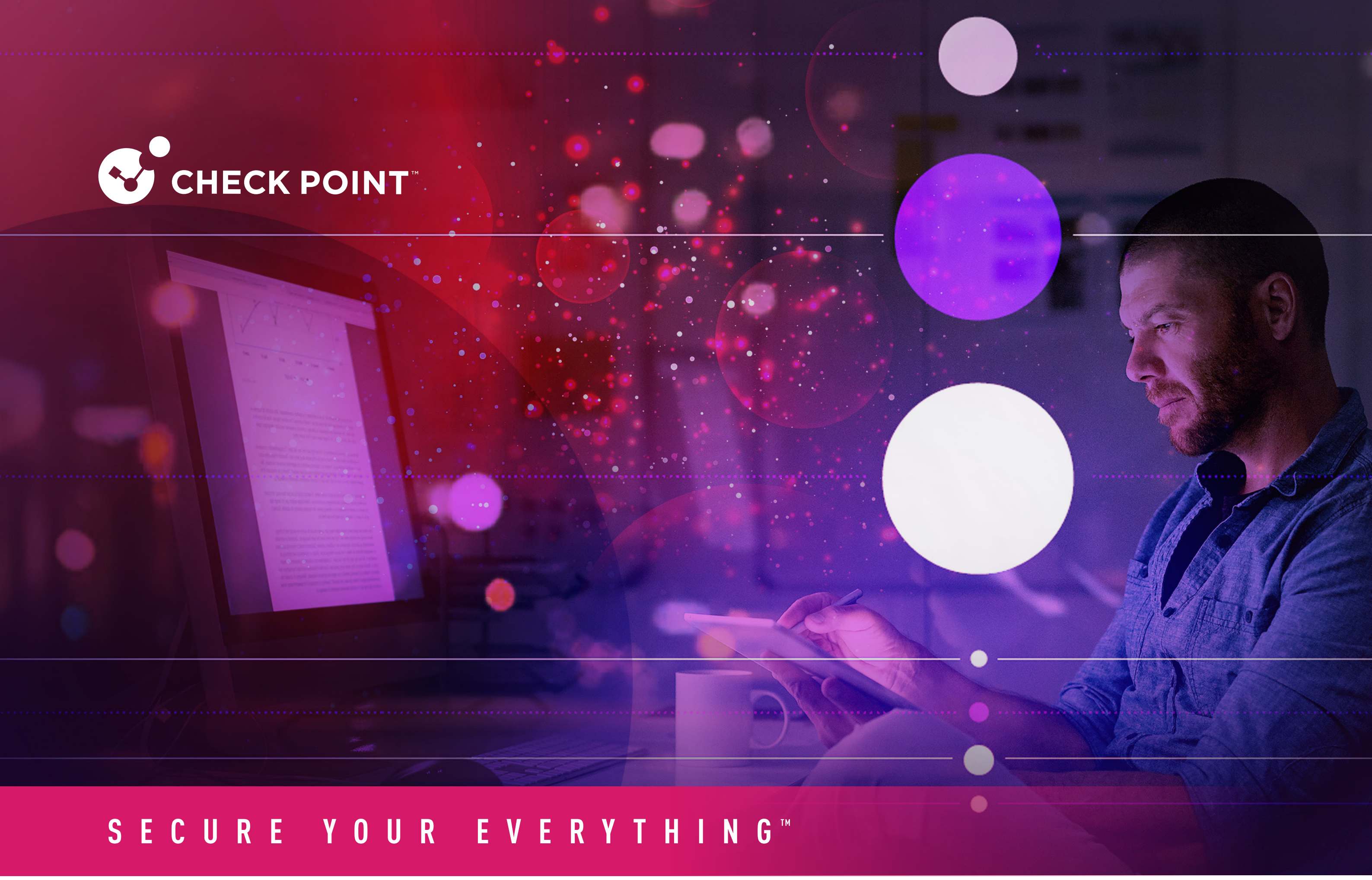


Network vs. Application Security in a Zero Trust World

Harmony Connect

Enterprises continue their rapid adoption of cloud-based technologies.

Many internal IT teams have found that integrating multiple cloud services with incompatible legacy IT environments has created complexities ranging from network interoperability issues to application, identity and access management security risks.

Common challenges associated with multi-cloud integration include assigning assets to different public or private cloud environments as well as integrating on-premise networks and third-party applications. Additional challenges include lack of visibility into cloud resources and lack of cloud security expertise with regulatory compliance and legal exposure.

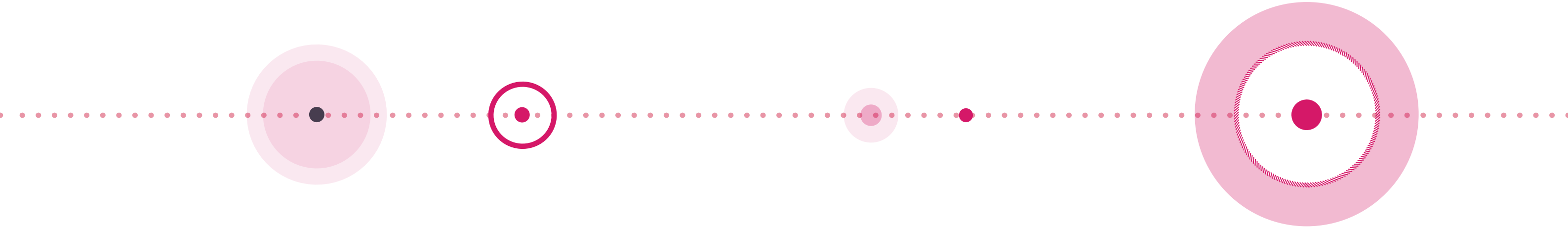
In a report released in April 2018, consulting firm McKinsey has noted that "most traditional IT environments adopt a perimeter-based, "castles and moats" approach to security, whereas cloud environments are more like modern hotels, where a keycard allows access to certain floors and rooms. Unless the legacy applications that have been developed and deployed for a castles-and-moats security model are reconfigured for the new security model, migrating to the cloud may have an adverse impact on cybersecurity."

Today, the security risk and impact of new cloud computing models has upended traditional application and network security paradigms, forcing organizations to re-think and re engineer their technology environments.

Network Security vs. Application Security

The idea of a corporate network perimeter has dramatically changed to the point of obsolescence.

Traditional network security defense has focused on scanning network traffic, ports and protocols, firewalls, intrusion prevention systems (IPS), secure web gateways (SWG), distributed denial-of-service (DDoS) protection and virtual private networks (VPN). However, with the adoption of decentralized corporate networks and cloud computing and the popularity of bring-your-own-device (BYOD) to work, the idea of a corporate network perimeter has dramatically changed to the point of obsolescence.



In today's new threat landscape, the perimeter is anywhere an access request is made, requiring new security models that mitigate security risks but also provide users with the access they need from anywhere and on any device. To mitigate against the security risks created by this new work environment, organizations are beginning to adopt zero trust security architecture that moves access control decisions from the network perimeter to individual devices, users, and applications, where business-driven security policies and access controls are best enforced. Zero trust starts with the premise that all devices and entities are untrustworthy until proven otherwise. Administrators should factor in contextual data about the device, the environment and the nature of the request, in order to make an access decision and then only grant as much access as is necessary for a person to do their job. Zero trust has also blurred the distinction between network security and application security. Afterall, what is network security when the traditional notion of a network is being questioned?

By 2021, 60% of enterprises will phase out network VPNs...

Traditional network security still does have a place in hybrid, multi-cloud IT environments but the increased need for visibility and granular access controls to every resource on a network means that securing applications combined with authorized access is critical.

Traditional application security includes web application firewalls, enterprise application security, database security, email security, web browser security, and mobile application security. Add to that public cloud application security, virtual machine security, container security, and IoT security, and the application security landscape starts to become quite complex.

When migrating workloads to the cloud, legacy applications must be upgraded or re-factored to meet public or hybrid cloud security requirements. According to McKinsey, "existing applications will need to be refactored at the infrastructure and application layers to align with the security and capacity requirements of the public cloud. Security must be baked into these applications, and they must work in a more automated fashion. This requires significant attention from application teams, which can be hard to get."

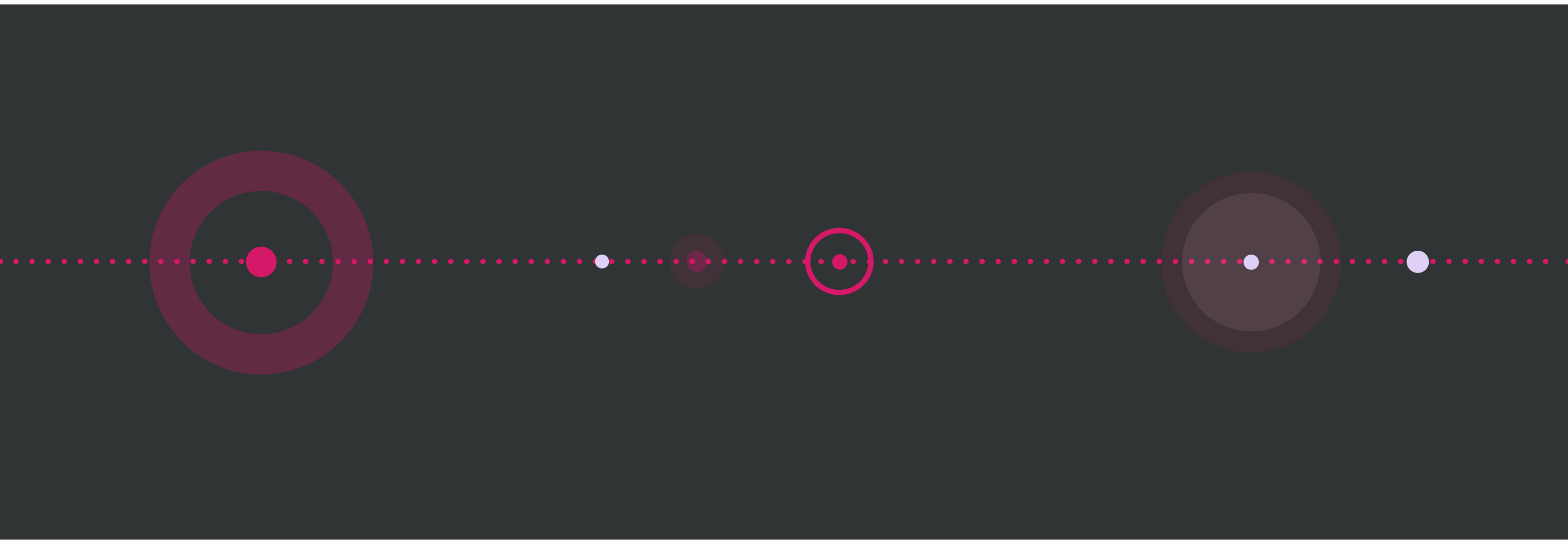
For security teams to create business cases for both legacy-application modernization and zero trust network security, they must highlight to executive management the high cost of data breaches not only from a technology standpoint but also an operational, brand marketing, customer and a legal perspective as well.

Migrating to a Zero Trust Security Model

Zero Trust is a security mindset that denies any network, application or resource access attempt inside or outside private or public network unless explicitly authorized.

The security concept is sometimes linked with another concept known as least privilege access where users and entities are only given the least privilege that is required to perform needed network or application functions, directly impacting both network and application security.

The zero trust security model matters in today's cloud-first world in that it improves control for IT and DevOps engineers by enabling active network and application access management on a continuous, real-time basis. It also reduces attack surfaces by only providing access to resources that have been authorized so that users cannot move laterally from one application or network segment to another. And risk is mitigated with Zero Trust by forcing all resource access to be regularly validated with continuous monitoring, improving overall visibility.



Key Zero Trust Concepts

Internal Threat Consideration

Network locality is no longer sufficient for determining trust in a network. Assume that external and internal threats exist on your network at all times.

Granular, Limited Access

Access to applications does not require access to the entire network. Users should only have granular connectivity to applications on a need-to-know basis and for a limited period of time.

Authenticate First, Connect Second

Every device and user attempting to access an application must first be authenticated and authorized. Authentication is based on contextual user attributes like credentials, device ID and state, time, location etc.

Network Blackening

External users, as well as internal users, should not be aware of unauthorized applications. Unauthorized resources should not only be inaccessible, they should be completely invisible.

Harmony Connect Remote Access – A Zero Trust Security Solution

The latest US Department of Defense's Digital Modernization Strategy report states that "the assumption zero trust makes - that you are compromised is particularly suited to cloud infrastructures" and is on their IT security implementation roadmap.

However, "the actual implementation and operationalization of zero trust has significant complexity in areas that include "identifying which data, applications, assets, and services to protect, and mapping transaction flows, policy decisions, and locations of policy enforcement."

Moving over to zero-trust is a major undertaking and Harmony Connect Remote Access solves the hardest parts. Its zero-trust architecture moves access control decisions from the network perimeter to individual devices, users, and applications where business-driven security policies and access controls are enforced, providing complete visibility across all network activity. Harmony Connect Remote Access is purpose built to give the fact that end users need frictionless access from any device and any location, but treats every access attempt as suspect until both the user and device have been authenticated and authorized.

Benefits of using Harmony Connect Remote Access include:

- Centralized management where access policies can easily be adjusted, enabling the addition of new applications, data centers, employees and contractors effortlessly.
- Full network access visibility for all network traffic for users, devices, locations, and applications.
- Reduced network attack surfaces.
- Limits on lateral user movement by blackening every unauthorized resource to prevent attackers from crawling the network.
- Elimination of credential theft by verifying users by multiple authentication factors such as device ID, location, time of day and user behavior.
- Encrypted traffic end-to-end and eliminates DDoS attacks by removing organizational DMZ internal and external resource protection.

Organizations of all sizes are looking to zero trust security platforms, like Check Point Corporate Access.

As cloud computing evolves and organizations continue their digital transformations away from legacy IT systems to hybrid and public cloud environments, traditional application and network security solutions are proving to be a real disadvantage when it comes to security, compliance and scalability. Organizations of all sizes are looking to zero trust security platforms, like Harmony Connect Remote Access, to reduce the operational complexity and mitigate against security risks.

Harmony
Connect

Discover Harmony Connect

Harmony Connect is part of the Check Point Harmonyproduct suite, the industry's first unified security solution forusers, devices and access. Harmony consolidates six products to provide uncompromised security and simplicity for everyone. It protects devices and internet connections from the most sophisticated attacks while ensuring Zero-Trust Access to corporate applications - all in a single solution that is easy to use, manage and buy.

Harmony Connect is redefining SASE making it **easy** to secure access to **corporate applications, SaaS and the internet** for any user or branch, from any device, without compromising on security.

To learn more, **contact us for a demo** or visit us at **checkpoint.com**.

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