Check Point + Infinipoint

Applying Device Identity to Zero Trust Access Verification

Infinipoint Device-Identity-as-a-Service (DIaaS) works with Check Point to deliver a comprehensive security solution for Zero Trust device access.

Infinipoint complements Check Point by integrating device state, risk-based policies, and one-click remediation for non-compliant devices. Verify device security posture, extend adaptive access, and enable auto-remediation as part of user authentication.

Insights

The increase in remote workers coupled with an increase in cyber-attacks has elevated urgency around a Zero Trust security approach for secure device access. Zero Trust reference architectures from the U.S. DOD, NIST and others are prioritizing more granular security controls for user devices to protect critical data and services.

With users accessing IT resources via new access solutions such as Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE), even the strongest user authentication is insufficient on its own. A comprehensive device security posture is now required to ensure devices connecting to IT services have the right level of security and have been verified as compliant with security policy. This includes context-aware policies that can identify devices that are compromised, have known vulnerabilities, or are not managed by the enterprise.

SOLUTION BENEFITS

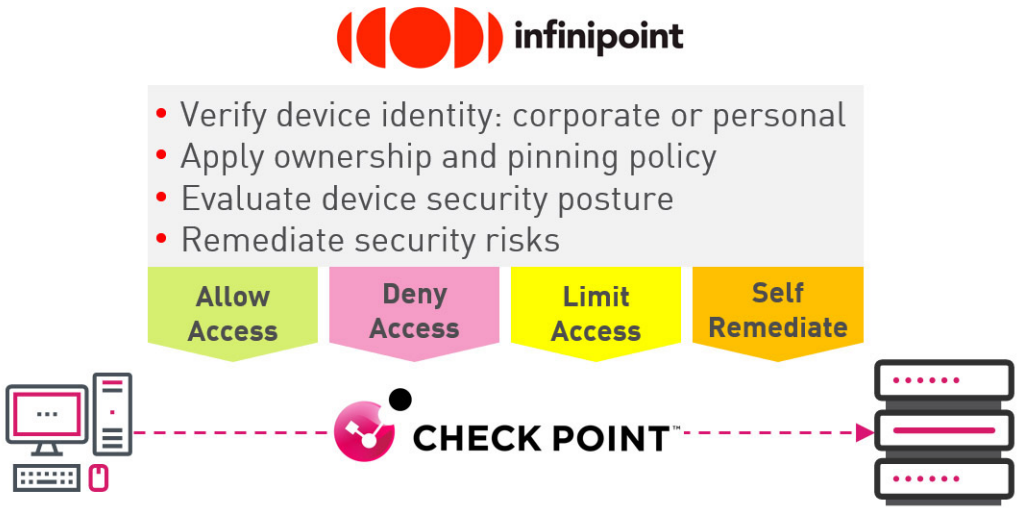
- **Enforce a true Zero Trust, phishing resistant user and device access policy**
- **Control access to sensitive data and applications for non-compliant devices**
- **Enable continuous adaptive access control based on granular device context**
- **Automate remediation for non-compliant devices**

© 2023 Check Point Software Technologies Ltd. All rights reserved.

Joint Solution

Infinipoint ensures endpoint devices are secure and continuously compliant when connecting to services via Check Point. Infinipoint performs a device identity and security posture check as part of the Check Point user access flow. This includes validating the Check Point Secure Configuration Verification (SCV) and identifying devices and users via Single Sign-On (SSO).

Infinipoint extends Check Point adaptive access controls, enabling conditional, granular policies for access based on device identity policies, for example, providing full cloud resource access to compliant devices, and blocking or limiting access to cloud services and data for non-compliant devices. Device identity policies managed by Infinipoint are based on rich context such as critical vulnerabilities, OS firewall settings, browser extensions, certificates, installed software, and more. Infinipoint also enables 1-click remediation for non-compliant devices, including installation of EPP/EDR agents. The result is an adaptive Zero Trust approach to device access while maintaining business continuity with no disruption to the workforce.



Access based on continuous device and user context verification

Use Cases

CONDITIONAL ACCESS: Ensure only compliant devices access sensitive services and data. For example, create a device policy where only devices with the latest Windows/macOS security update are allowed access.

ADAPTIVE ACCESS: Govern access permissions based on device context. For example, allow access but prevent files from being downloaded or restrict access to specific assets for non-compliant devices.

© 2023 Check Point Software Technologies Ltd. All rights reserved.

AUTO-REMEDIATION: Easily bring user devices to a secure, compliant state by enabling self-service remediation. For example, enable 1-click installation of a Check Point client for unmanaged devices.

USER OWNERSHIP AND PINNING POLICIES: Create user profiles of the types and number of devices pre-approved per user, to access data and services. For example, preconfigure that User X can access from one corporate device, one non-corporate device and one mobile device. Anything outside of this, would be blocked on access and require specific admin permission to access. This enables "anti-phishing" capabilities, as the system would identify out of the box, if a request to connect is originating from an unknown device or a wrong URL.

FULL EMPLOYEE & 3RD PARTY COVERAGE: Coverage includes both employee and any 3rd party (e.g., contractors, etc.) as well as connecting from every common device - whether corporate device, non-corporate device, tablet or mobile (iOS or Android).

About Check Point

Check Point Software Technologies Ltd. (www.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 Infinipoint

Infinipoint (infinipoint.io) provides a cloud-based security platform that protects access to all applications, for any user and device, from anywhere. Infinipoint is designed to be both easy to use and deploy while providing complete device visibility and control. Infinipoint verifies users' identities paired with deep insights into your users' devices, Infinipoint gives you the policies and controls you need to limit access based on users and their devices. Users get a consistent login experience with Infinipoint's Single Sign-On (SSO) that delivers centralized access to both on-premises and cloud applications. With Infinipoint, you can protect against risky devices, as well as unwanted access to your applications and data. This combination of user and device trust builds a strong foundation for a zero-trust security model.

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

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com

© 2023 Check Point Software Technologies Ltd. All rights reserved.