CHECK POINT + ARUBA
SECURE YOUR MOBILE WORKFORCE

SECURE YOUR MOBILE WORKFORCE

- Create a secure business environment and enable mobile and guest access
- Context is shared for end-to-end policy enforcement and visibility
- Block or quarantine users and devices from within and outside of the network
- Remediate compromised or vulnerable devices

INSIGHTS

Mobility has quickly changed the notion of fixed perimeter security. Enterprise users are no longer confined to office buildings with desktop clients connected to Ethernet ports for access. As user behavior has changed, security for the enterprise has also had to shift to a more granular approach that includes identifying the user, device, and location.

As many attacks now target both the intranet and the perimeter, the importance of traditional perimeter security solutions is shifting. Hackers have capitalized on the BYOD phenomenon by targeting users, who may have unsecure devices with suspect apps on the network, and may be unaware of the security implications.

The result of risky BYOD behavior has resulted in many high profile enterprise breaches. In the past, virtually all breaches came from outside the network, but a shift to target the weakest link in the security chain requires a new way to enable actionable enforcement to contain threats. Security must adapt to how users and businesses work today. A defense based on Adaptive Trust is needed.

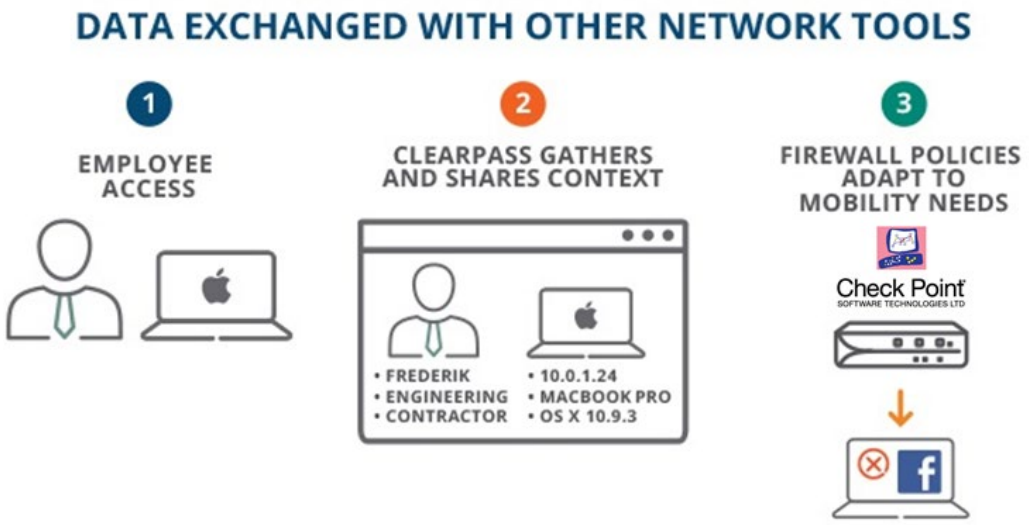
ADAPTIVE TRUST DEFENSE

Aruba ClearPass exchanges contextual information with Check Point to enable granular access control based upon user, group, device type, and location context. Our solution secures today's mobile workforce, providing defense based upon an Adaptive Trust model.

With granular user, device, and location information, along with contextual policies from ClearPass shared with Check Point Quantum Next Generation Firewalls organizations can extend perimeter security to take immediate action against new threats against mobile devices.

ARUBA CLEARPASS

Aruba ClearPass adds security at the user level via centralized authentication and authorization services. The ability to profile devices and capture granular user attributes creates a foundation for the exchange of usable data with a variety of third party solutions, like Check Point next generation security devices. This increased level of contextual information enhances visibility and allows the enterprise security perimeter and associated policies to extend to wherever the end user and device may roam.



CLEARPASS ATTRIBUTES

Check Point user attributes gathered from enterprise identity stores like Active Directory are extended with guest and visitor information from ClearPass to help control user sessions where the user data is held outside of normal enterprise IT resources. For example, if a user attempts to connect to a network with a personal device, ClearPass collects granular information about the user and the device. This information is then passed along to Check Point. At this point, Check Point Next Generation Firewalls will either allow or deny appropriate traffic types and then log the information. Furthermore, if there is any traffic or policy mismatch, the user and device can be quarantined from the network.

ClearPass Attributes Shared with Check Point	
Source IP	✓
Username	✓
User Role	✓
Domain	✓
Device Type	✓
Machine OS	✓
Machine Name *	✓

* Available from HTTP REST API calls, but not RADIUS

When user role context is collected at authentication, the ClearPass policy manager dynamically passes the device type, user profile, and location information to the firewall to ensure that policies are met even though a change in the user's posture, an expired device OS, user type, or other change occurs. We provide in-depth defense from threats both within and outside of the network.

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 ARUBA NETWORKS

Aruba, a Hewlett Packard Enterprise company, is the global leader in secure, intelligent edge-to-cloud networking solutions that use AI to automate the network, while harnessing data to drive powerful business outcomes. With Aruba ESP (Edge Services Platform) and as-a-service options, Aruba takes a cloud-native approach to helping customers meet their connectivity, security, and financial requirements across campus, branch, data center, and remote worker environments, covering all aspects of wired, wireless LAN, and wide area networking (WAN). To learn more, visit www.arubanetworks.com.

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