RESOURCE CENTER

What does zero trust mean? How to implement Zero Trust Architecture

Get the full interactive view at
https://bitwarden.comhttps://bitwarden.com/de-de/resources/how-to-implement-zero-trust-architecture/

bitwarden

Overview

Traditional security models, which rely on perimeter-based defenses, often leave organizations vulnerable to internal and external threats. Zero trust architecture presents a modern approach, addressing the core struggle of technology leaders: balancing stringent security needs with operational efficiency. This guide will explain what zero trust means, walk through its core components, and provide a roadmap for adopting a zero trust security model.

What is zero trust?

Zero trust is an architectural approach that assumes all users, devices, and data are potential threats until proven otherwise. The concept has evolved, but its core idea remains the same: verify the identity of every user, device, or process before granting access to sensitive resources.

The idea behind zero trust is that all users, whether they are inside or outside of an organization, be authenticated, authorized, and continually validated before being granted (or retaining) access to applications and data.

The benefits of adopting zero trust include:

- Greatly improved security: Zero trust reduces the attack surface of your organization by limiting access to sensitive resources.
- Reduced risk: Zero trust minimizes risk from insider threats, lateral movement, or external attacks.
- Compliance and regulatory requirements: Zero trust aligns with regulatory requirements for data protection and confidentiality.

Some of the common use cases for zero trust are:

- Cloud services: Used for securing cloud-based applications and data.
- IoT devices: Protect your IoT devices and networks from unauthorized access.
- Remote workforce: Ensures organizational security when employees work remotely or use public Wi-Fi.
- Data centers: Enhances network segmentation and isolation for sensitive resources.

Of course, zero trust does come with its share of challenges. First off, zero trust requires complex infrastructure, policies, and procedures in order to manage identity verification, access control, and monitoring. There's also the fact that zero trust can be rather resource intensive, requiring advanced security tools and expertise. Finally, there's user adoption, which can mean your organization users will have to adopt different processes for authentication.

Zero trust also employs the following concepts:

- **Microsegmentation** is a network segmentation technique used to isolate sensitive resources from the LAN by breaking them into smaller zones (or segments). This reduces the attack surface and limits lateral movement.
- L**east privilege access** is an approach to granting users and applications only the necessary permissions needed to perform their tasks. This principle aims to minimize the risk of unauthorized access, data breaches, and other security incidents.

Here's how zero trust works:

- Step 1 - Authentication: Users or devices attempt to authenticate themselves through a secure channel (e.g., VPN).

- Step 2 - Authorization: The system verifies the identity of the user or device against known credentials.
- Step 3 - Access control: If authentication is successful, access is granted based on pre-defined policies and least privilege principles.
- Step 4 - Monitoring and enforcement: Network activity is continually monitored, and security rules applied to prevent unauthorized access.

Examples of zero trust

- Example 1: An employee working remotely requires access to sensitive customer data. Under a zero trust model, their identity is verified through MFA, their device's security posture is checked, and their access is limited only to the necessary data, regardless of their physical location.
- Example 2: Cloud providers like AWS, Azure, and Google Cloud use zero-trust principles in their security models.
- Example 3: Companies segment their networks into smaller zones based on users' location and access rights.
- Example 4: Implementing Identity-Driven Security solutions that verify users' identities before granting them access to sensitive resources.
- Example 5: Applying zero trust principles to endpoint devices like laptops, desktops, and mobile devices.

Table of Contents

Key components of a Zero Trust Architecture

There are five primary components of Zero Trust Architecture.

Identity management

This component is responsible for verifying user identities and ensuring that all users are authenticated and authorized before accessing sensitive resources.

Access control policies

Access control policies establish rules-based access controls to ensure that only trusted users can access specific resources.

Encryption and key management

This ensures encryption of both data in transit and at rest, using secure key management practices.

Network segmentation (microsegmentation)

Network segmentation divides the network into smaller, isolated segments based on user roles or sensitive data types.

Endpoint security

This component protects endpoint devices, like laptops, desktops, and mobile devices with robust security measures to prevent lateral movement attacks.

Monitoring and incident response

To achieve zero trust, teams must continuously monitor system activity for suspicious behavior, as well as have an incident response plan in place to contain and remediate breaches.

Multi-factor authentication (MFA)

Adding MFA gives organizations an extra layer of security by requiring multiple forms of verification, further reducing the risk of unauthorized access, a core component of zero trust.

Zero-knowledge encryption

Zero-knowledge encryption ensures that only the user has access to their data.

Suggestion: Zero-knowledge encryption keeps data private so that only the intended users/system can see or use it, without exposing the data itself at any point. It can be an important component in a zero trust system.

> Read how end-to-end encryption paves the way for zero knowledge in this white paper.

Least privilege access

Least privilege access grants users only the minimum access necessary to perform their tasks, limiting the potential damage from a compromised account.

Read more:

Additional enterprise options for least privilege access control

Implementing a zero trust security model: A step-by-step roadmap

Implementing zero trust is a strategic journey, not a simple software installation/configuration, and this section will guide technology

leaders in planning a phased approach. Even before you decide to adopt zero trust security, it's important to have a roadmap for success. That roadmap should consist of at least five steps, including the following.

Step 1: Assessment and planning

During this phase, it's important to identify stakeholders, including IT teams, management, and users, to ensure buy-in and support for the new model.

Step 2: Identity and access management implementation

Deploy an identity management platform that provides real-time user profiling and threat intelligence, such as Okta Identity Cloud, CyberArk Idaptive, ForgeRock Identity Platform, SailPoint IdentityIQ, or IBM Identity and Access Management.

Step 3: Network microsegmentation

Implement network segmentation using VLANs, subnets, or other techniques to isolate sensitive data and/or resources.

Step 4: Continuous monitoring and threat response

Implement a Security Information Events Management (SIEM) system to monitor security-related events and provide real-time threat analysis and intelligence.

Step 5: Iteration and optimization

It's important to understand that each iteration of a zero-trust deployment will constantly evolve to work with an ever-changing landscape. With each new iteration, the platform should be further optimized through analysis and monitoring.

Once these steps are complete, determine how your team will handle training and testing, maintenance, and endpoint security.

Dos of zero trust

- **Implement multi-factor authentication (MFA)**: Always require users to provide multiple forms of authentication, such as passwords, 2FA codes, tokens, or biometric data.
- **Use encryption**: The encryption of sensitive data both in transit and at rest should be considered a must to prevent unauthorized access.
- **Segment network traffic**: Divide the network into smaller segments based on user roles or sensitivity levels to reduce the organization's attack surface.
- **Implement access controls**: Establish rules-based access controls to ensure only authorized users can access specific resources within your organization.
- **Monitor system activity**: Continuously monitor system activity for suspicious behavior and make sure the required teams can respond quickly to any and all potential security incidents.
- **Use artificial intelligence (AI) and machine learning (ML)**: Leverage AI/ML-powered security tools to detect anomalies in system activity and prevent potential breaches, as these types of systems can detect issues faster than their human counterparts.
- **Conduct regular security audits**: Perform regular security audits to identify vulnerabilities and ensure compliance with organizational policies. These are also a necessity for iteration and optimization.

Don'ts of zero trust

- **Don't overly restrict access**: Avoid overly restrictive access controls that hinder legitimate user activities, such as email or file sharing, as this can lead to a deluge of issues.

- **Don't neglect endpoint security**: Endpoint security failures can lead to lateral movement attacks across your LAN as well as data breaches. Deploy robust security measures to all endpoints.
- **Don't ignore identity management**: Identity management is key to zero trust, and failing to properly manage identities can result in unauthorized access to sensitive resources.
- **Don't depend on firewalls alone**: Firewalls are a good source of basic device and network security, but when used alone, they may not be sufficient to prevent advanced threats.
- **Don't fail to continuously monitor the organization's security posture**: Zero trust is an ever-evolving concept. Continuously monitor security posture to keep the organization ahead of ever-evolving threats.
- **Don't ignore incident response plans**: It's important to have plans for when incidents occur. If there is not an incident response plan in place, the organization might be too slow in its response to an event.
- **Don't neglect user education**: Zero trust may be a brand new concept to users, so it's important to educate them on this new policy to help promote and ease user adoption.

Read more:
The credential lifecycle: Stay ahead to strengthen your security and access management

Bitwarden supports zero trust transformations

Zero Trust Architecture offers a fundamental shift in how organizations approach cybersecurity, moving from a perimeter-centric view to a data-centric one. Technology leaders can significantly strengthen their security posture by understanding its core principles and implementing features like multi-factor authentication and zero-knowledge encryption.

The zero trust security model helps to deliver increased security, improved incident response, enhanced compliance, reduced risk from outsider threats, reduced security operations cost, improved user experience, better protection against advanced threats, data loss prevention, and future-proof security.

Begin your zero trust journey today by reviewing your current security infrastructure and identifying areas where Bitwarden can immediately enhance your security posture.

To get started, review these resources:

- Additional enterprise options for least privilege access control
- Accelerate audits with the Member Access report
- The credential lifecycle: Stay ahead to strengthen your security and access management
- Every second counts: 9 days to fix at-risk credentials is too long

- How end-to-end encryption paves the way for zero knowledge - White Paper