EXECUTIVE BRIEFING · IDENTITY CHALLENGE CARD

The Zero Trust Missing Pillar: Full Workforce Identity Coverage

Identity Challenge Card delivers 100% workforce coverage in one day, in 29 languages, and turns the MFA you already own into a four-factor defense — without replacing a single deployed system.

100% Coverage → 29 Languages → Four-Factor Defense

See How It Works | Book a Live Demo

Protecting the world's workforce since 1997. *Trusted by U.S. Air Force, U.S. Army, NASA, Pfizer, Visa, Volkswagen, Marriott, Starbucks, DHL, ESPN, Lockheed Martin, ING, Humana, BBC, and 250+ enterprises.*

AUDIENCE	DOCUMENT TYPE	VERSION
CEO · Board · CISO · CIO · Analysts	Executive Briefing	1.0

The Missing Pillar

Full Workforce Identity Coverage

Most MFA and Zero Trust strategies focus on:

- strong login
- device trust
- conditional access
- least privilege
- continuous monitoring

They are necessary. They are not sufficient. They leave one question unanswered:

THE CRITICAL QUESTION

Can we verify every worker, in every language, with every available factor of defense?

IF THE ANSWER IS NO, YOUR IDENTITY STRATEGY IS INCOMPLETE

This briefing makes a single, irrefutable case: **deviceless workforce identity coverage is the missing pillar of Zero Trust** — and Avatier's Identity Challenge Card is the only way to add it without rebuilding what you already own.

The Problem with Today's Strategy

Today's MFA and Zero Trust programs are usually built around four assumptions:

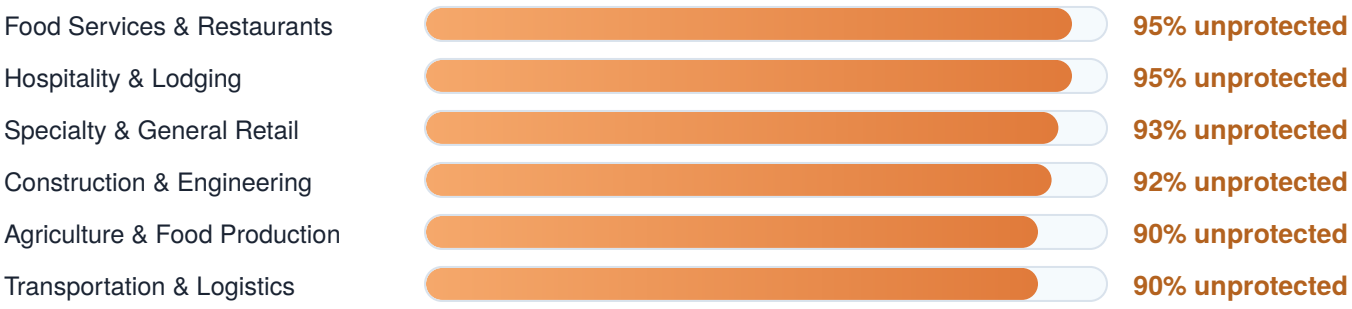
- managed devices
- enrolled users
- connected identity systems
- normal operating conditions

None of those assumptions hold uniformly across a real enterprise workforce. That leaves measurable, documented gaps in:

> - frontline workers
> - shared-device users
> - contractors and temporary staff
> - help desk and call center scenarios
> - workers without reliable device or app access
> - workers operating in countries where MFA apps have limited or no localization
> - outage and degraded-mode operations
>
> **The strategy looks strong on paper, but coverage is incomplete.**

The Coverage Gap by Industry

The number that matters to a board is not how many users *can* use MFA — it is how many *are* verified by it on every login. Across major industries, device-dependent MFA reaches only a small fraction of the workforce:



Roughly 80% of the global workforce is deskless. Without a device, there is no MFA enrollment, no Conditional Access signal, and no audit evidence of identity verification.

The Business Impact the CFO Cannot Ignore

The coverage gap is not an abstract compliance finding. It is a measurable, uninsured financial exposure. Every uncovered frontline worker is a potential credential theft vector — and every credential theft event costs real money in breach remediation, denied cyber-insurance claims, audit-finding remediation, and class-action exposure.

THE CFO REALITY

Every uncovered frontline identity is a seven-figure breach vector — one stolen credential from an incident, a denied cyber-policy claim, and an audit finding that pushes the next renewal.

Device-dependent MFA leaves 70–95% of the frontline workforce outside the verification perimeter. That is not a gap in a report. It is the shape of the next incident. Deviceless MFA is how that math stops working against the balance sheet.

THE HIDDEN COSTS OF INCOMPLETE COVERAGE

$4.9M	70–95%	30%+	$0
Average global breach cost	**Of frontline workers unprotected by device-based MFA**	**Breaches trace to compromised credentials**	**ICC replacement cost for existing MFA**
industry benchmarks, 2024	*industry segment data*	*threat intelligence consensus*	*integrates, never replaces*

The CFO equation: cost of one credential-theft incident » cost of closing the coverage gap. ICC's deviceless coverage converts an uninsured exposure into a covered one — at 75% less than the current MFA spend and with zero replacement cost for existing deployments.

The New Pillar Plan

A complete identity strategy rests on six pillars — five that most enterprises already invest in, and one that is consistently missing:

1. **Identity Governance**
   Make sure the right people get the right access at the right time.

2. **Access Control and Zero Trust Enforcement**
   Continuously evaluate access based on risk, context, and policy.

3. **Device-Dependent MFA and Passwordless**
   Protect standard workforce login paths with modern authentication.

4. **Privileged and Sensitive Access Protection**
   Apply stronger controls to admins, high-risk transactions, and critical systems.

5. **Detection, Audit, and Compliance Evidence**
   Monitor activity, prove control effectiveness, and support audit and regulatory needs.

6. **Deviceless Workforce Identity Coverage** THE MISSING PILLAR

   Verify the right human when:

   - devices are unavailable or have never been issued
   - workers operate in languages or regions traditional MFA cannot reach
   - identity systems are degraded
   - the help desk is targeted by social engineering or impersonation
   - the workforce is outside standard MFA enrollment models
   - the workforce must still operate during an incident

   This is where Avatier's Identity Challenge Card belongs.

Three Hard Truths Every Board Should Know

Pillars 1 through 5 are necessary. They are not sufficient. The case for adding the sixth pillar rests on three facts boards and analysts can independently verify:

1

Your MFA covers some of your workforce. Not all of it.

Frontline workers, contractors, deskless staff, shared-device users, kiosk operators, and workers in regions without smartphones routinely fall outside MFA enrollment. Even in enterprises where MFA is "deployed company-wide," real coverage rarely reaches 100% of identities. Auditors expect 100% MFA coverage; device-dependent solutions leave 70–95% of the workforce unprotected.

VERDICT: ANY COVERAGE BELOW 100% IS A MEASURABLE GAP

2

Your MFA stops at language and infrastructure barriers.

App-based MFA assumes a smartphone, an app store, reliable connectivity, and a user interface in a language the worker reads fluently. None of those assumptions hold uniformly across a global workforce. Authenticator apps with limited localization, push notifications in English, and onboarding instructions written for technical users systematically exclude the workers who need verification most.

VERDICT: A GLOBAL WORKFORCE NEEDS A GLOBAL AUTHENTICATION PATH

3

One or two factors is not defense in depth. It is the floor.

Security best practice has always favored multiple independent factors of authentication. Most enterprise MFA deployments stop at two. Adding additional, independent factors — factors that do not depend on the same device, network, or user account — is a strict security improvement. The math is simple: more independent verification factors mean exponentially more work for an attacker.

VERDICT: MORE INDEPENDENT FACTORS = STRICTLY STRONGER SECURITY

What Identity Challenge Card Adds

Identity Challenge Card (ICC) directly answers each hard truth. Four capabilities — each verifiable, each measurable, each strictly additive to the MFA an enterprise already owns:

1

100% Workforce Coverage Instantly via Mass Enrollment

ICC enrolls an entire workforce in a single day through automated mass enrollment — not the months-long, per-user rollout typical of app-based MFA. Every employee, every contractor, every shared-device worker is covered from day one, including the 70–95% of the workforce that traditional MFA never reaches.

Coverage: 100% · Time to Coverage: 1 day · Cost: 75% less than current MFA

2

Every Country, Every Language, Every Worker

Because ICC is deviceless, it inherits no app store, no infrastructure, and no platform localization dependency. Identity Challenge Cards ship in 29 languages — including English, Spanish, French, German, Portuguese, Simplified and Traditional Chinese, Arabic, Hindi, Japanese, Korean, Russian, Italian, Dutch, Polish, Swedish, Turkish, Thai, Indonesian, and more — covering every region a global enterprise operates in.

Languages: 29 · Devices Required: 0 · Network Required: 0

3

Four-Factor Defense — ICC's Three Factors Plus Your Existing MFA

ICC is itself a three-factor authenticator (Challenge Card, Private Knowledge, Identity Anchor). When deployed alongside the device-dependent MFA an enterprise already owns — Okta, Microsoft Authenticator, Ping Identity, Duo, CyberArk, FIDO2, YubiKey, SAML, OIDC — that existing MFA becomes a fourth, independent factor. The result: every login that matters is protected by four mutually independent factors instead of two or three.

Authentication Factors: 1–3 → 4 (ICC's 3 + Your MFA)

4

Zero Rip-and-Replace — Augments and Leverages What You Already Own

ICC is engineered to integrate with the major MFA providers enterprises have already standardized on, through a common adapter interface. There is no migration project, no re-enrollment of users in a new system, and no replacement of existing authentication infrastructure. ICC **proves** that the existing MFA investment was the right call by turning it into the fourth factor of an irrefutable defense.

Replacement Cost: $0 · Existing MFA: Preserved & Strengthened

ICC's Three Factors + Your Existing MFA = Four-Factor Defense

Identity Challenge Card is a three-factor authenticator on its own. Stacked with the device-dependent MFA an enterprise already owns, the customer's existing investment becomes the fourth, independent factor:

FACTOR 4	**Your Existing Device-Dependent MFA** — Okta · Microsoft Authenticator · Ping Identity · Duo · CyberArk · FIDO2 · YubiKey · SAML · OIDC
FACTOR 3	**Identity Anchor Factor (ICC)** — Organizational factor (employee ID, hire date) — something the worker was provided
FACTOR 2	**Private Knowledge Factor (ICC)** — Secure PIN known only to the user — useless without the card
FACTOR 1	**Challenge Card Factor (ICC)** — Randomized grid response; only the holder of the air-gapped card can answer

The integration story the board needs to hear: Avatier does not replace your MFA — Avatier **strengthens** it. ICC delivers three independent factors out of the box. Your existing MFA contributes the fourth. Every dollar already spent on Okta, Microsoft, Ping Identity, Duo, CyberArk, FIDO2, YubiKey, SAML, or OIDC is preserved, vindicated, and now part of an irrefutable four-factor defense.

NATIVE INTEGRATIONS ACROSS THE MFA MARKET

Okta IDENTITY PLATFORM	**Microsoft Authenticator** PUSH / OTP	**Ping Identity** IDENTITY PLATFORM
FIDO2 / WebAuthn HARDWARE KEY	**YubiKey** HARDWARE KEY	**SAML / OIDC** FEDERATED SSO

Why This Pillar Matters

Without this pillar, the company can invest millions in Zero Trust and MFA and still leave:

- a percentage of the workforce uncovered
- critical recovery workflows vulnerable
- support channels exposed to impersonation
- compliance teams unable to prove universal control coverage
- business continuity dependent on phones, apps, and network availability

> Zero Trust without full workforce identity coverage is incomplete.
>
> — THE CEO MESSAGE

If your strategy cannot verify every worker in every critical scenario, it is not a complete identity strategy.

How Deviceless MFA Fits the Larger Strategy

Deviceless MFA should not be sold as "another MFA option." It should be positioned as:

> **The coverage, continuity, and four-factor reinforcement layer inside the broader identity, security, and compliance strategy.**

It strengthens four areas of the business simultaneously:

Security

- closes workforce coverage gaps
- adds an independent fourth factor on top of existing MFA
- reduces help desk and social engineering exposure
- eliminates push fatigue and replay attack surface (air-gapped)

Compliance

- helps prove broader control coverage
- satisfies NIST 800-63B, SOC 2, PCI-DSS v4, ISO 27001 first-pass
- supports CMMC, HIPAA, GDPR, FERPA, EO 14028
- reduces exceptions and unmanaged users

Identity

- extends identity assurance beyond normal login
- covers edge cases traditional MFA misses
- fits into lifecycle, governance, and recovery processes
- provides a live identity check for service desk workflows

Business Continuity

- keeps identity verification available during outages
- supports workforce operations when device-based controls fail
- resilient by design during cyberattack conditions
- workforce verified and operational in a single day

What Each Buyer Gets — Outcomes by Role

Every buyer has different success criteria. Identity Challenge Card delivers a specific, measurable outcome to each role involved in the identity decision:

FOR THE CISO

Close the 70–95% MFA coverage gap with no exceptions

- **Full audit coverage:** no more documented MFA exemptions for frontline, contractor, or shared-device populations
- **Phishing-resistant by design:** air-gapped authentication eliminates push bombing, SIM-swap, and real-time phishing
- **Standards alignment:** satisfies NIST 800-63B, CISA EO 14028, SOC 2, ISO 27001 on first audit pass

FOR THE CIO

Deploy in days, not months — leverage the MFA you already own

- **Mass enrollment:** entire workforce covered in one day, no per-user rollout queue
- **Zero rip-and-replace:** integrates with Okta, Microsoft, Ping Identity, Duo, CyberArk, FIDO2, YubiKey, SAML, OIDC
- **No new infrastructure:** no MDM dependency, no app store, no network requirement at auth time

FOR THE CFO

Convert an uninsured exposure into a covered one

- **75% less than current MFA cost** for the populations that need coverage most
- **$0 replacement cost** — existing MFA investment is preserved and strengthened
- **Insurable risk profile:** complete workforce coverage supports cyber-policy renewal and reduces denied-claim exposure

FOR THE CEO & BOARD

A complete identity strategy you can defend to regulators, analysts, and shareholders

- **100% workforce coverage** — the number boards, auditors, and regulators expect
- **Business continuity during incidents:** verified identity when device-based controls fail
- **Category leadership:** first-mover position in Deviceless Workforce Identity Coverage

FOR SERVICE DESK LEADERS

Verify every caller, every time — no more social engineering risk

- **Live identity check:** caller reads challenge off their card; impersonation fails instantly
- **No deepfake voice works:** no password resets handed to the wrong person
- **Queue relief:** mass enrollment eliminates the re-enrollment treadmill

FOR ANALYSTS & INVESTORS

A defensible new sub-category of Workforce Identity

- **New category:** Deviceless Workforce Identity Coverage, adjacent to but distinct from MFA
- **Market wedge:** the ~80% of the global workforce that is deskless and systematically unserved by app-based MFA
- **Proven at scale:** U.S. Air Force, U.S. Army, NASA, Pfizer, Visa, Volkswagen, Marriott, DHL, and 250+ enterprises

The Math the Board Cannot Dispute

Reduced to four numbers, the case is simple:

DIMENSION	TODAY (EXISTING MFA ONLY)	WITH IDENTITY CHALLENGE CARD
Workforce Coverage	**Partial — typically 5–88%**	**100% in one day**
Language & Geography	**Limited by app localization & device access**	**29 languages, every country**
Authentication Factors	**1 to 3 (knowledge / possession / organizational)**	**4 (ICC's 3 + your existing MFA as the 4th)**
Replacement Cost	**— (status quo)**	**$0 — augments existing MFA, no rip-and-replace**

None of these four numbers move in the wrong direction. Coverage goes up. Reach goes up. Defense-in-depth goes up. Replacement cost stays at zero. There is no version of this comparison where the board's existing identity strategy is stronger than the strategy that adds ICC.

From Decision to Full Coverage — the Deployment Timeline

Most identity initiatives measure deployment in quarters. Identity Challenge Card measures it in days. Here is what the rollout actually looks like from the moment the decision is made:

WEEK BEFORE **Day 0**	**Directory sync & card generation** Avatier connects to the existing HR or identity directory. Unique, single-use challenge cards are generated and localized to the workforce's languages. No user action required.
LAUNCH **Day 1**	**Mass enrollment of the entire workforce** Every employee, contractor, and shared-device worker is auto-enrolled in a single workflow. Workforce coverage moves from 5–88% to 100% on the same business day.
FIRST WEEK **Week 1**	**Service desk adopts ICC as the live identity check** IT operations begin using ICC for every inbound verification call. Impersonation and social-engineering pathways close. Existing MFA continues running as the fourth factor.
FIRST MONTH **Month 1**	**Audit-ready evidence of full coverage** Complete audit trail of enrollment, issuance, authentication, and revocation is available to auditors. Compliance teams can document 100% MFA coverage with no exceptions.
ONGOING **Day N**	**Lifecycle in production — revoke, reissue, audit** Lost or compromised cards are revoked in seconds and reissued the same day. Card expiry, re-enrollment, and audit logs are policy-enforced. No MDM to rebuild, no re-enrollment treadmill.

Compare to today: the typical enterprise MFA rollout takes 6–18 months to reach partial coverage. Identity Challenge Card reaches 100% coverage in one day, with full audit evidence inside the first month — and without replacing a single existing MFA deployment.

Trusted by the World's Workforce Since 1997

CUSTOMERS WHO BUILT AVATIER

U.S. Air Force	U.S. Army	NASA	GSA
Lockheed Martin	Rockwell Collins	Pfizer	Bayer
Humana	Visa	ING	Volkswagen
Marriott	Starbucks	DHL	Sprint Canada
ESPN	BBC	Fox News	USA Today
Nordstrom	Vail Resorts	The Cosmopolitan	Build-A-Bear
SC Johnson	Welch's	MillerCoors	Emerson
Oscar Mayer	Steak 'n Shake	Broward County	Zep

COMPLIANCE & CERTIFICATIONS

SOC 2 Type II
Annual audit of security controls, availability, and confidentiality

ISO/IEC 27001
International standard for information security management

PCI DSS v4.0.1
Payment card industry data security standard

GDPR
European data protection and privacy regulation

FERPA
Federal student education records privacy protection

Section 508
Accessibility for screen readers, keyboard navigation, assistive tech

Live SecurityScorecard A rating · Avatier Trust Center: trust.avatier.com

The Category — Defined for Analysts and Investors

Identity Challenge Card is not a feature inside an existing category. It is the first production implementation of a new sub-segment of Workforce Identity — one that deserves its own analyst coverage and market sizing.

THE CATEGORY

Deviceless Workforce Identity Coverage

A sub-segment of Workforce Identity that verifies the human — not the device, the app, or the network — across **every worker, every language, and every operating condition**, including the frontline, shared-device, contractor, and outage-mode populations that device-dependent MFA systematically cannot reach.

Adjacent To	Distinct From	Positioned As
Traditional MFA, Passwordless, IGA	Device-based MFA, hardware tokens, SMS OTP	Additive coverage & continuity layer

MARKET SIZING SIGNALS

~80%	70–95%	29
Of the global workforce is deskless	Unprotected by device-based MFA in frontline industries	Languages supported today — global reach from day one

WHAT MAKES THE CATEGORY DEFENSIBLE

Air-gapped architecture
No network dependency at authentication time. Push bombing and real-time phishing have no vector.

Zero PII on the credential
No personal data encoded on the card. A lost card is not a data breach. Privacy by architecture.

Mass enrollment at scale
100% workforce coverage in one day. No MDM dependency. No re-enrollment treadmill.

Additive, not competitive
Turns every existing MFA deployment into the fourth factor of an irrefutable defense.

For analysts: the correct framing is not "another MFA vendor" but "the first vendor in Deviceless Workforce Identity Coverage — a category addressing the ~80% of the global workforce that device-based MFA systematically cannot serve."

Board / CEO-Ready Framework

TODAY'S STRATEGY

- MFA
- Zero Trust
- Passwordless
- PAM
- Governance

COMPLETE STRATEGY

- MFA
- Zero Trust
- Passwordless
- PAM
- Governance
- ★ **Full Workforce Identity Coverage (ICC)**

BEST WAY TO PRESENT IT

HEADLINE

The Zero Trust Missing Pillar: Full Workforce Identity Coverage

SUPPORTING COPY

100% of the workforce, in 29 languages, with a fourth factor of defense added on top of the MFA you already own. ICC closes the coverage gap, extends authentication globally, and strengthens existing MFA — without replacing a single deployed system.

The Complete Workforce Identity Strategy

Every pillar matters — but only one of them turns the others into a complete strategy. Reduced to its sharpest form, the case rests on facts the board, the CISO, and the analyst community can independently verify:

SIX PILLARS · ONE COMPLETE STRATEGY

What "complete" actually looks like

1. Identity Governance
2. Access Control and Zero Trust Enforcement
3. Device-Dependent MFA and Passwordless
4. Privileged and Sensitive Access Protection
5. Detection, Audit, and Compliance Evidence
6. **Deviceless Workforce Identity Coverage** THE MISSING PILLAR

Identity Challenge Card is not a competing MFA option. It is the missing pillar that turns Zero Trust into a complete workforce identity strategy — instantly, globally, and additively to every MFA investment already made.

See your workforce coverage gap in 15 minutes.

A 30-minute Deviceless MFA walkthrough · same-day response · no commitment.

Book a Live Demo | See How It Works

Executive briefing prepared for Avatier leadership, board engagement, and analyst-relations use. Position the Identity Challenge Card as the deviceless coverage and four-factor reinforcement layer of the modern identity strategy — additive to, never competing with, existing MFA investments. Avatier · 4733 Chabot Drive, Suite 201 · Pleasanton, CA 94588 · (800) 609-8610 · identitychallengecard.com