cake.

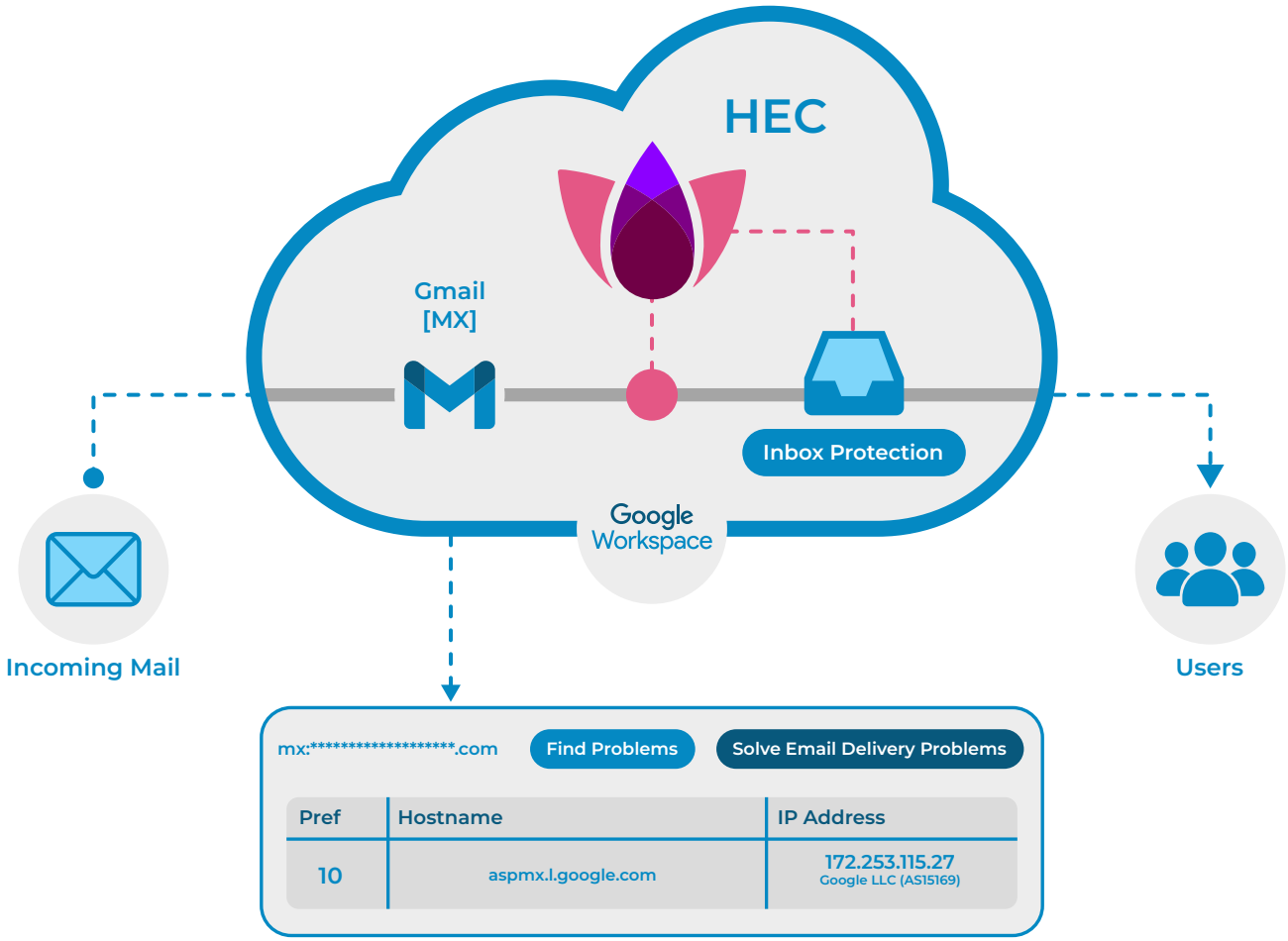
Customer Story

Equity Management Platform Company

Harmony Email and Collaboration Security Solution Google Integration

iSecureX
SIMPLIFYING CYBER SECURITY

Cake Equity HEC Architecture



Client Details

A prominent Equity Management Platform company, with a Global presence in AU and USA. All-offer an All-in-one system that lets you offer equity, plan your fundraising, and manage shareholders anywhere in the world.

- **Industry:** Fintech.
- **User Base:** 50+ staff and several Partners
- **Location:** Brisbane AU and California USA

Requirements and Challenges

Requirement

The client relied on Google's default email security for their Google workspace environment, supporting over 50+ global staff and partners globally, who depend heavily on email to manage daily operations, for product development and operations. The IT infrastructure is managed internally by their internal Ops team.

Challenges

The existing Google security solution offered limited protection, lacked strong anti-phishing, anti-malware and DLP capabilities and company executives were being severely hit with Phishing, Spam and Business Email compromise attacks.

The client was looking for a robust and flexible security solution which could integrate with both M365and Google Workspace environments and security for Collaborations apps viz Drop Box, Slack and OneDrive file storage. Clients were initially running Google workspace, however migrations were being planned to Azure.

Recognizing the need for a more robust, cloud-native email security solution with seamless API integration for GWS - with zero infrastructure changes - the provider sought an advanced, easily deployable email security solution.

Outcome

The deployment of Check Point Harmony Email & Collaboration has provided a fully managed, scalable, and highly secure email environment.

Currently, it is integrated with Google workspace, with the option to extend integrations to Collaboration applications viz Slack.

The client now benefits from

- Fast, API-in-line Email Security for proactive attack prevention
- Reduced operational costs through streamlined, cloud-native management.
- Enhanced security and scalability to adapt to evolving threats and organizational needs.
- Ongoing cybersecurity training for staff, boosting overall resilience.

iSecureX Solution

iSecureX partnered with the client to deliver a cutting-edge, cloud-native email security platform: Check Point Harmony Email & Collaboration (HEC). This API-in-line solution integrates seamlessly with Google Workspace and Microsoft Office 365, providing advanced detection and prevention of phishing, impersonation, malware, business email compromise (BEC) attacks as well as strong DLP detection for Google Mail and Google Drive.

Key features included

Cloud-based API-Inline Protection:

Rapid deployment with minimal disruption.

Comprehensive Threat Prevention: Anti-phishing, anti-impersonation, and malware threat prevention.

DLP for Gmail, Google Drive and Domain Authentication using DMARC and SPF.

24/7 Monitoring and Support: Proactive event detection and triage via the Check Point Infinity portal, with first-line support from iSecureX and premium escalation to Check Point.

The implementation began with a Proof of Concept (PoC) in Monitoring/Detect Mode, allowing the system to learn user and email patterns without impacting business operations. After a few weeks of observation, anti-phishing and security policies were fine-tuned before switching to Prevent (In-Line) Mode for real-time threat blocking.

Client Testimonial

"The user interface is simple and easy to navigate, making adoption straightforward. The Click Time Protection feature is excellent, providing an added layer of defense if any phishing or spam emails slip through initial filters. Implementation for Gmail is smooth and minimally disruptive, with only initial spam filtering tuning required. The Data Loss Prevention (DLP) capabilities for Personally Identifiable Information (PII) are robust. It would be beneficial to extend integrations to platforms like Notion to monitor external link sharing. Additionally, expanding general DLP monitoring beyond PII—for example, tracking a terminated user's file downloads—would further strengthen data security."
- Operations Manager

This case study demonstrates how iSecureX delivered a modern, cloud-native, highly flexible email security solution that addressed critical business challenges and significantly enhanced the client's email security posture.