Frequently
Asked Questions

FAQ: Email Protection Service powered by Check Point

Why is this move, SilverSky EPS to the Checkpoint Avanan solution, happening?

SilverSky conducted a comprehensive review of technology offerings over the past 12 months through our CTO team. SilverSky selected Checkpoint Harmony/Avanan for our replacement of EPS based on superior performance, competitive pricing, collaborative executive alignment, and a strong partnership.

Part of the evaluation was to implement EPS-CP (SilverSky Email Protect Service powered by Check Point) for a set of customers and for our own SilverSky organization. We implemented the solution for 12 customers starting in November 2024, with excellent results. SilverSky piloted and adopted the solution for the protection of our own organization in May 2025. We have found it to be a positive experience for both our users, with simplified quarantine and phishing protection, as well as for our internal IT team, which has seen significant performance and security improvements.

What's the comparison between SilverSky EPS and Check Point?

The Check Point EPS service provides many improvements over our existing SilverSky EPS, including:

- Better overall phishing and social engineering detection
- Faster evaluation of URLs for threats
- The ability to process password-protected attachments
- The ability to clean attachments using Content Disarm and Reconstruction
- For data loss protection policies, it provides a significantly larger list of data types that can be detected in messages if desired
- EPS-CP also provides a much easier way of configuring policies targeted at specific groups of users
- The management user Interface is better at showing events and allowing easy searching for messages
- EPS-CP provides improved dashboard reports

How does EPS-CP complement what I already get from Microsoft?

EPS-CP services are very complementary with Microsoft built-in capabilities for antivirus, anti-malware, anti-phishing, along with Safe Links and Defender for O365. Check Point will include Microsoft's verdict on messages when making its own decision on whether an email is a threat or not. Messages that are blocked will consist of information on whether the threat was detected by Microsoft or by Check Point. Check Point has its own version of click-time handling of URLs based on rewriting URLs that works well, but can be disabled if you want to rely only on Microsoft Safe Links.

Which customer console will I use for EPS-CP?

A new Check Point customer console will be provided to manage EPS-CP. Your customer console will be under avanan.net and will be based on a tenant name assigned by SilverSky (e.g., yourcompany.avanan.net).

How do I get credentials for the Check Point customer console?

Administrators in the Check Point customer console should log in using single sign-on via Microsoft. On the Check Point customer console login page, click on the **Sign in with Microsoft** button.

How do I change my password in the new Check Point customer console?

We recommend that you do not allow administrators to access using Check Point-specific passwords and only allow access via single sign-on.

Who will be able to use the new Check Point customer console?

The Check Point customer console is intended for administrators and support personnel in your company. You can control who in your company has access to the site and what role/permissions each user will have. See the "***Administrator User Interactions Dashboard***" guide in the EPS-CP Knowledge Center for more information.

How do I update my Data Loss Prevention (DLP) Rules in Check Point?

Check Point provides a significant number of DLP rules that can be used upon service setup. See the EPS-CP Knowledge Center section on "***Creating Data Loss Prevention (DLP) Rules***". Should you wish to configure your own DLP rules, see both the "***DLP Configuration Setup***" and the "***How to Configure DLP and Rules***".

Will the Check Point customer console have alerts and security activity updates?

Yes, the customer console includes a comprehensive section on email alerts and security activity. Reviewing and taking action steps are outlined in the "***Message Analysis***" guide on the EPS-CP Knowledge Center.

Will I work with the same SilverSky team for support?

Yes

Will I still have my quarterly business review meeting?

For customers who have subscribed to the *Email Protect Quarterly Security and Compliance Checkpoint*, this service will continue with the SilverSky consultant assisting with your Check Point service.

Understanding how Advanced Threat Protection helps monitor MFA

EPS-CP Advanced Threat Protection (ATP) is a prevention-focused security solution designed to block sophisticated cyberattacks before they execute, protecting against malware and data exfiltration. It is built into EPS-CP to provide advanced detection and prevention capabilities against various threats by anticipating attack vectors and using behavioural analysis. EPS-CP will be configured for ATP to use Microsoft logins, specifically Multi-Factor Authentication (MFA) function for login, and therefore all authentication attempts will be monitored, and alerts will follow any rules that are currently set up.

What is meant by the "Unified Email Protect Dashboard"?

The unified dashboard means that Check Point can display information from both Check Point and Microsoft security checks. It can also provide a consolidated quarantine view, allowing administrators a single place to view and manage the quarantine.

For customers who also use SilverSky MxDR services with our Lightning customer portal, our roadmap includes pushing Check Point alerts into Lightning for centralized security alerting.

Do I still need to add Enhanced Email Phishing protection from Ironscales?

SilverSky recommends Ironscales for additional protection against targeted spear phishing attacks with the Enhanced Email Phishing service (EEP). Ironscales differs from Check Point in that EEP is architected to detect individual mailbox-tailored attacks, and can be detected, blocked, and notify the user in real-time. Companies can choose to purchase EEP for a subset of their users rather than across the entire domain, and clients find significant benefit in protecting C-Level Executives and Finance team members. These roles are the aim of sophisticated phishing attacks designed for a single individual.

Is the SilverSky EPS service officially in an End-of-Life status?

SilverSky EPS does not yet have a formal End-of-Life (EOL) date. The official EOL date will require estimates of migrating our current customer base, but will likely be in mid-2026.

SilverSky EPS will announce on an End-of-Sale date in the October/November timeframe. After that date, any new SilverSky EPS agreements will be provisioned on EPS-CP.