ZOHO

Tigon Advisory
Start-ups, cure your disconnects

STATE OF WORKFORCE PASSWORD SECURITY 2026

A decision-maker's guide to workforce credential risk, password management maturity,and the security investments that define resilient organizations in 2026 and beyond.
Based on 3,322 verified responses across 9 regions, 6 industries, and 12 roles.

3,322 Verified Respondents

9 Regions Covered

6 Industries Covered

12 Roles Represented

Conducted by Tigon Advisory Corp. | Sponsored by Zoho Corporation

TABLE OF CONTENTS

EXECUTIVE SUMMARY

59%
Use 15+ apps for work

1 in 3
Suffered a cyberattack

74%
Lack identity visibility

90%
Believe AI strengthens security

80%
Stack NOT future-ready

65%
No Zero Trust strategy

Workforce password security sits at a critical inflection point. As organizations grow more dependent on digital applications with most employees now accessing more than 15 business apps daily, credentials have become the most consistently exploited vulnerability in modern organizations. Yet fewer than one in four businesses have deployed a dedicated password manager, even as one in three experienced a cyberattack in the past year alone.

This report presents findings from 3,322 professionals across nine regions, six industries, and twelve roles worldwide. The data surfaces a persistent and troubling disconnect. Organizations understand the risk in theory but have not converted that understanding into deployed security infrastructure. The gap is widest at the intersection of AI belief and AI readiness. 90% of respondents believe AI will strengthen their security posture, yet only 8% are ready to act on that belief today.

Three structural forces underlie every gap this report documents: a global cybersecurity talent shortage that leaves even funded teams under-resourced, a platform fragmentation crisis in which credential management tools operate in isolation from the HR and IT systems that should govern them, and an SMB capability deficit that leaves the majority of the world's businesses exposed with no dedicated security staff.

The organizations that will navigate the next five years most effectively are those investing in architectural simplicity, building governance models that scale with identity growth, and adopting AI-enabled orchestration to reduce friction. Budget is not the primary constraint on security maturity; architecture, talent, and visibility infrastructure are. The data in this report is a call to sequence correctly: fix foundations before chasing advanced capabilities.

— **Helen Yu,** Founder & CEO, Tigon Advisory Corp.

KEY FINDINGS

59%

Application Sprawl

Of employees use more than 15 apps for work. Each represents a credential that must be created, remembered, and protected across remote and hybrid environments, yet most organizations cannot fully govern this surface area.

1 in 3

Cyberattack Exposure

Businesses suffered a confirmed cyberattack in the past year. A further 7% were not certain whether they had been attacked, a visibility failure that is itself a governance risk.

74%

Identity Visibility Gap

Organizations lack complete visibility over workforce identities. Only 11.6% report full visibility and control. A separate measure finds 88% lack complete visibility when orphaned accounts and undocumented access are included.

90%

AI Promise vs. Reality

Believe AI can strengthen their security posture, but only 8% are ready to deploy AI-powered security right now. An 82-point gap between belief and deployment readiness defines the most critical inflection point in workforce security.

80%

Future-Readiness Crisis

Say their security stack is NOT future-ready. Despite 72% pledging increased budgets over five years, four in five acknowledge their current architecture cannot handle tomorrow's threats. Budget is not the binding constraint, architecture is.

65%

Zero Trust Gap

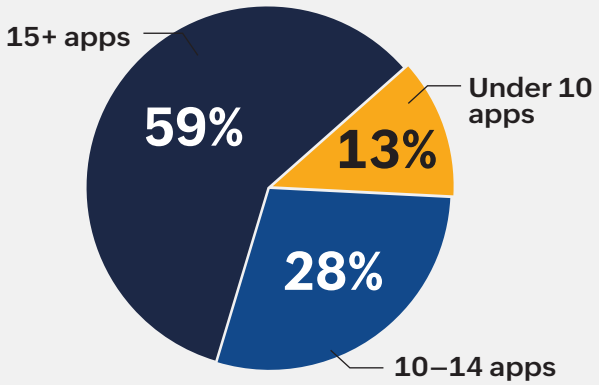
Still lack a Zero Trust security strategy. Of those without one, most expect to adopt within 1–3 years, creating a critical window of vulnerability for credential-based attacks.

1

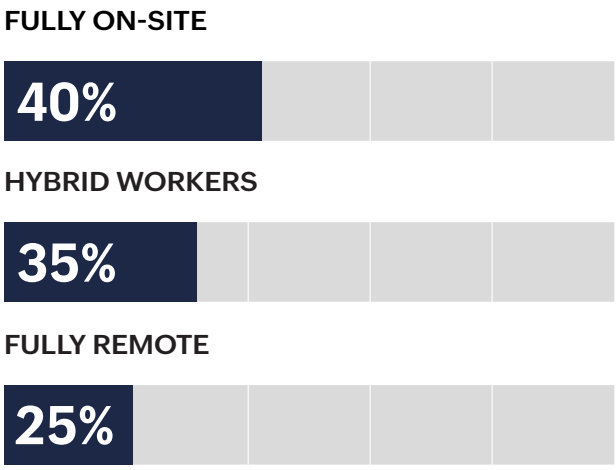
THE APPLICATION SPRAWL PROBLEM

The modern workforce no longer operates from a single login. Employees access a sprawling constellation of business applications. Each application represents a credential that must be created, secured, and governed, creating an attack surface that most organizations cannot fully see.

BUSINESS APP USAGE PER EMPLOYEE



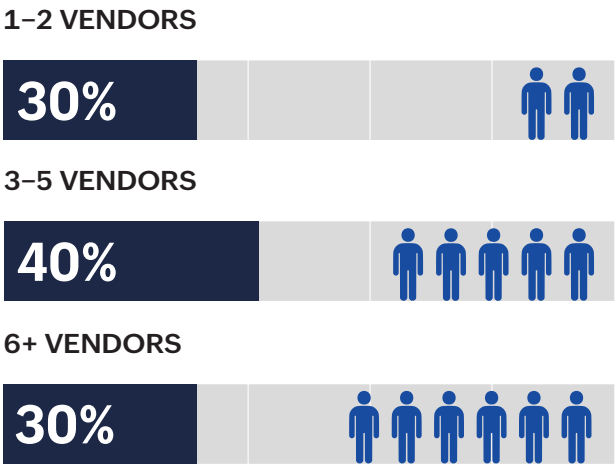
WORKFORCE DISTRIBUTION



The SMB Credential Blind Spot:

Smaller organizations face unique risk. With fewer IT resources and constrained budgets, they often rely on manual password hygiene, shared spreadsheets, and informal policies. More than half of respondents in organizations under 250 employees report having no dedicated security team, making credential management a critical unaddressed vulnerability.

NUMBER OF SECURITY VENDORS



2

THE THREAT LANDSCAPE

When asked to name the top threats to business-critical identities, respondents painted a consistent picture: the most dangerous threats are not exotic technical exploits; they are everyday human vulnerabilities exploited at scale through phishing, weak passwords, and unmanaged access.

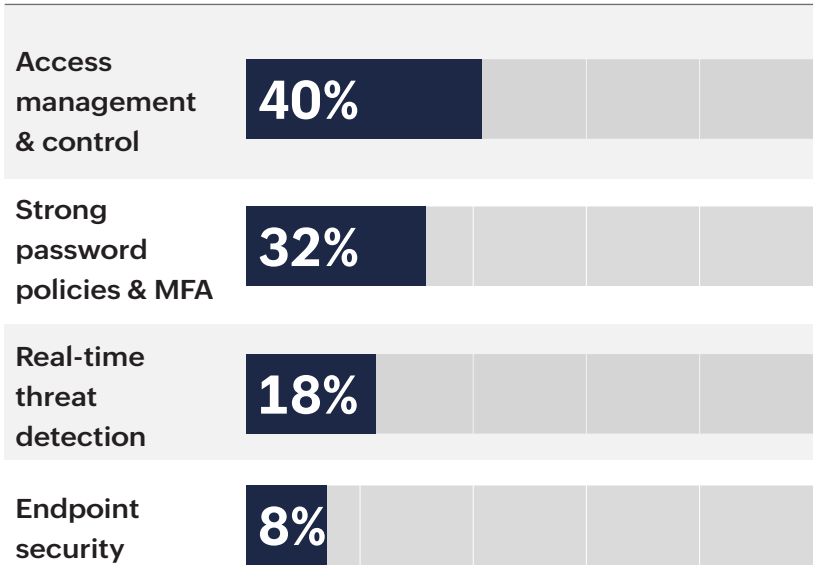
32%
of businesses hit last year

7%
weren't sure — a visibility problem

87%
of attacked orgs had response tools

13%
had no tools at all

TOOLS CREDITED IN ATTACK PREVENTION



TOP THREATS RANKED

68%
Phishing & social engineering

61%
Weak or reused passwords

54%
Insider threats

47%
Credential stuffing attacks

41%
Unmanaged third-party access

THE IDENTITY VISIBILITY GAP

A stark finding: the vast majority of organizations cannot fully account for who has access to what within their own systems. This 'identity visibility gap' is not a peripheral concern — it is the central vulnerability enabling unauthorised access, insider threats, and compliance failures.

74% Lack complete identity visibility

11.6% Have complete visibility and control

88% Lack visibility incl. orphaned accounts

IDENTITY VISIBILITY & CONTROL

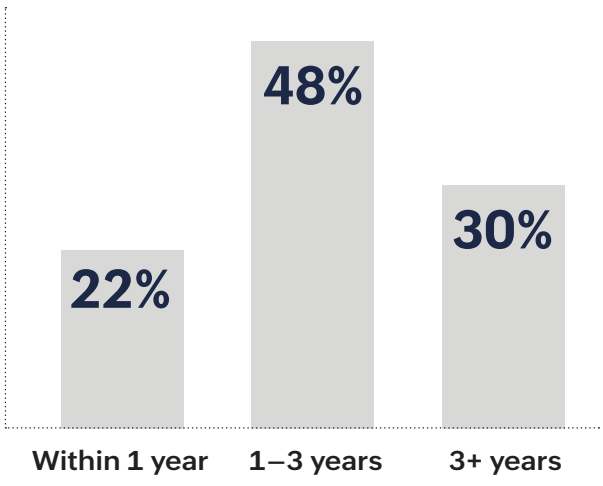
12%
Complete visibility & control

36%
Partial visibility only

38%
Limited visibility

14%
No visibility at all

ZERO TRUST ADOPTION TIMELINE (NON-ADOPTERS)



BARRIERS TO ZERO TRUST ADOPTION

54%
Unmanageable identity growth

32%
Lack of processes and tools

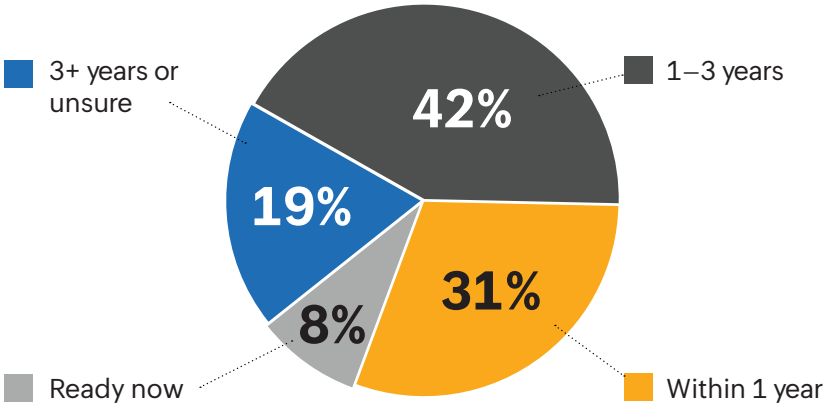
15% Fear of productivity disruption

4

AI IN WORKFORCE SECURITY

AI enthusiasm in security has reached near-universal levels. Nearly 90% of respondents believe AI can strengthen their security strategy. But enthusiasm does not translate to deployment: only 8% are ready to adopt AI-powered security right now, creating an 82-point belief-to-deployment gap.

AI ADOPTION TIMELINE



90%
Believe AI will strengthen security

8%
Ready to adopt AI right now

82pts
Belief-to-deployment gap

DESIRED AI SECURITY FEATURES

68%
Anomaly & threat detection

61%
Automated policy enforcement

54%
Behavioural analytics

47%
Risk-based access controls

TOP BARRIERS TO AI ADOPTION

Legacy infrastructure	52%	Cost and budget constraints	41%
Fear of migration complexity	48%	Lack of internal expertise	38%

5

BUDGET OUTLOOK & INVESTMENT PRIORITIES

Despite cost ranking as the second-largest security challenge, the budget picture for 2026 is broadly optimistic. Most organizations plan to increase security spending. However, increased budget is a necessary but not sufficient condition — the critical question is where those funds are directed.

72%
Plan to increase security spending

20%
Maintain current budget

8%
Anticipate decreases

SIX IMPERATIVES FOR 2026

1. Deploy a Centralized Password Manager

With 32% of organizations experiencing an attack last year and only 25% using password management, centralized credential vaulting is the most under-deployed table-stakes security measure available.

2. Close the Identity Visibility Gap

88% lack complete identity visibility. Implement access logs, session controls, and audit trails to eliminate orphaned accounts and undocumented access.

3. Pair Password Management with MFA

MFA alone is deployed by 43% — but without strong underlying credentials enforced by a password manager, MFA is a speed bump, not a barrier.

4. Build a Zero Trust Roadmap

65% lack Zero Trust. The path starts with fundamentals: strong credentials, least-privilege access, and continuous verification.

5. Treat Integration as a Security Requirement

98% say security integration is essential. Choose a password manager that connects with HRMS, SSO, directory services, and your productivity stack — disconnected tools create the visibility gaps this report documents.

6. Pilot AI-Powered Credential Security in 2026

90% believe in AI's security value. Organizations that begin piloting AI-enhanced anomaly detection in 2026 will be ahead when full adoption accelerates within 1–3 years.

6

ANALYST PERSPECTIVE

- **Platform Unification Is a Security Prerequisite**

  The finding that 88% of organizations lack complete identity visibility is an architecture failure. When credential management operates as a standalone tool disconnected from the systems that govern HR, IT provisioning, and application access, visibility gaps are inevitable. Platform unification is not an IT convenience — it is a security prerequisite.

- **The AI Gap Is an Infrastructure Problem**

  Ninety percent of respondents believe AI will strengthen their security posture, yet only 8% are prepared to act on that belief now. This gap extends beyond AI skepticism to infrastructure readiness. Organizations that own their AI delivery infrastructure end-to-end will have a meaningful advantage as adoption accelerates.

- **The SMB Security Gap Is the Market Opportunity Most Vendors Are Missing**

  More than half of organizations in this survey have fewer than 250 employees. These businesses face the same credential threats as large enterprises — phishing, ransomware, insider risk — without the same resources. Affordable, integrated security platforms designed for SMBs represent the most critical unaddressed market need in workforce security.

- **Consolidation Is Coming — The Question Is Who Leads It**

  Nearly 30% of organizations manage four or more security vendors. 80% acknowledge their stack is not future-ready. AI is eroding the differentiation of point solutions. The organizations that will navigate the next five years most effectively are those with the most coherent architecture, not the most tools.

REGIONAL SNAPSHOTS

UNITED STATES

34%

Experienced cyberattack

62%

Lack Zero Trust

91%

Believe AI strengthens security

METRIC	USA	GLOBAL AVG	VS. GLOBAL
Experienced a cyberattack	**34%**	32%	**+2%**
Use 15+ business apps	**63%**	59%	**+4%**
Lack Zero Trust strategy	**62%**	65%	**-3%**
Believe AI strengthens security	**91%**	90%	**+1%**
Plan to increase security budget	**75%**	72%	**+3%**
Lack complete identity visibility	**76%**	74%	**+2%**

Analyst Insight : *U.S. organizations lead in security investment but face the largest AI belief-to-deployment gap globally (91% belief, only 9% ready to act). Legacy infrastructure is the primary blocker.*

INDIA

47%

Experienced cyberattack

70%

Lack Zero Trust

93%

Believe AI strengthens security

METRIC	INDIA	GLOBAL AVG	VS. GLOBAL
Experienced a cyberattack	**47%**	32%	**+15%**
Use 10+ business apps	**29%**	59%	**-30%**
Lack Zero Trust strategy	**70%**	65%	**+5%**
Believe AI strengthens security	**93%**	90%	**+3%**
Plan to increase security budget	**91%**	72%	**+19%**
Lack complete identity visibility	**34%**	74%	**-40%**

Analyst Insight : *India's rapidly digitizing workforce shows the highest app sprawl globally (29%). AI enthusiasm is the highest of any region (93%) and budget growth intent leads globally (91%), yet 70% still lack Zero Trust — a critical window for platform-native adoption.*

UK & EU

31%

Experienced cyberattack

61%

Lack Zero Trust

88%

Believe AI strengthens security

METRIC	UK & EU	GLOBAL AVG	VS. GLOBAL
Experienced a cyberattack	**31%**	32%	**-1%**
Use 15+ business apps	**57%**	59%	**-2%**
Lack Zero Trust strategy	**61%**	65%	**-4%**
Believe AI strengthens security	**88%**	90%	**-2%**
Plan to increase security budget	**69%**	72%	**-3%**
Lack complete identity visibility	**75%**	74%	**+1%**

Analyst Insight : *Regulatory pressure from GDPR and NIS2 is accelerating identity governance investment, yet 75% still lack full identity visibility — a direct compliance liability. UK & EU organizations show the strongest regulatory awareness of any region.*

CANADA

30%

Experienced cyberattack

63%

Lack Zero Trust

89%

Believe AI strengthens security

METRIC	CANADA	GLOBAL AVG	VS. GLOBAL
Experienced a cyberattack	**30%**	32%	**-2%**
Use 15+ business apps	**60%**	59%	**+1%**
Lack Zero Trust strategy	**63%**	65%	**-2%**
Believe AI strengthens security	**89%**	90%	**-1%**
Plan to increase security budget	**71%**	72%	**-1%**
Lack complete identity visibility	**73%**	74%	**-1%**

Analyst Insight : *Canadian organizations track closely with U.S. security maturity but show stronger MFA deployment (47%) and more cautious AI timelines. 63% still lack a Zero Trust strategy despite elevated attack rates.*

MEA (MIDDLE EAST & AFRICA)

36%

Experienced cyberattack

71%

Lack Zero Trust

87%

Believe AI strengthens security

METRIC	MEA	GLOBAL AVG	VS. GLOBAL
Experienced a cyberattack	**36%**	32%	**+4%**
Use 15+ business apps	**55%**	59%	**-4%**
Lack Zero Trust strategy	**71%**	65%	**+6%**
Believe AI strengthens security	**87%**	90%	**-3%**
Plan to increase security budget	**73%**	72%	**+1%**
Lack complete identity visibility	**79%**	74%	**+5%**

Analyst Insight : *MEA has the highest confirmed cyberattack rate (36%) and the lowest identity visibility of all regions (79% lack it) — a dangerous combination as cloud adoption accelerates.*

ANZ (AUSTRALIA & NEW ZEALAND)

33%

Experienced cyberattack

64%

Lack Zero Trust

90%

Believe AI strengthens security

METRIC	ANZ	GLOBAL AVG	VS. GLOBAL
Experienced a cyberattack	**33%**	32%	**+1%**
Use 15+ business apps	**58%**	59%	**-1%**
Lack Zero Trust strategy	**64%**	65%	**-1%**
Believe AI strengthens security	**90%**	90%	**=**
Plan to increase security budget	**70%**	72%	**-2%**
Lack complete identity visibility	**74%**	74%	**=**

Analyst Insight : *Australia and New Zealand show strong cybersecurity awareness, driven by government-led frameworks, but face an SMB affordability gap. Over half of businesses under 250 employees lack a dedicated security team.*

JAPAN

27%

Experienced cyberattack

68%

Lack Zero Trust

85%

Believe AI strengthens security

METRIC	JAPAN	GLOBAL AVG	VS. GLOBAL
Experienced a cyberattack	**27%**	32%	**-5%**
Use 15+ business apps	**52%**	59%	**-7%**
Lack Zero Trust strategy	**68%**	65%	**+3%**
Believe AI strengthens security	**85%**	90%	**-5%**
Plan to increase security budget	**66%**	72%	**-6%**
Lack complete identity visibility	**77%**	74%	**+3%**

Analyst Insight : *Japan's security posture is evolving rapidly under digital transformation mandates. Despite the lowest confirmed attack rate (27%), 68% still lack Zero Trust and 77% lack identity visibility — a combination that may not persist as infrastructure modernisation accelerates.*

CHINA

28%

Experienced cyberattack

67%

Lack Zero Trust

85%

Believe AI strengthens security

METRIC	CHINA	GLOBAL AVG	VS. GLOBAL
Experienced a cyberattack	**28%**	32%	**-4%**
Use 15+ business apps	**61%**	59%	**+2%**
Lack Zero Trust strategy	**67%**	65%	**+2%**
Believe AI strengthens security	**92%**	90%	**+2%**
Plan to increase security budget	**76%**	72%	**+4%**
Lack complete identity visibility	**71%**	74%	**-3%**

Analyst Insight : *China shows high AI optimism (92%) and strong budget growth intent (76%), positioning it for rapid security modernization. However, 67% still lack a Zero Trust framework — mirroring the pattern seen across high-AI-enthusiasm markets globally.*

APAC (OTHER)

32%

Experienced cyberattack

66%

Lack Zero Trust

91%

Believe AI strengthens security

METRIC	APAC (OTHER)	GLOBAL AVG	VS. GLOBAL
Experienced a cyberattack	**32%**	32%	=
Use 15+ business apps	**64%**	59%	+5%
Lack Zero Trust strategy	**66%**	65%	+1%
Believe AI strengthens security	**91%**	90%	+1%
Plan to increase security budget	**74%**	72%	+2%
Lack complete identity visibility	**73%**	74%	-1%

Analyst Insight : *Across broader APAC (excluding Japan and China), digital-first economies face compound credential risks from mobile-first workforces and multi-cloud sprawl. APAC has the highest app sprawl in the region (64% use 15+ apps). Integrated credential governance is the top unmet need.*

THE TALENT SHORTAGE

The Hidden Force Behind Every Adoption Gap

Every major finding in this survey has an unexamined root cause. Why do 65% of organizations lack a Zero Trust strategy? Why do 80% say their stack is not future-ready yet 72% plan to increase budget? Why does an 82-point gap exist between believing in AI and being ready to deploy it? The answer underlying each gap is the same: a shortage of skilled identity and security practitioners capable of executing on security strategy.

> *Organizations cannot hire their way into security maturity. They must architect around the talent they have.*

3.5M

Global cybersecurity vacancies projected through 2026

38%

Cited lack of internal expertise as top AI barrier

1 in 2

SMBs have no dedicated security team at all

Survey Finding	How Talent Shortage Explains It	Implication
65% lack Zero Trust strategy	Zero Trust requires skilled architects to design access policies and implement continuous verification — capabilities most security teams do not have in-house.	Hire or partner for architecture expertise; prioritize platforms with opinionated Zero Trust defaults.
80% say stack is not future-ready	Keeping a fragmented multi-vendor stack current requires deep expertise. Most teams cannot maintain what they have, let alone modernize it.	Consolidate to reduce the number of platforms requiring specialized expertise.

Survey Finding	How Talent Shortage Explains It	Implication
82 -point AI belief-to-deployment gap	Deploying AI-powered security requires data scientists, ML engineers, and identity operations practitioners — rare skills.	Adopt vendor-managed AI features rather than building internal capabilities from scratch.
Only 26% use password management	Even deploying a password manager requires IT staff to configure integrations and enforce policies. Under-resourced teams deprioritize even basic credential governance.	Choose platforms with minimal configuration overhead and native HRMS integration.
74% lack identity visibility	Building comprehensive identity visibility requires ongoing audit, access review, and governance work — exactly the work that falls behind in under-staffed teams.	Invest in automated discovery and reporting to reduce the human effort required for ongoing visibility.

8

VENDOR FRAGMENTATION & THE CONSOLIDATION IMPERATIVE

Why platform sprawl is a credential security problem

This survey reports that 30% of organizations work with 6+ security vendors and 40% work with 3–5. This fragmentation is a direct structural cause of the identity visibility gap, the Zero Trust adoption gap, and the credential management gap that define the survey's core findings. When credential management operates disconnected from HR systems, SSO platforms, and directory services, visibility gaps are not a configuration problem — they are an architecture inevitability.

The Integration Failure

Full credential governance requires integration across four systems that most fragmented stacks fail to connect in real time: HRMS/Directory (provisioning & deprovisioning) → SSO/Identity Provider (MFA enforcement) → Password Vault (credential storage & audit) → Access Governance (ongoing certification & orphaned account detection).

> *In fragmented stacks, these systems rarely share data in real time. Employees who leave remain in the vault. Role changes do not trigger access reviews. Orphaned accounts accumulate. The 74% identity visibility gap this survey documents is not a tool failure — it is an integration failure.*

3 in 1

Security teams spend more time managing vendors than managing threats

41%

Cite higher total cost of ownership as primary pain

37%

Cannot hire or train staff for all tools in their stack

34%

Cite integration complexity as top operational burden

98% Say security integration is essential

80% Say stack is NOT future-ready

88% Lack complete identity visibility

9

CROSS-REGIONAL SYNTHESIS

THREE STRATEGIC PATTERNS

Pattern 1: High AI Enthusiasm Correlates with Low Zero Trust Adoption

India (93% AI belief, 70% lack Zero Trust), China (92%, 67% lack Zero Trust), and APAC (91%, 66%) all show the same dynamic: the region's most enthusiastic about AI have not yet implemented foundational security architecture. This suggests a risk of skipping foundational security layers in pursuit of advanced capabilities, a sequencing error that creates vulnerabilities rather than eliminating them.

> *Recommended sequence: Credential governance first → Zero Trust framework second → AI-enhanced monitoring third.*

Pattern 2: Attack Rate and Identity Visibility Gap Are Independently Variable

MEA has both the highest attack rate (36%) and the lowest identity visibility (79% lack it), the most dangerous combination in this dataset. Japan has the lowest attack rate (27%) but 77% lack identity visibility, suggesting historical security posture may not persist as digital transformation accelerates. Low attack rates should not be read as low risk where visibility gaps are high.

Pattern 3: Budget Intent Does Not Predict Security Maturity

India leads in budget growth intent (78%) but lags in foundational deployments. The US leads in security investment (75% plan increases) but shows the largest AI belief-to-readiness gap globally. This reinforces the report's core thesis: budget is not the primary constraint on security maturity, architecture, talent, and visibility infrastructure are.

SMB DEEP DIVE

THE SMB SECURITY PARADOX

More than half of respondents come from organizations with fewer than 250 employees, making this the most comprehensive global dataset on SMB credential security currently available. SMBs face the same threats as enterprises, but with a fraction of the defensive capability.

>50% Respondents from orgs under 250 employees

>50% Of SMBs report no dedicated security team

Dimension	Enterprise Reality	SMB Reality
Threat exposure	Equivalent to enterprise for most attack vectors	No material difference
IT security team	Dedicated team averaging 5–15 FTEs	Often 0–1 FTEs; frequently outsourced or nonexistent
Password management	Centralized enterprise vault with policy enforcement	Shared spreadsheets, browser-saved passwords, informal policies
Zero Trust adoption	Under-adopted at enterprise level (35%)	Effectively nonexistent at SMB level
AI readiness	Low enterprise readiness (8–9%)	Near-zero readiness without managed service delivery

THREE REFORMULATED PRINCIPLES FOR SMBS

1. Managed-first over self-deployed

SMBs benefit most from security capabilities delivered as managed services rather than platforms requiring configuration, integration, and ongoing maintenance. A cloud-managed password vault with opinionated defaults delivers more SMB security value

than a feature-rich enterprise platform requiring a full-time administrator.

2. **Consolidation as a starting point, not an end state**

   For SMBs, the goal should be a single integrated platform covering identity, access, and credential management — rather than best-of-breed selection across specialized vendors. The integration overhead that is merely painful for enterprises is genuinely unmanageable for SMBs without dedicated IT staff.

3. **Training designed for non-security employees**

   The insider threat and phishing risks that rank highest in this survey are primarily human behavior problems. SMBs without security awareness programmed need lightweight, role-appropriate training that can be delivered without a dedicated security team.

GLOSSARY OF KEY TERMS

Term	Definition
Credential stuffing	An automated attack in which stolen username/password combinations are tested against multiple services, exploiting the tendency to reuse passwords across accounts.
Identity visibility	The degree to which an organization can fully account for all user accounts, their access rights, and their activity across all systems. Complete visibility means no orphaned, undocumented, or unreviewed accounts exist.
MFA (Multi-Factor Authentication)	A security method requiring users to provide two or more verification factors to gain access to a system — typically something they know (password), something they have (device), and/or something they are (biometric).
Orphaned account	A user account that remains active in a system after the person who owned it has left the organization or changed roles — a common source of unauthorized access.
Password manager / credential vault	A secure, centralized system that stores, generates, and manages credentials on behalf of users and enforces password policy across an organization.
Phishing	A social engineering attack in which a malicious actor impersonates a trusted entity to trick individuals into revealing credentials or other sensitive information.
SSO (Single Sign-On)	An authentication scheme allowing a user to log in once and gain access to multiple systems without re-authenticating for each.
Zero Trust	A security framework built on the principle that no user, device, or system should be trusted by default — even those inside the network perimeter. Access is continuously verified based on identity, context, and behavior.

ABOUT

Helen Yu is the Founder & CEO of Tigon Advisory Corp. and Host of CXO Spice. A globally recognized thought leader at the intersection of cybersecurity, digital transformation, and artificial intelligence, she is ranked among the Top 50 Global Thought Leaders in Cybersecurity & AI and serves as a Board Director across multiple organizations.

With over fifteen years of executive experience spanning Fortune 500 companies and high-growth startups, Helen brings a rare operator's lens to complex security challenges. Her expertise bridges technical depth with strategic leadership, making her a trusted advisor to organizations navigating today's rapidly evolving threat landscape.

A prolific author, sought-after keynote speaker, and board director, Helen advises enterprises worldwide on building resilient security architectures that scale with modern workforce demands.

Connect with her on LinkedIn at *linkedin.com/in/yuhelenyu*.

ABOUT ZOHO CORPORATION

Zoho Corporation is a privately held, profitable technology company. Founded in 1996, Zoho Corporation has grown into a multinational technology corporation, operating four distinct brands: ManageEngine, Zoho, Qntrl, and Trainer Central. Headquartered in Chennai, India, Zoho Corporation has a significant global presence, with 90+ offices across 28 countries, 19,000 employees worldwide, and a growing customer base across both Enterprise and SMB organizations.


ZOHO