Zero Trust Zero Password

Jennifer Morales (C)
Contingent Worker

Zero Trust is Not "Zero Trust" - Zero Trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. - NIST

Zero trust is a security paradigm that replaces implicit trust with continuously assessed explicit risk/trust levels based on infrastructure that adapts to risk-optimize the organization's security posture. - Gartner

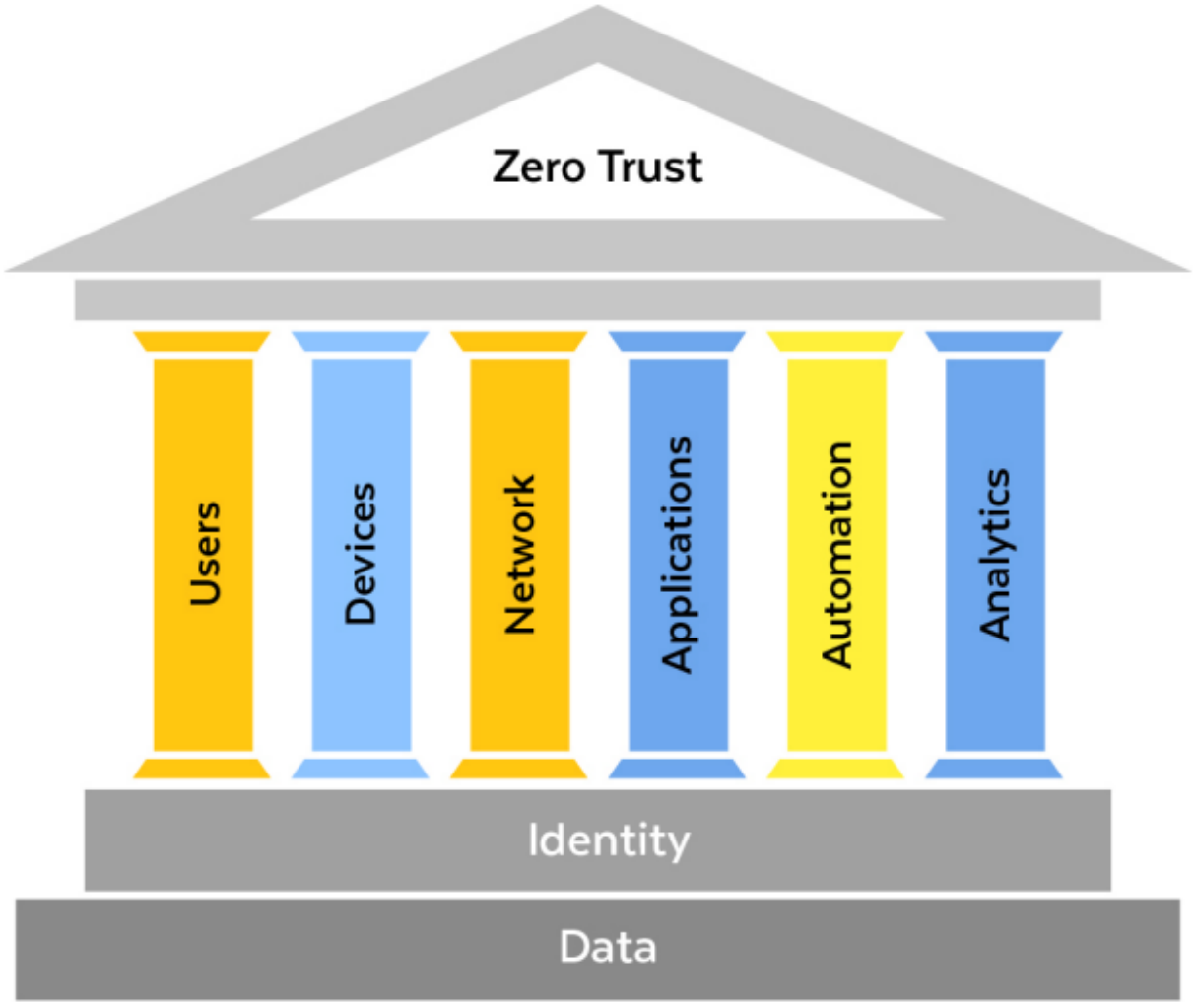
The shift to a decentralized, identity-centric operational model has placed critical importance on ensuring secure access for users. The future of authentication demands both a **secure** and **usable** method of authorizing users to both cloud and on-premises

systems.

Zero Trust should include Zero Password (*but it does not*)!

Zero Trust should mean Zero Password, but since marketing and solution providers are influencing the market that is not the case. There is not one single solution/vendor that addresses all the needs, the topic is just too wide. Because of this, both topics are mentioned below separately and you will see the synergies.

What is Zero Trust?



Six Pillars of a Zero Trust Security Model

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. **Zero Trust assumes that there is no traditional network edge**; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location. Zero Trust is a framework for securing infrastructure and data for today's modern digital transformation. It uniquely addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ransomware threats. While many vendors have tried to create their own definitions of Zero Trust, there are several standards recognized. NIST 800-207 is a vendor neutral, industry recognized standard, that encompasses other elements from organizations like Forrester's ZTX and Gartner's CARTA. The NIST standard ensures compatibility and protection against modern attacks for a cloud-first, work from anywhere model most enterprise need to achieve.

Why a Zero Trust security model is needed

With the modern workforce accessing applications from outside of the business perimeter, enterprises have adopted a "verify, then trust" model — which means if someone has the correct user credentials, they are admitted to whichever site, app, or device they are requesting. This has resulted in an increasing risk of exposure, dissolving what was once the trusted enterprise zone of control and leaving many organizations exposed to data breaches, malware, and ransomware attacks. Protection is now needed where applications and data, and users and devices, are located.

- Users, devices, applications, and data are moving outside of the enterprise perimeter and zone of control
- New business processes driven by digital transformation increase risk exposure
- "Trust but verify" is no longer an option, as targeted, advanced threats are moving inside the corporate perimeter
- Traditional perimeters are complex, increase risk, and are no longer compatible with today's business models

To be competitive, businesses need a Zero Trust architecture able to protect enterprise data, wherever users and devices are, while also ensuring that applications work quickly and seamlessly. Existing security patterns leave too much implicit trust.

Today, IT security is moving toward passwordless authentication using advanced

technologies like biometric verification and public/private key cryptography. Open standards like W3C WebAuth and Fast IDentity Online 2 (FIDO2) CTAP2 are enabling passwordless authentication across platforms. These standards are intended to replace passwords with authenticator devices/processes that are easy to use and may take advantage of investments organizations have already made—such as laptops, smartphones, fingerprint scanners, and cameras with facial recognition.

What is Zero Password? (or Passwordless)

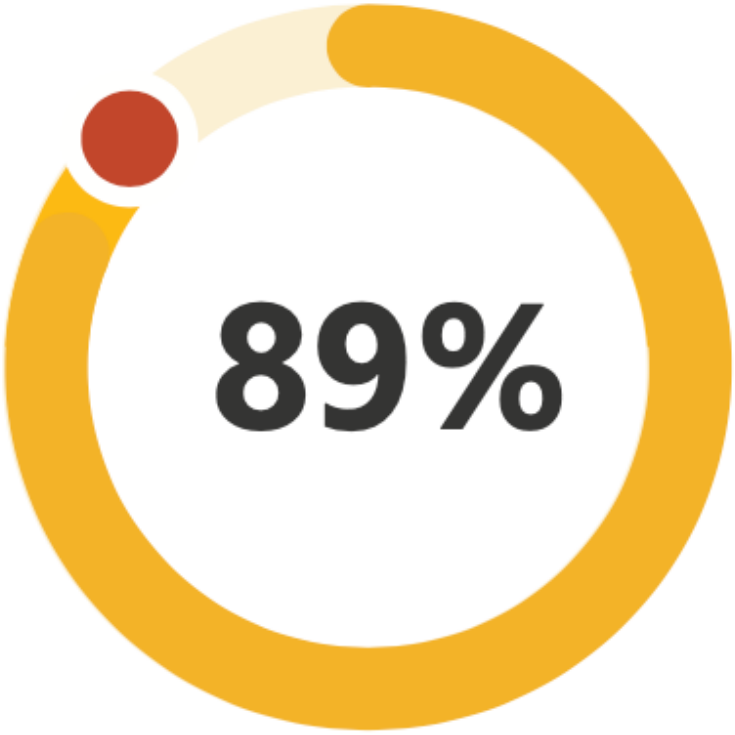
Passwordless authentication is an authentication method in which a user can log in to a computer system without the entering (and having to remember) a password or any other knowledge-based secret. In most common implementations users are asked to enter their public identifier (username, phone number, email address etc.) and then complete the authentication process by providing a secure proof of identity through a registered device or token. Passwords are the weakest link for security

Passwords are the weakest link for security

The cost of using passwords and the associated security risk now outweigh the benefits. Even the strongest passwords are easily phishable and vulnerable to attacks, and user resistance to password requirements is high. The motives to eliminate password authentication are endlessly compelling and all too familiar to enterprise IT organizations today.

"Your password, in the case of breach, just doesn't matter – unless it's longer than 12 characters and has never been used before" – Microsoft

"Hackers log in, they don't break in, proving your identity is the thing you really have to spend the most amount of time on." - Microsoft



"89% of web application breaches involved some sort of credential abuse (either use of stolen credentials or brute force)."

(Verizon 2021 Data Breach Investigation Report)

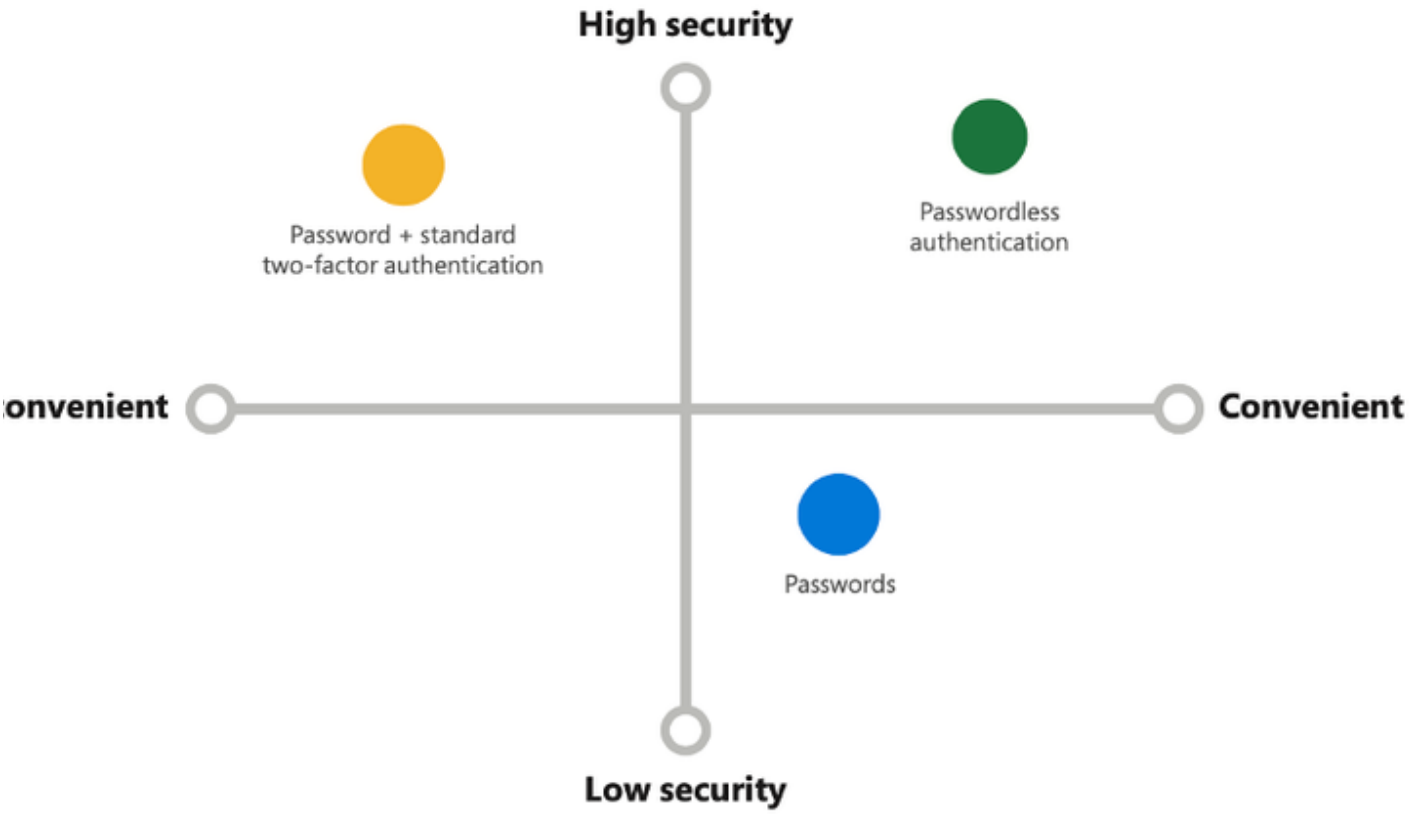
The origin of the password arrived in the mid-1960s at the Massachusetts Institute of Technology (MIT) with the development of the Compatible Time-Sharing System (CTSS), according to **Computer History** and **Wired**. It allowed hundreds of users to share the computer with a common mainframe. The password was developed as an accounting tool to allow users access to their specific resources for a certain amount of time.

As time went on, some users shared passwords and others demanded better security, and the emphasis shifted to authentication. In the 1980s, Security Dynamics Technologies patented a "method and apparatus for positively identifying an individual" and paved the way for additional factors of authentication. In the last two decades, multi-factor authentication (MFA) has matured as a secondary authentication which provides an additional layer of security to the primary password authentication.

The password primary authentication and the MFA secondary authentication became imperative as password theft and data dumps became routine. The 60-year-old single-factor password simply hasn't stood the test of time. In 2019, an anonymous creator released 2.2 billion usernames and passwords freely across attacker forums, known at that time to be the largest collection of breaches (**Wired**).

Advances in secondary factors, from the proliferation of smartphones to the consumerization of biometrics, has led many to question the need for and the use of the password at all. If strong authentication is based on multiple factors, and passwords are the most vulnerable factor, why even require them? This realization has led the industry to move toward replacing passwords altogether with more secure, simplified methods of authentication.

Tech and security analysts predict enterprises will shift to implementing passwordless authentication for their users to enable this modern digital transformation.



Verify first, then trust Passwords

To increase account security and provide added protection, many organizations are adopting a Zero Trust approach—a security model which assumes breach and verifies every request for access. Knowing who is requesting access is essential, and that identity must be validated explicitly, not inferred from the environment. Ensure you are secure at the point of access by bringing users into a common identity system with strong passwordless authentication and then using threat intelligence to validate.

Moving the World Beyond Passwords

FIDO2 is the overarching term for FIDO Alliance's newest set of specifications. FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments. The FIDO2 specifications are the World Wide Web Consortium's (W3C) Web Authentication (WebAuthn) specification and FIDO Alliance's corresponding Client-to-Authenticator Protocol (CTAP).

FIDO2 reflects the industry's answer to the global password problem and addresses all of the issues of traditional authentication:

SECURITY

FIDO2 cryptographic login credentials are unique across every website, never leave the user's device and are never stored on a server. This security model eliminates the risks of phishing, all forms of password theft and replay attacks.

CONVENIENCE

Users unlock cryptographic login credentials with simple built-in methods such as

fingerprint readers or cameras on their devices, or by leveraging easy-to-use FIDO security keys. Consumers can select the device that best fits their needs.

PRIVACY

Because FIDO cryptographic keys are unique for each internet site, they cannot be used to track users across sites. Plus, biometric data, when used, never leaves the user's device.

SCALABILITY

Websites can enable FIDO2 through a simple JavaScript API call that is supported across leading browsers and platforms on billions of devices consumers use every day. What is a Zero Trust Architecture?

Almost all of the tech companies that you know are currently supporting the FIDO2 standard. Just a quick look at everyone in the FIDO Alliance will tell you this is the leading direction for the future.

Different types of passwordless authentication for different users/use cases

With traditional username-password authentication, users must input something they know (a password) to verify their identity. Passwordless authentication, in contrast, requires users to demonstrate that they have something (sometimes called a Possession Factor) or that they are something (referred to as an inherence factor). These factors are much harder for bad actors to circumvent than knowledge-based factors.

Biometrics

Instead of a password, biometric authentication uses unique physical traits to verify a user's identity. You've probably used facial recognition to unlock your smartphone without entering your passcode or your fingerprint to access your laptop without typing in a password.

Biometric authentication is more secure than a password because no one has your exact fingerprint (even if you are an identical twin) or your exact face (the chances of two faces being similar enough to bypass facial recognition is extremely unlikely, even in the case of identical twins).

Biometrics rely on inherence factors: something that is inherent to the user, like their facial features, fingerprint, or voice.

Magic links

Magic links are another method of passwordless authentication in which users are prompted to enter their email address instead of a username-password combination. The user then receives an email containing a "magic link" they can click to be instantly logged in. This process is repeated every time the user needs access to the platform.

One-time passwords

One-time passwords (OTP), sometimes called one-time codes (OTC), work similarly to magic links. Customers receive a password or code via email or SMS text message that they use to log in. As their name suggests, one-time passwords are good for one use only; every time a user logs in, the process is repeated with a different single-use password.

One-time passwords and magic links sent through email are **knowledge factors:** you need to know the password for the email account to access the magic links.

One-time passwords and magic links sent via SMS are **possession factors:** they rely on something the user has, like a secondary device, to validate identity.

Push notifications

Push notifications are a mobile-centric form of passwordless authentication. To access an app on a mobile device, users receive a push notification that allows them to open the

app and verify their identity.

All of the types of passwordless authentication we've discussed here, from biometrics to push notifications, can be deployed as part of multi-factor authentication (MFA). We'll talk more about MFA in the next few pages.

What is a Zero Trust Architecture?

Zero Trust has become one of cybersecurity's most used buzzwords. It's imperative to understand what Zero Trust is, as well as what Zero Trust isn't.

Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern environments and enable digital transformation by using strong authentication methods, leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular, "least access" policies.

Zero Trust was created based on the realization that traditional security models operate on the outdated assumption that everything inside an organization's network should be implicitly trusted. This implicit trust means that once on the network, users – including threat actors and malicious insiders – are free to move laterally and access or exfiltrate sensitive data due to a lack of granular security controls.

With digital transformation accelerating in the form of a growing hybrid workforce, continued migration to the cloud and the transformation of security operations, taking a Zero Trust approach has never been more critical. If done correctly, a Zero Trust architecture results in higher overall levels of security, but also in reduced security complexity and operational overhead.

Building the Zero Trust Enterprise

Although Zero Trust is typically associated with securing users or use cases such as Zero Trust Network Access (ZTNA), a comprehensive zero trust approach encompasses Users, Applications and Infrastructure.

Users - step one of any Zero Trust effort requires strong authentication of user identity, application of "least access" policies and verification of user device integrity.

Applications - applying Zero Trust to applications removes implicit trust with various components of applications when they talk to each other. A fundamental concept of Zero Trust is that applications cannot be trusted and continuous monitoring at runtime is necessary to validate their behavior.

Infrastructure - everything infrastructure-related—routers, switches, cloud, IoT and supply chain—must be addressed with a Zero Trust approach.

How Zero Trust Works

A Zero Trust framework combines advanced technologies such as risk based multi-factor authentication, identity protection, next-generation endpoint security and robust cloud workload technology to verify a user or systems identity, consideration of access at that moment in time and the maintenance of system security. Zero Trust also requires consideration of encryption of data, securing email, and verifying the hygiene of assets and endpoints before they connect to applications.

Zero Trust is a significant departure from traditional network security which followed the "trust but verify" method. The traditional approach automatically trusted users and endpoints within the organization's perimeter, putting the organization at risk from malicious internal actors and legitimate credentials taken over by malicious actors, allowing unauthorized and compromised accounts wide-reaching access once inside. This model became obsolete with the cloud migration of business transformation initiatives and the acceleration of a distributed work environment due to the pandemic that started in 2020.

Zero Trust architecture therefore requires organizations to continuously monitor and validate that a user and their device has the right privileges and attributes. It also requires enforcement of policy that incorporates risk of the user and device, along with compliance or other requirements to consider prior to permitting the transaction. It requires that the organization **know all of their service and privileged accounts**, and can establish controls about what and where they connect. **One-time validation simply won't suffice**, because threats and user attributes are all subject to change

As a result, organizations must ensure that **all access requests are continuously vetted prior to allowing access** to any of your enterprise or cloud assets. That's why enforcement of **Zero Trust policies rely on real-time visibility** into 100's of user and application identity attributes such as:

- User identity and type of credential (human, programmatic)
- Credential privileges on each device
- Normal connections for the credential and device (behavior patterns)
- Endpoint hardware type and function
- Geo location
- Firmware versions
- Authentication protocol and risk
- Operating system versions and patch levels
- Applications installed on endpoint

- Security or incident detections including suspicious activity and attack recognition

The use of analytics must be tied to trillions of events, broad enterprise telemetry, and threat intelligence to ensure better algorithmic AI/ML model training for hyper accurate policy response. Organizations should thoroughly assess their IT infrastructure and potential attack paths to contain attacks and minimize the impact if a breach should occur. This can include segmentation by device types, identity, or group functions. For example, suspicious protocols such as RDP or RPC to the domain controller should always be challenged or restricted to specific credentials.

More than 80% of all attacks involve credentials use or misuse in the network. With constant new attacks against credentials and identity stores, additional protections for credentials and data extend to email security and secure web gateway (CASB) providers. This helps ensure greater password security, integrity of accounts, adherence to organizational rules, and avoidance of high-risk shadow IT services.

What are the Core Principles of the Zero Trust Model?

The Zero Trust model (based on NIST 800-207) includes the following core principles:

- **Continuous verification.** Always verify access, all the time, for all resources.
- **Limit the "blast radius."** Minimize impact if an external or insider breach occurs.
- **Automate context collection and response.** Incorporate behavioral data and get context from the entire IT stack (identity, endpoint, workload, etc..) for the most accurate

1. Continuous Verification

Continuous verification means no trusted zones, credentials, or devices at any time. Hence the common expression "Never Trust, Always Verify." Verification that must be applied to such a broad set of assets continuously means that several key elements must be in place for this to work effectively:

- Risk based conditional access. This ensures the workflow is only interrupted when risk levels change, allowing continual verification, without sacrificing user experience.
- Rapid and scalable dynamic policy model deployment. Since workloads, data, and users can move often, the policy must not only account for risk, but also include compliance and IT requirements for policy. Zero Trust does not alleviate organizations from compliance and organizational specific requirements.

2. Limit the Blast Radius

If a breach does occur, minimizing the impact of the breach is critical. Zero Trust limits the scope of credentials or access paths for an attacker, giving time for systems and people to respond and mitigate the attack.

Limiting the radius means:

- **Using identity based segmentation.** Traditional network based segmentation can be challenging to maintain operationally as workloads, users, data, and credentials change often.
  Least privilege principle. Whenever credentials are used, including for non-human accounts (such as service accounts), it is critical these credentials are given access to the minimum capability required to perform the task. As tasks change, so should the scope. Many attacks leverage over privileged service accounts, as they are typically not monitored and are often overly permissioned.

3. Automate Context Collection And Response

To make the most effective and accurate decisions, more data helps so long as it can be processed and acted on in real-time. NIST provides guidance on using information from the following sources:

- User credentials – human and non-human (service accounts, non-privileged accounts, privileged accounts – including SSO credentials)
- Workloads – including VMs, containers, and ones deployed in hybrid deployments
- Endpoint – any device being used to access data
- Network
- Data
- Other sources (typically via APIs):
  - SIEM
  - SSO
  - Identity providers (like AD)
  - Threat Intelligence

Stages of Implementing Zero Trust

Although each organization's needs are unique, the following is a generic Zero Trust model:

- **Stage 1:Visualize** – understand all of the resources, their access points, and

visualize risks involved
- **Stage 2: Mitigate** – detect and stop threats or mitigate impact of the breach in case a threat cannot be immediately stopped
- **Stage 3: Optimize** – extend protection to every aspect of the IT infrastructure and all resources regardless of location while optimizing the user experience for end-users, IT, and security teams

Update May 2022

Passwordless sign-ins are already a practical reality, but they're sometimes clunky — and three of the biggest tech companies believe they can reduce the friction. Apple, Google and Microsoft are teaming up to expand support for a password-free sign-in standard from the FIDO Alliance and World Wide Web Consortium. You'll get to use FIDO authentication on a phone or tablet to sign into an app or website on a nearby device, regardless of platform. Likewise, you'll often have automatic access to your FIDO credentials without having to add every account on a given device, even on brand new hardware.

The aim is to allow "end-to-end" passwordless sign-ins for apps and websites, not just at certain stages. You'd only need to use biometric scans (such as your face or finger) or a device PIN to sign in at every step. The effort will hopefully prevent successful phishing attacks that trick you into sharing passwords with hackers and scammers.

Apple, Google and Microsoft all plan to make the enhanced zero-password features available on their platforms throughout the "coming year." You may have to wait for a significant operating system update to see the upgrade. The wait might be endurable, though, if passwords are far less necessary than they are today.

Links to additional information

Gartner's Zero Trust Recommendation/Strategy Link

Auth0 Passwordless Authentication Link

Cisco Zero Trust Link

Source articles for this page:

- Passwordless authentication | Microsoft Security
  - ‘Microsoft Security – Passwordless Protection’ 2021 document
- Passwordless - The Future of Authentication
  - ‘Cisco Duo – Passwordless – The Future of Authentication’ document
- FIDO2 - FIDO Alliance
- WebAuthn
- Apple reveals more on its plans to kill off passwords for good
- What is a Zero Trust Architecture
- What is Zero Trust Security? Principles of the Zero Trust Model
- Zero Trust Security: A Comprehensive Guide | OneLogin
- https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
- FIDO Alliance - Open Authentication Standards More Secure than Passwords
- Apple, Google and Microsoft commit to 'end-to-end' password-free sign-ins | Engadget