WEBINAR SUMMARY

June 4, 2020

A Surprise Trip to Zero Trust Land

Wendy Nather, Head of the Advisory CISOs Team, Duo Security at Cisco
Baber Amin, CTO, Ping Identity

KEY TAKEAWAYS

- Zero Trust implements security at the resource level, not just at the firewall.
- With Zero Trust, "Digital Trust" replaces "Static Trust."
- The Zero Trust Journey Begins with Identification and Authentication.
- Ping Identity focuses on identity and access controls—simplified but secure.

in partnership with

OVERVIEW

The COVID-19 pandemic has forced many businesses to suddenly move their entire workforce from working within a physical office to working from anywhere. This unplanned shift to remote connectivity for all workers, no matter where they are or what devices they are using, significantly increases the security risk of an organization. In response, many are now accelerating their efforts to implement Zero Trust.

Zero Trust security helps organizations implement dynamic security controls that are better equipped for remote work. It abandons the notion of network perimeters and instead moves the perimeter to wherever access control decisions are made. This improves the organizational security posture despite the growing attack surface brought on by the increase in remote work.

Ping Identity provides a comprehensive suite of identity services to the large enterprise market, and delivers secure and seamless digital experiences. Organizations leverage Ping for strong authentication, centralized authentication services, intelligent policies, API security, and an extensibility that can integrate all of their application and technology ecosystems.

CONTEXT

Wendy Nather provided an overview of the Zero Trust security model and highlighted what organizations should consider when implementing it. Baber Amin described how Ping Identity provides a simple yet powerful approach toward a Zero Trust environment within the enterprise.

KEY TAKEAWAYS

Zero Trust implements security at the resource level, not just at the firewall.

The sudden shift to remote work has amplified the need for businesses to adopt Zero Trust security. The model moves the perimeter any place where access control decisions are made, overriding the idea that any traffic inside the firewall can be trusted.

> A basic first principle is you shouldn't trust something just because it's on the inside of your firewall. We've seen a lot of breaches where that led to a problem.
>
> *Wendy Nather, Duo Security at Cisco*

Zero Trust focuses on enforcing policies at the point of access. Four key controls are used to implement the model:

1. Least privilege (defined roles and segmentation);
2. Multi-factor authentication (MFA);
3. Endpoint security; and
4. Continuous monitoring.

Table 1: Four Controls for Zero Trust Security

Control	How it is used
1. Least privileged (defined roles and segmentation)	– Microsegmentation at the network layer with new technology. – Authenticate first, then allow connection.
2. MFA	– Needs to be used for anyone accessing systems, not just a group of pre-determined employees. – Multiple factors enables flexibility and improves user experience (e.g., cell phones may be a good MFA for many, but not for those users who have poor cellular signals where they typically work). – Don't rely on just the internet protocol (IP) or media access control (MAC) address for authentication; MFA creates extra layers of security.
3. Endpoint security	– No longer assume the device is corporate owned and managed; allows personal device connections while mitigating risk. – Check the endpoint at every authentication, not just once. – Make access contingent on compliance; ensure devices comply with security policy before allowing access. – Bind the user directly to the device, requiring users to use an assigned device for access.
4. Continuous monitoring	– Use behavior analytics to ensure the users are authenticating as expected. – Step up authentication and ask for more factors if analytics detect anomalies.

Other key differences between traditional network security and Zero Trust include:

- Not using IP addresses as proxies for geolocation.
- Accounting for different workloads and devices, including Internet of Things (IoT) and industrial control systems (ICS).
- Leveraging more secure enclaves and trusted computing.
- Improving the user experience with mobile-friendly authentication, offering more opportunities for single sign-on (SSO), and looking to WebAuthn and CTAP2 to move toward passwordless authentication.

Is it Zero Trust?

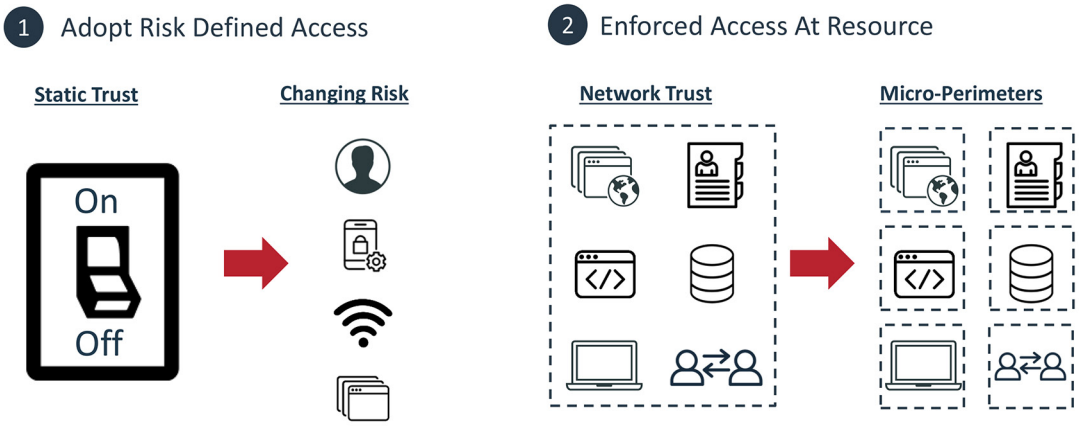
If the business is doing one or more of the following, regardless of location, some version of the Zero Trust model is being used.

- Consistent use of MFA
- Device inspection at authorization time
- Least-privilege segmentation
- Adaptive access policies
- SSO
- Encryption everywhere
- Reverse proxies

With Zero Trust, "digital trust" replaces "static trust."

Zero Trust assumes that the network is hostile, and that external and internal threats exist at all times. Static trust based on network locality is no longer sufficient for deciding trust; instead, every device, user, and network flow is authenticated and authorized using dynamic policies that calculate information from as many sources of data as possible to provide a snapshot of digital trust.

Figure 1: Zero Trust Depends on Identity to Determine Digital Trust and Risk



Digital trust provides a dynamic level of trust above and beyond what static trust can provide. Dynamic trust cannot be based on ownership and control. It is ephemeral and only valid for the current instance, used only for the minimal amount of time and purpose for which it was intended.

The model also assumes digital risk, which can be assigned separately from digital trust. A variable level of confidence, digital risk moves dynamically to match the organization's current risk tolerance. Each interaction dynamically assesses requested behavior under the current context to determine how much digital risk is associated.

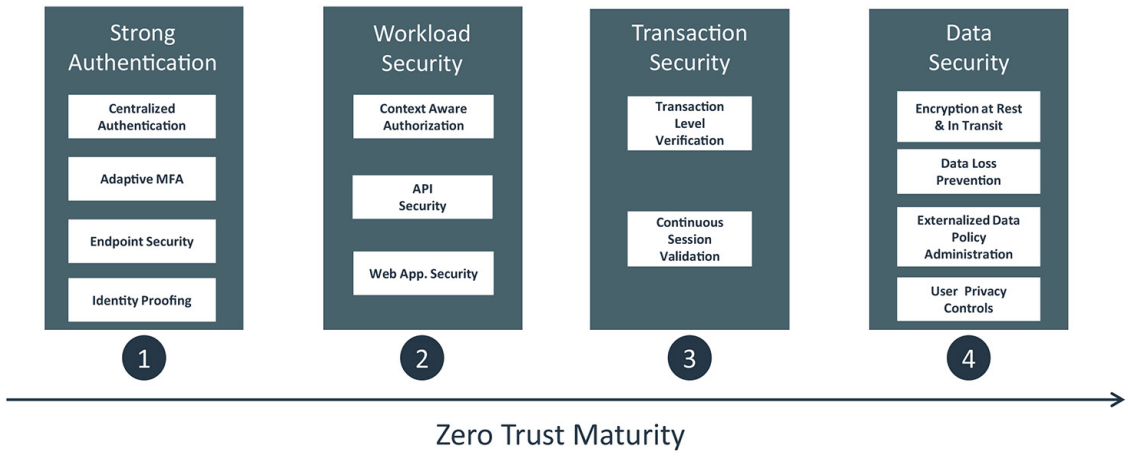
The Zero Trust journey begins with identification and authentication.

To get started with Zero Trust, you need identification and strong authentication capabilities. Then you move through workload security, transaction security, and data security. While Zero Trust maturity increases as these security concepts are implemented, the dynamic aspect means it never reaches an end.

> Zero Trust is really a journey and a process; it's not a destination.
>
> *Baber Amin, Ping Identity*

Strong authentication requires authentication that is centralized, normalized, and externalized across the organization, and not handled just on a per application basis. Once authenticated, dynamic and contextual authorization is handled at the workload level, defining what access a user has to a specific application or application programming interface (API). Once these credentials are passed, the rights to create transactions are verified and validated. Finally, security at the data level allows access to specific data, and determines how data at rest and data in motion are handled. Just as with the authentication step, data security decisions are centralized, normalized, and externalized to take decisions out of the hands of individual applications.

Figure 2: A Suggested Approach to Zero Trust



Ping Identity focuses on identity and access controls—simplified but secure.

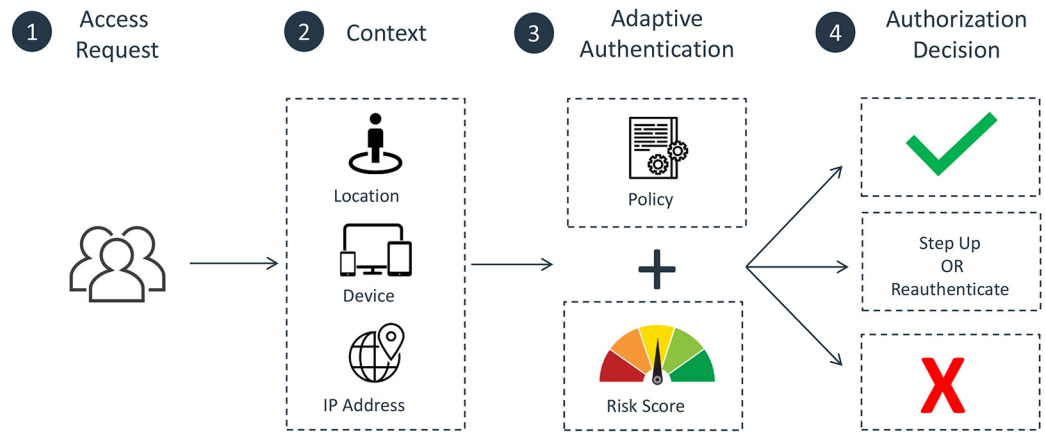
Ping Identity strives to be more than just an identity and access management vendor the enterprise; its mission is to be a trusted partner that can deliver extraordinary digital experiences through security and simplicity.

> Simple security is always the best security.
>
> *Baber Amin, Ping Identity*

Ping Identity is trusted by more than 1,500 global enterprise customers—including more than 60% of the Fortune 100. Based on its experience, they recommend organizations that are looking to implement the Zero Trust model do the following:

- **Centralize Authentication:** Ensure authentication can cover all of your resources. That means your identity platform must be flexible enough to support new technologies and standards. It will allow you keep up with changes to the business as they occur.
- **Implement Strong Authentication Policies:** Leverage multiple risk signals to make authentication decisions. Gather as much context as possible without sacrificing the user experience.

Figure 3: Strong Authentication Policies



- **Re-Visit MFA:** MFA is the best way to reduce password risk. Modern MFA is user friendly, supports broad use cases, and has advanced security capabilities. For example, not all users will have access to features like biometrics or in some cases, an internet connection. Think about your use cases and determine if your provider has options to enable multiple login methods, passwordless, offline authentication, etc.
- **Don't Discount Integration:** Analyze your application requirements both on-premises and cloud. Examine if you can provide coverage for your entire ecosystem and predetermine any perceived gaps. Zero Trust should try to cover all your login/access scenarios.

BIOGRAPHIES

Wendy Nather

Head of the Advisory CISOs Team, Duo Security at Cisco

Wendy Nather is head of the Advisory CISO team at Duo Security (now Cisco). She was previously the Research Director at the Retail ISAC, as well as Research Director of the Information Security Practice at independent analyst firm 451 Research. Wendy led IT security for the EMEA region of the investment banking division of Swiss Bank Corporation (now UBS), and served as CISO of the Texas Education Agency.

She is co-author of *The Cloud Security Rules*, and was listed as one of *SC Magazine's* Women in IT Security "Power Players" in 2014, as well as an "Influencer" in the Reboot Leadership Awards in 2018. She serves on the advisory board for Sightline Security, an organization that helps nonprofits improve their cybersecurity.

Baber Amin

CTO, Ping Identity

Mr. Amin is a senior technology executive experienced in building and scaling businesses at software, networking, public and private companies. He has a broad background in enterprise security, identity and access management, identity proofing, authentication, privacy, and API security. He is a strong strategic thinker with operational execution, portfolio, and P&L management skills.

At Ping Identity, Mr. Amin is currently CTO for West, helping customers with their IAM best practices, strategy execution, zero trust architecture, IoT Identity, and modeling for a privacy first approach. At Ping Identity he is also guiding product roadmap for Zero Trust, AI/ML strategy, championing privacy by design principals, and evaluating M&A.