Zero Trust Security:

What it is and How to Achieve it

BEYOND IDENTITY

BEYOND IDENTITY

Contents

Much is made of the changes in how the modern workplace operates as a result of the pandemic. But our work habits were changing long before COVID-19, with online collaboration making it possible to work from just about anywhere and on any device.

Such a move is not without security risks. No longer can we automatically assume a device on the network is secure. Security patches might be missing, or worse yet, the device itself is compromised. Employees want to bring their own device (BYOD) to work, and the dramatic increase in work from home across companies means that organizations will have to figure out ways to adapt, yet still keep their networks secure.

That's where the idea of "zero trust" comes from. It allows for maximum freedom in how and from where your employees work while still maintaining a high level of security.

What is Zero Trust?

Computer networks traditionally operated on a "trust but verify" security model: as long as they could authenticate themselves, any person or device was trusted. That worked fine for early computer networks because organizations could essentially control who and what connected to their networks and where, because by and large, they all worked from one central location (or on-premises).

Telecommuting and the rise of mobile devices changed the threat landscape. IT departments now balanced network security with the demands of an increasingly mobile workforce. Organizations needed a new model to ensure networks remained secure, as hackers were also discovering that once they had an "in" there wasn't much resistance afterward from looking at and taking whatever they wanted.

Coined in 2010 by Forrester Research's then-vice president and principal analyst Jon Kindervag, zero trust operates on the concept of "never trust, always verify." The network does not treat any user, packet, interface, or device differently regardless of where they originate. Everybody starts with the same level of trust and must prove what or who it is to gain access to critical assets. Users can only access what they need to complete the request.

Thinking about network security in this manner makes it much easier to contain security incidents. There is less risk from compromised BYOD devices, or insider threats. By compartmentalizing security past the login screen, the attacker doesn't have free reign over what's inside if a break-in occurs.

Zero Trust Basics

At its core, three basic ideas make up the concept of zero trust:

- Eliminating the concept of trust in a network
- Employing key preventative security measures
- Enabling responsive real-time monitoring techniques to deal with breaches

Eliminating the concept of trust in a network

With zero trust, there are no trusted sources. Every packet that comes across the network must be authorized, authenticated, and encrypted. By treating traffic (whether inside or outside the network) the same and continuously authenticating the user, hackers have a far harder time compromising network security.

Employing key preventative security measures

Zero trust is only a strategy: to build a network based on this architecture, IT departments must develop their networks with a few critical preventative security measures in mind.

Identity and device verification is key to zero trust. Is the person or the device connecting who they say they are? Is the device adequately secured? Is any unusual activity occurring? These are questions that a zero trust authentication system will answer.

When looking to secure their applications further, developers typically look to multi-factor authentication (MFA). A second (or more) form of authentication past the typical username and password login is required. The factors fall into three categories: something you know, something you have, or something you are.

Zero trust networks also ensure that the lowest level of access possible is granted at all times to users and devices. Authorization is limited to what is required to complete a given task. This way, when an attack occurs, the attacker's movement beyond the break-in point is limited.

In practice known as microsegmentation, developers abandon the traditional "castle and moat" mentality in conventional network architecture, where most of the security is on the network perimeter. Instead, smaller zones are created within the traditional perimeter to further separate portions of the network from one another, either by device, function, or identity. With limited access to the rest of the network, hackers cannot explore outside of these smaller zones.

While a vastly more complicated process, the result is a network built on the assumption that an attack can come at any time and from anywhere. And if it does happen, any losses are minimized.

Enabling responsive real-time monitoring techniques to deal with breaches

While the above methods will dramatically improve network security, break-ins can still occur. Network managers should also employ real-time monitoring techniques to improve response times to incoming threats.

In addition to monitoring, automated remediation is key. A computer can move faster than a person can, and many zero trust solutions offer some type of automated system to detect, investigate, remediate, and prevent further attack attempts.

How to Achieve Zero Trust

Each organization will have different requirements and needs, but your transition to a zero trust architecture will occur in three phases.

1 Perform an initial security assessment.

In this first step, the primary goal is to understand your overall risk. Identify any potential attack surfaces, as well as potential targets such as sensitive data, assets, applications, and services (DAAS). Review credentials across your organization and remove any old or unused accounts. Among those accounts that remain, ensure privileges are both necessary and current. Look for gaps within the existing security infrastructure and address these first. Make sure your most critical assets in your network are also adequately protected.

It's important to note that zero trust can be extended to not trusting the hardware users are operating on. Hackers can compromise hardware so it's important that you take this into account in your zero trust strategy and not blindly trust equipment.

2 Know where your data is and where it goes.

Next, you'll want to map where your data is and who needs access to it. Keep track of what third-party services you connect to and what they might have access to. Use passwordless authentication to further secure your network: stolen alphanumeric passwords are the most common entry point for hackers. In any case, limit data access to only what is needed to complete the task.

3 Get on offense when it comes to security.

Too often, network security is reactive rather than proactive. In today's threat environment, that's taking a significant risk. Preventative measures like MFA, have a strong access control policy, and employing micro-segmentation techniques in planning out your security infrastructure will go a long way in keeping your network secure. Real-time monitoring is essential.

Why Zero Trust May (Or May Not) Be a Good Fit

While zero trust offers a host of benefits, it's not for everyone. Smaller and newer businesses will easily transition to a zero trust architecture since many common software platforms are already compatible. However, older and larger companies will need considerably more time to implement zero trust.

Regardless of the organization's size, you'll need reliable data on who and what is on your network and what access they or it requires. You'll also need to remain nimble: technology changes quickly, your network architecture strategy may change with it.

Zero trust also requires complete buy-in. The entire organization should implement the core concepts of zero trust at the same time to limit confusion. But it's important to note that achieving zero trust also requires patience and time. A good deal of preparation goes into executing a zero trust strategy, even in the most modern and security-conscious organizations. Protect your most vital assets first when transitioning to zero trust. This ensures critical parts of your infrastructure are well protected from the start.

If you plan to pursue a zero trust strategy, you must plan for the amount of work involved. Since so much of it is dependent on authentication, using a platform like Beyond Identity makes your authentication processes zero trust-compliant quickly and easily.

81% of breaches involve stolen passwords

51% use the same password for personal and work

57% would prefer passwordless authentication

How Beyond Identity Can Help

"Never trust, always verify" is the basis of zero trust.

However, as long as the alphanumeric password is being used, no network can genuinely claim it is compliant with that principle. While random password generators within browsers and stricter password policies have slightly improved security, they don't solve the issue of verifying the identity of the user. Any hacker with a database of stolen credentials can log in with no issue in a network that doesn't employ zero trust architecture. While MFA takes steps to address that problem, it is not without its issues.

Traditional MFA has become the de facto method of increasing network security, but it doesn't truly make things any more secure. At its core, legacy MFA is still based on an inherently insecure concept: the alphanumeric password and doesn't do risk assessments of the user.

Traditional MFA is also a poor user experience. While adding an extra layer of authentication, it's a time-consuming process that can hurt company productivity since you'd want to regularly reauthorize connections after long periods of inactivity to prevent unauthorized access through an unattended device.

Beyond Identity believes that true zero trust isn't possible as long as the traditional password remains the primary digital authentication method. As we've all found out, password leaks are the single biggest threat to modern networks with far too many users either using the same password across multiple accounts, or selecting simple passwords that are easily hacked.

Instead, Beyond Identity's platform replaces the password with secure credentials based on X.509 certificates and public-private key pairs. Beyond Identity's solutions help achieve zero trust by continuously assessing risk and never inherently trusting any device or user.

Trust the Identity

Bind identity to the device to eliminate passwords. All users are cryptographically bound to their device to verify the identity of the person and device with confidence.

Trust the Device

Establish confidence that the device is secure by checking that all security settings and software are configured and running correctly on every device at every transaction.

Trust the Technology

Use asymmetric keys and X.509 certificates without the need for a Certificate Authority. Unmovable, unclonable private keys are stored on the user's existing hardware.

The patented solution leverages secure, industry-standard asymmetric-key cryptography for authentication, and our cloud-based platform runs on an app on endpoint devices that creates and manages these keys. The result is a frictionless experience for the end-user while offering dramatically better security than any MFA solution on the market.

And the best thing is that the platform integrates easily with most existing SSO solutions with only a few lines of extra code, helping organizations in their efforts to move towards a zero trust architecture.

See how the cloud-native solution enables customers to increase velocity, implement new business models, and reduce operating costs by requesting a demo today.

Conclusion

Zero Trust Security Highlights:

- Zero trust operates on the concept of "never trust, always verify"
- Zero trust allows for maximum freedom in how and from where your employees work while still maintaining a high level of security
- Many zero trust solutions offer some type of automated system to detect, investigate, remediate, and prevent attack attempts
- Zero trust also requires complete buy-in—the entire organization must implement the core concepts at the same time
- Beyond Identity solutions help achieve zero trust by continuously assessing risk and never inherently trusting any device or user.

About Beyond Identity

Beyond Identity ensures that every user and device accessing SaaS resources is both authorized and secured-supporting zero-trust access and providing the device identity verification needed to secure hybrid and fully remote work environments. Our innovative architecture replaces passwords with device-bound identity, an immovable, inimitable solution for secure user identity verification and access management. We remove inherent trust, force device security policy adherence, continuously assess devices and users for risk and trustworthiness, and create immutable records of the interaction before every login attempt.

Ready to Explore Zero Trust Security?

GET A DEMO

beyondidentity.com | info@beyondidentity.com

BEYOND IDENTITY