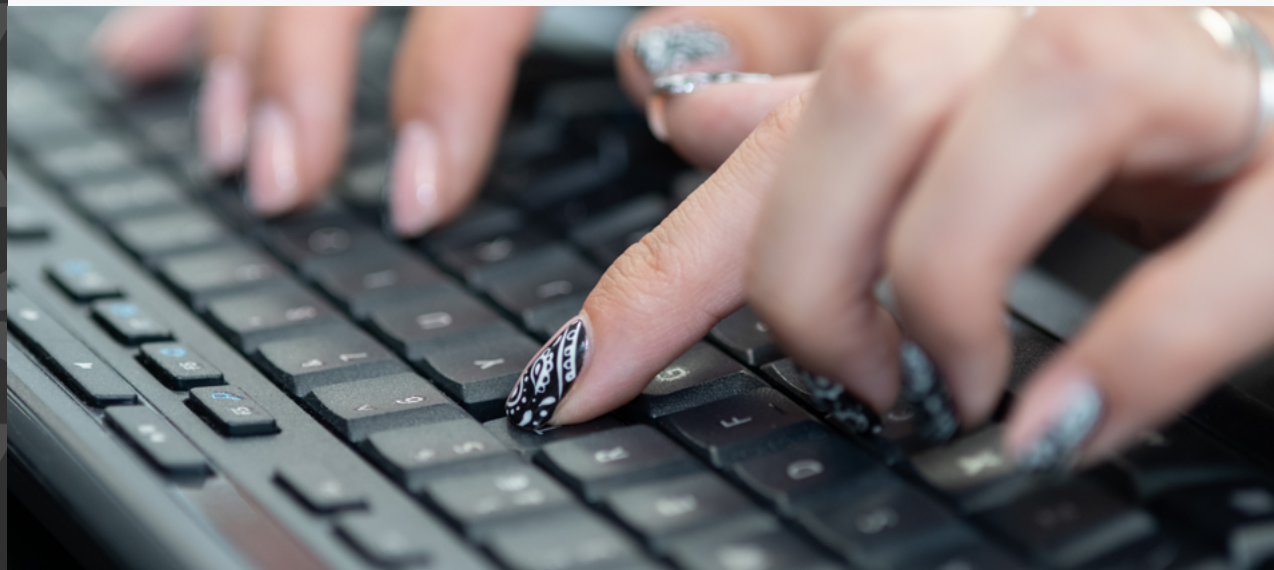
TECH DRIVEN. PEOPLE POWERED.

Solution Brief: Wingman Human Risk

In an era where digital communication is the backbone of business operations, organisations face a dual-front challenge: sophisticated technical exploits and the persistent factor of human error. Researchers from Stanford University and Tessian found that approximately 88% of all data breaches are caused by employee mistakes, while over 90% of attacks against organisations start with malicious emails. Wingman Human Risk is a comprehensive managed service designed to secure your digital environment by combining advanced technical defences with high-impact behavioural training to transform your weakest link into your strongest asset.

SEP2 utilise technical and training/testing to give complete coverage for the Human Risk factor, powered by Check Point's Email Security and KnowBe4 for end-user empowerment.



Educate and Empower Your Workforce

The strongest cyber security defence you can provide is an educated workforce. Wingman Human Risk delivers on-demand, interactive, and engaging training that moves beyond static presentations. By using storytelling and real-life examples, the service builds rapport with users, making security training an engaging experience rather than a burden. This education is validated through simulated phishing campaigns that allow you to analyse results and strengthen your team's resilience against real-world social engineering.

Engaging Security Content

Sitting through a presentation may deliver on providing the material to access, but it doesn't always resonate with the target audience. Through storytelling using real-life examples and building rapport with the characters and situations they are facing, you'll find that completing, understanding and engaging with the security training for your employees is no longer a burden that they must endure.

Protect Against Social Engineering

Block sophisticated social engineering attacks such as impersonation, zero-day phishing and Business Email Compromise (BEC) using AI-trained engines. SEP2's Email Security solution inspects metadata, attachments, links and language, as well as all historical communications, to determine prior trust relationships. It also inspects internal communication in real-time to prevent lateral attacks and insider threats. Combined with training the workforce, ensure that your attack surface is as small as possible.

Advanced Technical Protection

To ensure malicious threats never reach your users, this solution utilises patented inline flow technology powered by Check Point's Email Security. AI-trained engines block sophisticated attacks, including impersonation, Business Email Compromise (BEC), and zero-day phishing. By inspecting metadata, attachments, and historical communications, the system determines trust relationships in real-time, preventing lateral attacks and protecting internal communications across Microsoft Teams and Slack.

Check Point's Email Security is in both the Visionary and Leaders category (top right) of the Gartner Magic Quadrant for Email Security.

File-sharing security

Secure major file-sharing services (Google Drive, ShareFile, OneDrive, SharePoint, Box and Dropbox) from malware, ransomware, east-west attacks, and prevent accidental or malicious data loss.

Data Loss Prevention (DLP)

Enforce leakage policies across subject lines, bodies, and attachments to prevent the accidental or malicious sharing of sensitive data like credit card details.

Behavioural testing beyond the inbox

Evaluate user behaviour using USB sticks and QR codes to demonstrate that security risks exist outside of traditional email. Utilise the Security Awareness Proficiency Assessment (SAPA) to create tailored testing schedules weekly, monthly, or ad-hoc focused on your organisation's specific gaps.

Rapid Onboarding

Deployment is completed in as few as 7 clicks for Microsoft 365 and similar for Gmail users, with retroactive scans identifying existing threats within hours.

Service Support Packages - Delivered from SEP2's Leeds ISO27001 SOC

Human Risk Complete includes your choice of package from both Email Security and Security Awareness

EMAIL SECURITY			
FEATURES*	BASIC	STANDARD	ENHANCED
ANTI-PHISHING FOR INCOMING AND INTERNAL EMAILS	✓	✓	✓
KNOWN MALWARE PREVENTION (ANTI-VIRUS)	✓	✓	✓
MALICIOUS URL PROTECTION & RE-WRITING	✓	✓	✓
ACCOUNT TAKEOVER PREVENTION	✓	✓	✓
UNAUTHORISED APPLICATION DETECTION (SHADOW IT)	✓	✓	✓
MALWARE AND ZERO-DAY PROTECTION (SANDBOXING)	✓	✓	✓
ATTACHMENT SANITISATION (CDR, THREAT EXTRACTION)		✓	✓
EMAIL-BASED SUPPORT 10 REQUESTS INCLUDED		✓	✓
EMAIL-BASED SUPPORT UNLIMITED REQUESTS		✓	✓
EMAIL, PHONE AND TEAMS OR ZOOM-BASED SUPPORT UNLIMITED REQUESTS			✓

SEP2

SECURITY AWARENESS

FEATURES*	BASIC	STANDARD	ENHANCED
UNLIMITED PHISHING SECURITY TESTS	✓	✓	✓
AUTOMATED TRAINING CAMPAIGNS	✓	✓	✓
PHISH ALERT BUTTON & REPLY TRACKING	✓	✓	✓
AD, SCIM, SSO, SAML INTEGRATION	✓	✓	✓
MONTHLY EMAIL EXPOSURE CHECK	✓	✓	✓
OPTIONAL - KNOWBE4 STUDENT EDITION	✓	✓	✓
REPORTING, USER EVENT AND WEBHOOK APIS		✓	✓
SOCIAL ENGINEERING INDICATORS (SEI)		✓	✓
USB DRIVE TEST		✓	✓
SMART GROUPS		✓	✓
AI-DRIVEN PHISHING			✓
PASSWORDIQ* CHECK REUSED & WEAK PASSWORDS			✓
CALLBACK PHISHING			✓

ONLY AVAILABLE FOR THOSE USING ACTIVE DIRECTORY

To build a culture of security and empower your staff to defend your digital backbone, please get in touch at info@sep2.security.