SERVICE
OVERVIEW

SilverSky Email Protection Service powered by Check Point

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 powered by Check Point (EPS-CP) is a modern, cloud-delivered security solution that protects your Microsoft 365, Google Workspace, and collaboration tools from phishing, malware, account takeover, and data leaks. EPS-CP includes the Check Point Harmony Email & Collaboration suite of services. With seamless integration and advanced AI-powered threat prevention, SilverSky EPS-CP ensures your users stay secure and your data remains protected — without disrupting productivity.

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

Service Benefits

- Real-Time Defense – Blocks phishing and malware before it hits the inbox or collaboration stream, even detecting zero-day threats and business email compromise (BEC).
- Data Loss Prevention (DLP) and Compliance – Automatically enforces data loss prevention policies across email and collaboration platforms to ensure compliance with HIPAA, PCI, and other regulations.
- Account Takeover Protection – Stops suspicious logins using behavior-based algorithms and integrated threat signals.
- Easy Deployment – Deploys in minutes with no MX record changes needed; integrates directly through APIs.
- Powered by Check Point's AI and ThreatCloud – Combines advanced machine learning with the world's largest threat intelligence platform to stop emerging threats in real-time.
- Comprehensive Coverage – Protects email and collaboration apps like Microsoft Teams, Slack, OneDrive, SharePoint, Google Drive, and more.

Key Capabilities

Phishing & Impersonation Defence

- Stops social engineering and impersonation attacks using AI-trained engines
- Analyzes sender history, metadata, and language patterns to detect BEC and fraud

- Inspects internal, inbound, and outbound emails in real-time

Advanced Malware & Ransomware Protection

- Blocks malicious attachments and URLs before delivery using CPU-level sandboxing and threat emulation
- Sanitizes files within seconds to ensure uninterrupted workflow

Click-Time Protection for URLs and QR Codes

- Rewrites and inspects embedded URLs and QR codes “at the moment of click” to stop delayed or redirected phishing attempts
- Prevents access to malicious websites even if the threat is introduced post-delivery

Data Loss Prevention (DLP)

- Predefined and customizable policies detect and block sensitive data sharing across emails and file shares
- Monitors subject, body, and attachments for compliance-triggering content

Account Takeover Prevention

- Monitors login behavior and blocks unauthorized access in real time
- Leverages signals from endpoint, network, and SaaS platforms to detect malicious activity

Optional Add-on Service: Collaboration & File-Sharing Security

- Scans files and links in tools like Teams, Slack, Google Drive, OneDrive, Dropbox, and SharePoint
- Quarantines threats and applies per-org policy filters for granular control

Optional Add-on Service: Email Policy Review & Quarterly Checkpoint

- Review the efficacy of existing email and DLP rules, adjusting email policies to meet changing business needs
- Recommend configuration changes based on our knowledge of the current threat landscape for your industry

Components of the Service

- API-Based Integration – Invisible to attackers, no email routing or MX record changes required
- Retroactive Scanning – Automatically index users, groups, alias’s, and distribution lists
- Unified Dashboard – View, manage, and act on email and collaboration threats in one place
- Single License Model – One license covers email and collaboration security with all features included
- Rapid Deployment – Get started in less than 5 minutes; see threat prevention results within hours

ThreatCloud Features

- 150,000 connected networks reporting into ThreatCloud with millions of endpoints worldwide
- Daily metrics:
  - 86 billion transactions processed
  - 7,000 detections of zero-day threats detected
  - 650K suspicious websites detected
- Detections and blocking within the last 12 months
  - 6.8 billion malicious website connections blocked
  - 185 million malware downloads blocked
  - 778 million vulnerability exploit attempts
- 200+ full time Check Point threat research team members discovering some of the most significant unknown software vulnerabilities

Service Definition

SilverSky will implement the following processes and service elements

Email Protection Service	Definition
Kickoff Meeting	Implementation project team virtual meeting, sharing project scope, pilot phase and information collection.
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. The instructions will include granting access to the customers M365 Tenant, and may include DNS changes for MX, SPF, DMARC, and DKIM records, and may include firewall changes and AD account settings.
EPS-CP 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-CP Service Training	SilverSky will provide a training session for customer administrators during the initial EPS-CP Service Setup so administrators understand how to use the EPS-CP Console to manage EPS-CP services and to view reports.
EPS-CP Cutover	SilverSky will work with the customer to plan the cutover to switch the customer's mail to flow through EPS-CP, and will verify with the customer that mail is flowing properly after.

Reporting	SilverSky will provide a reporting system within the EPS-CP 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-CP. 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 EPS-CP Service deployment as the date when the following steps have been completed:

(1) API established to the SilverSky EPS-CP platform
(2) Confirm that email is flowing through the platform
(3) Customer access to the EPS-CP Knowledge Center and training materials

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 EPS-CP service:

Activity	SilverSky	Customer
Solution evaluation	RA	CIR
Participation in kickoff meeting	AC	IR
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
Initial EPS-CP Service configuration, initially in "learning mode" and then upon customer approval will switch over to "active mode" for protection	RA	RIC
EPS-CP administrator training	RA	IC
EPS-CP mailflow cutover	RAIC	RAIC
Provide customer support for EPS-CP	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
Provide access to the Check Point customer console for summary information and reports	RA	IC