authx

ZERO TRUST

FOR THE MODERN WORKFORCE

How enterprises can build continuous trust across users, devices, and applications?

CONTENT

A QUICK OVERVIEW

At **AuthX**, we help enterprises build continuous trust;
ONE IDENTITY, ONE DEVICE, ONE ACCESS AT A TIME.

THREE QUICK TRUTHS

68 %

of breaches start with compromised credentials.

(Verizon DBIR 2025).

82 %

of security leaders are moving toward identity centric Zero Trust.

(Gartner 2025)

40 %

faster breach containment for teams that connect identity, device, and policy layers.

(Ponemon Institute 2025)

THE NEW REALITY

Perimeters didn't vanish; they multiplied. Every remote login, mobile device, and SaaS app is now part of your security edge. Traditional network walls can't keep up, but identity can.
This whitepaper breaks down what a Zero Trust mindset really means in practice, how to start with user and device trust, and how AuthX brings it all together through adaptive MFA, SSO, and real-time device intelligence.
Our goal is simple: help you protect access without slowing anyone down.

THEN

Network Perimeter

NOW

Identity + Device Perimeter

FOREVER

Continuous Trust

THE PERIMETER DIDN'T DISAPPEAR; IT MOVED.

Once upon a time, your firewall defined safety. If users were inside the corporate network, they were trusted. That perimeter is gone. In today's cloud-first, remote, and device-diverse world, identity and context define access. The modern perimeter is no longer physical; it's who and what is connecting.

Remote work, SaaS, and BYOD have expanded the attack surface beyond recognition.

nearly

74%

of breaches involve the human element

over

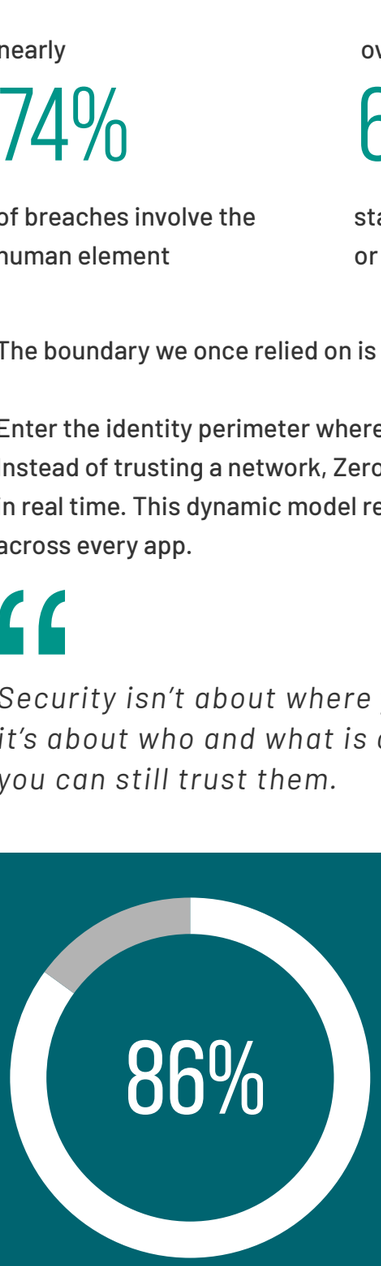
61%

start with stolen credentials or phishing.

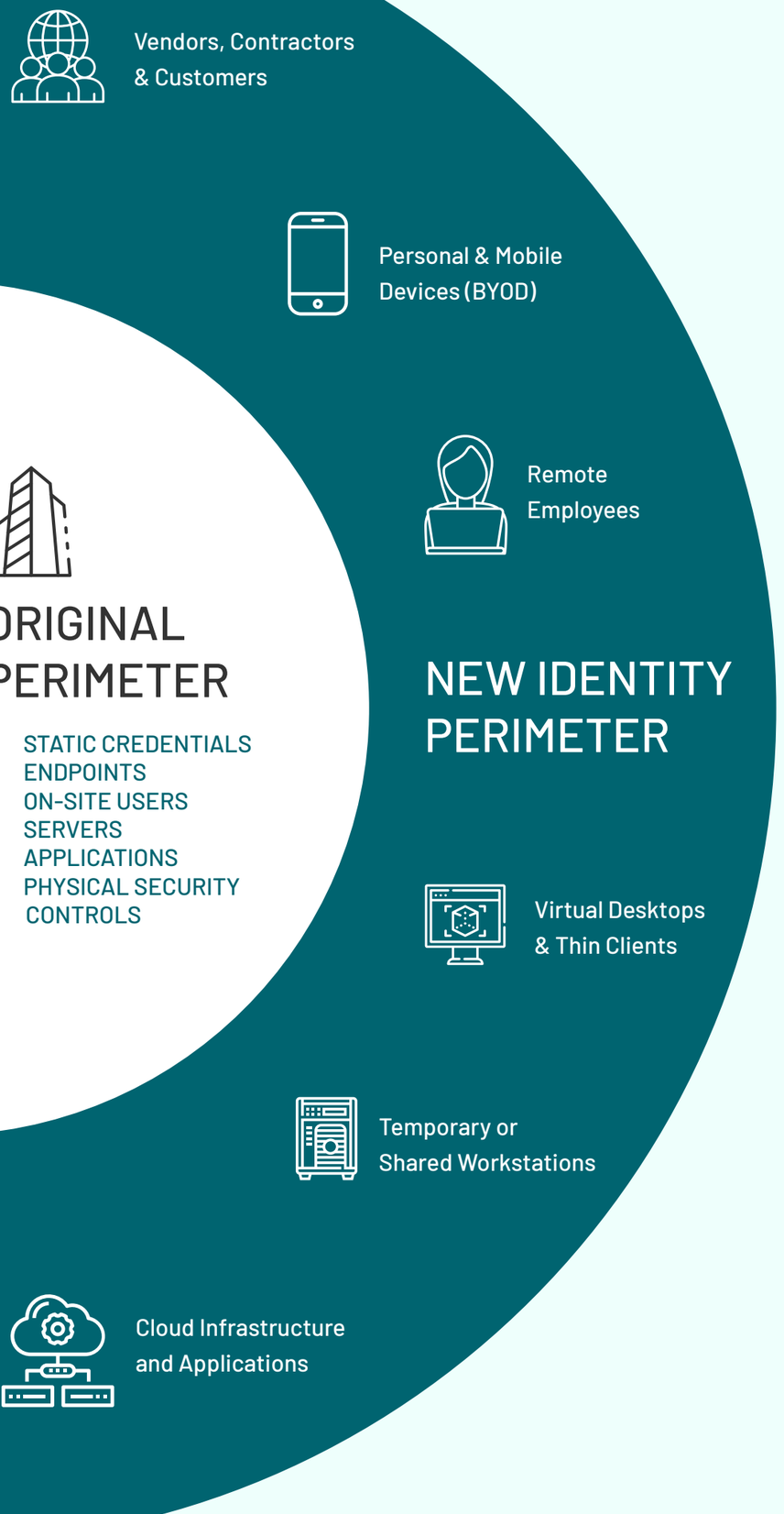
The boundary we once relied on is porous, mobile, and constantly changing.

Enter the identity perimeter where each user and device becomes the new security checkpoint. Instead of trusting a network, Zero Trust models verify each request, each session, and each signal in real time. This dynamic model reflects how modern work happens, from anywhere, on any device, across every app.

> *Security isn't about where you are connected from; it's about who and what is connecting, and whether you can still trust them.*



Stolen credentials are tied to 86% of security breaches involving web-based applications and platforms, which includes everything from online retail websites and email services to cloud storage and social media platforms.



ZERO TRUST ISN'T A PRODUCT. IT'S A PRACTICE.

Zero Trust isn't about buying another security tool; it's about changing how you think about trust itself. The old model assumed "inside = safe." The new model questions every access request, every device, every connection, continuously. Because in a hybrid, distributed world, "inside" doesn't really exist anymore.

At its core, Zero Trust operates on a simple rule:

Never trust, always verify.

But that doesn't mean "never trust anyone." It means trust is earned, and re-earned every time someone, or something, tries to connect.

THE GUIDING PRINCIPLES OF ZERO TRUST

Verify Explicitly

Validate every user and device with all available context; identity, location, device posture, and risk level.

Use Least Privilege Access

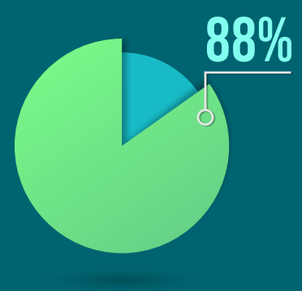
Give users only what they need, for as long as they need it. Nothing more.

Assume Breach

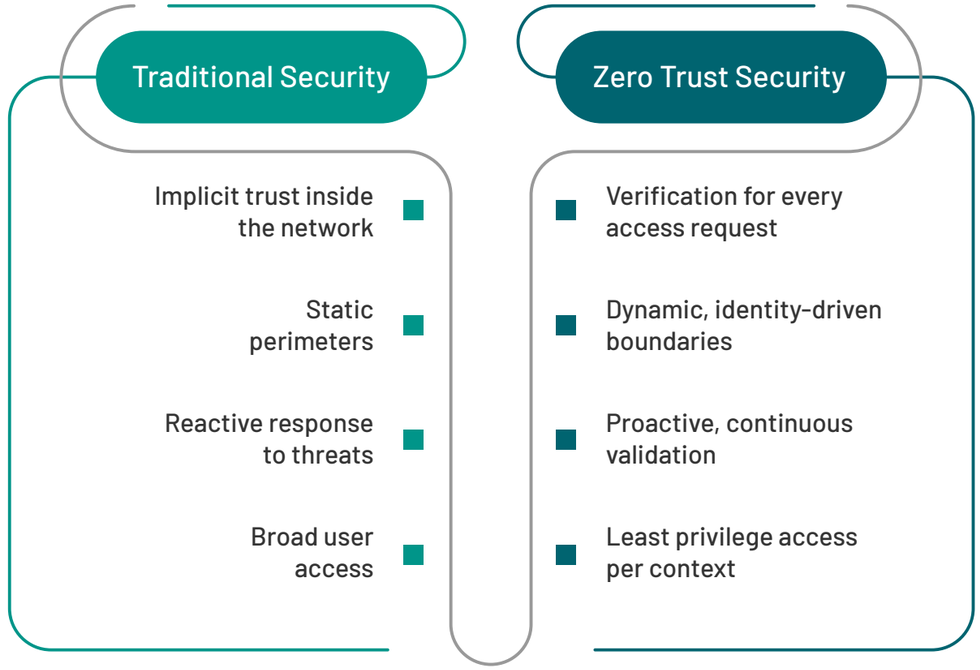
Design your security posture as if an attacker is already inside. Continuous validation ensures one compromised credential doesn't open every door.

NEW IDENTITY PERIMETER RISK

Compromised credentials remain a dominant attack vector because they grant direct access without exploiting technical vulnerabilities. Phishing, brute-force, and password-based attacks continue to scale, allowing attackers to bypass traditional defenses. According to Verizon, 88% of the breaches involve the Use of stolen credentials, which sometimes serves as both the first and only action, while other times, it is just one piece of a larger attack chain.



TRADITIONAL VS ZERO TRUST



Think of it like a secure facility:
Before anyone enters, they show ID (identity verification), their badge must be active (device trust), they get access only to approved rooms (least privilege), and they're monitored during their stay (continuous validation). That's Zero Trust in action.

> *Zero Trust isn't about saying no. It's about saying yes, but only to the right person, on the right device, under the right conditions.*

DIFFERENT NAMES. SAME MISSION — CONTINUOUS TRUST.

Zero Trust has many interpretations, but they all circle back to one core idea: verify everything, every time. Whether you follow Gartner's CARTA, Forrester's ZTX, or Google's BeyondCorp, the goal is the same; to make access adaptive, context-aware, and resilient against identity-driven attacks. Instead of chasing frameworks, smart organizations blend the best parts of each into their own Zero Trust strategy.

Gartner

Gartner CARTA (Continuous Adaptive Risk and Trust Assessment)

Focuses on continuous evaluation. Trust isn't static; it adapts as context changes. CARTA emphasizes ongoing risk assessment and dynamic policy adjustments.

FORRESTER®

Forrester ZTX (Zero Trust eXtended Framework)

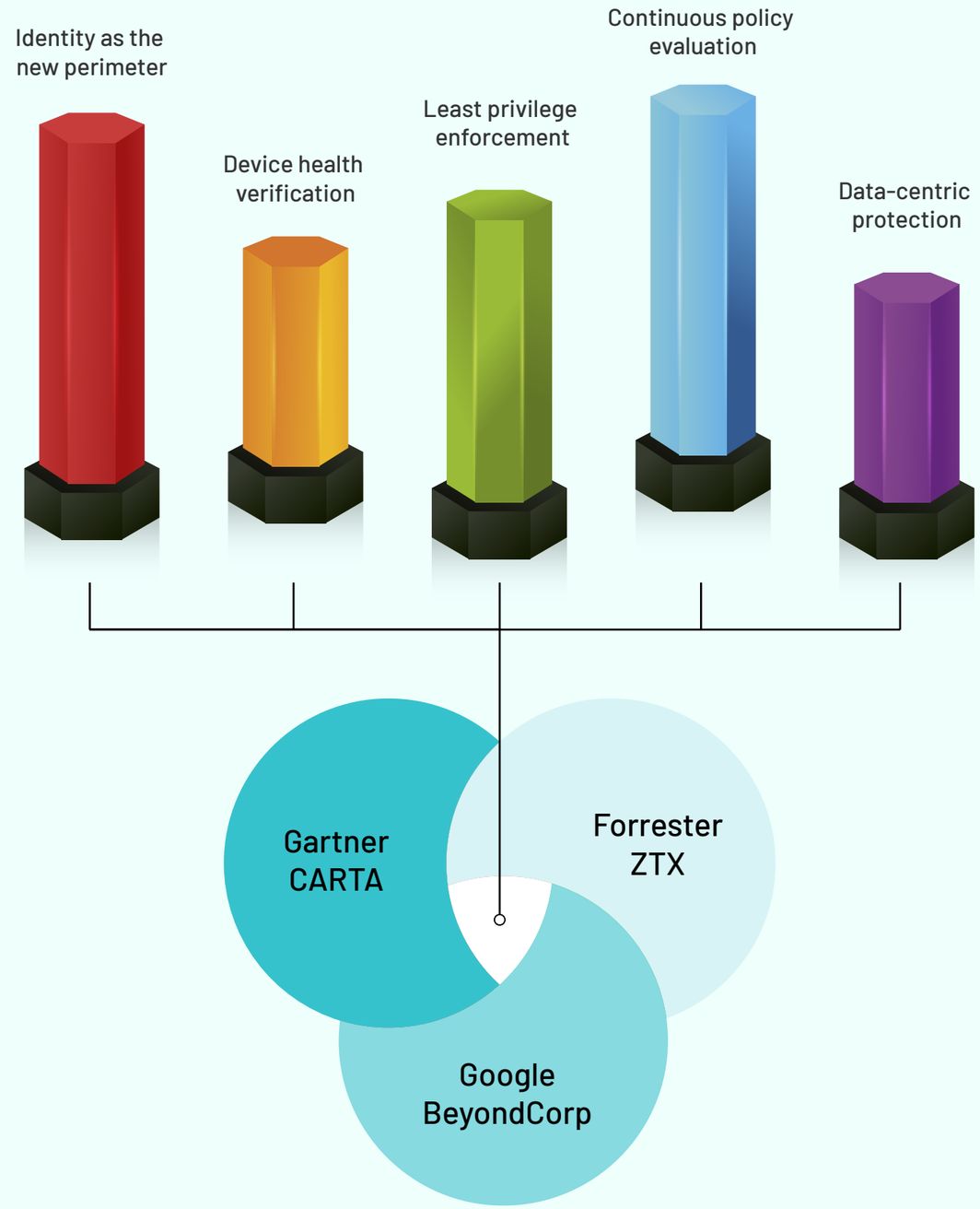
Centers around visibility and analytics. Every user, device, app, and workload must be authenticated, monitored, and logged. ZTX promotes least privilege and continuous enforcement.

Google

Google BeyondCorp

Pioneered network-independent access. Employees connect to corporate apps from untrusted networks, with access decisions based purely on user identity and device posture, no VPN required.

> *Choosing a model is less important than adopting the mindset. Zero Trust works when it's continuous, not configured once and forgotten.*



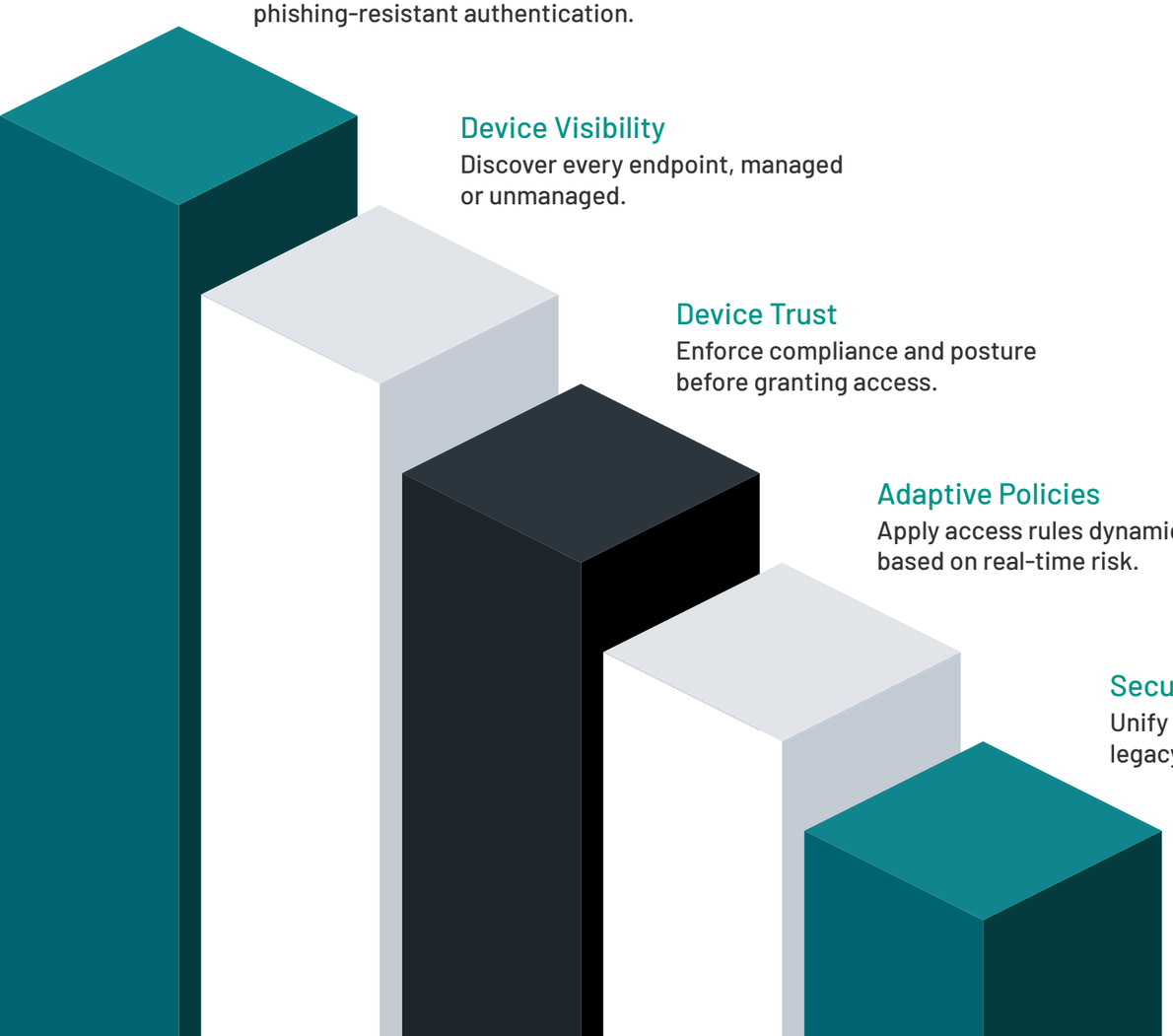
AuthX aligns across these frameworks by bringing continuous authentication, adaptive MFA, device trust, and contextual access under one platform, helping organizations operationalize Zero Trust without complexity.

START WHERE IT MATTERS MOST: YOUR PEOPLE.

Zero Trust can feel massive, but most successful programs start with one focus: the workforce. Employees, contractors, and partners are the ones connecting daily from different devices, networks, and locations. When you secure who they are and what they use, everything else follows.

The workforce perimeter is now the front line of enterprise defense. Identity and device are your two most reliable signals to determine trust. By linking them together, you can enforce smarter policies that adapt to user context without creating friction.

THE FIVE PILLARS OF WORKFORCE ZERO TRUST



User Trust
Verify identity with strong, phishing-resistant authentication.

Device Visibility
Discover every endpoint, managed or unmanaged.

Device Trust
Enforce compliance and posture before granting access.

Adaptive Policies
Apply access rules dynamically based on real-time risk.

Secure App Access
Unify protection across SaaS, legacy, and private apps.

NEVER TRUST, ALWAYS VERIFY.

These five steps lay the foundation for continuous trust, and it's exactly where AuthX simplifies Zero Trust for the modern workforce.

1. ESTABLISH USER TRUST

Every Journey Starts with Strong Identity.

Before you protect devices or apps, start with who's behind the keyboard. Establishing user trust is the core of Zero Trust. Strong, phishing-resistant MFA combined with identity assurance ensures access decisions are made only for verified users — not stolen credentials.

Modern MFA isn't just about adding another step; it's about using smarter signals. Passkeys, biometrics, and device-based verification reduce prompt fatigue and defeat phishing attempts before they start.
Automation and user-friendly self-enrolment turn security from a chore into a seamless part of everyday access.

BEST PRACTICES

- Use adaptive MFA to trigger verification only when context changes.
- Automate onboarding so users can self-register safely.
- Offer multiple factors but prioritize phishing-resistant methods.
- Make it fast; security that slows users down eventually fails.

> *Security that slows users down eventually fails. The best MFA disappears into the background.*

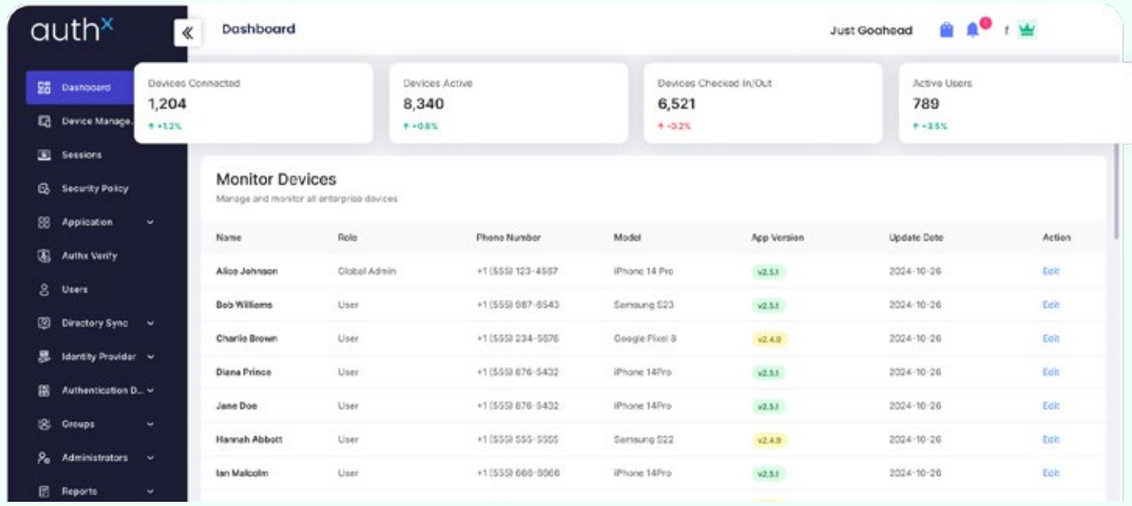
2. GAIN VISIBILITY INTO DEVICES

You Can’t Trust What You Can’t See.

Once user identity is secured, the next challenge is understanding the devices that connect. Laptops, phones, tablets, and even unmanaged endpoints all carry risk. Zero Trust begins with visibility, knowing exactly which devices are accessing your systems and what state they’re in.

An effective Zero Trust strategy relies on a live inventory of all devices, managed and unmanaged. It’s not just about listing them, it’s about assessing their posture: encryption, OS version, patch status, and compliance. Agentless discovery tools and integrations with MDM or SIEM solutions give security teams the visibility they need without slowing down operations.

When integrated with AuthX, device insights sync in real time flagging high-risk endpoints and dynamically updating access rules.



OUR RECOMMENDATIONS

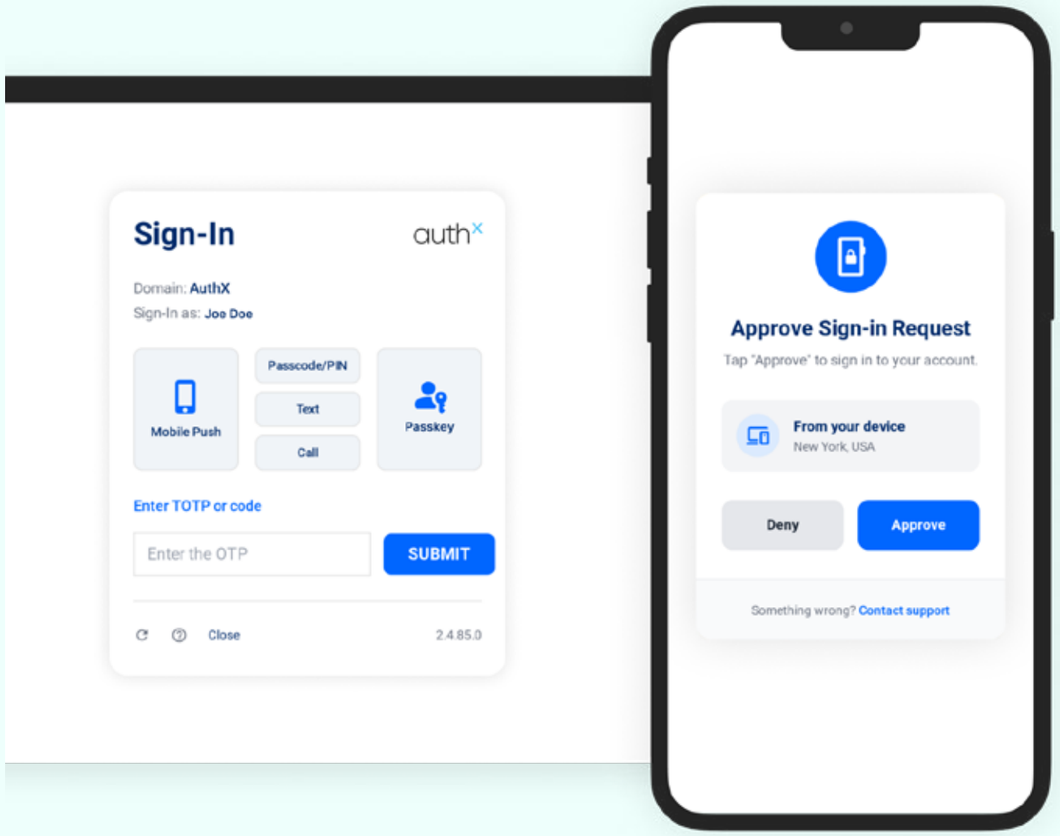
1. Map every device connecting to your network or apps.
2. Use agentless discovery where installation isn’t possible.
3. Identify OS versions, patch levels, and encryption status.
4. Integrate device data into your access policies automatically.

> *Visibility is power. The moment you see your devices clearly, Zero Trust becomes measurable.*

Once devices are visible, the next step is validating which ones deserve access. Zero Trust turns visibility into device trust, enforcing real-time posture checks before access is granted. It's not just about detecting devices; it's about verifying that each one is secure and compliant.

Device trust relies on posture assessment at the moment of access. Is the device encrypted? Is the OS up to date? Is it managed under corporate MDM or personal and unverified?
If a device fails a posture check, AuthX triggers a self-remediation workflow instead of blocking the user outright. This guided path helps users update their systems, re-scan, and regain access without IT intervention, reducing helpdesk tickets and keeping productivity intact.

With AuthX, device trust and user identity work together. Risk signals from both continuously update, allowing policies to evolve dynamically. For example, if a device suddenly loses MDM registration or shows an outdated antivirus, AuthX can automatically require re-authentication or revoke access until fixed.



> *Zero Trust works best when users can fix problems themselves, not wait for IT.*

3. ESTABLISH DEVICE TRUST

Visibility Is Step One. Trust Is Step Two.

4. ENFORCE ADAPTIVE POLICIES

Static Rules Don't Work in a Dynamic World.

The real power of Zero Trust comes from adaptive policies, rules that evolve with context. Instead of one-size-fits-all access, adaptive models consider identity, device posture, role, location, and even time of day to decide what's allowed.

Adaptive policies analyze context continuously to apply the right level of verification. For example, a clinician accessing EHR systems like Epic from a trusted workstation may get instant access, while the same user logging in from a new laptop triggers step-up MFA.
Similarly, if an administrator tries to connect to cloud infrastructure like Microsoft Azure or Google Cloud from an unmanaged device, AuthX can automatically block access and alert IT.

By integrating signals from identity, device posture, MDM, and network telemetry, AuthX builds a unified adaptive policy engine. Risky devices or users trigger real-time actions, from MFA prompts to session termination. Admins also receive instant notifications for unusual devices or access behavior.

An example of a Policy Matrix Table

User Type	Device State	App Risk	Action
Employee	Healthy	Low	Allow
Contractor	Unknown	Medium	MFA Required
Executive	New Device	High	Step-up Auth
Guest	Unmanaged	High	Block

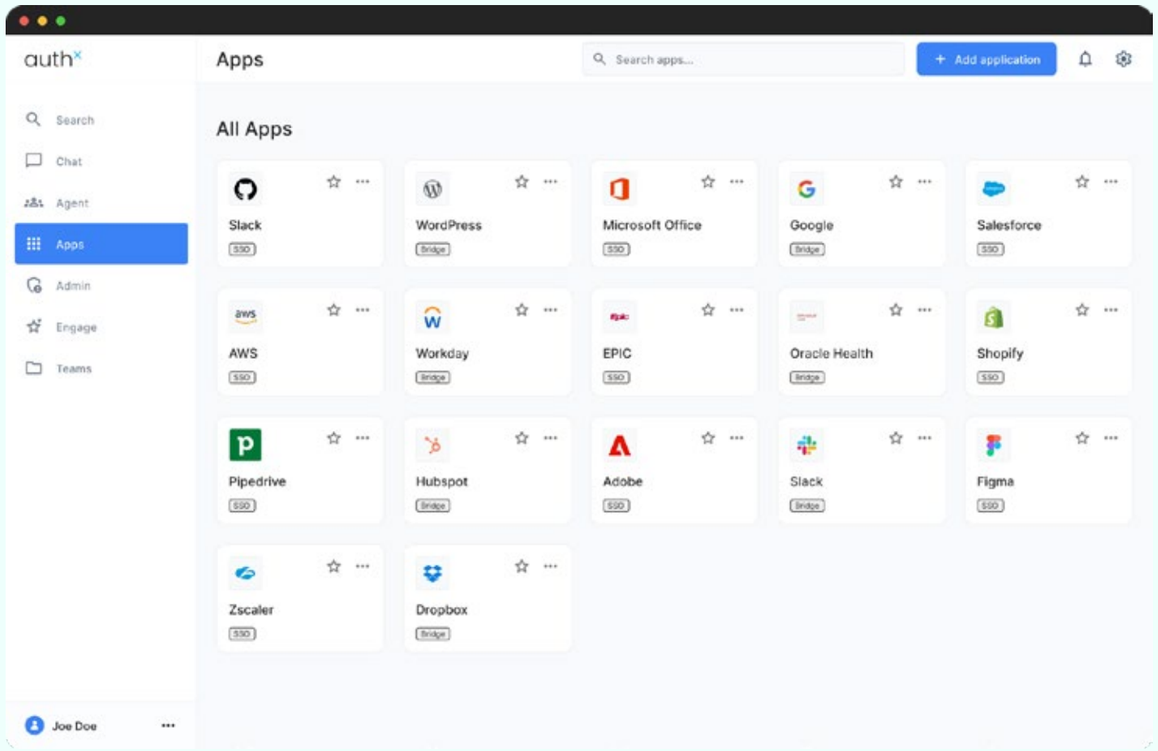
Ultimately, adaptive policy enforcement allows Zero Trust to operate at machine speed, not human speed. Instead of relying on manual reviews or delayed responses, access decisions are continuously adjusted as conditions change. Whether users are interacting with clinical platforms like **Epic**, managing infrastructure in **Microsoft Azure**, or deploying workloads in **Google Cloud**, adaptive policies ensure access remains appropriate, minimal, and secure at every moment. This approach reduces attack surfaces, limits blast radius, and preserves user productivity; turning Zero Trust from a static framework into a living, responsive security model.

> *Adaptive access isn't about control; it's about confidence. You verify just enough to stay secure and seamless.*

A true Zero Trust program unifies access across every application — cloud, legacy, and internal. Fragmented logins frustrate users and expose gaps. With integrated identity and adaptive access, users enjoy one consistent experience while IT gains centralized visibility.

Securing all applications means going beyond SaaS. VPNs, SSH, RDP, and private apps need the same protection and convenience. AuthX delivers this through single sign-on (SSO) paired with contextual verification and strong authentication, ensuring users get the right access, every time.

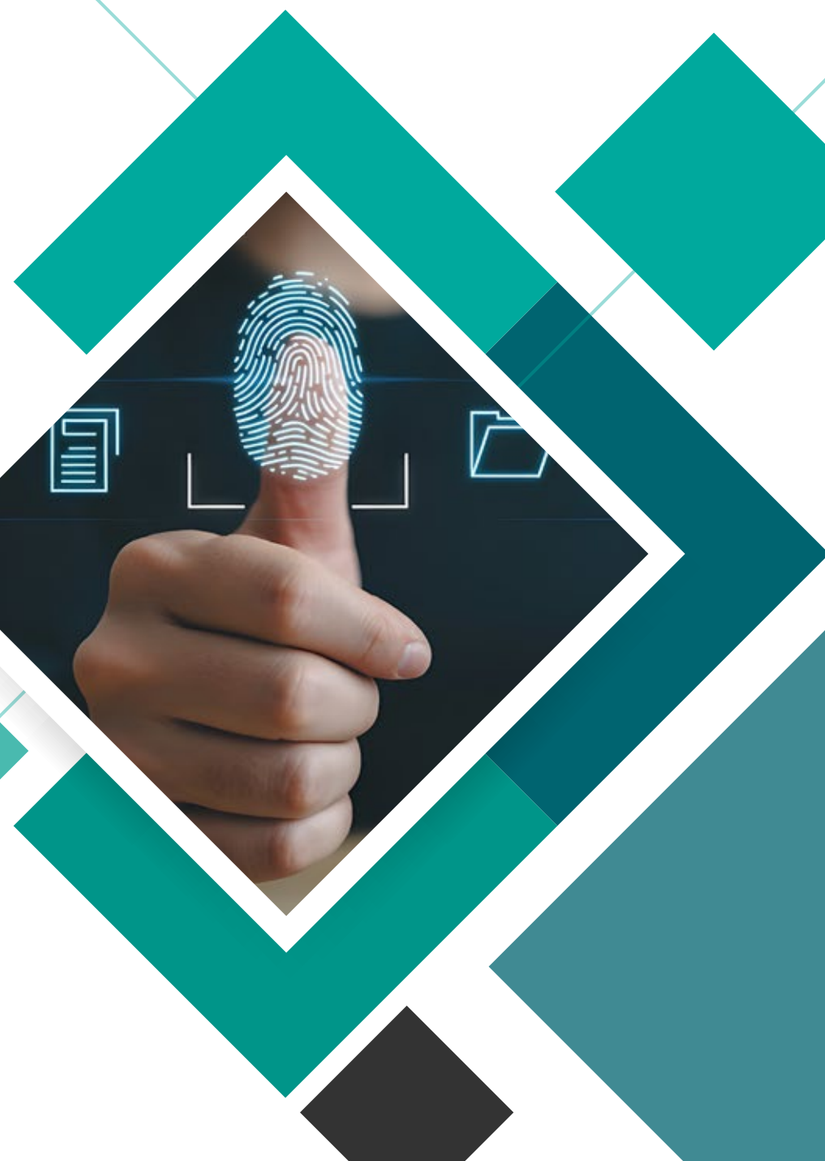
High-risk apps can trigger step-up authentication automatically, while lower-risk apps allow seamless sign-in. The result: reduced friction, improved security, and full audit trails across your digital ecosystem.



Zero Trust isn't about blocking, it's about informed access. The right person, the right app, at the right time.

5. SECURE ACCESS TO ALL APPLICATIONS

One Experience. Every App. Anywhere.



BEYOND AUTHENTICATION: CONTINUOUS TRUST

Zero Trust Doesn’t Stop at Login.

Authentication is just the start. True Zero Trust continues after access is granted. Continuous trust means monitoring sessions, user behavior, and device health in real time, and adapting permissions when risk changes.

Modern threats don’t always appear at login. A user might start safe and later become risky — through malware, session hijacking, or policy drift. Continuous trust systems re-evaluate context mid-session, applying controls like re-authentication or session isolation automatically.

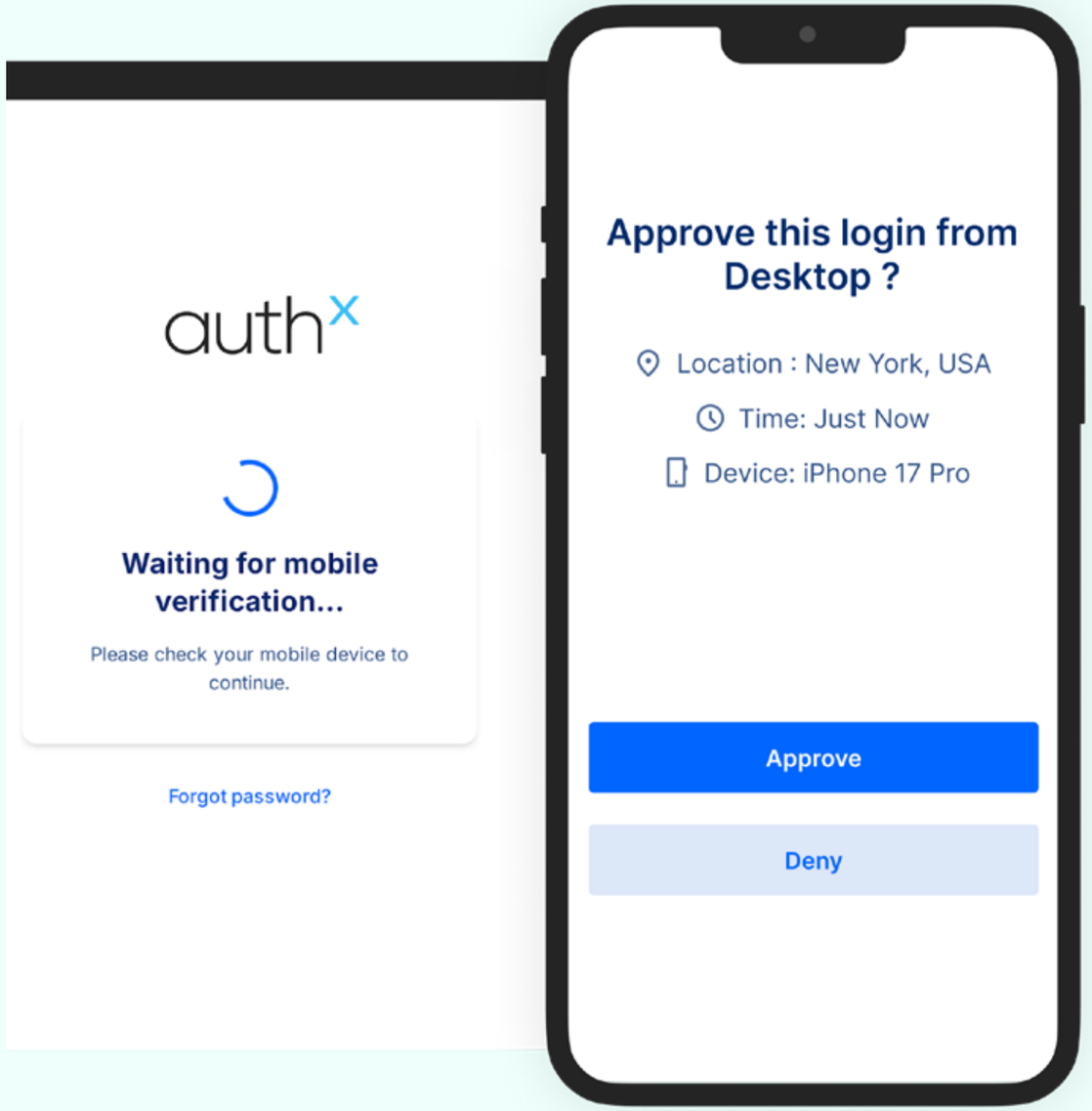
AuthX integrates with UEBA, SIEM, and endpoint tools to constantly update trust levels and trigger

AuthX monitors behavioral signals in real time.

Unusual patterns trigger contextual re-authentication

Device health changes lead to instant policy updates.

Trust isn’t a single event; it’s a loop. The moment risk changes; your defenses should too.

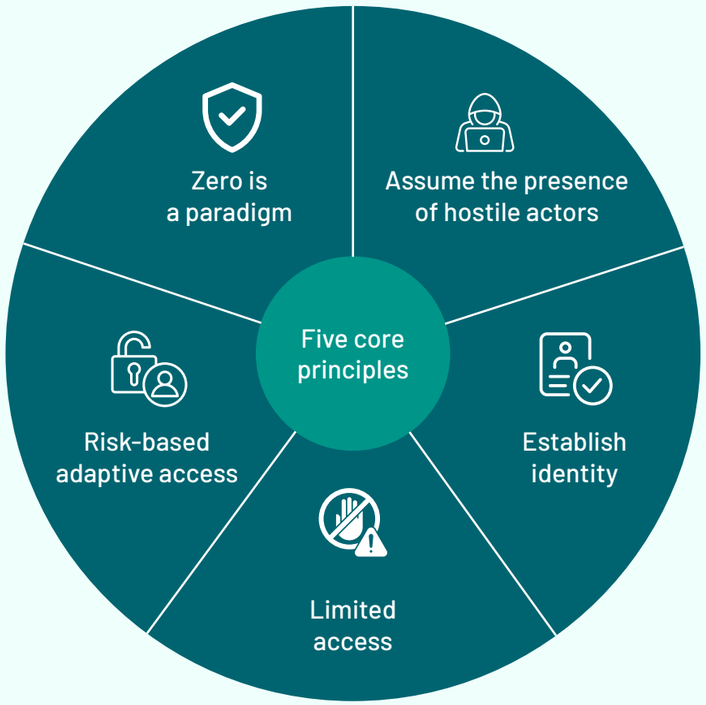


IMPLEMENTATION FRAMEWORK

Zero Trust Isn't a Project. It's a Program.

Zero Trust doesn't flip on like a switch. It's a journey that touches identity, devices, data, and people, and each phase needs structure. Most organizations stumble because they try to roll out too much at once or treat Zero Trust as a single product. The key is to make it measurable, staged, and culturally owned.

At AuthX, we've seen the most successful rollouts follow a "crawl-walk-run" model that builds confidence without disruption.



> *Zero Trust fails when it's treated like a sprint. Think marathon — with milestones you can measure.*

Phase 1: Assess

Map your identity landscape who has access to what, from where, and on which device. Use discovery tools to reveal unmanaged endpoints, duplicate accounts, and shared credentials.

Phase 2: Prioritize

You don't need to secure everything on day one. Start with your highest-risk entry points; contractors, remote admins, or legacy VPNs. Create small, high-impact wins that demonstrate visible value to leadership.

Phase 3: Deploy

Introduce AuthX Adaptive MFA and SSO for critical apps. Tie identity to device posture checks before granting access.
Gradually replace passwords with passkeys or hardware-backed factors.

Phase 4: Integrate

Expand coverage to SaaS, cloud, and on-prem systems. Use contextual policies to unify them; "one identity, many edges."
Leverage APIs to extend Zero Trust beyond IT into HR, finance, and third-party portals.

Phase 5: Optimize

Automate continuous verification and anomaly detection. Add machine-learning-based risk scoring so trust adapts in real time.

LEADERSHIP BUY-IN

Zero Trust Starts with Executive Trust

A Zero Trust strategy only sticks when the top brass believes in it. Technology sets the guardrails, but leadership sets the direction. The challenge: translating technical security into business value.

Executives care about three things: risk, cost, and agility. Zero Trust directly touches all three.

1

Business Impact

Boards understand breach headlines. Framing Zero Trust as brand protection rather than IT expense gets faster buy-in. According to IBM's 2025 Cost of a Data Breach report, companies with mature Zero Trust models saved $1.6 million per breach compared to those without.

2

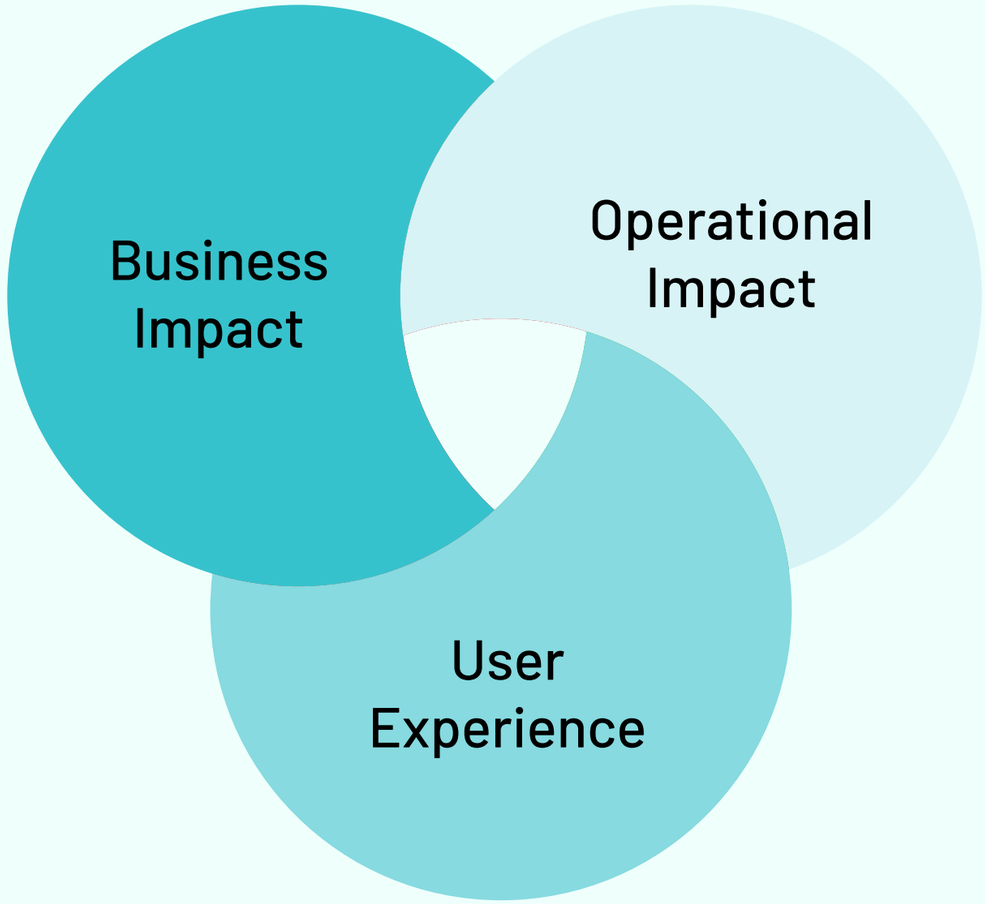
Operational Impact

CIOs appreciate efficiency. Zero Trust simplifies audits, centralizes access control, and reduces help-desk tickets through SSO.
Every integration with AuthX consolidates identity silos: fewer passwords, fewer resets, happier users.

3

User Experience

End-users are often overlooked, yet their friction defines success. Adaptive MFA and device trust make security feel invisible.
If users can log in faster while being safer, adoption skyrockets.



EXECUTIVE SIDEBAR:

- Create a joint steering committee (CISO + CIO + HR).
-
- Link metrics to quarterly risk reports.
-
- Celebrate early wins publicly inside the company.

> *Zero Trust isn't a security upgrade; it's a culture upgrade.*

MEASURING ZERO TRUST PROGRESS

If You Can't Measure It, You Can't Improve It

You can't manage what you can't measure. Without clear metrics, Zero Trust becomes a buzzword rather than a framework.
Measurement turns intent into accountability.

IDENTITY & ACCESS METRICS

By deploying AuthX's passwordless MFA and SSO, one American IT company achieved 90 % employee adoption of MFA.

That same case study reported a 70% reduction in help-desk tickets for password resets/credential issues after AuthX implementation.

AuthX reports that with its combined authentication stack (passwordless + biometrics + device posture) organisations "effectively diminish operational costs linked with security breaches and productivity interruptions."

AuthX's press materials state that the average cost of a cyber-attack in the healthcare sector is approximately USD 5 million, and they suggest their passwordless IAM reduces risk and cost in that context.

RISK & RESPONSE METRICS

75%
drop in phishing-based access incidents

2 HOURS
mean time to detect and respond to abnormal access

60%
reduction in failed login attempts

85%
policy automation coverage

TRANSLATING METRICS INTO BUSINESS VALUE

Zero Trust maturity is reflected in reduced risk exposure, lower operating costs, and sustained business continuity. The metrics above provide clear evidence of return on security investment. Fewer successful phishing incidents, reduced authentication failures, faster response times, and high levels of policy automation directly translate into lower breach probability and reduced operational overhead.

By quantifying outcomes such as avoided incident costs, reduced help-desk workload, and automated enforcement at scale, AuthX enables organizations to connect Zero Trust controls to measurable financial impact. This allows leadership teams to assess security posture with the same rigor applied to other business initiatives, ensuring that Zero Trust is both technically effective and economically justified while supporting long-term growth and resilience objectives.

> *The success of Zero Trust is not defined by the number of controls deployed, but by the risks avoided, the costs reduced, and the speed at which threats are contained. Measurement is what transforms security spend into business value.*

COMMON ROADBLOCKS (AND HOW TO BREAK THEM)

Every Transformation Meets Resistance

Even with momentum, Zero Trust programs hit friction: cultural, technical, or operational. Recognizing these early keeps you from stalling halfway.

"It's Too Complex"

Complexity is often a perception issue. Start with identity and grow outward.

AuthX Insight: 70% of successful deployments begin with just SSO + MFA for top 10 apps.

"It'll Slow Us Down"

Performance concerns fade when adaptive authentication replaces rigid policies. Real-world clients saw login times drop 30 % once passkeys replaced OTPs.

"We Don't Have the Resources"

Leverage automation. AuthX orchestrates identity checks, risk scoring, and session validation without manual overhead.

"Users Will Hate It"

Communicate early. Frame Zero Trust as protection for users, not against them. Offer self-service portals and clear UI cues that build confidence, not confusion.

> *Resistance means you're innovating where comfort used to be.*

TECHNOLOGY BLUEPRINT

Building a Zero Trust Architecture That Works (and Lasts)

Zero Trust isn't about ripping out what you already have — it's about connecting what's been fragmented. The right architecture doesn't add tools; it orchestrates them. The goal is a living ecosystem that can evolve with your threat landscape and workforce needs.

When enterprises deploy AuthX, we see that the strongest foundations share one thing: interoperability. Every tool, signal, and policy talks to the others — in real time.

CORE COMPONENTS OF A ZERO TRUST STACK

Layer	Function	
Identity Provider	Central authority for user authentication	AuthX as your single control plane for workforce, contractor, and device identities
Policy Engine	Applies contextual rules and adaptive decisions	AuthX Adaptive Access Engine evaluates identity, device, and behavior signals
Device Trust Layer	Tracks and validates device posture	AuthX integrates with MDM and EDR tools for posture checks
App Access Broker	Enforces granular authorization across hybrid apps	Unified SSO with session-level visibility
Analytics & SIEM	Detects anomalies and compliance drift	AuthX pushes continuous trust telemetry to SIEMs like Splunk or Sentinel

> *Zero Trust isn't one big lock, it's thousands of tiny verifications working in harmony.*

BEYOND AUTHENTICATION: CONTINUOUS TRUST

Trust Doesn't End at Login

Most breaches don't happen because someone got in — they happen because someone stayed in too long, unnoticed. Continuous trust is the invisible guardrail that never sleeps.

With AuthX Continuous Access Evaluation, verification doesn't stop once a session begins. Every minute, context signals; device health, user behavior, network location are reassessed. If risk changes, access adjusts automatically.

HOW CONTINUOUS TRUST WORKS

Authenticate: Strong, phishing-resistant MFA validates identity.

Monitor: AuthX sensors track posture, device status, and usage patterns.

Evaluate: Machine learning scores trust in real time.

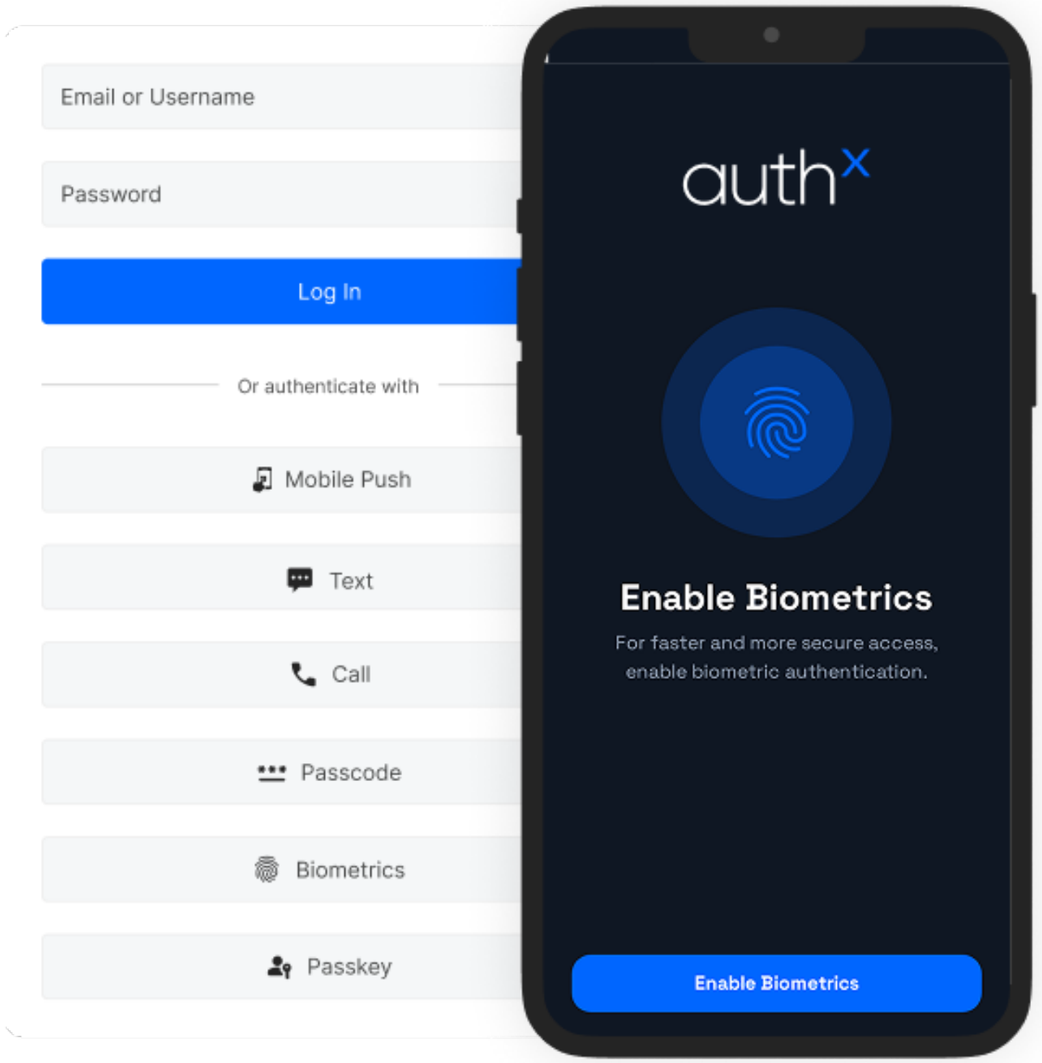
Adapt: High-risk sessions are reverified or terminated instantly.

WHY IT MATTERS

- Prevents lateral movement after compromise.
- Reduces dwell time (median now under 30 minutes for AuthX customers).
- Makes zero trust feel invisible for legitimate users.

EXAMPLE:

A user logs in from a corporate laptop. Thirty minutes later, their IP shifts to an unknown network. AuthX triggers re-authentication automatically; no manual intervention needed.



> *Trust isn't permanent — it's earned again, every second you stay connected.*

THE HUMAN LAYER: CULTURE OF TRUST

Technology Builds Walls. People Build Trust.

Zero Trust fails when people see it as control instead of care. A sustainable program depends as much on culture as code.

Every phishing click, password reuse, or device bypass traces back to one factor — human behavior. So, teach users to see security as part of their success, not their burden.

CULTURAL ANCHORS FOR ZERO TRUST

Transparency: Communicate why new controls exist. Users comply when they understand the "why."

Empowerment: Give self-service recovery options to reduce frustration.

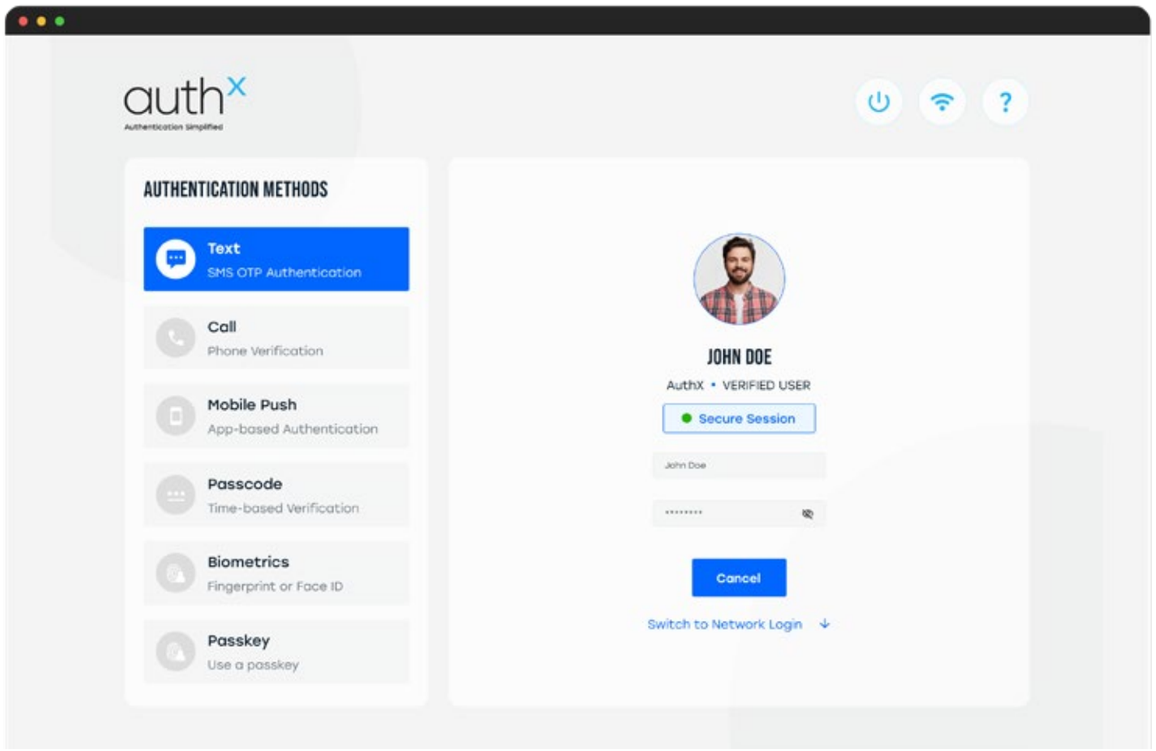
Recognition: Celebrate compliance champions in company updates.

Training: Replace boring security videos with live threat demos and scenario roleplays.

AUTHX IN PRACTICE

AuthX integrates security nudges, contextual reminders during login to guide users toward better habits.
Example: "Your device OS is 60 days outdated. Update now to avoid future login blocks."

It's subtle reinforcement, not punishment.



People won't secure what they don't feel responsible for.

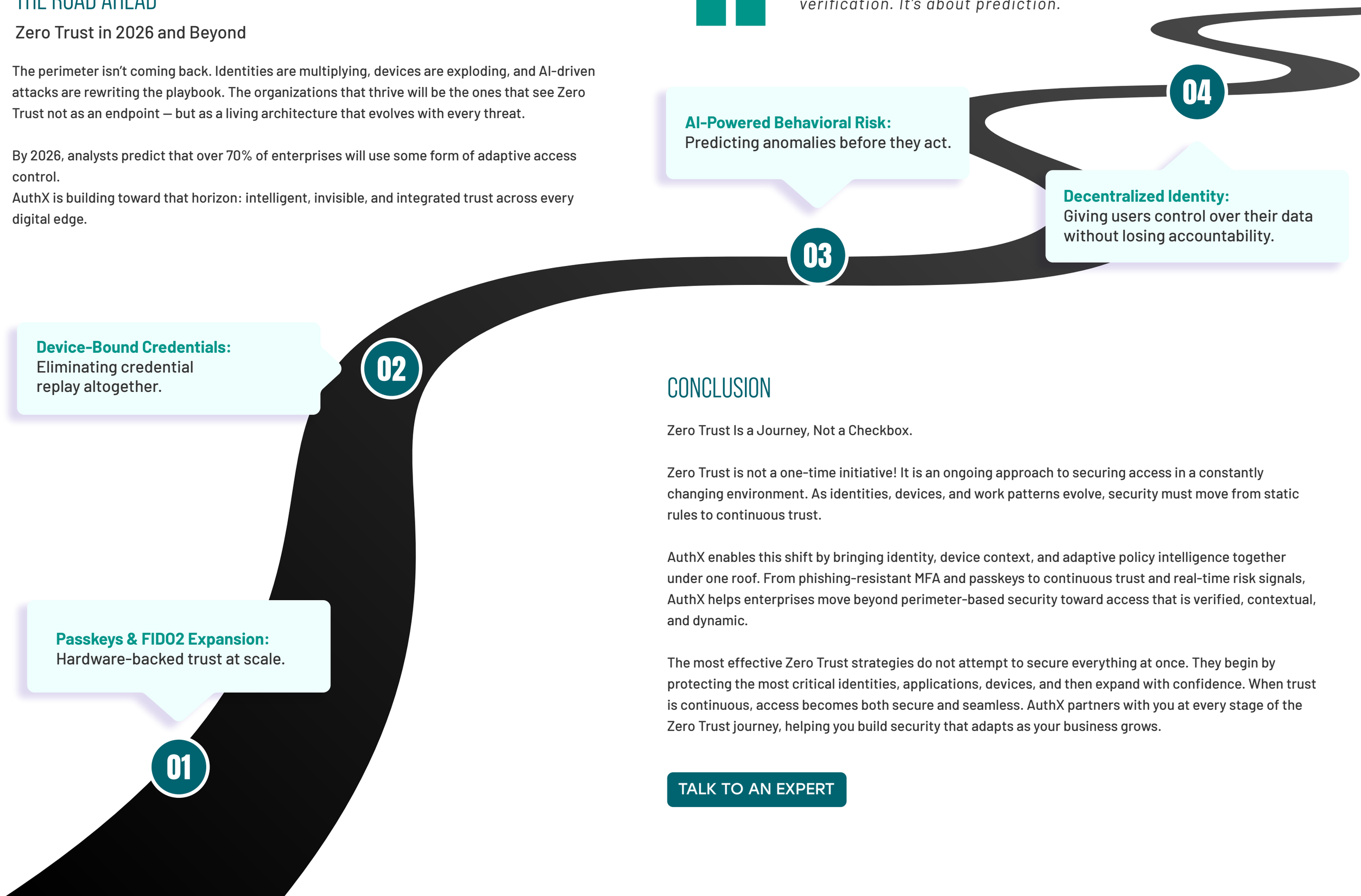
THE ROAD AHEAD

Zero Trust in 2026 and Beyond

The perimeter isn't coming back. Identities are multiplying, devices are exploding, and AI-driven attacks are rewriting the playbook. The organizations that thrive will be the ones that see Zero Trust not as an endpoint — but as a living architecture that evolves with every threat.

By 2026, analysts predict that over 70% of enterprises will use some form of adaptive access control.
AuthX is building toward that horizon: intelligent, invisible, and integrated trust across every digital edge.

> *Tomorrow's Zero Trust isn't about verification. It's about prediction.*



CONCLUSION

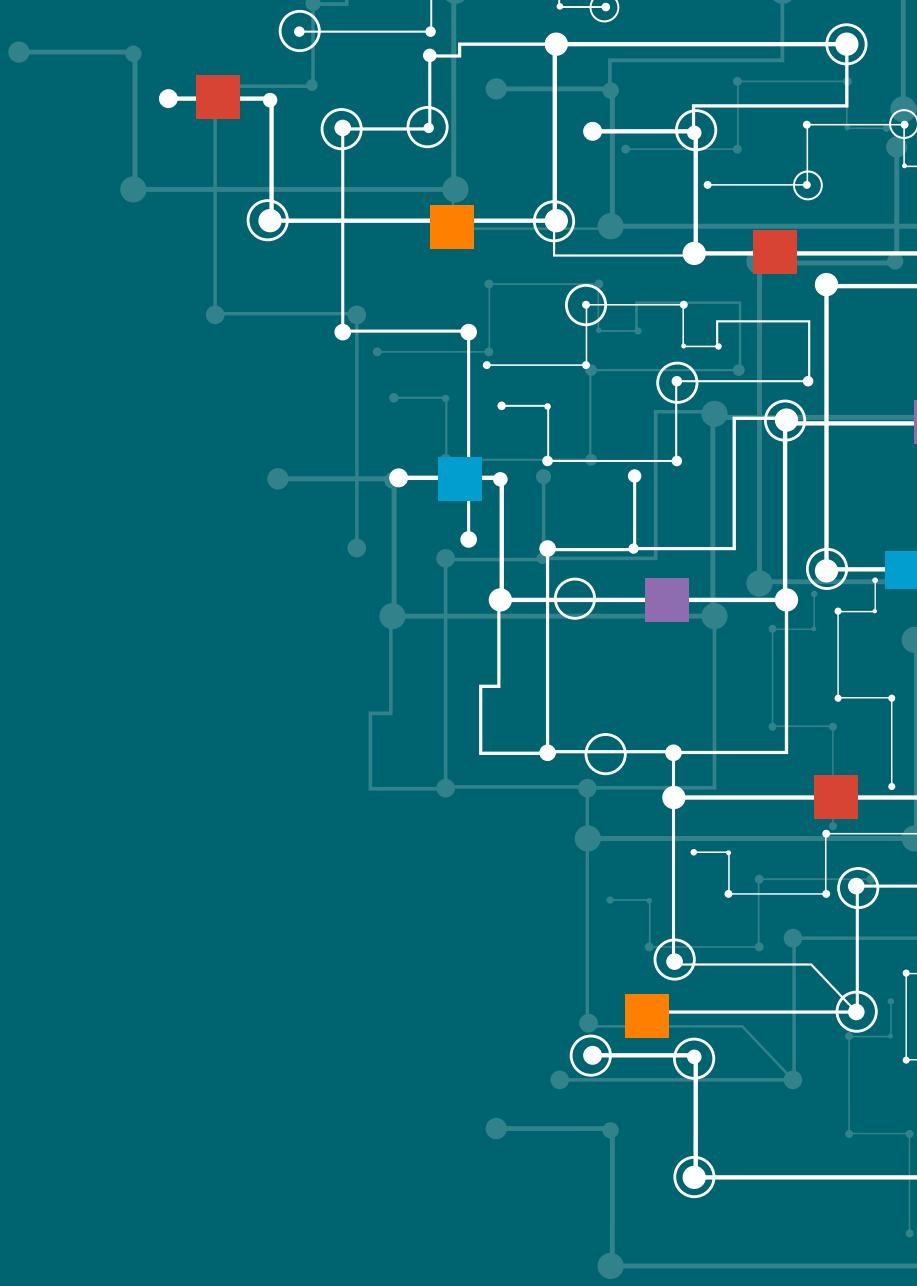
Zero Trust Is a Journey, Not a Checkbox.

Zero Trust is not a one-time initiative! It is an ongoing approach to securing access in a constantly changing environment. As identities, devices, and work patterns evolve, security must move from static rules to continuous trust.

AuthX enables this shift by bringing identity, device context, and adaptive policy intelligence together under one roof. From phishing-resistant MFA and passkeys to continuous trust and real-time risk signals, AuthX helps enterprises move beyond perimeter-based security toward access that is verified, contextual, and dynamic.

The most effective Zero Trust strategies do not attempt to secure everything at once. They begin by protecting the most critical identities, applications, devices, and then expand with confidence. When trust is continuous, access becomes both secure and seamless. AuthX partners with you at every stage of the Zero Trust journey, helping you build security that adapts as your business grows.

TALK TO AN EXPERT



authX

AuthX is a cloud-based Identity and Access Management platform offering passwordless features, including Single Sign-On, Multi-Factor Authentication, RFID Tap & Go, Passkeys, and Biometric Authentication. It helps enterprises implement seamless user authentication and security with its advanced authentication workflow feature, enabling security for end-users across workstations, web, network, and mobile endpoints. AuthX unifies login credentials, applications, and devices into a secure ecosystem, simplifying access to essential tools and data.

AuthX's cloud-based solution enables Zero Trust Security through dynamic risk management, proactively identifying threats, securing networks, and safeguarding endpoints for organizations and their end-users. AuthX's commitment to providing secure solutions to enterprises is backed by its partnership with industry leaders; Citrix, Epic, Google, IGEL, Stratodesk, and VMWare(Broadcom).

Email - sales@authx.com

Phone - +1 650-410-3700

Global Headquarters USA - 656 Quince Orchard Rd,
Suite 300, Gaithersburg, MD 20878