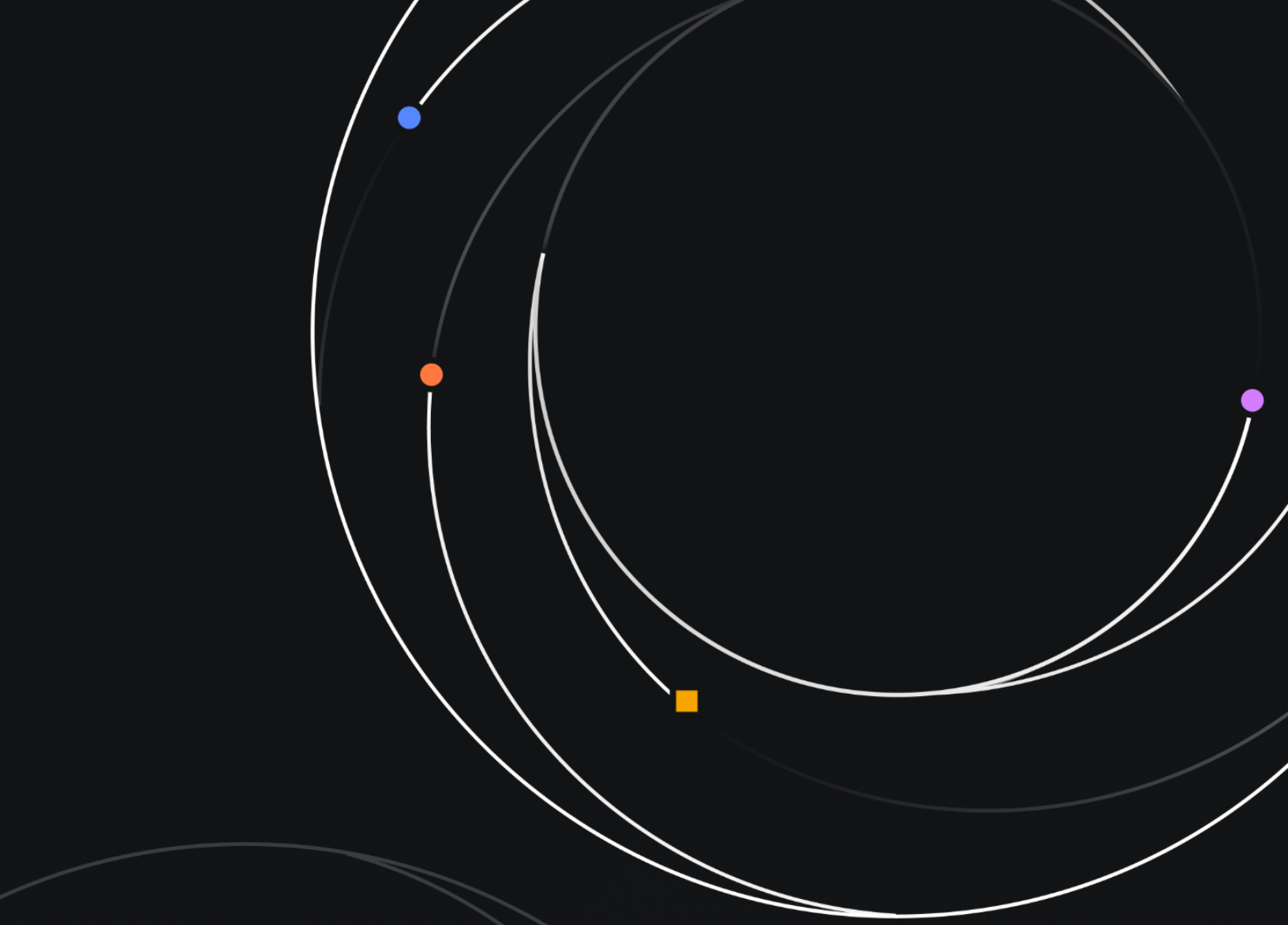


Identity Providers Critical Role in Zero Trust Adoption

Twingate

April 2022

The state of work is changing, and distributed teams have become the norm. Instead of securing a singular perimeter around your organization's network, employees, contractors, and vendors regularly require access to resources from anywhere and from any device. Along with the shifting paradigm of how we work, the number and types of accounts needed to perform daily tasks have multiplied. Today, many organizations manage the myriad of digital identities employees need to access tools and services with an identity provider (IdP).

Many of us have touched on concepts tied to digital identity management — such as using a single account to log in to many different services, a concept called single sign-on (SSO). However, many may not realize that SSO and multifactor authentication (MFA) are identity and access management (IAM) concepts representing the first steps toward adopting Zero Trust.

The Basics: Identity Access Management (IAM)

To understand IdP, it's essential to understand the broader category of identity and access management (IAM). According to Gartner, IAM is the "mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments and meet increasingly rigorous compliance requirements." To achieve this, IAM uses systems and processes to allow IT administrators to assign a single digital identity that is authenticated and authorized to access company resources.

IAM applies to more than just employees, contractors, and customers. IoT devices, APIs, and processes such as a CI/CD pipeline can all fall under the umbrella of IAM. They all require a combination of authentication and authorization to perform work-related tasks.

Over the last two years, as organizations continue to embrace remote work models, the criticality of IAM has come into focus. According to the March 2021 Ping Identity survey of more than 1,300 executives, "70% of global business executives plan to increase spending on IAM for their workforce over the next 12 months, as a continuation of remote work increases demand on IT and security teams."

Gartner has identified six IAM trends that can help shape how organizations mature their IAM roadmaps.

- Connect anywhere computing will further drive the need for smarter access control
- Improving user experience for all users will be essential for secure digital business
- Keys, secrets, certificates, and machines will require more attention
- New applications and APIs will need to leverage the latest IAM development guidelines
- Hybrid cloud and multi-cloud will drive ongoing IAM architecture maintenance/evolution
- Identity governance and administration (IGA) functions will evolve to enable decentralized architecture

What is an Identity Provider (IdP)?

An Identity Provider (IdP) is a service that creates and manages digital identities and the attributes associated with those identities. IdPs authenticate users through third-party service providers using these identities.

According to Okta, IdP workflows typically involve these steps:

- Requests: Users enter credentials from another service, such as a Google account.
- Verification: The IdP checks the user's authorized account against what they should access.
- Unlocking: After verification, the user is authorized to access specific resources, and the interaction is logged.

To end users, the IdP process is invisible, taking seconds; but to organizations, it provides a much-needed layer of security between critical business resources and threat actors that could potentially steal those resources for ill-intent. Today's users balance a seemingly never-ending list of accounts for home and work, often leading to password fatigue and password reuse. As the number of passwords a user has to remember to manage their digital identities climbs, so do the associated risks. IdPs lower the burden of passwords by creating a centralized repository for an organization's identities and associated accesses. This, in turn, helps to reduce the number of accounts — and passwords — users must protect.

According to NIST SP 800-63A, IdPs need to "manage and store subscriber credentials appropriately for the types of credentials in use" but should also implement phishing-resistant technologies. To do this, IdPs must follow data minimization practices, not divulging more attributes about a subscriber than necessary to identify them and fulfill the initial request.

The credentials associated with digital identities, primarily a username and password, can be the keys to the kingdom for a threat actor. Threat actors often use an initial compromise such as gaining a username and password to move laterally within a network, elevating their accesses, and making resources available.

What an IdP is not (Authentication vs. Authorization)

While IdPs are critical to establishing identity, they are not a one-stop solution. IdPs primarily focus on authentication. However, authentication and authorization are two distinct and required steps in a company's access control process. You cannot have one without the other and preserve the integrity of your network's security.

	Authentication	Authorization
Purpose	• Verifies user identity	• Permits access to resources
Requirements	• Identity credentials based on knowledge, possession, and/or inherence • Authentication solution	• Authenticated identity and access control policies • Authorization solution
Responsibilites	• Network security staff determine which factors to adopt • Users provide authentication factors when requesting access	• Leadership sets security strategies • Departments and workgroups define access criteria • Network security staff implement and maintain access control system

- Authentication does nothing beyond confirming identity. The user cannot access network directories, files, or other resources
- Authorization does nothing without authentication. The authorization system must know who the user is before granting access permissions

Working together, authentication and authorization give your company more control over who accesses which resources. According to NIST, while IdPs should *"manage and store subscriber credentials appropriately for the types of credentials in use,"* that does not inherently make them an appropriate solution to take the place of a password manager. Many IdPs handle credentials through the implementation of single sign-on (SSO).

Authentication-focused vendors commonly target the below niches:

- **Cloud-first authentication vendors:** Okta and Auth0 provide authentication solutions for cloud-first enterprise infrastructures.
- **Traditional networking vendors:** Cisco and Aruba Networks offer access control solutions optimized for companies standardized on their hardware.
- **Cloud service providers:** Microsoft Azure and Amazon Web Services offer their own identity management systems and work with third-party providers.
- **Mixed authentication solutions:** Yubico and RSA Security develop hardware and software authentication solutions.
- **Social single sign-on providers:** through OpenID and proprietary systems, users are authenticated through Facebook, Twitter, and other social media accounts.

What is Single Sign-On?

Okta defines SSO as being built on the concept of federated identity, which is the sharing of identity attributes across trusted but autonomous systems. Essentially, this means that when a user is trusted by one system, they are trusted to access all other systems that have a trusted relationship with the system that initially authenticated the user.

To further build on the example, when a user signs in to a service with an SSO login, an authentication token is created and stored in their browser or the SSO solution's servers. Apps and websites will check with this server and grant the user trust (and with it access) based on their SSO token, authenticating the user's identity.

Open source IdP options

There is a diverse ecosystem of vendors and service providers ready to enhance your organization's IAM posture. However, open-source and custom options are available.

OAuth 2.0 is a standard that provides secure delegated access, which allows an application to take actions or access resources on behalf of a user.

OpenID Connect is an open standard that organizations use to authenticate users. IdPs in turn use OpenID Connect to allow the user to sign into the IdP and access websites and apps without having to log in or share sign-in information.

SAML enables users to log into their corporate internet or IdP and access additional services without re-entering credentials. SAML is an XML-based standard for exchanging authentication and authorization data between IdPs and service providers.

System for Cross-domain Identity Management (SCIM) is an open standard that allows for the automation of user provisioning. It communicates identity data between IdPs and service providers.

IdP and Zero Trust

At its core Zero Trust is a simple framework that answers the question: should this user on this device under this context access this resource? Zero Trust offers a path towards securing a world that supports distributed workforces, a blended network perimeter, and does not make broad assumptions about who or what should have access to data.

While Zero Trust has been in development for decades, Forrester Research first popularized the concept in 2010. More of a philosophy than a technology, ZTNA is based upon three principles:

- **Assume breach** - Since cyberattacks can happen at any time, no user, device, or network can ever be trusted. Every connection request must be challenged.
- **Verify explicitly** - Going beyond user identity, ZTNA evaluates the risk of each request, from device posture to source network, to inform the degree of authorization.
- **Least privilege** - The degree of access to resources users receive is based on their immediate needs. These ephemeral permissions are revoked when sessions end, after defined windows expire, or when any aspect of trust changes.

These three principles transcend specific technologies. Adopting Zero Trust requires organizations to change the way they view trust. Traditional network architectures implicitly trust employees using managed devices on the local network, and often that trust is extended to employees receiving access through a VPN gateway.

As organizations worldwide pivot to support hybrid and fully remote teams, network perimeter walls are disappearing. Additionally, today's organization's critical resources are co-located, cloud-hosted, or sourced from third parties. Thus, the network perimeter extends beyond company walls and intersects the networks of other companies and the general internet. While this paradigm shift supports a diverse workforce, it does bring additional challenges and risks when attempting to secure critical resources from threat actors.

As the NIST notes, “When balanced with existing cybersecurity policies and guidance, **identity and access management**, continuous monitoring, and best practices, a ZTA can protect against common threats and improve an organization’s security posture by using a managed risk approach.”

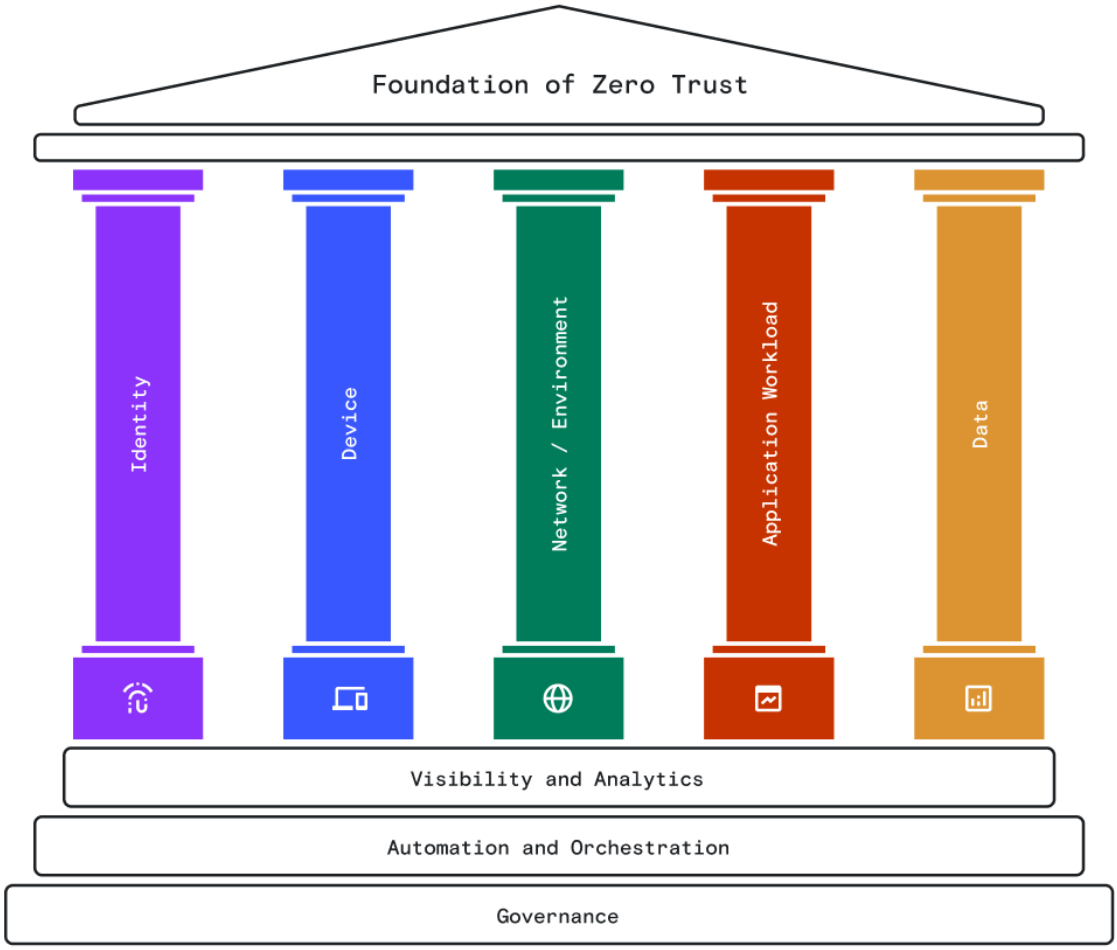
U.S. Government’s Push to Zero Trust by 2024

On January 26, 2022, the Office of Management and Budget (OMB) released the Federal strategy to move the U.S. Government toward a Zero Trust approach to cybersecurity. In short, the strategy and memo kick off the initial steps towards a significant digital transformation that requires top-down changes, from policies to tools, and will impact every employee that works with the federal government.

One of the more relevant areas of OMB’s Zero Trust strategy is the push to make applications internet-accessible. Today, many organizations still rely on on-prem resources, which don’t align with distributed workforces. To truly move towards Zero Trust, OMB has tasked all agencies to make at least

one application that is not currently accessible via the internet, accessible via the public internet within the next year by following a Zero Trust approach.

Identity and access management is a key pillar of OMB's foundation of Zero Trust. They note that government agencies should use enterprise-managed identities to access the applications they use in their work. Additionally, Phishing-resistant MFA will protect personnel from sophisticated online attacks.



About Twingate

Twingate provides a secure access platform that replaces or augments legacy VPNs with a modern Zero Trust Network Access (ZTNA) solution that combines enterprise-grade security with a consumer-grade user experience. It can be set up in less than 15 minutes and integrates with all major cloud providers and identity providers. Twingate helps companies move towards a Zero Trust architecture by tying every network event to an identity—user, device, and service—giving businesses unparalleled control and visibility over activity across their entire network.

Twingate is delivered as a software-as-a-service (SaaS) product, with downloadable software components that are installed on end-user and other devices.

Contact Us

Twingate Inc.

541 Jefferson Ave, Suite 100

Redwood City, CA 94063

USA

Online

www.twingate.com

sales@twingate.com

support@twingate.com