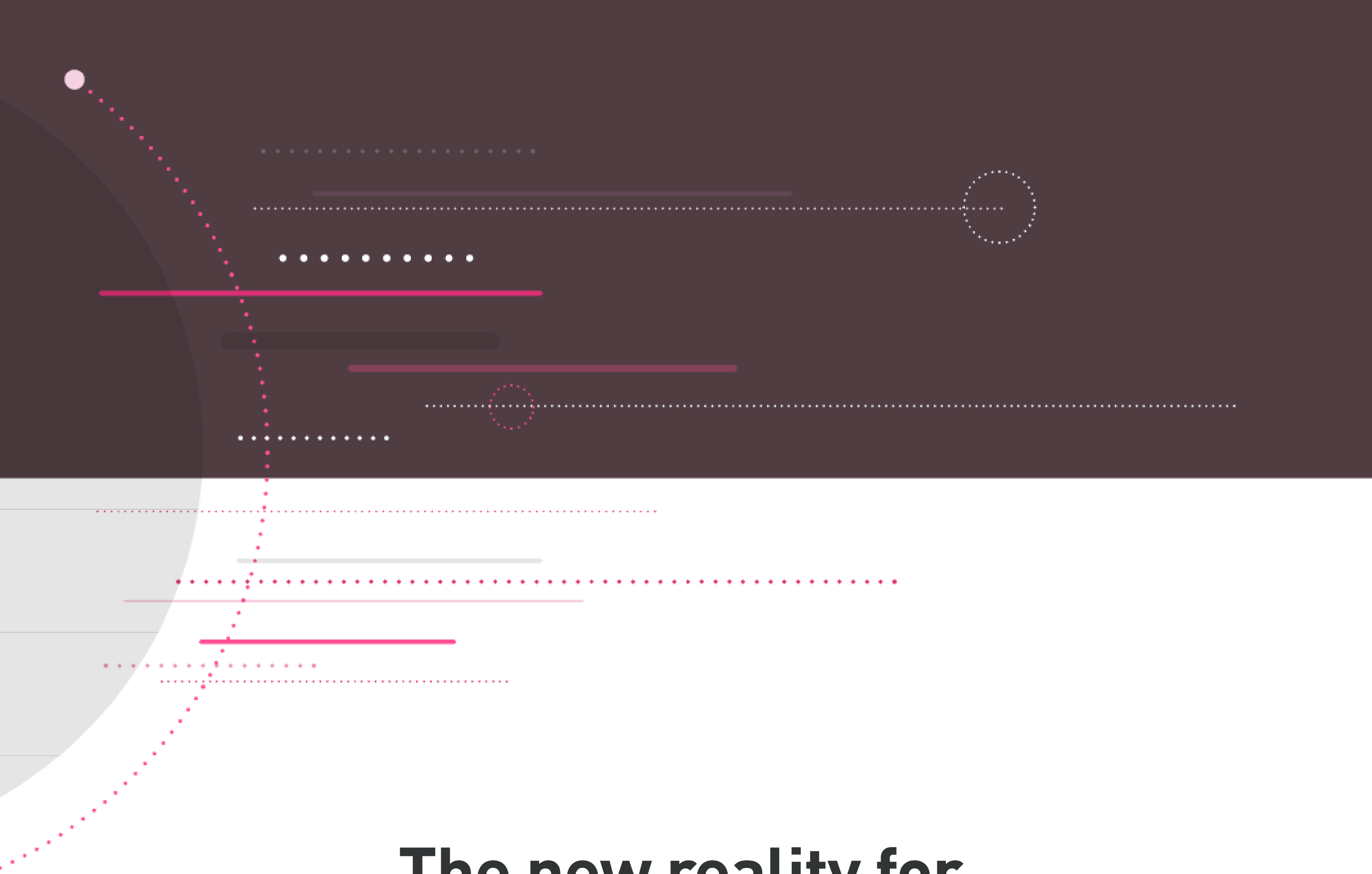
SECURE YOUR EVERYTHING™

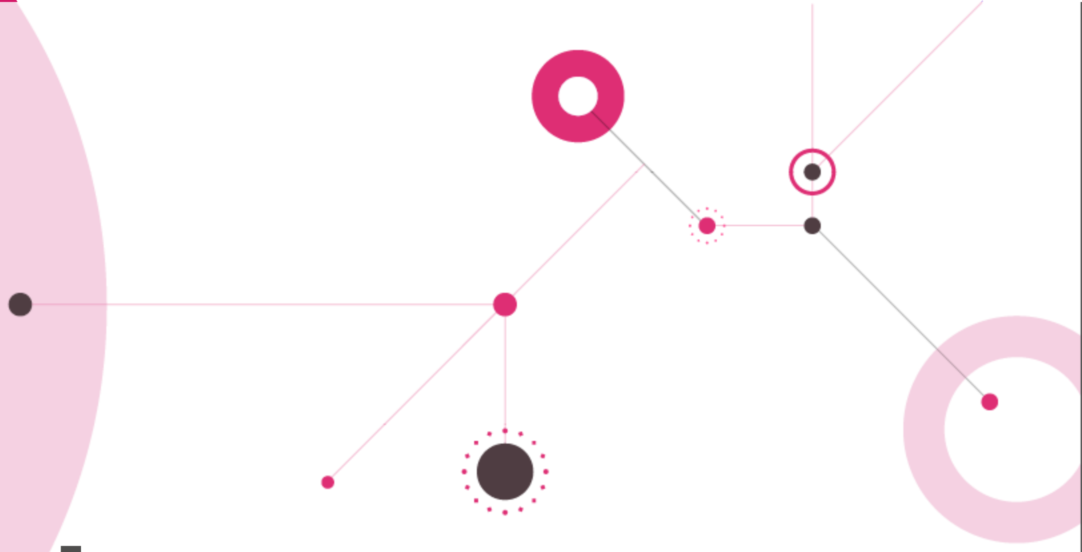
6 Best Practices
for Zero Trust Corporate Access

Harmony
Connect



The new reality for IT and DevOps engineers is defined by the cloud, mobility, and increasing demands for agility.

In this new landscape, the traditional "perimeter-based" security model is not aging well and binary access tools like VPNs, firewalls, and jump servers are proving to be cumbersome and unscalable. Working environments are no longer governed by fixed perimeters. Users work off their own devices and sensitive company data is stored in third-party cloud services. Companies can no longer rely on binary security models that focus on letting good guys in and keeping bad guys out. For modern enterprises, the challenge is how to give users the access they need while reducing set-up and maintenance costs and without compromising security.



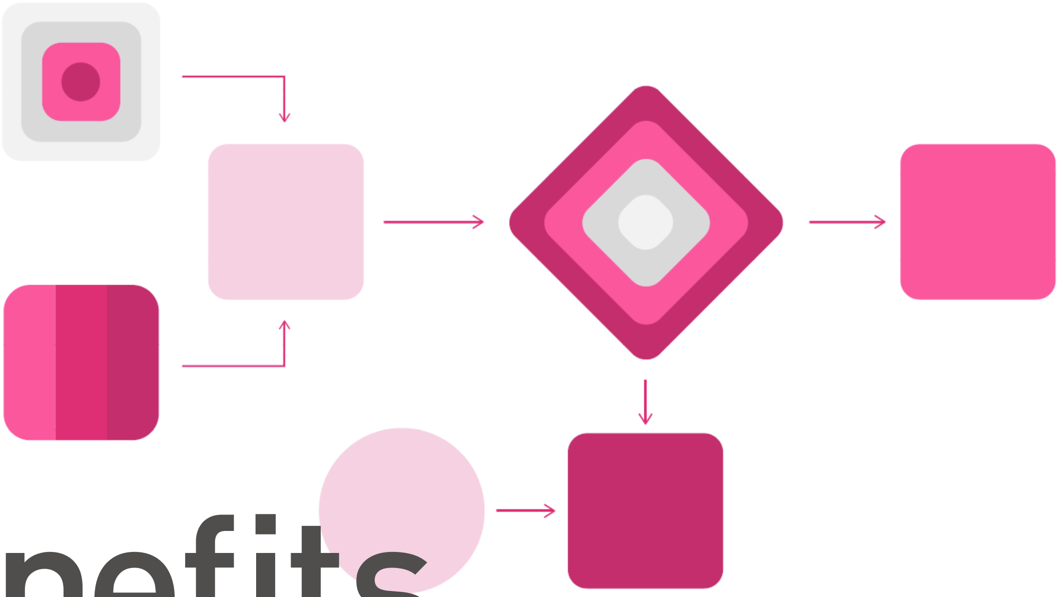
What is Zero Trust?

If traditional network access is rooted in the principle of "trust but verify," zero trust access is rooted in the principle of "never trust, always verify".

What does this mean? If we think of network like a nightclub, then traditional network access is like having the host confirm your reservation and simply open the door, zero trust access is like having the host confirm your reservation (using multiple IDs) and then having someone escort you to your table.

The zero trust model says:

- Do not automatically trust anything (inside or outside your network).
- Verify the person requesting access, the context of the request, and the risk of the access environment prior to granting access.
- Give users only as much access as needed and eliminate network exposure.
- Utilize micro-segmentation to break up the perimeter and create small zones with separate access for each.
- Require more than one piece of evidence to authenticate a user.



Benefits of Zero Trust

Improves Control

Without zero trust, access is not actively managed on a continuous basis.

Reduces the Attack Surface

By only providing access to resources that have been authorized, it is less likely that an attacker can move laterally from one segment to another.

Helps to Manage Risk

Not implicitly trusting every user and resource and forcing all access to be regularly validated means that risk is managed.

Adds Visibility

Without zero trust, access is simply a matter of having the right credentials Zero trust networks provide context aware security that continuously monitors multiple variables, helping to improve overall visibility.

6 Best Practices for Zero Trust Corporate Access

Zero trust security is not a product, it's a process.
Below are six best practices that organizations should observe on the path to zero trust security.

1 Verify all users with multi-factor authentication (MFA)

It is often said that zero trust is rooted in the principle of "never trust, always verify." But, properly implemented, is it more accurate to say that zero trust is rooted in the principle of "never trust, always verify and verify again." Gone are the days where a username and password would be enough to validate a user's identity. Today, these credentials must be fortified using multi-factor authentication (MFA). Additional authenticating factors may consist of one or more of the following:

Something you know

This can be a password, a security question, a PIN, zip code, or any other piece of information that is personal.

Something you have

Usually a verification SMS, a prompt sent to your phone, generated codes in authenticator apps, a hardware token, etc.

Something you are

This can be a biometric such as a fingerprint scan, retina scan, face scan, or voice.

When implementing zero trust architecture, the identity of every user accessing your network (privileged user, end-user, customers, partners…) should be verified using multiple factors. And these factors can be adjusted depending on the sensitivity of the data/ resources being accessed.

2 Verify all devices

Verifying your users is necessary but not sufficient. The principles of zero trust also extend to endpoint devices. Device verification includes ensuring that any device used to access your internal resources meets your company's security requirements. Look for a solution that allows you to track and enforce the status of all devices with easy user onboarding and offboarding.

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

Gartner

3 Implement the Principle of Least Privilege

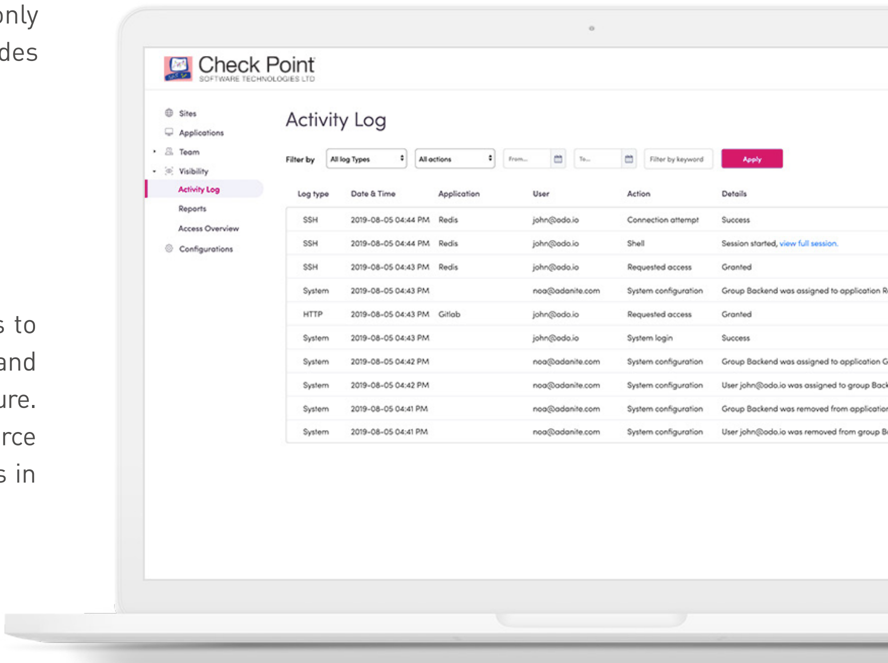
The principle of least privilege (PoLP) it determines what you can access in a zero-trust environment. It is based on the idea that a particular user should only be granted just enough privileges to allow them to complete a particular task. For example, an engineer who only deals with updating lines of legacy code does not need to access financial records. PoLP helps contain the potential damage in the event of a security compromise.Least privilege access can also be expanded to include "just in time" privileged access. This type of access restricts privileges to only the specific times when they are needed. This includes expiring privileges and one-time-use credentials.

5 Adopt Attribute-Based Controls

Use attribute-based controls to authorize access to resources across your security stack – from cloud and on-prem applications, to APIs, to data, and infrastructure. These will let the administrator easily adjust and enforce access policies in order to block suspicious events in real-time.

4 Monitor & Audit Everything

Apart from authenticating and assigning privileges, you should also monitor and review all user activity across the network. This will help identify any suspicious activity in real time. Visibility is especially important for users who have administrative rights due to the sheer scope of their access permissions and the sensitivity of the data they can reach.



Activity Log

Log type	Date & Time	Application	User	Action	Details
SSH	2019-08-05 04:44 PM	Redis	john@odo.io	Connection attempt	Success
SSH	2019-08-05 04:44 PM	Redis	john@odo.io	Shell	Session started, view full session.
SSH	2019-08-05 04:43 PM	Redis	john@odo.io	Requested access	Granted
System	2019-08-05 04:43 PM		noa@adanite.com	System configuration	Group Backend was assigned to application R
HTTP	2019-08-05 04:43 PM	Gitlab	john@odo.io	Requested access	Granted
System	2019-08-05 04:43 PM		john@odo.io	System login	Success
System	2019-08-05 04:42 PM		noa@adanite.com	System configuration	Group Backend was assigned to application G
System	2019-08-05 04:42 PM		noa@adanite.com	System configuration	User john@odo.io was assigned to group Back
System	2019-08-05 04:41 PM		noa@adanite.com	System configuration	Group Backend was removed from applicatio
System	2019-08-05 04:41 PM		noa@adanite.com	System configuration	User john@odo.io was removed from group B

6 Consider your end users

Don't let the perfect be the enemy of the good. Implementing the perfect zero trust strategy that your end-users hate to use is not a very good strategy. You end-users just want to work. Consider a strategy and products that create the most frictionless and SaaS-like experience for your team.

Harmony Connect Remote Access Model

As you outline your own organization's zero trust roadmap, consider Harmony Connect Remote Access — Check Point's agentless, zero trust access platform.

Discover Harmony Connect

Harmony Connect is part of the Check Point Harmony product suite, the industry's first unified security solution for users, 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**.

Harmony Connect Remote Access is the most simple and secure way to provide access to internal resources. The solution helps modern enterprises cover major aspects of zero trust like segmentation and privileged access with ease while providing all other elements from verification to real-time alerts regarding suspicious activities.

Some of the benefits to implementing Harmony Connect Remote Access include:

- Eliminating network layer access.
- Visibility into all user activity.
- Reducing time-to-breach detection.
- Minimize the time and energy IT and DevOps engineers spend maintaining infrastructure.
- A more streamlined security stack.
- Eliminating the need for users to remember complex passwords and re-authenticate throughout the day.

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