Zero Trust

Identity as the new perimeter for Zero Trust

Whitepaper

Executive Summary

COVID-19 changed many aspects of our lives—including how and where we work. With the dramatic rise in remote work, previous IT security default options, like using a virtual private network (VPN), quickly proved insufficient and insecure for many companies. Organizations need to be able to establish trust relationships in order to securely enable access for various people (employees, partners, contractors, supply chain, etc.) regardless of their location, device, or network. Unfortunately, traditional IT security perimeters framed around weak, password-based access credentials have proven ineffective for protecting your remote workforce, API ecosystem, and digital transformation initiatives.

Zero Trust is a security strategy that challenges the notion that there is a "trusted" internal network and an "untrusted" external network, and it views unverified trust as a vulnerability. There is no denying that the perimeter has shifted permanently and we can no longer rely solely on a network perimeter-centric view of security. This transformation has accelerated more recently to a fully distributed and hybrid working environment requiring a new model for security. There is a new modern perimeter that needs to be protected, and that perimeter begins with a strong secure identity.

This paper explores why effective access management solutions offer the core technology that organizations should start with on their zero trust journeys. There is no easy solution when it comes to achieving a zero-trust security architecture: this is not something that happens overnight, or is in fact ever actually 'complete'. Here, we'll explore the shifts in the security landscape that led to the creation of zero trust, what a zero-trust strategy looks like today, and how organizations can utilize 1Kosmos as the foundation for a successful zero trust program now, and into the future. Adopting a zero-trust security strategy provides the ability for organizations to transform and innovate, simplify security infrastructure by adopting new technologies and practices, optimize user productivity and reduce their risk surface.

What is Zero Trust

Zero Trust is a security framework requiring all users, whether inside 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.

It uniquely addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ultimately mitigating threats from ransomware, phishing and data breach threats.

As the world emerged from the pandemic, many organizations made the decision to continue supporting a dynamic work model, meaning they must maintain flexibility while securing fully distributed workforces and hybrid working models. Most operations have now shifted to support remote work overnight, effectively dismantling traditional security models, accelerating the adoption of cloud technologies, and forcing the shift to support remote work outside the safety of a corporate network. The modern workforce—comprised of employees, contractors, partners, and suppliers—are all accessing more resources and data (stored in the cloud and on-premises), from more devices and locations than ever before.

> "Where today's security approaches fail to protect data, Zero Trust is the best, most modern way to keep your network secure."
>
> **John Kindervag**
>
> **VP and Principal Analyst at Forrester**

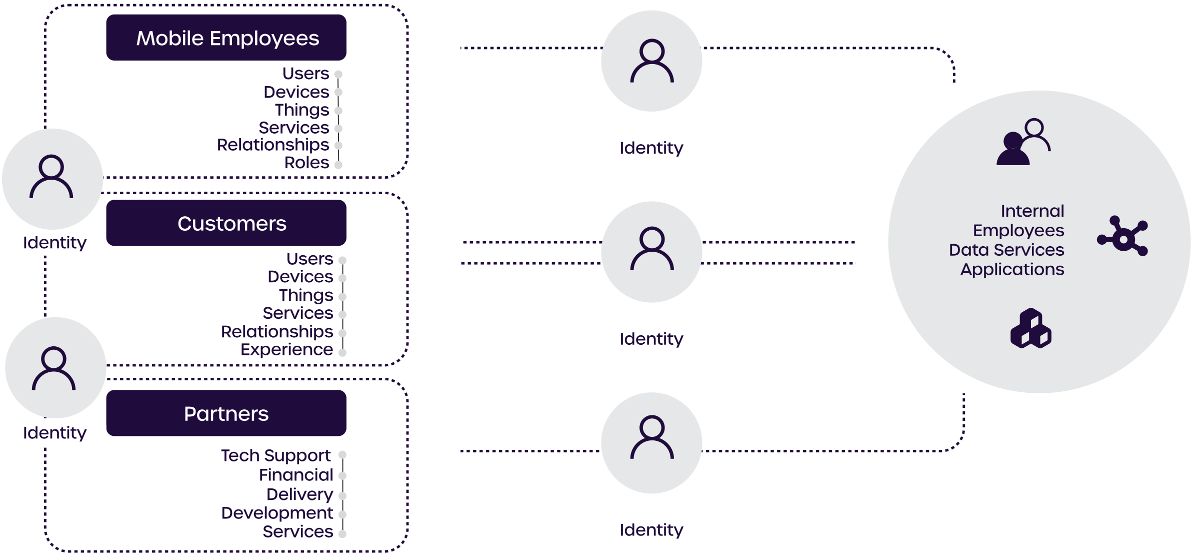
Evolution of Zero Trust

Although a Zero Trust model was introduced in 2009, Google's BeyondCorp research published in 2014, significantly made advancements towards the Zero Trust architecture as this model shifts access controls from the perimeter to individual devices and users. Gartner has published their CARTA framework and Forrester has published the Zero Trust extended ecosystem in 2019, both calling out the need for multi-factor authentication (MFA) to reduce access threats exponentially.

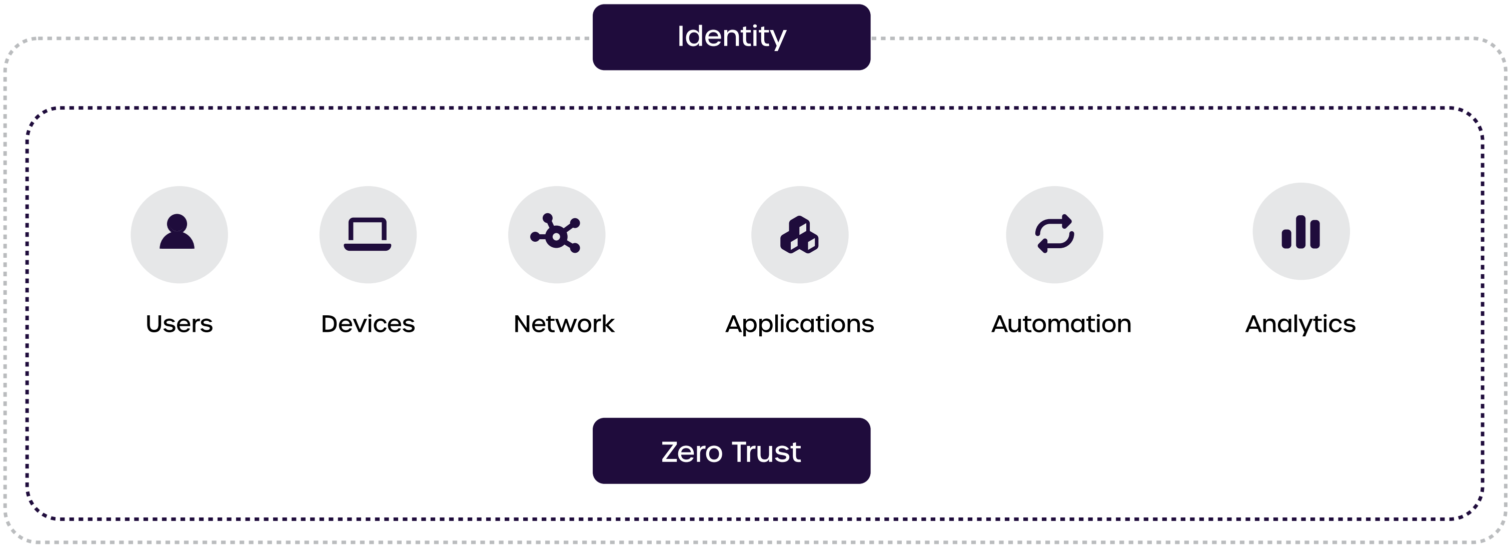
The industry, practitioners, and analysts have developed a collective understanding of zero-trust security strategies over the past 20 years to match technological advances and the way that we work. In all cases, the approach has become increasingly more risk-based and identity-centric — this is where 1Kosmos can support organizations. The 1Kosmos platform can help you address your business challenges and accelerate the adoption of zero-trust security by providing the foundation for secure identity-based authentication that protects the modern perimeter.

Identity as the new perimeter for Zero Trust

In their whitepaper, the Identity Defined Security Alliance states that "Zero Trust" starts with "identity", whose goal is to gain access to "data." In most transactions, identity is the "credential" provided to a trusted user within the enterprise. Security organizations can use an identity-centric approach to ensure that the right people have access to the right resources in the right context. A centrally managed authentication system is required to ensure strong, adaptive authentication. The right level of authentication assurance is to be granted depending on the risk associated with the transaction. Continuous authentication is also required across all systems, devices, and control points. This monitors changes in behavior and context to let you know if another user takes control of the session.



"Zero Trust" starts with **"identity"**, whose goal is to gain access to "data." In most transactions, identity is the "credential" provided to a trusted user within the enterprise.



Identity

Users

Devices

Network

Applications

Automation

Analytics

Zero Trust

Kill the Password

Passwords are more insecure than ever. Organizations relying on passwords serve up, on a silver platter, a large and easy-to-exploit threat surface: **27% of breaches are carried out using lost or stolen credentials**, and **18% are carried out as phishing attacks**[1].

85%

of breaches had a human element involved

35%

of all breaches involve social engineering

61%

involve credentials

13%

of all incidents now involve ransomware

Kill the Password

The 2021 Verizon Breach report highlights that 85% of breaches had a human element involved. It reiterates that social engineering is the leading way for bad guys to get into the front door. This makes sense, humans are the weakest link in any system. You can see here that about 35% of all breaches involve social engineering. 61% involve credentials, and 13% of all incidents now involve ransomware. Put these together and you have a major problem due to reliance on passwords. In addition, employee behavior makes this even more challenging.

Employees will reuse passwords. Users will still select phrases that hackers can easily guess from culling social networks. Phishing will still be very effective for attackers. This is also problematic when the email address is the username since people are inclined to use the same password for a given email address. So, if they're using their corporate email for external sites, this exposes the organization to greater security risk.

Passwordless Authentication can solve these challenges as well as reduce friction when implementing a zero-trust framework. In addition, employee behavior makes this even more challenging. Single-factor mobile authenticator apps are used by organizations with single-factor biometrics or third-party-verified digital certificates. Multi-factor passwordless authentication methods may be used by security-conscious organizations that rely on both "something you have" or "something that you are". It is crucial to use automated intelligent authentication such as continuous, contextual, and/or risk-based authentication (RBA) at this stage. Network (IP-based) authentication may be used for contextual authentication.

[1] 465 global security decision makers with network, data center, app security, or security ops responsibilities who experienced an external attack when their company was breached. Source: Forrester Analytics Global Business Technographics® Security Survey, 2019.

Identity at the center of your authentication

Passwordless Authentication is often interpreted in 3 ways:

Single Sign On (SSO)

This is where a user is asked to enter their credentials once and then are signed on to all the applications connected to the SSO Server without entering a credential

Two Factor Authentication (2FA)

In this case, the user is asked to enter their username and an OTP is sent via SMS / Email that they are asked to enter

Multi-factor Authentication (MFA)

This is a more advanced method, where a user is asked to enter their username and then a notification is sent to a paired device which can be a smartphone and a user is asked to swipe or approve the request.

All the above methods may look like an effective method to implement passwordless authentication, but they are not secure and full of friction for a user. OTPs can be stolen. The security of SMS OTP is directly dependent on the safety of the receiving device, and just like the device, the OTP may be vulnerable to physical attacks. An attacker – who doesn't have to be miles away – can gain physical access to the device and steal it. In addition, the actual device of a user can be compromised or stolen making any of the 2FA / MFA methods highly problematic.

Biometrics or more specifically device biometrics on a user's smartphone are an effective way to combat the challenges listed above. Fast Identity Online (FIDO) standards support multifactor authentication (MFA) and public key cryptography. Unlike password databases, FIDO stores personally-identifying information (PII), such as biometric authentication data, locally on the user's device to protect it.

FIDO supports the Universal Authentication Framework (UAF) and the Universal Second Factor (U2F) protocols. With UAF, the client device creates a new key pair during registration with an online service and retains the private key; the public key is registered with the online service. During authentication, the client device proves possession of the private key to the service by signing a challenge, which involves a user-friendly action such as providing a fingerprint, taking a selfie, etc.

With U2F, authentication requires a strong second factor such as a Near Field Communication (NFC) tap or USB security token. The user is prompted to insert and touch their personal U2F device during login. The user's FIDO-enabled device creates a new key pair, and the public key is shared with the online service and associated with the user's account. The service can then authenticate the user by requesting that the registered device sign a challenge with the private key.

In addition to the device-based biometrics that can be implemented, a more secure method is to check if the user authenticating every time is the actual user who registered. The 1Kosmos platform provides a feature called LiveID that checks for the liveness of a user every time they authenticate. This ensures that the user authenticating into the device is the actual user who registered and they are present "live" while authenticating into a system.

A user can be verified while registering for access and this verification can be done based on the NIST 800-63-3 standard for identity verification. This allows an identity assurance level to be assigned to a user which adds more context behind the identity of a user and every authentication event.

New employees or high-valued customers, can be guided through a self-enrollment process to capture and verify their identity credentials like their government-issued document such as driver's license or a passport.

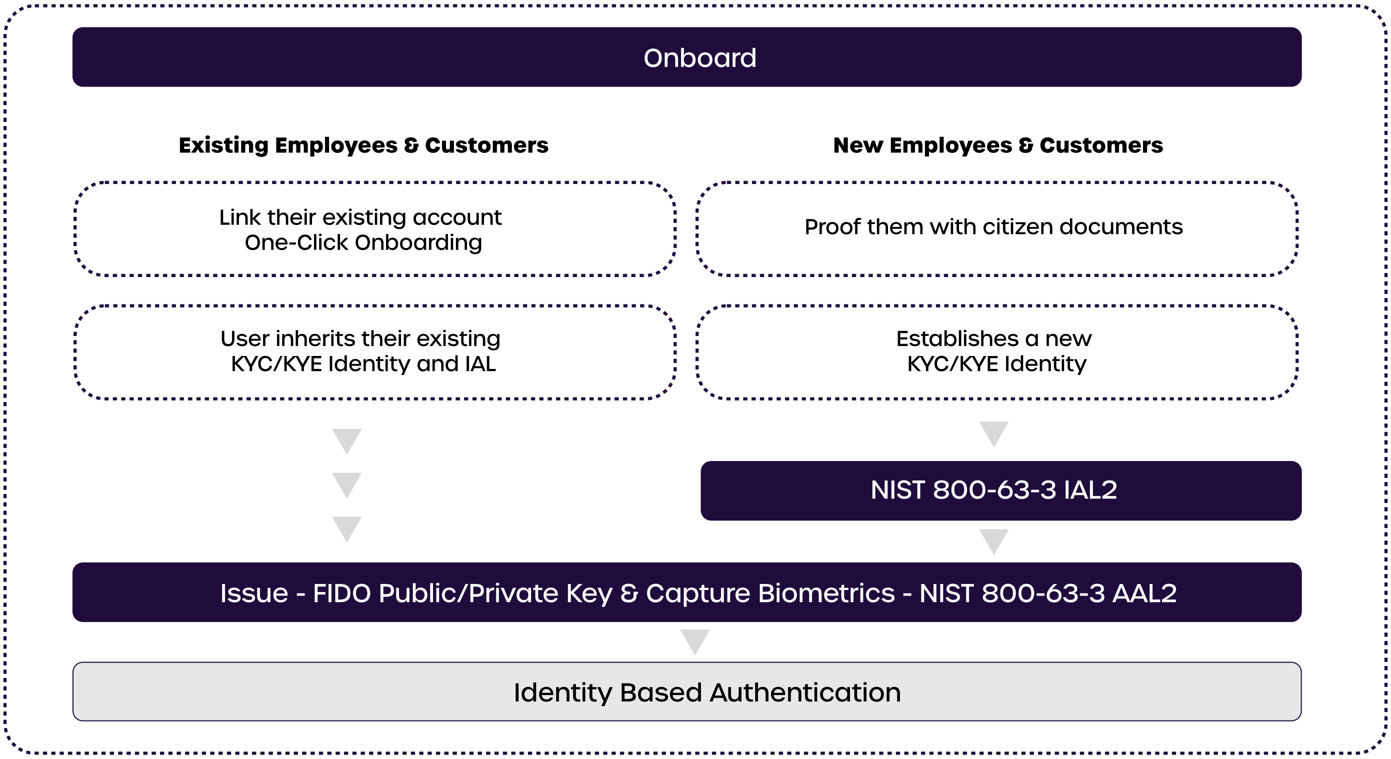
Future of Zero Trust

While protections at the authentication layer—such as MFA, device fingerprinting, location checks, etc.—are valuable at the time of authentication, it's also important to have frequent checks after the initial authentication. In a cloud and mobile-centric world, most people access both corporate and personal apps from a variety of different devices. And login sessions across apps can often last for hours, days, or even weeks (especially in the case of native mobile applications). When your device is stolen, or you log into an app on a shared computer, the initial MFA prompt becomes meaningless if your app session remains active. A bad actor could open up the app and easily access your data.

Future of Zero Trust

Any Zero Trust Implementation must answer the question of "Who" behind every authentication and having a real identity behind every authentication reduces security risk, as well as reduces user friction and increases adoption within the organization. This is the anchor point of the new modern perimeter.

1Kosmos provides the foundation to provide continuous visibility into multiple contextual aspects in order to establish and adapt trust controls for access.


Onboard
Existing Employees & Customers
New Employees & Customers
Link their existing account
One-Click Onboarding
Proof them with citizen documents
User inherits their existing
KYC/KYE Identity and IAL
Establishes a new
KYC/KYE Identity
NIST 800-63-3 IAL2
Issue - FIDO Public/Private Key & Capture Biometrics - NIST 800-63-3 AAL2
Identity Based Authentication

About 1Kosmos
1Kosmos enables remote identity verification and passwordless multi-factor authentication for workers, customers and residents to securely transact with digital services. By unifying identity proofing, credential verification and strong authentication, the 1Kosmos platform prevents identity impersonation, account takeover and fraud while delivering frictionless user experiences and preserving the privacy of users' personal information. 1Kosmos performs millions of authentications daily for government agencies and some of the largest banks, telecommunications, higher education, and healthcare organizations in the world.