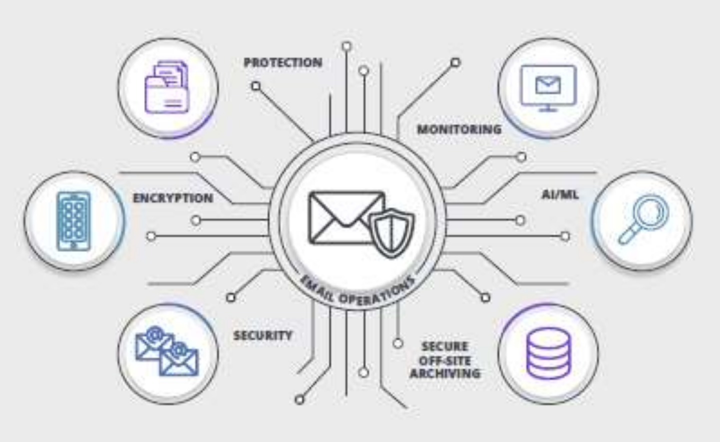
SERVICE
OVERVIEW

SilverSky Email Protection Service

Proactive protection for your most vulnerable system

Email is the core of your critical business communications – and the number one attack vector. We make sure your email is safe and compliant. From sophisticated payloads like malware and ransomware that result in data leakage and loss to social engineering tactics that prey on human endpoints, email attacks can stop your business cold. As a result, organizations must strengthen their email operations against external attacks and insider threats, whether intentional or negligent. They also must ensure compliance with stringent and evolving regulations to protect sensitive customer and corporate data – at rest and in transit.

SilverSky Email Protection Services (EPS) makes it simple to defend your email operations against threats, ensure business continuity, and meet compliance and audit obligations. Whether you need protection for your existing on premise, cloud-based, or hybrid email solution, SilverSky simplifies email protection. Our sophisticated and comprehensive suite of email security services seamlessly integrates to reduce your operational overhead and bolster security for your most critical business communications tool.



SilverSky EPS delivers secure and multi-layered protection for your business-critical email. Our advanced, adaptable tools include AI/ML for protection against social engineering attempts, encryption, data loss prevention (DLP), and proactive monitoring by our security operations analysts who sort through and prioritize alerts from your email system for you. The result? Powerful, advanced protection against modern email threats.

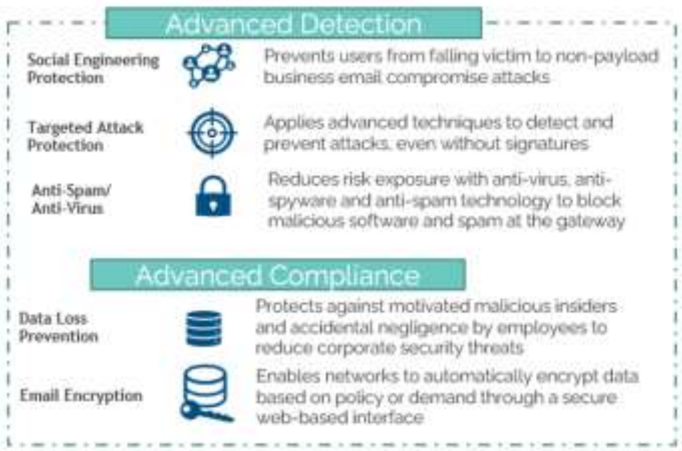
SilverSky integrates easily with Google, Office 365, and other services both on-premises and in the cloud. Secure off-site archiving ensures business continuity and provides easy access for e-discovery and audit requests.

With SilverSky EPS, your data and communications remain secure and compliant, without the burden and cost of staffing, implementing, and maintaining an in-house email security solution.

Service Benefits

- Leverages global threat intelligence capabilities to ensure EPS detection remains relevant with the changing threat landscape
- Ability to bundle services with MSS and MAS offerings
- Analyzes malicious emails and distil wider threat trends to continually update analytical models
- Readymade industry policy packs satisfy regulatory needs
- Fully customizable engine to meet a broad spectrum of needs as well as specific use cases
- One integrated portal to control and set policies for all email protection services

Components of the Service



Advanced Detection

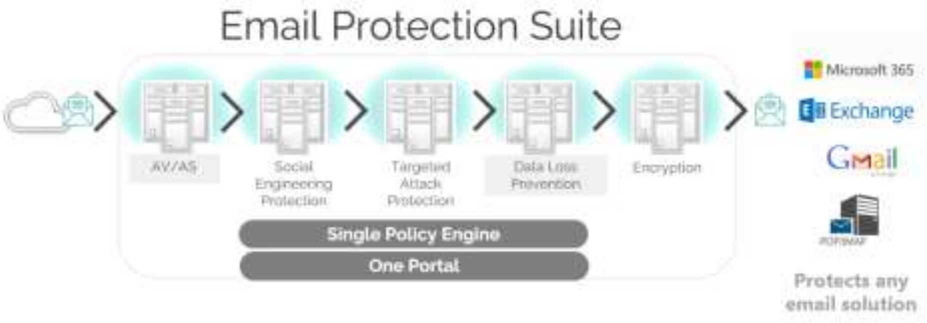
Social Engineering Protection	Prevents users from falling victim to non-payload business email compromise attacks
Targeted Attack Protection	Applies advanced techniques to detect and prevent attacks, even without signatures
Anti-Spam/ Anti-Virus	Reduces risk exposure with anti-virus, anti-spyware and anti-spam technology to block malicious software and spam at the gateway

Advanced Compliance

Data Loss Prevention	Protects against motivated malicious insiders and accidental negligence by employees to reduce corporate security threats
Email Encryption	Enables networks to automatically encrypt data based on policy or demand through a secure web-based interface

How It Works

SilverSky's provides a multi-layered detection engine to protect our customers, with a single policy engine and email portal to empower our customers to tune the service to meet their needs.



Email Protection Suite

Advanced Detection: Social Engineering Protection

The challenge with social engineering tactics center around emails with no malware to detect

- Social engineering attacks bypass traditional security defenses
- No files containing malware
- No links to malware download site
- Uses emotion to elicit action
- Too many parameters to monitor
  - Domain impersonation
  - Authentication
  - Email from different countries
  - Previous history
- Cannot expect end users to check all possibilities on every single message

[illegible]

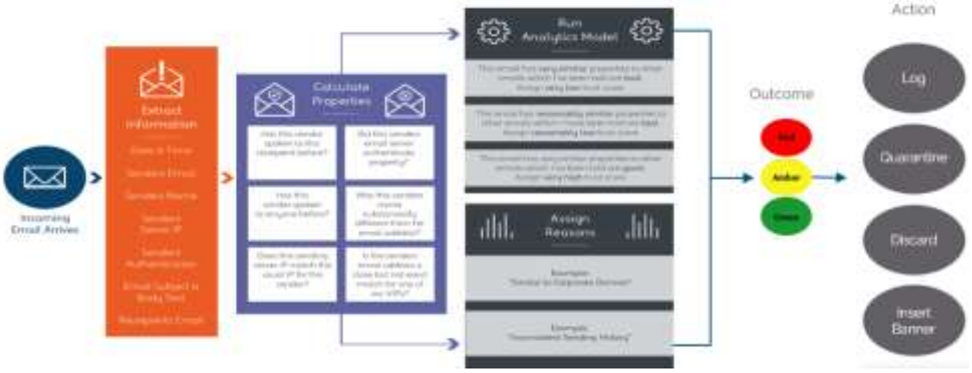
[illegible]

Forgot to give the conference our [illegible] details to charge. They are threatening to cancel.

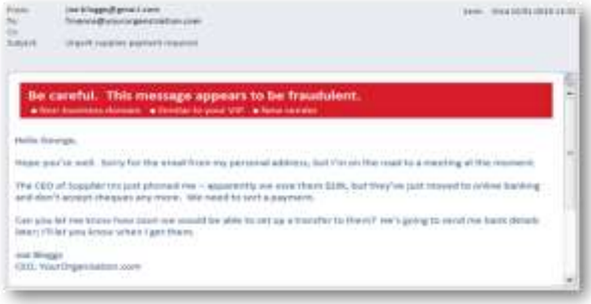
Make this your priority... send over the company account details to [illegible]

[illegible]

SilverSky utilizes machine learning to identify a social engineering attack:



The message banners for Social Engineering Protection ("SEP") give a clear indication to the user and reinforce the company policies:



From: joe.bloggs@gmail.com
To: finance@yourorganisation.com
Cc:
Subject: Urgent supplier payment required
Sent: [illegible]

Be careful. This message appears to be fraudulent.
● Non business domain ● Similar to your VIP ● New sender

Hello George,

Hope you're well. Sorry for the email from my personal address, but I'm on the road to a meeting at the moment.

The CEO of Supplier Inc just phoned me – apparently we owe them $18K, but they've just moved to online banking and don't accept cheques any more. We need to sort a payment.

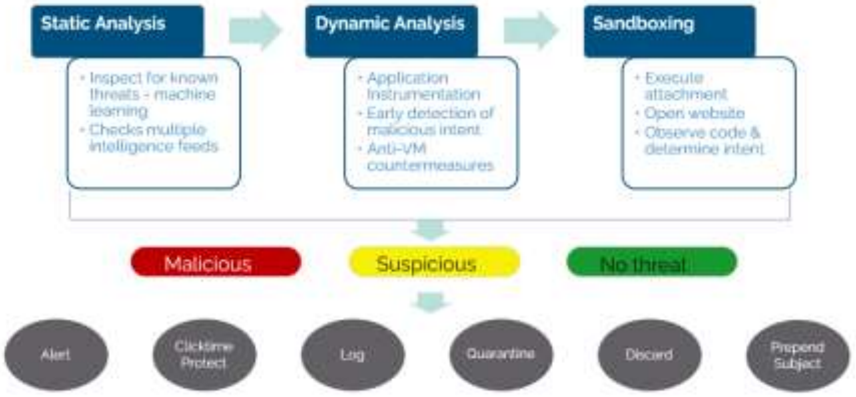
Can you let me know how soon we would be able to set up a transfer to them? He's going to send me bank details later; I'll let you know when I get them.

Joe Bloggs
CEO, YourOrganisation.com

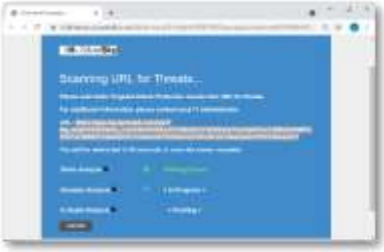
Advanced Detection: Targeted Attack Protection

The Targeted Attack Protection ("TAP") component of EPS addresses the challenge of continuously evolving malicious emails that are designed to evade signature-based virus scanning, weaponized documents and links to malicious websites. The TAP solution provides:

- Detection of malicious attachments and links before they reach the mailbox
- Stops advanced and undetected threats, including spear-phishing, APTs, targeted attacks and zero-day exploits
- Proprietary instrumented browser detects malicious intent early in the process
- Runs inline and blocks in real-time


Static Analysis
• Inspect for known threats - machine learning
• Checks multiple intelligence feeds
Dynamic Analysis
• Application Instrumentation
• Early detection of malicious intent
• Anti-VM countermeasures
Sandboxing
• Execute attachment
• Open website
• Observe code & determine intent
Malicious
Suspicious
No threat
Alert
Clicktime Protect
Log
Quarantine
Discard
Prepend Subject

TAP provides click-time protection for links, addressing the hacker subversion of email security scanning upon delivery, by scanning the website when the link is clicked. This protects the organization by scanning and approving in real time the access to embedded links.



Scanning URL for Threats...

Advanced Compliance: Data Loss Protection

Advanced Policy Editor

- Create policies to automatically detect and restrict inappropriate or risky inbound/outbound emails to protect against confidential and proprietary information loss

Advanced filtering policies

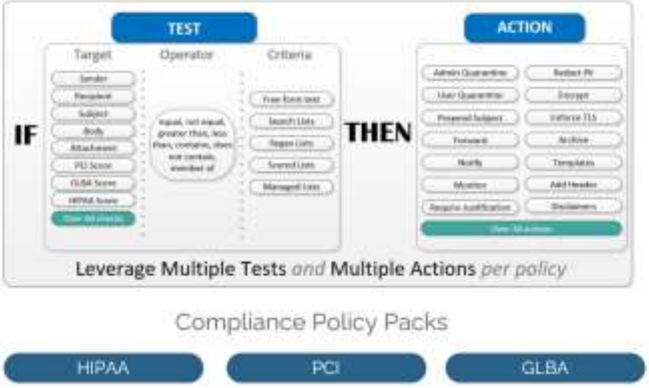
- 50+ global policies for inappropriate key words, suspect file attachments, and sensitive numeric string values

Tailor-made vertical solution bundles

- Pre-built policy packs for healthcare (HIPAA), retail (PCI), and financial industry (GLBA) compliance

Finite control over mail flow at every phase

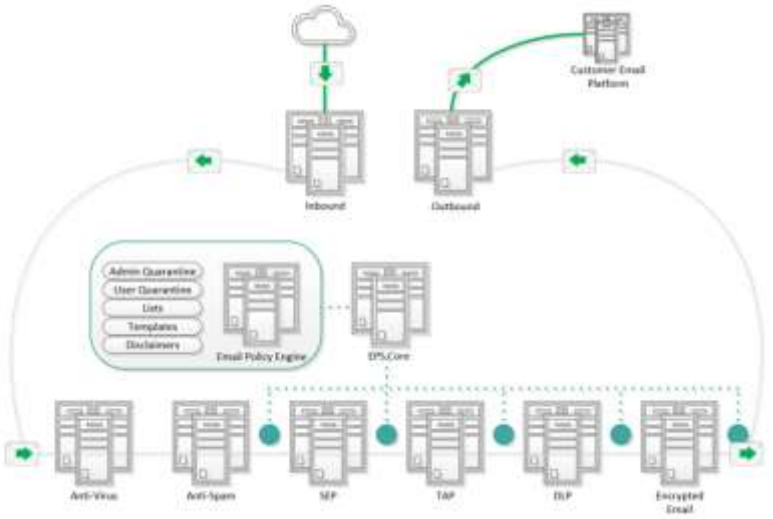
- Applies polices to AV/AS, SEP, TAP, DLP & Encrypted Email



Policy Engine can manage different types of inbound and outbound rules:

Inbound	Outbound
White and blacklists	Block sensitive data
Enforce message authentication	Encrypt sensitive data
Block dangerous files	Require sender justification
Block unscannable content	Role-based rules (block for some, allow for others)
Block files with macros enabled	

The policy engine informs and enhances all related services across the SilverSky EPS suite.



Service Definition

SilverSky will implement the following processes and service elements:

Email Protection Service	Definition
Kickoff Meeting	Meet to discuss and agree on customer goals and the rules of engagement for the services. This includes general project scoping, deployment timelines, review of services to be enabled, and procedures to follow should any issues occur during deployment.
Information collection	Customer will complete questionnaire related to email security setup and SilverSky's deployment team will review to make sure all answers are understood.
Instructions for customer-controlled changes	SilverSky will provide instructions for any changes that need to be made by the customer, depending upon the customer's setup. These will include DNS changes for MX, SPF, DMARC, and DKIM records, and may include firewall changes and AD account settings.
EPS Service Setup	SilverSky will deploy the service and assist with the initial configuration of the service, including loading user information, enabling administrative access for the customer, configuring policy rules, and testing SMTP connectivity. For customers migrating from other platforms, this can include replication of allow and block lists and policy rules from the old email security provider.
EPS Service Training	SilverSky will provide a training session for customer administrators during the initial EPS Service Setup so administrators understand how to use the Security Management Console to manage EPS services and to view reports.
EPS Cutover	SilverSky will work with the customer to plan the cutover to switch the customer's mail to flow through SilverSky's Email Protection Service, and will verify with the customer that mail is flowing properly after.
Social Engineering Protection Setup	SilverSky will provide assistance to the customer with enabling Social Engineering Protection (SEP). After cutover, SEP will be in a learning mode for a period of time before it can start taking actions on customer emails. SilverSky's deployment team will assist the customer in switching from learning mode to active mode.

Reporting	SilverSky will provide a reporting system within the Security Management Console to provide various summary and detail reports about message processing. Message detail reports can be used to track delivery status of any customer emails. For reports outside the scope of our existing reports, custom reports may be available for additional fees.
Support	SilverSky will provide support to customers for any issues that may arise from the use of EPS. For customers that desire more assistance with the creation of Email Security policy rules, Professional Services may be needed.
Periodic Policy Reviews	SilverSky's Professional Services team will be available for quarterly or as needed policy reviews for additional fees.

Service Deployment

Note that SilverSky defines a completed Email Protection Service deployment as the date when the following steps have been completed:

(1) MX Record is pointed to SilverSky EPS platform
(2) Confirm that email is flowing through the platform
(3) EPS Customer training completed (using SMC portal to manage & view quarantine, white/black list, etc.)

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

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 Email Protection service:

Activity	SilverSky	Customer
Solution evaluation	RA	CIR
Participation in kickoff meeting	AC	IR
Provide technical details via completion of questionnaire	IC	RA
Technical customer resource to assist with service implementation & participation in deployment. Customer resource understands Customer’s email policy needs and has the authority to recommend policy configuration and updates.	IC	RA
Provide technical details, IP address, policies, procedures relevant to the service prior to service initiation kickoff	IC	RA
Provide instructions for any customer-controlled changes (e.g., DNS, firewall, AD access)	RA	IC
Initial EPS Service configuration	RA	RIC
EPS administrator training	RA	IC
EPS mailflow cutover	RAIC	RAIC
Social Engineering Protection Setup	RA	IC
Provide customer support for EPS	RA	IC
Evaluate SilverSky services and immediately notify SilverSky of any perceived problems or issues with SilverSky services	IC	RA
Manage email policy and supporting lists, including allow and block lists, URL ‘do not protect’ list, and VIP lists, and manage email quarantines	IC	RA
Maintain user lists, either manually or via automated syncs into Customer Reporting console	IC	RA
Provide summary and detail messaging reports	RA	IC