



SilverSky Enhanced Email Phishing

SilverSky has over 20 years of experience delivering security services to thousands of customers, many of whom trust us with their email security. SilverSky has developed a managed enhanced email phishing service in partnership with IRONSCALES that blocks advanced phishing and business email compromise (BEC) attacks (and never seen before threats) with Adaptive AI—dynamically sharpened by real-world user insights and a community of over 20,000 IRONSCALES threat hunters.

Key Benefits

- Improved security posture—SilverSky's Enhanced Email Phishing Adaptive AI builds a distinct baseline profile for each protected inbox, addressing over 99% of email threats.
- Strengthen your existing SEG (Secure Email Gateway)
- Skilled cybersecurity team – Our cybersecurity experts work with you for efficient installation and system tuning.
- Maximize ROI – SilverSky's affordable Enhanced Email Phishing provides deployment guidance and support services to maximize your investment.
- Flexible mail options—can be deployed to O365 or G-Suite and are priced by the number of users you want to protect.
- For Lightning MxDR customers, the Enhanced Email Phishing alerts can feed into the MxDR platform 24/7. With a 24/7 Security Operations Center (SOC), SilverSky helps you proactively eliminate threats and meet compliance objectives.

Enhanced Email Phishing Security Features

The Enhanced Email Phishing service includes several advanced security features, including:

- Inbound Email Protection – Adaptive AI email security against advanced attacks missed by other security controls
- Account Takeover Protection (ATO) – Eliminate ATO risk with advanced prevention, detection and response – additional purchased product
- Image-Based Attack Protection – Protect your organization from image-based attacks like malicious QR codes
- SOC Automation –Automated email remediation
- Crowdsourced Threat Intelligence – Leverage insights from 20,000+ security analysts in our community for email remediation

Deployment Types

- **SilverSky Enhanced Email Phishing (with Customer-supplied Email Protection)** is for customers who have already invested in a Secure Email Gateway. This includes SilverSky EPS, Mimecast, Defender for 365, and others. This version does not include link, visual, or attachment scans.
- **SilverSky Enhanced Email Phishing (with NO Customer-supplied Email Protection)** is for customers who may not have a Secure Email Gateway or are using limited free versions of Secure Email Gateway platforms that have reduced functionality. This version includes link, visual, and attachment scans.

Scope of Work

SilverSky will provide the customer with the following services:

- Provide instructions for the customer to integrate Enhanced Email Phishing into their Microsoft or Google environment.

- We will configure Enhanced Email Phishing following the Service Implementation below.
- Enhanced Email Phishing portal training: incidents, reporting, whitelisting, and configuration settings with the customer retaining administrative credentials.

Service Implementation

The onboarding process will be performed in three stages:

1. Service Orientation Call

Your assigned Project Coordinator will contact you to schedule a Service Orientation Call for the implementation team to assist during deployment. The goals of the call will be:

- Introduce the SilverSky team members.
- Review requirements for the service.
- Discuss notification and escalation procedures and customer points of contact.

2. Installation Call

After your Service Orientation Call, the implementation team will work with you to complete the prerequisites and schedule the installation call. The goals of the installation call will be:

- Begin installing Enhanced Email Phishing:
 - Authorize Enhanced Email Phishing Integration in the Enhanced Email Phishing portal
 - Add email alert address and set up collaboration app
 - Set up 911 mailbox
 - *Install the Report Phishing Add-on*
 - *Deploy Report Phishing Add-on to select group of users for testing*
 - *Note for KnowBe4 users: <https://support.ironcales.com/hc/en-us/articles/7255977800732-KnowBe4-Integration>*
 - Identify VIP users
 - Review Scan Back Incidents
 - Deploy Report Phishing Add-on to remaining users identified
 - Client training and end-user guides
 - SilverSky to provide an overview of the Enhanced Email Phishing portal.
 - “Authoritative body” in the customer environment to verify that they have trained their users.
 - SilverSky will provide one-pagers on the training options, but training is the customer's responsibility.
 - Our partner IRONSCALES has a large training library to support training

3. Service Operations

Service onboarding for Enhanced Email Phishing is typically a 1-to-2-week process, depending on the size and complexity of your network. The app authorization, 911 mailbox, report phishing add-on configuration, and identification of VIP users are on the first installation call, and the deployment of the report phishing add-on, review of scan back incidents, and portal overview are on the second installation call. The typical time required by our customer for all steps is 2 hours, not including employee training. The following phases will proceed after the installation call.

- *Configuration* – as defined by the Implementation steps above.
- *Tuning* – Respond to customer tune requests for incident threshold and response.

Moving from Implementation to Operations

SilverSky defines a completed Enhanced Email Phishing service deployment as the date when the following steps have been completed:

- 1) Enhanced Email Phishing is authorized in the customer's email platform.
- 2) Confirm that the report phishing add-on is deployed.



3) Basic Enhanced Email Phishing customer training completed.

Any changes requested after that date will be managed through our service operations, customer portal service tickets, or customer support team.

Service Features:

The SilverSky Enhanced Email Phishing service provides clients with the following deliverables:

Service	Deliverable
Installation	<p>SilverSky will assist customers with deploying Enhanced Email Phishing licensed through SilverSky as outlined in Service Implementation.</p> <p>Customer is responsible for the following:</p> <ul style="list-style-type: none"> • Designating a primary point of contact who will be available to assist SilverSky with installation is an appropriately qualified and trained technical lead who will be a permanent stakeholder throughout the engagement. • Providing information about the organization's email inventory and configuration. • Deploying software and adjusting network settings as directed by SilverSky and IRONSCALES. Responsible for the quality of data and any remediation efforts necessary to complete service implementation. • The authority and responsibility for decisions made regarding this service implementation. • The responsibility for any direct or physical remediation.
Policy Tuning	<p>SilverSky will respond to policy tuning and update requests based on priority.</p> <ul style="list-style-type: none"> • Adding or removing exceptions • Modifying automated response policies • Tuning alert notification rules
Product Support	<p>SilverSky will respond to product support requests based on priority. We will handle L1 support and may escalate to the IRONSCALES support team for L2 support.</p>

Service Definition

Service Feature	Description	Benefit
Coordination of technical issues with email technology partner IRONSCALES	As part of the service, SilverSky is the primary line of support for all technical issues with IRONSCALES. Our analysts will troubleshoot issues as they arise. Should further direct engagement with the email technology supplier be needed, SilverSky will perform that on the customer's behalf. We will troubleshoot any issues we can and engage with IRONSCALES when necessary to solve them and drive to a solution, including a customer.	<ul style="list-style-type: none"> - Experts on hand to help resolve issues who are familiar with your environment and Enhanced Email Phishing portal - Escalation to partners performed on the customer's behalf. The Customer is only brought in to troubleshoot when necessary
Direct console access	All customers are given independent access to the Enhanced Email Phishing portal as part of the service. This allows customers to review the contents of their portal as needed and to confirm configurations match their expectations on an ongoing basis. Access is restricted to ensure that changes do not disrupt alert handling.	<ul style="list-style-type: none"> - Access to the portal
Automated and Manual response actions	The Enhanced Email Phishing technology will execute built-in blocking of threats like phishing, BEC, and malware targeted to end users. Manual blocks can be added for emails that do not trigger automatic mitigation.	<ul style="list-style-type: none"> - Industry-leading technology-backed protection against threats - Response capability 24/7/365
24/7/365 Coverage	All actionable incidents routed to our monitoring platform are reviewed by an analyst 24/7/365. Analysts will review, analyze, and document their findings in our monitoring platform. Customers get complete visibility into notified and non-notified incidents	<ul style="list-style-type: none"> - Filling the skills gap by providing highly skilled security analysts who monitor and investigate alerts on our customers' behalf

RACI Matrix

Roles and Responsibilities are used to assign the level of task responsibility for various components of the SilverSky services:

Responsible	The person who is responsible for doing the work
Accountable	The person who is ultimately accountable for the process or task being completed properly
Consulted	People who are not directly involved with carrying out the task, but who are consulted
Informed	Those who receive output from the process or task, or have a need to stay in the know

Task ownership for the SilverSky Enhanced Email Phishing Service:

Activity	SilverSky	Customer
Solution evaluation	RA	CIR
Participation in the kickoff meeting	AC	IR
Provide technical details via the completion of a questionnaire or phone call	IC	RA
Technical customer resource to assist with service implementation & participation in deployment.	IC	RA
Provide technical details for users and support users deployment of the services	IC	RA
Provide training for the key customer contact	RA	IC