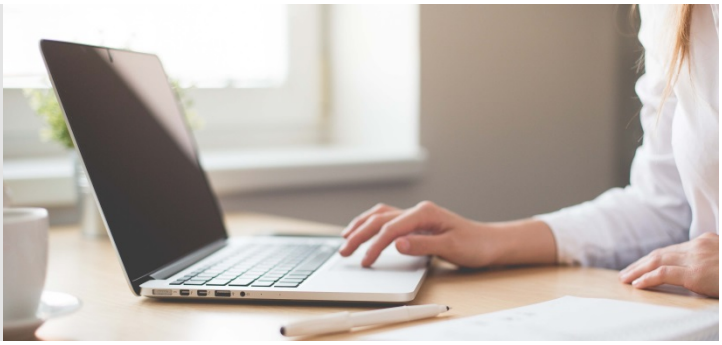
# CHECK POINT + CRYPTOPHOTO

## SOLVING HUMAN-FACTOR RISKS WITH ADVANCED TECHNOLOGY



### Mutual-Authentication and Signing with industry-leading AAL3-class assured strength.

The world's fastest and easiest high-security login solution is now available as an add-on to selected Check Point Software Blades.

### Product Benefits

- Block social-engineering of staff
- Prevent phishing attacks from working
- Neutralize credential-theft malware
- Accelerate and simplify secure logins
- Works reliably on all devices in every environment, online and offline too, with secure self-service and anti-bypass plus anti-downgrade built in

### Product Features

- NIST SP800-63-3 AAL3 verifier impersonation resistance compliance, the highest-strength login security available in the industry
- Cloud or on-premise solution
- High-security independent appliance mitigates server-side intrusion damage
- Easy-to-install, easy-to-use: self-service user setup and enrollment
- Isolated architecture separates identity from authentication, eradicates single-point-of-compromise risks and simplifies installation
- Broad security coverage delivers effective protection against 100+ security-risk, human-factor, and security-reducing user-experience and/or bypass/downgrade issues

## INSIGHTS

Today's users want internet accessibility everywhere they go, and they want it now. Cyber criminals know this. An estimated 9 out of every 10 cyber-intrusions are attributable to human factor risks like spear-phishing and social-engineering. Now more than ever is the time to fortify user and admin remote access to corporate resources with strong Multi-Factor Authentication (MFA).

## SECURE MOBILE ACCESS

With the Check Point Mobile Access Software Blade users can connect safely and easily to corporate applications over the internet with a smartphone, tablet or PC. Providing enterprise-grade remote access via both Layer-3 VPN and SSL VPN, end user connectivity to corporate applications is simple, safe and secure.

## CRYPTOPHOTO SOLUTION

Solving security is not just about technology. It's also about the user experience. Users embrace security that is fast, easy-to-use and strong. CryptoPhoto's rapid mutual-authentication and digital-signing add-on to the Mobile Access Software Blade delivers effective protection against human fallibility. Protection is extended to Check Point end users and system administrators. CryptoPhoto also supports access to the GAiA web UI fortifying administrator access to the Check Point device.

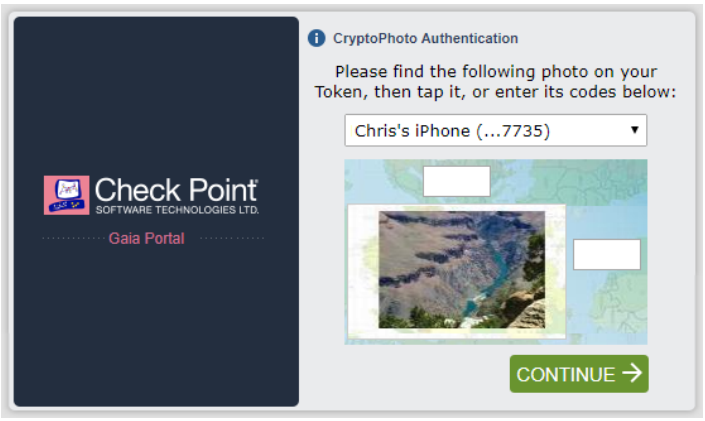
Unlike legacy 2FA techniques, CryptoPhoto is broadly effective against a wide variety of modern-day threats such as spear-phishing, social-engineering, scams, spoofing, man-in-the-middle attacks, and malware that steals credentials.

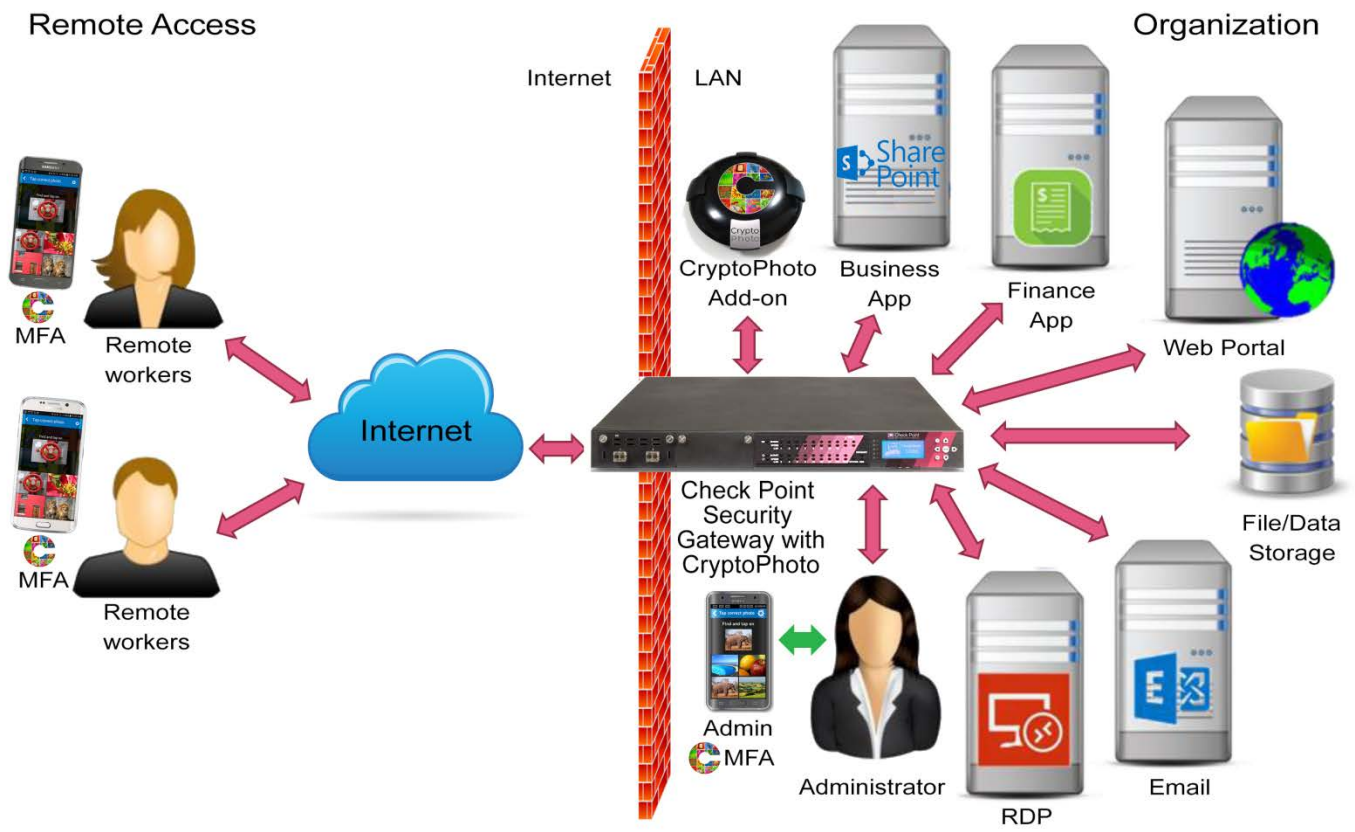
In addition CryptoPhoto complies with the industry's highest-rated Authenticator Assurance Level available: AAL3 (NIST SP800 63-3). Verifier impersonation resistance is a key requirement of this top rating. In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s).

The CryptoPhoto add-on for Check Point installs in minutes, supports self-service end-user enrollment, and comes with automatic configuration. CryptoPhoto's architecture includes independently-secured stand-alone authentication appliance(s), available as either on-premise real or virtual machine(s), or via subscription to CryptoPhoto's dedicated cloud. The mutual-authentication multi-factor component is available as a smartphone (or tablet) app (iOS, Android, Blackberry, and Windows Phone – including current-release and legacy device support), or physical component. In-device biometrics are optionally supported, or can be made mandatory to increase security and standards compliance. Secure self-enrollment, self-management, and secure self-service loss-handling are all included. Multi-device support allows users with more than one phone/tablet to enroll and use as many different authenticator devices as they may need, while reducing lost-device social-engineering risks.

## THE END USER EXPERIENCE

Trust is a two-way street. CryptoPhoto visually engages the user as part of a two-way second-factor authentication protocol, *preventing* human-factor exploits. During login, authorized machines prove authenticity to users by presenting a unique one-time secret, knowable only to the legitimate machine: a protected, one-time display of a random photograph. To complete login, the user taps the matching photo which automatically shows on their authentication device, typically a smartphone or tablet. The tap sends a private-key encrypted OTP directly to the predefined authentication endpoint, which auto-completes the login. The photo-match does not require user competence, attention, memory, or even training. It is not a CAPTCHA, but it does also block robots. Imposters are blocked from impersonating endpoints (AAL3). All attackers are blocked from stealing or guessing credentials. CryptoPhoto's visual mutual authentication does not rely on user education, understanding, or even competence. If a socially-engineered or systems attack is in progress, the user is simply unable to proceed. An AAL3-strength CryptoPhoto login typically takes just 2 seconds. Critical actions, like password updates, device reconfiguration, security changes etc. are additionally protected with out-of-band digital signatures (with multi-party approvals if desired). This blocks even high-level attacks like specialized malware and RATs from circumventing protection or exploiting sessions, and additionally provides non-repudiable user activity logs.




**Check Point Security Gateway with CryptoPhoto Add-on Installed**

CONTACT US

**Worldwide Headquarters** | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
**U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com