Verified™

WHITE PAPER

Never Trust. Always Verified.

A Comprehensive Guide to Zero Trust Implementation for 2023 and Beyond

authID HUMAN FACTOR AUTHENTICATION™

Introduction

Zero Trust has been around for a decade but increased MFA circumvention, supply-chain and ransomware attacks, the rapid adoption of largely remote workforces, and finally the White House issuance of Executive Order 14028 has propelled Zero Trust forward as a focus for professionals concerned with data security.

In this paper, we will discuss Zero Trust architecture, what it is, why we need it, and common implementation challenges. You will also learn how organizations can use authID's Verified™ to fortify enterprise security, support Zero Trust Architecture, enable Zero-Trust Access, and satisfy orders from the White House, even to protect legacy and disparate systems, as well as diverse device environments.

What is Zero Trust?

Zero Trust replaces implicit trust with continuously assessed explicit risk and trust levels, based on identity and context; supported by security infrastructure that adapts to the risk optimized posture of the organization.

NIST defines "Zero Trust" as an evolving set of cybersecurity paradigms that assumes all traffic is hostile and allows no implicit trust to be granted to assets or users.

In a nutshell, Zero Trust:

- ✓ Requires that both users and devices be authenticated before connecting to or accessing an enterprise resource to protect it from unauthorized access.
- ✓ Does not assume that everything that has access to an environment should have access to everything else within that environment like legacy network environments often do.
- ✓ Focuses on individual and small groups of resources and granular control of access to them vs. the defense of a wide network perimeter.

Components of Zero Trust

The US National Institute of Standards and Technology (NIST) asserts that Zero Trust architecture include the following core components:

The Policy Enforcement Point 1

is the gateway to secure access for corporate resources, and is responsible for enabling, monitoring, and terminating connections between users, devices, and enterprise data.

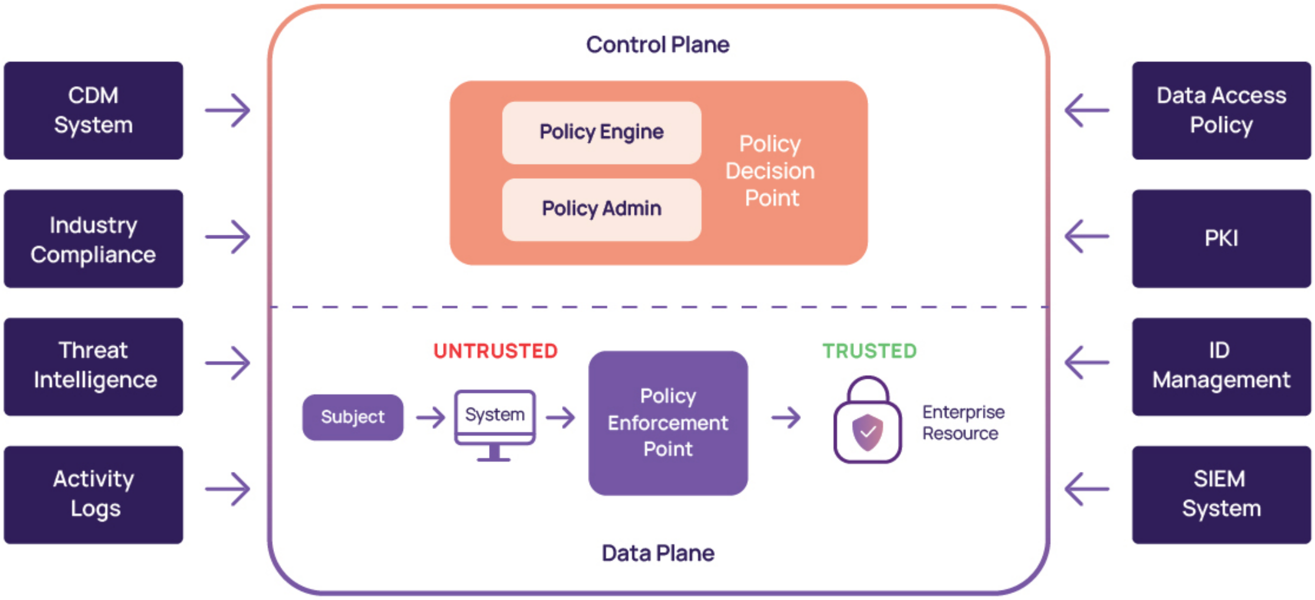
The Policy Engine 2

decides whether to grant access to organizational resources based on policies set by the organization's security team.

The Policy Administrator 3

is responsible for executing the access decisions made by the policy engine; this component allows or denies communication between a user and a protected resource.

As shown in this NIST diagram, these three components work together to control access to organizational resources, monitor activities on the network, and ensure that trust is never implicit.



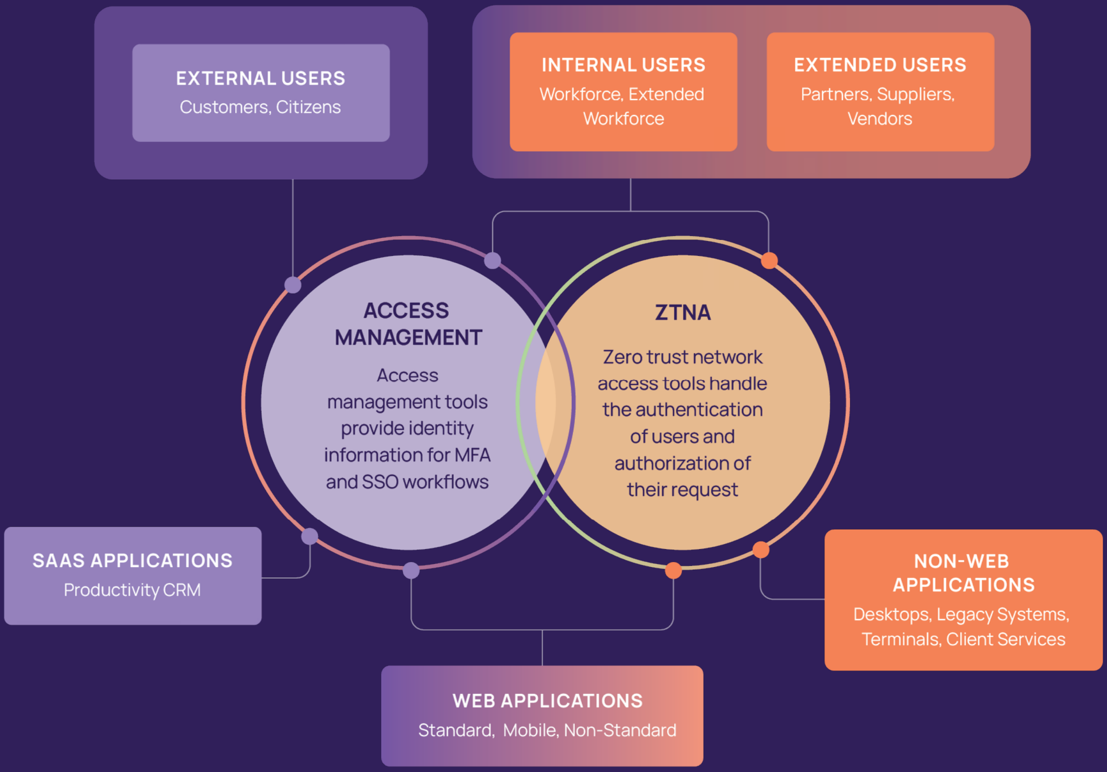
Why Zero Trust?

In the past, security teams have focused on protecting the "perimeter" - protecting access to trusted enterprise networks by implementing access controls like CASBs and VPN.

With this methodology, however, security holes and authentication vulnerabilities leveraging passwords and transient trust still arise. On the other hand, a Zero Trust approach centralizes access mechanisms, and grants access based on the risk and trustworthiness of both the user and the device, resulting in a more secure and resilient environment.

How Does Authentication Fit into Zero Trust Architecture?

Zero Trust Architecture is centered around identity and data, as the goal of Zero Trust implementation is to protect access to data by specific, authorized identities dynamically. The authentication of both users and devices is core to Zero Trust Architecture as their verification prevents unauthorized access to networks, applications, and databases.

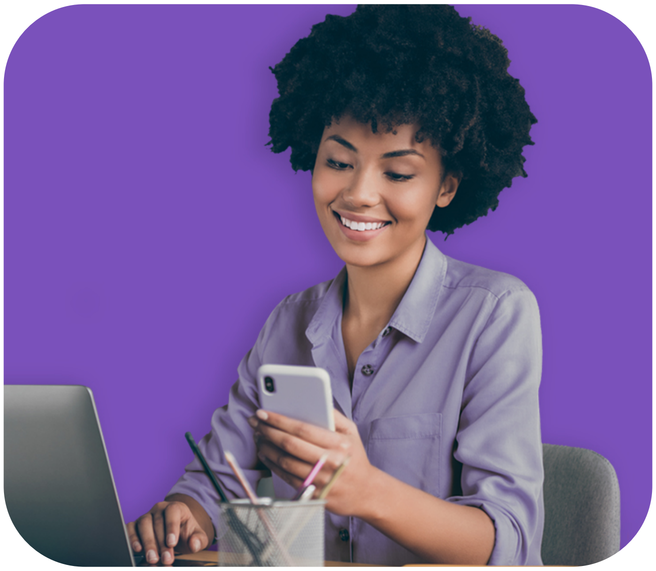

EXTERNAL USERS
Customers, Citizens
INTERNAL USERS
Workforce, Extended Workforce
EXTENDED USERS
Partners, Suppliers, Vendors
ACCESS MANAGEMENT
Access management tools provide identity information for MFA and SSO workflows
ZTNA
Zero trust network access tools handle the authentication of users and authorization of their request
SAAS APPLICATIONS
Productivity CRM
NON-WEB APPLICATIONS
Desktops, Legacy Systems, Terminals, Client Services
WEB APPLICATIONS
Standard, Mobile, Non-Standard

Without strong authentication protocols in place to confirm the identity of the user and the device requesting access, security teams cannot obstruct unauthorized access to resources.

Zero Trust Authentication is Secure Access Using Zero Trust Principles

Zero Trust solutions must leverage Zero Trust principles to secure access to any resource the organization chooses, both on premise and in the cloud.

Zero Trust Authentication is an essential element for Zero Trust deployments – together they deliver invaluable benefits to the deploying organization from a more secure and productive workforce to simplified compliance support and robust auditing trails.



Zero Trust, Zero Blind Spots

Real-time authentication right before each access attempt and the assumption that all traffic is hostile allows organizations to be more granular in their access controls – providing optimal protection for organizational resources.

Reduce Lateral Movement Risk

Zero Trust Architecture gives users least privileged access in real-time to reduce the risk of lateral movement. By giving each user the minimum privileges needed to complete their work, and shrinking the amount of time between user authentication and action, the "blast radius" of a breach event is controlled – as fewer users have access to sensitive organizational information.

Reduce Attack Surfaces

Zero Trust Architectures reduces the "ways in" by securing the vectors of compromise most used by cybercriminals to gain unauthorized access to organizational assets. Zero Trust deployments using passwords are still susceptible to most attacks and can only provide moderate levels of identity assurance as passwords are shareable and reusable.

Common Challenges When Implementing Zero Trust

Organizations and government entities developing Zero Trust architecture face several challenges on the road to Zero Trust.

Legacy Systems and Implicit Trust

Legacy systems leverage implicit trust allowing users who have access to enterprise digital environments to access data, without proving who they are. This directly conflicts with Zero Trust security paradigms – as all traffic should be considered hostile and thus monitored and authenticated prior to allowing interaction with organizationally owned resources.

Legacy Systems and Cost

For organizations adopting Zero Trust, the cost to completely remove, rebuild, or replace IT infrastructure may be prohibitive. Many solutions that enable Zero Trust access will require the replacement of legacy solutions – or an overhaul of disparate technologies, an often significant monetary investment on behalf of these organizations..

Many MFA Solutions Rely on Only "Assumed" Trust

Device–dependent authentication places a level of assumed trust in the possession of the device. Most device-based authenticators do not require a "live" biometric for user identity verification or access authorization. Instead, these solutions assume that the registered device is in the possession of the account holder based on other factors, leaving the door open for unauthorized access.

The Road to Zero Trust is Murky

Though direction has come from the White House that federal agencies must adopt Zero Trust practices, there is still no formal consensus around the adoption of a maturity model for Zero Trust architectures. Private and government organizations in critical infrastructure sectors will need to search for Zero Trust Access and architecture solutions.

There is No Such Thing as Perfection

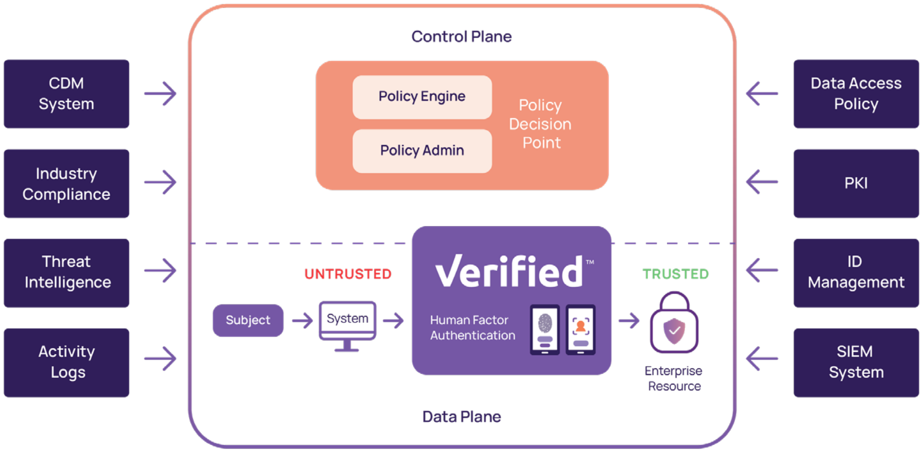
Zero Trust is not a product, but a framework of guiding principles that at their core reflect the concept of "Never trust, always Verify." Organizations beginning their Zero Trust journey may feel overwhelmed, or hit roadblocks concerning their people, systems, and processes but should remember that perfection is not the goal, heightened security is.

authID's Verified™ Supports Zero Trust With Human Factor Authentication™

Verified, authID's best-in-class identity authentication platform, delivers Human Factor Authentication (HFA) that combines FIDO2 passwordless authentication with cloud biometric security, to identify the human behind the device, anywhere.

HFA delivers a biometric chain of trust to authenticate both the device and account holder, thereby making no assumptions on who is accessing your network or requesting a privileged activity. Unlike other FIDO2 solutions, HFA delivers seamless portability, allowing users to reaffirm user identity with their cloud biometrics in the event of lost, stolen or replaced devices. Providing strong identity assurance, Verified supports Zero Trust Access that can be easily adapted to any application or existing authentication workflow.

How Verified™ Supports Zero Trust Access



1. Verified sits between the "untrusted zone" – the area before login and the "implicit trust zone" the area where all users are assumed to be trustworthy, behind login. Because our solution operates in real-time and can be invoked whenever deemed necessary, we shrink the "implicit trust zone" to whatever the organization decides.

2. Verified will disallow any connection to a resource where the user fails biometric verification.

3. Verified supports conditional access with role-based access policies and the ability to be invoked based on the organizational risk acceptance.

Verified authenticates devices leveraging FIDO2 compliant protocol and NIST conforming cryptographic standards to provide a truly flexible, strong authentication solution.

Verified shrinks "trust zones" - performing biometric multifactor authentication in real-time before allowing access to resources, wherever and whenever you choose.

Getting Started with Zero Trust HFA

Remove Implicit Trust From Your Environment

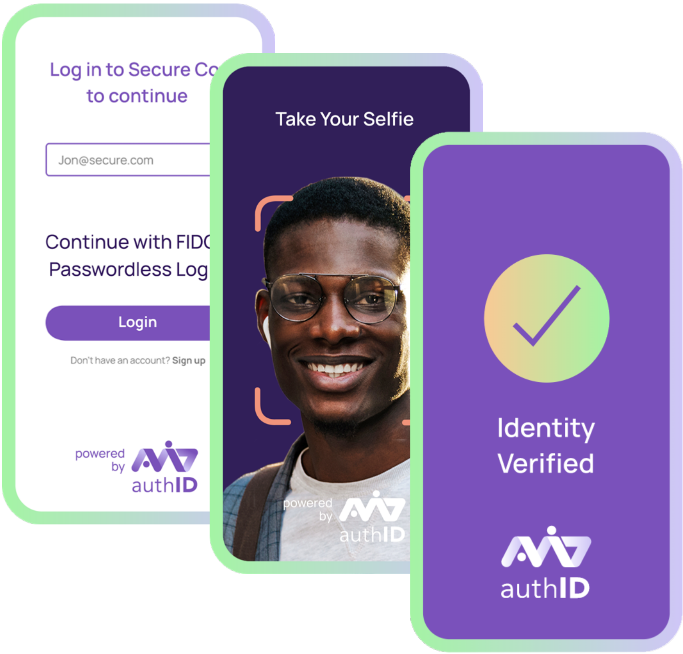
Verified's Human Factor Authentication can be invoked anywhere in the user journey, across systems and applications to remove transient trust between applications and login sessions.

Reduce Zero Trust Transformation Costs

Verified does not require you to rip out existing MFA or SSO solutions. Verified can be deployed as a second factor in a password-based authentication workflow or as a completely passwordless solution anywhere you choose to invoke secure authentication. We also offer low-code and no-code implementations that seamlessly integrate with existing security infrastructure including SSOs, IDPs, and EDRs.

Protect Access From Every Device

Verified is a device agnostic solution that allows users to authenticate in a browser using any registered mobile or desktop device.



Conclusion

Getting started with Zero Trust is not as daunting as it seems. authID can help you get started on the road to Zero Trust in less than ten minutes. Verified can connect disparate applications, devices, and user access cases with a centralized authentication mechanism. To protect your workforce environment, Verified supports Zero Trust Architecture with adaptive access capabilities, simplified and secure device recovery, immutable logs, and truly portable identity.

For more information on how authID's Verified Human Factor Authentication can accelerate your journey to Zero Trust, visit authid.ai/verified-workforce