
Offboarding & Data Export 10

Version History

Version	Date	Author	Summary of Changes
1.0	09/21/2026	VP of Services	Initial creation.
1.1	09/28/2026	VP of Services	Alignment of SL Enhanced and SL Premium SLO definitions and exclusions, containment authorization, remediation boundary, service limitations, offboarding.
1.2	10/08/2026	VP of Services	SL Enhanced and SL Premium feature updates: SLO clock start and definitions, after-hours escalation, log retention, Okta coverage, Enhanced containment model, Premium application control scope.

Current version: 1.2

Overview

SureLock Technology SOCaaS delivers enterprise-level security operational capabilities through a unified platform combining EDR and MDR security monitoring. The service is focused on delivering comprehensive visibility across attack surfaces with expert-guided threat response. Security monitoring and automated notification operate 24/7/365; live conversation with a SOC analyst is available Monday–Friday, 7am to 6pm ET (see Support).

In Scope / Out of Scope Services

In-Scope

- ✓ SureLock AI XDR with AI-powered detection and engineer analysis
- ✓ SureLock EDR & MDR protection with AI-powered detection and engineer analysis
- ✓ Microsoft security integration
- ✓ Google Chromebook

Out of Scope

- ✕ IOT Devices
- ✕ Office Devices (Conferencing Equipment, Printers, Scanners, Copiers, Fax)
- ✕ Assets, log sources, and activity not onboarded to the platform or not observable from the telemetry provided
- ✕ System administration, patching, reimaging, backup restoration, disaster recovery, and business continuity (see Remediation, Recovery & Evidence)

Customer Requirements

For a successful implementation, protection, and delivery of services, the customer is responsible for the following:

Information Sharing

- **Network Visibility:** Network diagrams, current software levels, vendor information.
- **Change Notification:** To ensure accurate monitoring and protection of the environment, SureLock requests 72-hour notice of client changes that could impact the service, or technical changes requiring SureLock execution within the service (travel, IP/domain changes, thresholds, etc.).

Access & Security

- **Remote Access** for proper deployment of the security platform.
- **Credentials & Supported Configurations:** Administrative credentials, API and integration access, and supported versions and configurations for covered systems.
- **Required Telemetry:** Enablement and continued delivery of the log sources and integrations identified during onboarding.

Support Engagement

- Contacts for security alerts, notifications, and escalations.

- **Authorized Contacts:** Maintain a current list of authorized contacts, including after-hours escalation contacts, and promptly notify SureLock of changes. SureLock may rely on instructions and approvals from listed authorized contacts.
- **Containment Authorization (SL Premium):** Pre-authorize containment actions or designate approvers as described in Containment Authorization.
- **After-Hours Response (SL Enhanced):** Maintain designated contacts able to act on Critical and High escalations 24/7/365. At the Enhanced tier the SOC advises and does not execute containment; clients without overnight or weekend IT coverage should subscribe to SL Premium.
- Timely response to critical security notifications.
- Engagement in incident response that requires additional human actions.
- Ongoing assurance that security agents are deployed on covered devices.
- Uptime and availability of network connectivity for monitoring components.
- Support and implementation of security best practices, recommendations, and policies.

Operations & Compliance

- **Operational Responsibilities:** Maintain independent backups, patching and hardening of systems, endpoint and identity administration, and business continuity plans, unless assigned to SureLock under a separate service or statement of work.
- **Compliance Obligations:** Determine applicable legal and regulatory obligations and retain overall compliance responsibility.

Services Description

Essential Services: Baseline coverage included in our Threat Deception SOC Service

✓ **24/7/365 Security Monitoring —** Continuous monitoring of in-scope log sources and alerts by SOC analysts, year-round. Alerting and notification are 24/7/365; analyst communication is M–F 7am to 6pm ET (see Support).

✓ **Alert Triage & Prioritization —** AI and analyst review of alerts against defined use cases, with false-positive filtering and severity classification.

✓ **Managed Threat Deception Protection —** AI XDR technology.

✓ **Log Collection & Aggregation —** Centralized ingestion of logs from agreed sources into the SIEM/monitoring platform.

SL Enhanced and SL Premium are delivered as a separate service line from Essential Services. Enhanced and Premium include only the deliverables listed for those tiers below.

Enhanced Services: Baseline coverage included with our Total Protect SOC Service

✓ **24/7/365 Security Monitoring —** Continuous monitoring of in-scope log sources and alerts by SOC analysts, year-round. Alerting and notification are 24/7/365; analyst communication is M–F 7am to 6pm ET (see Support).

✓ **Alert Triage & Prioritization —** Analyst review of alerts against defined use cases, with false-positive filtering and severity classification.

- ✓ **Core Correlation & Detection Rules —** Standard use case library covering common attack patterns and threat behaviors.
- ✓ **Incident Notification —** Notification to designated client contacts per defined severity-based targets (see Service Level Objectives).
- ✓ **Support Microsoft Defender & Windows Security Integration**
- ✓ **AD, Entra ID & M365 Monitoring —** Continuous monitoring of Active Directory, Entra ID, and Microsoft 365 identity and access activity.
- ✓ **Okta & Google Workspace Coverage —** Monitoring of Okta and Google Workspace identity and access activity.
- ✓ **Six Security Domains Monitored —** Coverage spanning endpoint, identity, network, cloud, email, and data domains. At the Enhanced tier, network visibility is limited to telemetry from endpoint and identity sources; network and firewall log ingestion is an SL Premium deliverable.
- ✓ **Compliance Framework Reporting (Baseline) —** Reporting mapped to common compliance frameworks, included at the Enhanced tier. Reports support, but do not certify or guarantee, the client's compliance.
- ✓ **EDR-Agnostic Platform —** Runs on top of whatever EDR the client already owns (Defender, SentinelOne, Carbon Black, CrowdStrike); nothing gets uninstalled.
- ✓ **Log Collection & Aggregation —** Centralized ingestion of logs from agreed sources into the SIEM/monitoring platform, with no data ingestion caps on onboarded sources.
- ✓ **Standard Log Retention —** 90 days of searchable log retention and seven (7) years of archive retention. One (1) year of searchable retention is included in SL Premium.
- ✓ **Monthly Security Reporting —** Summary report covering alert volume, trends, and monitoring coverage.
- ✓ **Quarterly Service Review —** Light-touch check-in on coverage, performance, open items, recommendations, and account health.
- ✓ **Asset Inventory —** Inventory of covered assets reporting to the platform.
- ✓ **Client Portal Access —** Access for authorized client users to alerts, cases, and reports for the client's environment.
- ✓ **Containment Escalation —** At the Enhanced tier, the SOC advises and does not execute containment. Recommended containment actions are escalated by SureLock to designated client contacts; the client executes the action, or may authorize SureLock to execute it where SureLock manages the affected system under a separate service.

Premium Services: Deliverables defined below, in addition to all "Enhanced Services"

- ✓ **ITDR & Dark Web Monitoring —** Full identity threat detection and response, plus monitoring for compromised credentials on the dark web.
- ✓ **Extended Log Retention (SIEM) —** One (1) year of searchable retention and seven (7) years of archive retention for investigation or compliance needs. SL Premium meets solicitations requiring twelve (12) months of searchable log retention.

- ✓ **SOC-Executed Containment (ThreatContain) —** The SOC executes containment actions directly (isolate host, disable account, block indicator) rather than advising the client's team to act. Actions are limited to those the client has pre-authorized (see Containment Authorization); all other actions are escalated for approval.
- ✓ **Network & Firewall Log Ingestion —** Network and firewall logs are ingested and correlated into the SIEM.
- ✓ **MFA Fatigue & Lateral Movement Detection —** Detection use cases targeting MFA fatigue attacks and lateral movement.
- ✓ **Expanded Compliance Reporting —** Reporting mapped to HIPAA, PCI DSS, NIST CSF, and CMMC frameworks. Reports support, but do not certify or guarantee, the client's compliance.
- ✓ **Application Control —** Monitoring and alerting on application allow/block policy events on covered endpoints, where supported. Policy configuration and enforcement remain with the client unless provided under a separate SureLock service.

Add-On Services: Individual deliverables that can be added to your existing Essential, Enhanced, or Premium Services

- ✓ **Security Awareness Training —** Ongoing phishing simulation and end-user training program.
- ✓ **Incident Response Retainer —** Pre-negotiated access to DFIR resources with response times defined in the Incident Response Retainer addendum.
- ✓ **Tabletop Exercises —** Facilitated incident response simulations to test the client's plan and stakeholders.
- ✓ **Dedicated Named Analyst —** A consistent, assigned analyst for continuity on larger or more complex accounts.

Support

Service	Serviceability
Proactive Monitor & Notification	24x7x365
Automated Communication	24x7x365
Analyst Communication	M-F 7am to 6pm ET
Deploy & Maintain the Platform	M-F 7am to 6pm ET
Microsoft 365 / Google Workspace Integration	24x7x365
Log Collection	24x7x365
Extended Environment Remediation	M-F 7am to 6pm ET
On Site Security Engineer	On Demand as Additional Service
VCISO Support	On Demand as Additional Service

Note: Monitoring and notification run 24x7x365; live analyst conversation is M–F 7am to 6pm ET. Critical and High escalations to designated client contacts are delivered 24x7x365 for SL Enhanced and SL Premium (see Service Level Objectives). A Dedicated Named Analyst is an Add-On Service.

SOCaaS Roles & Responsibilities Matrix

A checkmark indicates the deliverable is included for that column at the referenced tier.

Deliverable	Client	SL Essential	SL Enhanced	SL Premium	Add On
Security Platform Implementation	✓	✓	✓	✓	
Security Platform Tuning	✓		✓	✓	
24/7/365 Security Monitoring		✓	✓	✓	
Alert Triage & Prioritization		✓	✓	✓	
Core Correlation & Detection Rules		✓	✓	✓	
Incident Notification		✓	✓	✓	
Managed Threat Deception Protection		✓			
Support Microsoft Defender & Windows Security Integration			✓	✓	
Extended Environment Remote Remediation	✓				✓
On Site Support	✓				✓
AD, Entra ID & M365 Monitoring			✓	✓	
Okta & Google Workspace Coverage			✓	✓	
Six Security Domains Monitored			✓	✓	
Compliance Framework Reporting (Baseline)			✓	✓	
EDR-Agnostic Integration (Works with Existing EDR)			✓	✓	
Log Collection & Aggregation			✓	✓	
Standard Log Retention			✓	✓	
Asset Inventory			✓	✓	
Client Portal Access			✓	✓	
Monthly Security Reporting			✓	✓	
Quarterly Service Review			✓	✓	
ITDR & Dark Web Monitoring				✓	
Application Control				✓	

Deliverable	Client	SL Essential	SL Enhanced	SL Premium	Add On
Extended Log Retention (SIEM)				✓	
SOC-Executed Containment (ThreatContain)				✓	
Network & Firewall Log Ingestion				✓	
MFA Fatigue & Lateral Movement Detection				✓	
Expanded Compliance Reporting (HIPAA, PCI DSS, NIST CSF, CMMC)				✓	
Security Awareness Training					✓
Incident Response Retainer					✓
Tabletop Exercises					✓
Dedicated Named Analyst					✓

Service Level Objectives (Essential)

Notification targets by severity, measured from confirmed detection.

Severity	Notification Target	Example
Critical	15 minutes	Active compromise, ransomware indicators, confirmed data exfiltration
High	30 minutes	Malicious activity confirmed, contained to a single host
Medium	4 hours	Suspicious activity requiring investigation, no confirmed impact
Low	Next business day	Policy violations, informational findings

Enhanced Response services (e.g., MDR, IR Retainer) carry their own action-time SLOs, defined in the relevant service addendum.

Service Level Objectives (SL Enhanced & SL Premium)

For SL Enhanced and SL Premium, SureLock targets the following response times by ticket severity. Each target is measured from confirmed detection: the point at which the SOC has triaged a qualifying alert and confirmed it as a security event with sufficient telemetry for action. Targets measure the time to initiate each action, not the time to resolve an incident or recover systems.

Definitions: Acknowledge means a live SOC analyst engaging the alert, not an automated notification. Investigate means the SOC has begun analysis of scope and impact. Escalate means SureLock has contacted the client's designated contact. Customer Updates are status communications to the designated contact while the ticket is open.

Hours: Escalate and Customer Update targets for Critical and High severity apply 24/7/365. Medium and Low escalations that fall outside M–F 7am to 6pm ET are delivered at the start of the next business day.

Severity	Acknowledge	Investigate	Escalate	Customer Updates	Example
Critical	5 minutes	10 minutes	15 minutes	Every 30 minutes until contained	Ransomware outbreak
High	15 minutes	30 minutes	30 minutes	Hourly	Malware execution
Medium	1 hour	2 hours	2 hours	Every 4 hours	Foreign login
Low	4 hours	1 business day	As warranted	Daily while open	Single failed login

- ✓ **Triage and Investigation —** Alerts are triaged and investigated within the Acknowledge and Investigate targets above for their assigned severity.
- ✓ **Containment —** Under SL Premium, the SOC targets initiating pre-authorized containment actions on Critical and High alerts within the Escalate target. Under SL Enhanced, the SOC advises and recommended containment actions are escalated to designated client contacts to execute.
- ✓ **Escalation Path —** Severity is assigned by the SOC based on the evidence available. The client can request a higher severity at any time and it is re-assessed immediately.
- ✓ **Service Level Exclusions —** Targets exclude the portion of any delay caused by missing or delayed telemetry, unsupported or misconfigured systems, client action or inaction, required approvals not received, third-party service outages, scheduled maintenance, force majeure, or events outside the contracted scope.
- ✓ **Service Credits —** Unless a service credit schedule is stated in the client agreement, these targets are service level objectives and do not carry service credits. Where credits apply, they are the client's sole and exclusive monetary remedy for a missed target.
- ✓ **Reporting —** SureLock maintains records sufficient to determine whether a target was met and provides service level information on reasonable request.

Containment Authorization (SL Premium)

SOC-executed containment is limited to actions the client has pre-authorized in writing for its environment. During onboarding, the client designates each action below as Pre-Authorized, Approval Required, or Not Included, and may update a designation on written notice.

- ✓ **Endpoint Isolation —** Network isolation of a compromised or suspected host.
- ✓ **Account Disablement —** Disabling a compromised or suspected user or service account.
- ✓ **Indicator Blocking —** Blocking malicious hashes, domains, IP addresses, or URLs in supported controls.
- ✓ **Email Quarantine / Purge —** Quarantining or removing malicious messages from mailboxes, where supported.

SureLock is not responsible for delay caused by approvals that are unavailable or not received from designated contacts.

Remediation, Recovery & Evidence

SOCaaS remediation is limited to security analysis, recommendations, and the security control actions included in the subscribed tier. Unless provided under a separate SureLock service (such as Managed Backup & Disaster Recovery or Managed Server Management) or statement of work, the client remains responsible for system administration, patching, reimaging, configuration repair, application remediation, backup operation and restoration, disaster recovery, business continuity, and system rebuilding.

The SOC preserves available platform evidence within the stated retention periods. The client is responsible for preserving endpoint, network, application, backup, and business records outside the SOC platform.

Service Limitations & Dependencies

- ✓ **Security Services Are Not Insurance —** Cybersecurity services reduce risk but cannot eliminate it. SureLock does not warrant that every threat will be detected, prevented, contained, or remediated, or that data or systems will always be recoverable. This does not reduce any express commitment in this guide or the client agreement.
- ✓ **Scope & Visibility —** SureLock is not responsible for events or assets outside the defined scope, or for conditions that cannot reasonably be observed from the telemetry provided.
- ✓ **Third-Party Services —** The service depends on third-party platforms such as Microsoft, Google, Okta, and the client's EDR. SureLock is not responsible for outages, defects, or changes to those platforms outside its reasonable control.
- ✓ **Compliance —** Compliance reporting supports the client's compliance program. The client remains responsible for determining and meeting its legal and regulatory obligations.
- ✓ **Data Processing Location —** Service personnel and subprocessors may be located inside and outside the United States. Clients requiring U.S.-only access to their data must specify that requirement in the client agreement.

Service Implementation & Delivery

Service implementation and delivery specifics will be defined within the Implementation SOW.

On Boarding Outline

SureLock will aid and drive onboarding through the following milestones.

1. **Assessment —** Evaluation of current security infrastructure.
2. **Planning —** Design log retention and security architecture.
3. **Account & Contact Repository —** Collect and compile support account details, contacts, and requirements.
4. **Deployment —** Implementation of the security agents.
5. **Enablement & Tuning —** Initiate the services in a tuning phase for data collection and optimization (30 days).

6. **Test & Validation —** Verification of monitoring and alerting capabilities.
7. **SOC Handoff —** Integration with the 24/7 monitoring team and processes.
8. **Client Acceptance —** Client reviews deliverables and signs off on the transition to support and lifecycle management
9. **Report Enablement —** Configure the collection and distribution of included reports.

Offboarding & Data Export

Upon termination, the client may request an export of available log and case data within 60 days after the termination date. SureLock will deliver a standard export (such as CSV or JSON, as supported by the platform) within 20 business days of the request. Custom migration or transformation work may be scoped separately. After the 60-day period, data may be deleted in accordance with SureLock's retention practices.

Disclaimer: *This Service Guide is subject to change with time.*