



Applying Zero Device Trust to Secure Workforce Access Verification

Executive Summary

Infinipoint and Check Point have partnered to deliver a comprehensive security solution that ensures secure workforce access by integrating Zero Device Trust into the Workforce Access Verification Process.

This collaboration enhances traditional identity-centric security with deep insights into the connecting device, verifying its identity, security posture, and compliance before and during every session. By combining Infinipoint's advanced device security capabilities with Check Point's industry-leading network security, organizations can enforce true Zero Trust access, prevent account takeovers via phishing, MFA fatigue attacks, and maintain seamless productivity through intelligent, automated remediation.

The Challenge: Securing Access in a Device-Driven World

Today's distributed workforce and the increasing sophistication of cyber threats demand a more holistic approach to access security than relying solely on user authentication. Even with strong user authentication, compromised, vulnerable, or unmanaged devices can be exploited to gain unauthorized access to critical resources. Organizations need to ensure that both the user and the device accessing their systems are trusted and secure. This requires a solution that goes beyond verifying "who" is accessing resources to also validate "what" device is being used and its security standing.

Introducing the Infinipoint + Check Point Solution: Comprehensive Access Security with Device Trust

Our joint solution provides a powerful and seamless way to achieve secure workforce access by extending Check Point's access controls with Infinipoint's advanced device trust capabilities. This integration ensures that every access request is evaluated based on both the user's identity and the security integrity of their device.

How It Works:

1. Device Identification and Authentication:

Infinipoint uniquely identifies and authenticates the connecting device, ensuring it is a known and approved device for the user. This establishes a foundation of device trust from the moment of login.

2. Deep Device Posture Verification: As part of the Check Point user access flow, Infinipoint performs a comprehensive, real-time evaluation of the device's security posture. This includes examining:

- Operating system configuration and updates
- Installed security agents and their status
- Critical vulnerabilities and patch levels
- Browser and application security settings
- Presence of risky software or configurations
- Compliance with organizational security policies

3. Adaptive Access Enforcement: Leveraging the rich device context provided by Infinipoint, Check Point dynamically enforces granular access policies. This allows organizations to:

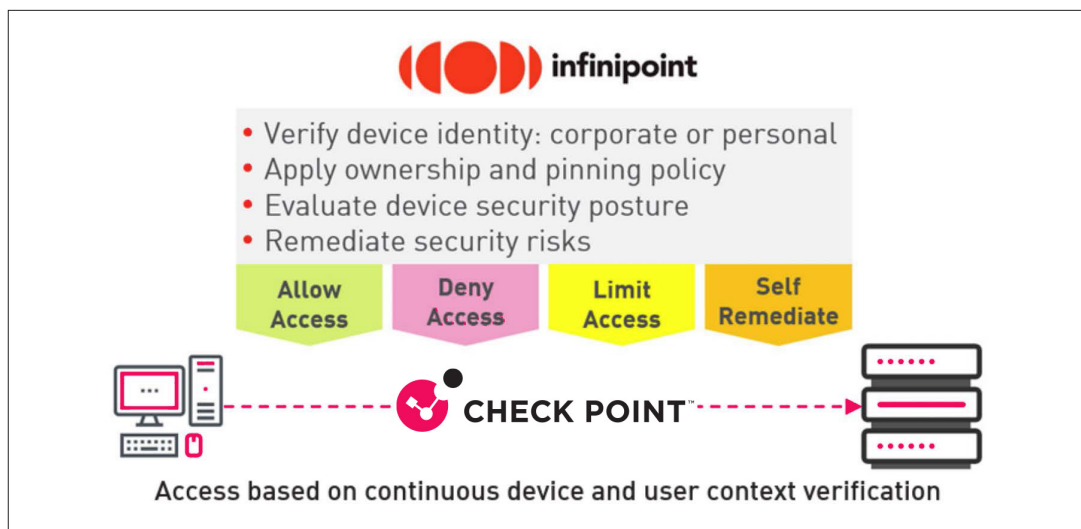
- Grant full access to trusted and compliant devices.
- Limit access or restrict specific actions (e.g., file downloads) for devices with medium risk.
- Block access entirely for high-risk or unrecognized devices.

4. Continuous Compliance and Verification:

Unlike point-in-time checks, our integration continuously monitors device security posture throughout the user session. If a device falls out of compliance, Check Point can automatically adjust access privileges in real-time, ensuring ongoing security without disrupting legitimate user workflows.

5. Intelligent, In-Flow Remediation:

When devices are found to be non-compliant, Infinipoint offers users intuitive, self-service remediation options directly within the access flow. This empowers users to quickly resolve common security issues (e.g., installing security agents, updating software) and regain secure access, minimizing IT intervention and maximizing productivity.



Key Benefits of the Integrated Solution:

- **Phishing-Resistant Access:** By verifying both the user and their trusted device, the solution significantly reduces the risk of account takeovers resulting from phishing and MFA bypass attacks. Access requires not just user credentials but also a secure and recognized device.
- **Granular Device-Based Access Control:** Organizations gain precise control over which devices can access sensitive resources, based on device ownership, type, and security posture. This minimizes the attack surface and prevents unauthorized device access.
- **Continuous Adaptive Security:** Access policies dynamically adapt based on the real-time security posture of the device, ensuring ongoing protection without hindering user productivity.
- **Automated, User-Friendly Remediation:** Empower users to resolve security issues independently with one-click remediation, reducing IT workload and ensuring continuous access for legitimate users.
- **Comprehensive Coverage:** The solution supports a wide range of devices (corporate and personal, laptops, desktops, mobile devices) and operating systems, providing consistent security for the entire workforce, including employees and third-party contractors.
- **Simplified Zero Trust Implementation:** By seamlessly integrating device trust into the access flow, the solution makes it easier to implement a robust Zero Trust security model without complex integrations or disruptions.

Use Cases:

- **Enhanced Protection Against Account Takeovers:** Prevent successful phishing attacks and MFA bypass attempts by ensuring only trusted and compliant devices can gain access, even with compromised user credentials.
- **Secure Access for BYOD Environments:** Enable secure access from personal devices by enforcing robust device security policies and providing users with the tools to maintain compliance.
- **Conditional Access to Sensitive Data:** Restrict access to critical applications and data based on granular device security posture, ensuring only healthy and compliant devices can access sensitive resources.
- **Automated Enforcement of Security Policies:** Automatically verify and enforce a wide range of security policies on devices at the point of access and continuously throughout the session.
- **Streamlined Compliance and Audit:** Gain comprehensive visibility into device security posture and access events, simplifying compliance reporting and audits.

The Path Forward: Secure Access with Confidence

The integration of Infinipoint and Check Point delivers a powerful solution for achieving true Zero Trust access by extending security beyond user identity to encompass the critical element of device trust. By ensuring that every access request originates from a verified, secure, and compliant device, organizations can significantly strengthen their security posture, prevent sophisticated attacks, and empower their workforce with seamless and secure access.

For more information on how Infinipoint and Check Point can help your organization secure workforce access, please contact your respective representative today.

#ZeroTrust #Cybersecurity
#DeviceSecurity

#AccessControl
#Infinipoint #CheckPoint

#SecureAccess
#WorkforceSecurity

About Check Point Software Technologies Ltd

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Core Services for collaborative security operations and services.

About Infinipoint

Infinipoint is an Identity and Access Management (IAM) security platform delivering secure workforce access to all applications, for any user and device, from anywhere. Its Zero Trust Architecture combines phishing-resistant authentication with comprehensive device posture verification and one-click remediation. Protect your organization against sophisticated threats including phishing attacks, MFA bypass attempts, and account takeovers by preventing access from unknown and risky devices. Infinipoint Zero Device Trust ensures robust security while maintaining a seamless login experience for your end users.

Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters

100 Oracle Parkway, Suite 800 Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com