CHECK POINT + KEYLESS
ZERO TRUST PASSWORDLESS ACCESS

Benefits and Use Cases

Secure access with passwordless MFA

Ensure authorized and secure access to Check Point protected assets for remote users from anywhere, at any time, and on any device.

Security with improved user experience and privacy assurance

Reduces authentication friction and MFA fatigue - on any device, without compromising on UX.

Prevent unauthorized remote access using stolen credentials

Keyless embeds strong anti-fraud technology and behavioral authentication to minimize risk.

Quick and easy integration connects users to corporate applications

Connect Check Point and Keyless via standard SAML and RADIUS flows.

Hardware Agnostic

Since we do not rely on the device hardware or sensors, Keyless can be deployed on a large set of devices and appliances.

Unique Identification

On top of device authentication, Keyless natively identifies your user in every touchpoint, so you can make sure that the user logging in is the correct user

Today we live in a world where we are always connected, from any device, everywhere we go. With the proliferation of connected devices, the boundaries of the enterprise domain now extend beyond the corporate infrastructure. As a result of this surge in mobility, IT managers and security executives face enormous challenges to effectively secure access to company resources and Internet applications.

Now organizations can securely connect their remote workforce with zero trust passwordless access. Check Point provides the security. Keyless provides passwordless authentication, improving the user experience without compromising on security.

ADOPT A ZERO TRUST SOLUTION

Check Point combined with Keyless passwordless authentication enables enterprises to secure access to Internet applications and their corporate resources. Users establish a remote access connection by connecting to a Check Point Next Generation Firewall, either on-premises, in a private or public cloud, or as a service in a Secure Access Service Edge (SASE) deployment.

Keyless integrates with Check Point using SAML or RADIUS to provide users with zero-knowledge biometrics (ZKB) as an additional authentication factor. Customers can also fully embrace passwordless authentication with Keyless next-gen privacy-preserving biometrics access to Check Point Virtual Private Networks (VPN) and SASE protected applications.

THE KEYLESS VALUE

Keyless eliminates the need for businesses to store and protect biometric data, passwords, personal cryptographic keys and other sensitive information without compromising on convenience and privacy. Keyless replaces something you need to remember, with who you are by pioneering in privacy-preserving biometrics.

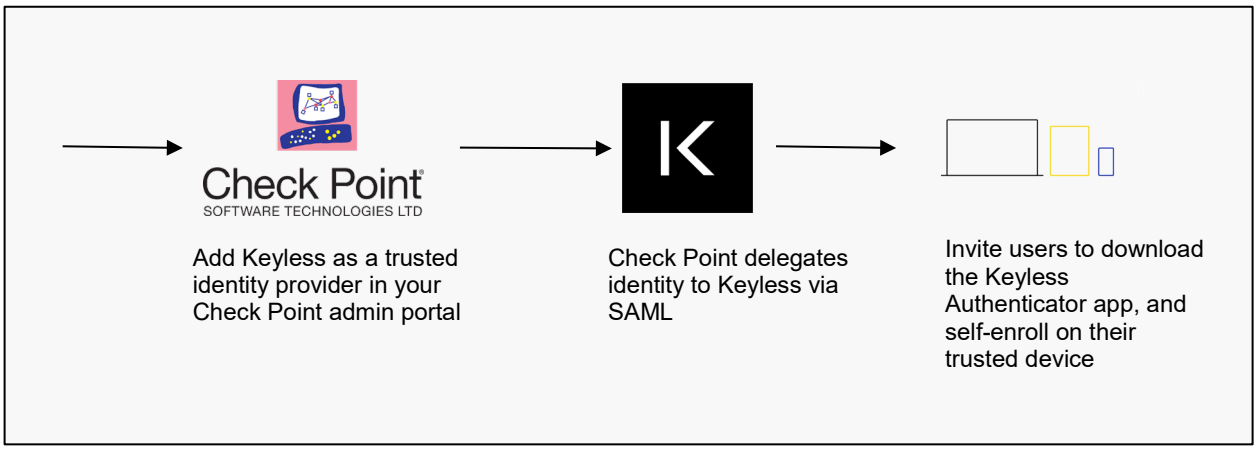
SECURE ACCESS WITH CUTTING EDGE TECHNOLOGY

Passwords are a prime target of threat actors and phishing is a predominant tool used by them to trick users into giving up their credentials. With a person's username and password they have their same access and may be able to impersonate them and send emails as that person in hopes of tricking another employee in a Business Email Compromise (BEC) attack.

Enhance employee experience and protect their privacy through passwordless multi-factor authentication and eliminate fraud, phishing and credential reuse. With Keyless, strong multi-factor authentication connects users to Check Point solutions without compromising on user experience, privacy or security.

DEPLOY IN JUST 1 HOUR

Keyless is a cloud-native solution that employs standard SAML and RADIUS flows. To get started with the SAML integration, simply add Keyless as a trusted Identity Provider in the Check Point portal. The integration requires only a few quick configuration settings within Check Point and does not require any coding. When an end user requests access to an enterprise application or a consumer facing application, Check Point will delegate authentication responsibilities to Keyless.



Check Point Keyless SAML Integration Flow

Keyless Check Point RADIUS Integration

RADIUS is another method to authenticate to Check Point connected devices using a Keyless RADIUS appliance. This can be used to connect to Check Point VPN as well as an SSL VPN Mobile Access portal enabled on a Check Point Next Gen Firewall. To get started with the Keyless RADIUS integration, start by setting up Keyless as a RADIUS server in the Check Point SmartConsole. The full integration steps are documented on the Keyless site shown below.

docs.keyless.io/workforce/vpn/check-point-vpn

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

ABOUT KEYLESS

Keyless is a deep-tech cybersecurity company that offers privacy-first passwordless authentication and personal identity management solutions for the enterprise. They are the first to combine multi-modal biometrics with privacy-enhancing technologies and a distributed cloud network. Keyless' proprietary technology eliminates the need for businesses to centrally store and manage passwords, biometric data, and other sensitive personally identifiable information.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan 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: 650-628-2117 | www.checkpoint.com