MANAGED EMAIL SECURITY SERVICES

Service Guide — Essential & Protect Tiers

Contents

Overview 2
In Scope / Out of Scope Services 2
Customer Requirements 3
Services Description 3
Support 4
Email Security Roles & Responsibilities Matrix 5
Service Level Objectives 6
Service Implementation & Delivery 6
Onboarding Outline 7
Offboarding Services and Data Copies 7

Version History

Version	Date	Author	Summary of Changes
1.0	09/15/2026	VP of Services	Initial creation.

Current version: 1.0

Overview

SureLock Technology's Managed Email Security service delivers advanced, multi-layered protection against today's evolving email-borne threats. This solution helps organizations prevent, detect, and respond to threats including spam, phishing, malware, zero-day attacks, impersonation, and Business Email Compromise (BEC). By leveraging modern AI-powered cloud filtering and threat detection technologies, this service significantly reduces the risk of malicious email reaching end users, helping minimize the operational, financial, and reputational impact of cyber incidents.

In Scope / Out of Scope Services

In-Scope

Managed Email Security services include:

Support Services during business hours:

- ✓ Spam sensitivity change support
- ✓ Whitelist and blacklist change support
- ✓ Adding/removing email domains including DNS changes (MX/A/TXT/DKIM/SPF)
- ✓ Adding/removing users
- ✓ Release quarantined emails

Features:

- ✓ AI phishing, BEC & impersonation detection — at the inbox
- ✓ Malicious link & attachment scanning
- ✓ Autonomous remediation across every mailbox
- ✓ Warning banners + one-click report-phishing button
- ✓ Community threat intelligence from thousands of orgs
- ✓ API deploy — no MX changes, live in minutes
- ✓ Account-takeover (ATO) protection
- ✓ QR-code, image & deepfake / Teams protection
- ✓ Adaptive AI, tuned to your environment
- ✓ Security Awareness Training — automated, ongoing
- ✓ Phishing simulations — personalized, unlimited
- ✓ Human risk scoring + targeted coaching
- ✓ Sims scheduled, training assigned, results to leadership
- ✓ Tuning, quarantines, monthly reporting

Out of Scope Services

The following are excluded unless expressly included in a SOW:

- ✕ Support of M365 / Google user access, email software, email backup, and email recovery requires an additional SureLock Managed Service.
- ✕ Additional features such as email legal hold, MFA, and DLP require a specific Microsoft 365 subscription tier and SureLock Managed Services.
- ✕ Implementation or removal of the service requires a project statement of work.

Customer Requirements

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

Access & Security

- Remote Access / Tenant management for proper support.

Support Engagement

- Contacts for alerts, notifications, and escalations.
- 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.
- Support and implementation of security best practices, recommendations, and policies.
- **Change Notification:** To ensure accurate monitoring and protection of the environment, SureLock requires 72-hour notice of client changes that could impact the service, or of technical changes that require SureLock execution within the service (travel, IP/domain changes, thresholds, etc.).

Services Description

Email Essential Services: Baseline coverage for organizations that need core inbox protection

- ✓ AI phishing, BEC & impersonation detection — at the inbox
- ✓ Malicious link & attachment scanning
- ✓ Autonomous remediation across every mailbox
- ✓ Warning banners + one-click report-phishing button
- ✓ Community threat intelligence from thousands of orgs
- ✓ API deploy — no MX changes, live in minutes
- ✓ Account tuning
- ✓ Quarantine email releases
- ✓ Monthly business review — Analytics, reporting, recommendations

Email Protect Services: Essential Services plus the features below

- ✓ Account-takeover (ATO) protection
- ✓ QR-code, image & deepfake / Teams protection
- ✓ Adaptive AI, tuned to your environment
- ✓ Security Awareness Training
- ✓ Phishing simulations
- ✓ Human risk scoring & targeted coaching
- ✓ Prevention & Planning — Sims scheduled, training assignment/tracking

Support

Service	Serviceability
Automated Monitor & Notification	24x7x365
Automated Communication	24x7x365
Analyst Communication, Investigation, Remediation	M-F 7am to 6pm ET
Deploy, Maintain & Configure the Platform	M-F 7am to 6pm ET
Vendor Escalation (Microsoft, Google, Platform Partner)	M-F 7am to 6pm ET
Microsoft 365 / Google Workspace Integration	24x7x365

Email Security Roles & Responsibilities Matrix

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

Deliverable	Client	Email Essential	Email Protect
Security Platform Implementation	✓	✓	✓
Security Platform Tuning	✓	✓	✓
24/7/365 Email Monitoring		✓	✓
AI phishing, BEC & impersonation detection — at the inbox		✓	✓
Malicious link & attachment scanning		✓	✓
Autonomous remediation across every mailbox		✓	✓
Warning banners + one-click report-phishing button		✓	✓
Community threat intelligence from thousands of orgs		✓	✓
API deploy — no MX changes		✓	✓
Account tuning		✓	✓
Quarantine email releases		✓	✓
Monthly business review: Analytics, reporting, recommendations		✓	✓
Account-takeover (ATO) protection			✓
QR-code, image & deepfake / Teams protection			✓
Adaptive AI, tuned to your environment			✓
Security Awareness Training			✓
Phishing simulations			✓
Human risk scoring & targeted coaching			✓
Prevention & Planning: Sims scheduled, training assignment/tracking			✓

Service Level Objectives

Notification targets by severity, measured from confirmed detection.

Severity	Notification Target	Example(s)
Critical	15 minutes	Active phishing/malware campaign successfully bypassing filters and landing in multiple inboxes Business Email Compromise (BEC) confirmed — attacker has access to an executive or finance mailbox Mail flow completely down (inbound or outbound) for the organization Ransomware payload delivered via email and executed on an endpoint
High	30 minutes	Spike in phishing emails targeting a specific department (e.g., finance, HR) with credential-harvesting links Suspicious mailbox rule detected (auto-forwarding to external domain) but not yet confirmed as compromise Single user's mailbox compromised (password reset already completed, containment needed)
Medium	4 hours	User reports a suspicious email that turns out to be a lower-risk phishing attempt (no credentials entered) Delayed mail delivery (not a full outage) affecting a subset of users False positive/false negative tuning requests for spam filter or transport rules
Low	Next business day	User requests to whitelist/blacklist a sender or domain Minor formatting/display issues with security banners or warning tags on emails General awareness training follow-up after a simulated phishing test Non-urgent requests to adjust quarantine notification settings

Service Implementation & Delivery

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

Onboarding Outline

SureLock will aid and drive onboarding through the following milestones.

1. **Assessment —** Evaluation of current email security.
2. **Planning —** Design policies, trainings, and phishing campaigns.
3. **Account & Contact Repository —** Collect and compile any support account details, contacts, and requirements.
4. **Deployment —** Implementation of the security appliance/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. **Report Enablement —** Configure the collection and distribution of included reports.
9. **Client Acceptance —** Client reviews deliverables and signs off on the transition to support and lifecycle management.

Offboarding Services and Data Copies

Cancellation of email security services will be handled under a separate statement of work (SOW) project.

Mail flow will be changed, and access to quarantine reports, mail flow logs, and message traces will be lost.

Once services are terminated and the offboarding project is complete, the process is irreversible.

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