Your Identity Is Under Siege

Fight Back Before It's Too Late

Presentation by **Kishore Ganti**

April 2026

Let me introduce myself

pwc

20 years in IT
16+ in Identity and Access Management

Identity Architect delivering large Global IAM programs

From ‘Hack the Gibson’ to ‘Click Here to Attack’”

Then

Now

Risk and threat landscape: Geopolitics are reshaping cyber vulnerabilities

60%

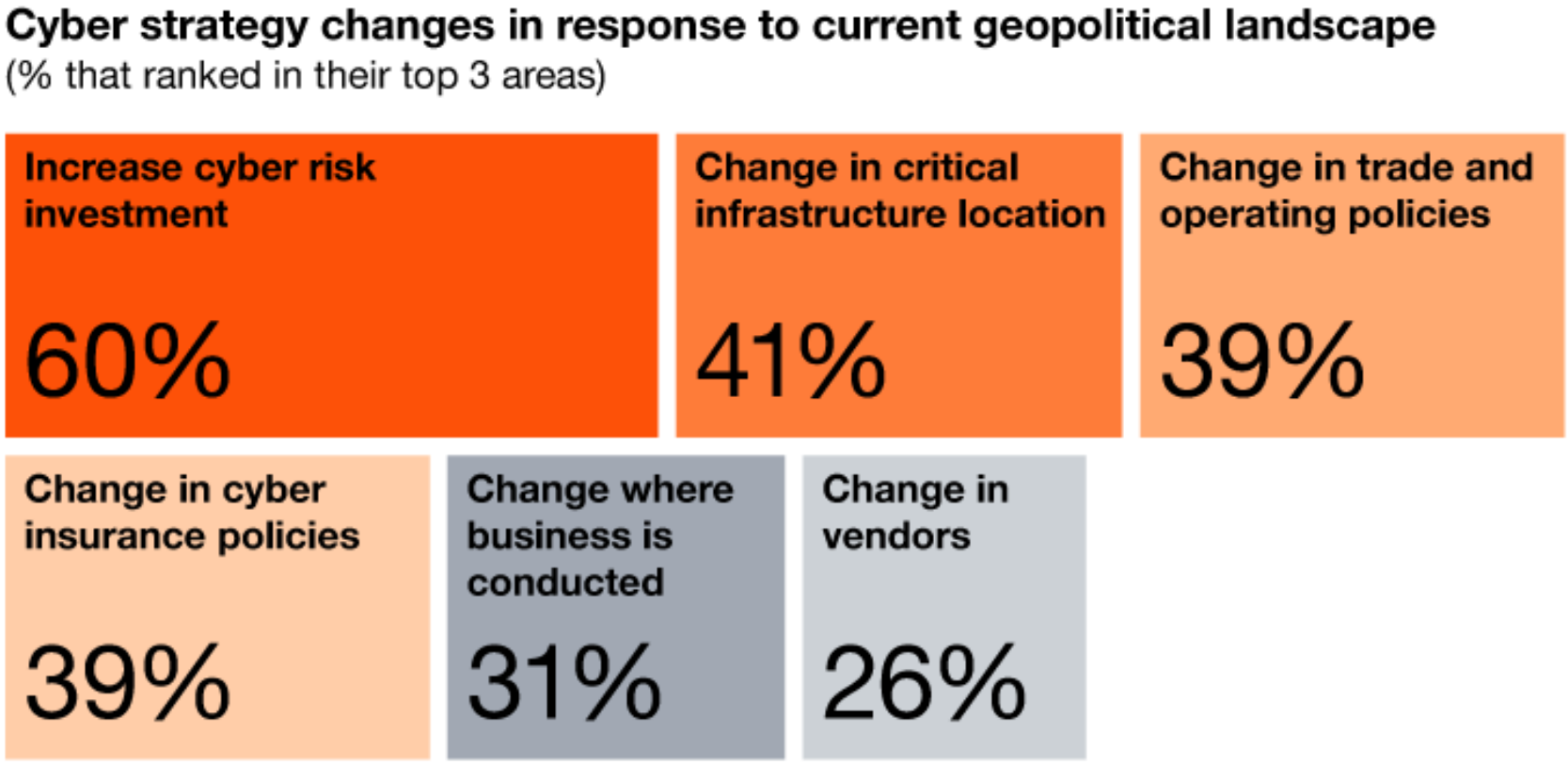
are increasing cyber risk investment in response to geopolitical volatility

6%

are 'very capable' of withstanding cyber attacks across all vulnerabilities surveyed given the geopolitical landscape

Top 2

cyber threats organisations are least prepared to address: Cloud and connected products



Q2. Over the next 12 months, which of the following areas of your organisation's cyber strategy is changing in response to the current geopolitical landscape? Base: All respondents=3887
Source: PwC 2026 Global Digital Trust Insights

Cyber strategy and operations: Where investment meets impact

Only 24%

are spending significantly more on proactive vs reactive cybersecurity measures

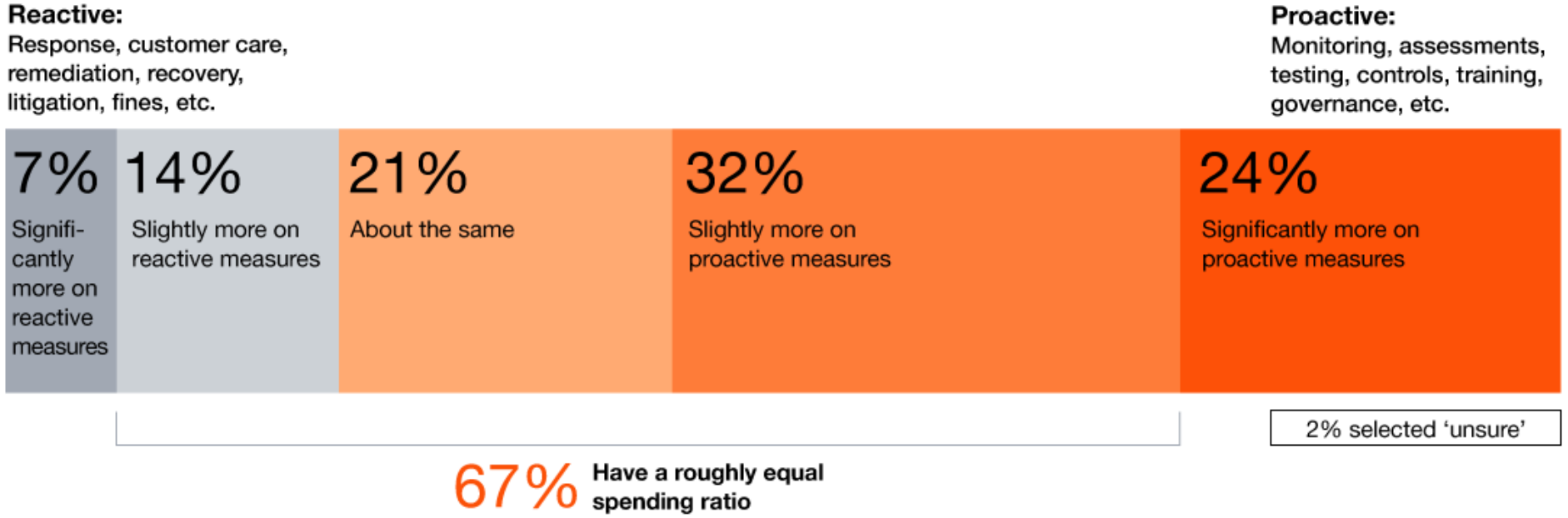
78%

expect their cyber budget to increase over the coming year

Only 16%

are measuring the financial impact of cyber risks to a significant extent

Spending on reactive vs proactive measures



Q13. Is your organisation spending more resources on reactive or proactive cybersecurity measures? Base: All respondents=3887
Source: PwC 2026 Global Digital Trust Insights

AI in cybersecurity: From promise to priority

No. 1

cyber investment priority for security leaders is AI

No. 1

AI security capability prioritised by security leaders is AI threat hunting

No. 1

areas of priority for agentic AI are cloud security, data protection and cyber defense

Agentic AI among the top prioritised AI security capabilities
(Ordered based on those who ranked as their top priority)

Q18. Which of the following AI security capabilities will your organisation prioritise over the next 12 months? Base: Security leaders=1740
Source: PwC 2026 Global Digital Trust Insights

Looking ahead

The threat landscape in 2026 will be defined by stealthier, persistent, and identity-centric operations, and still heavily converge with real-world events.

Trust is the attack surface.

Identity is the control plane.

Speed is the differentiator.

IRL drivers and influences

Expect and prepare for spillover from geopolitical, ideological, and other issues from real-world events into cyber threat activities

Stealth is the new normal

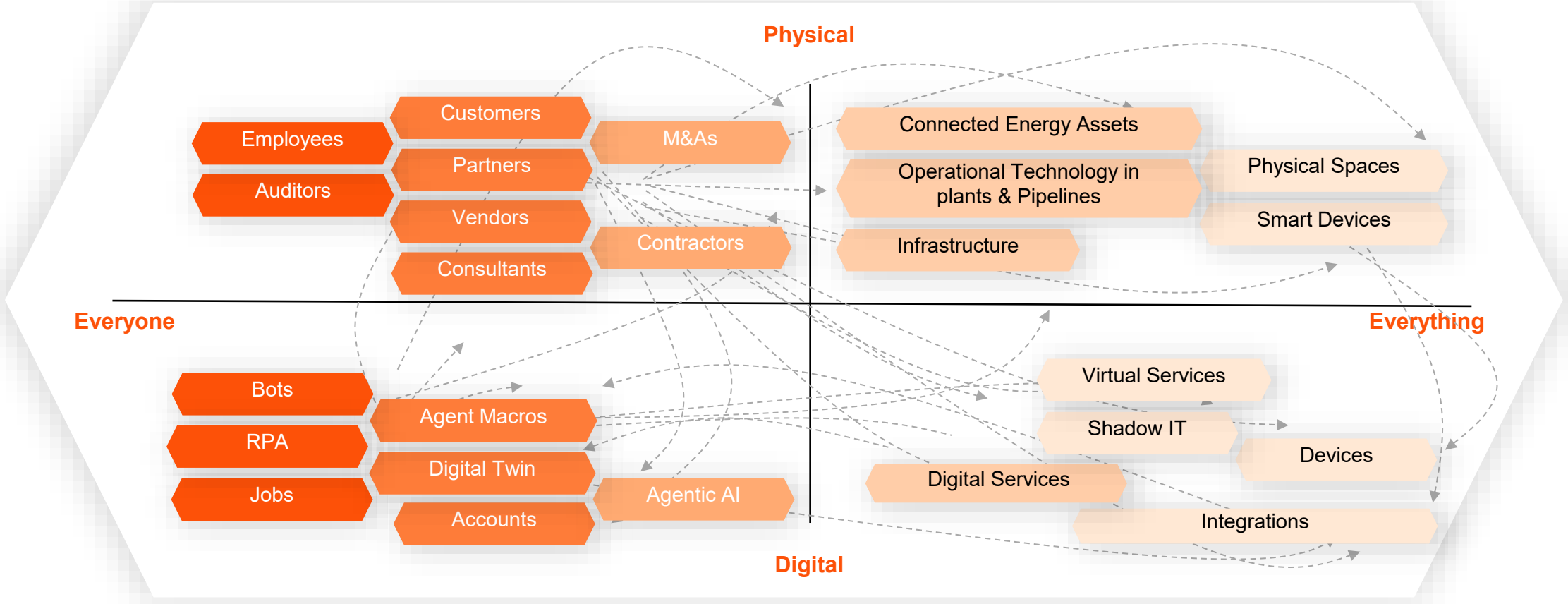
Threat actors want to remain invisible through covert networks/capabilities, legitimate identities, and everyday tools within your environment

AI and tech advancements

Streamlined processes and tooling (e.g., phishing kits, malware development) that lowers the barrier to entry (i.e., time, skill, resources)

The Identity Universe is Expanding – and So Are the Risks

As digital and physical worlds converge, every connection becomes an identity to protect – from people to machines to algorithms.



Attackers are shifting to identity tactics targeting OT and IT convergence.

Breaches surged due to third-party and contractor exposure.

Supply chain vulnerabilities remain a critical risk.

The perfect storm continues….

Field Insights: What Clients Worry About Most with AI Agents

"We know we need AI agents, but we don't yet have a clear governance model. Who actually approves and controls what gets deployed in government?

"How do we govern external AI APIs, connectors, and integrations into our environment?"

"How do we ensure least-privilege access for agents, not just humans?

"How do we scale AI agent development responsibly across multiple departments?

"Our data is spread across multiple departments and systems—how do we apply consistent data-protection and DLP rules whenever an AI agent interacts with it?

"We don't have a secure environment for building agents.

"How do we make sure AI agent outputs are accurate, explainable, and compliant—especially when new regulations keep coming?

"Teams are already building agents without security review. How do we get visibility before something breaks?

"How do we monitor agent actions, track decisions, and detect misuse in real time?

"We don't know what data our agents are accessing or exposing. How do we stop oversharing before it happens?

"What AI agents exist today, and what are they connected to? We simply don't have an inventory.

"We want AI to accelerate delivery, but we need confidence that security won't slow us down."

"Agents are acting on behalf of users — but who governs their permissions, lifecycle, and access revocation?

Field Insights: What Clients Worry About Most about Data Security

"We're confident data exists — we're less confident about where it all ended up.

"We don't have a simple way to separate low-risk content from high-risk content."

"If sensitive data is sitting in the wrong place, we wouldn't spot it quickly."

We don't routinely question who still needs access — only who needs new access. Risk creeps in gradually, not all at once."

"Access decisions made years ago still apply today, even though the business has changed."

"Permissions tend to outlive the projects they were created for."

"Some sites are tightly governed, others are essentially wide open."

"Security depends too much on who set the site up in the first place."

"The same type of data is treated very differently depending on where it lives."

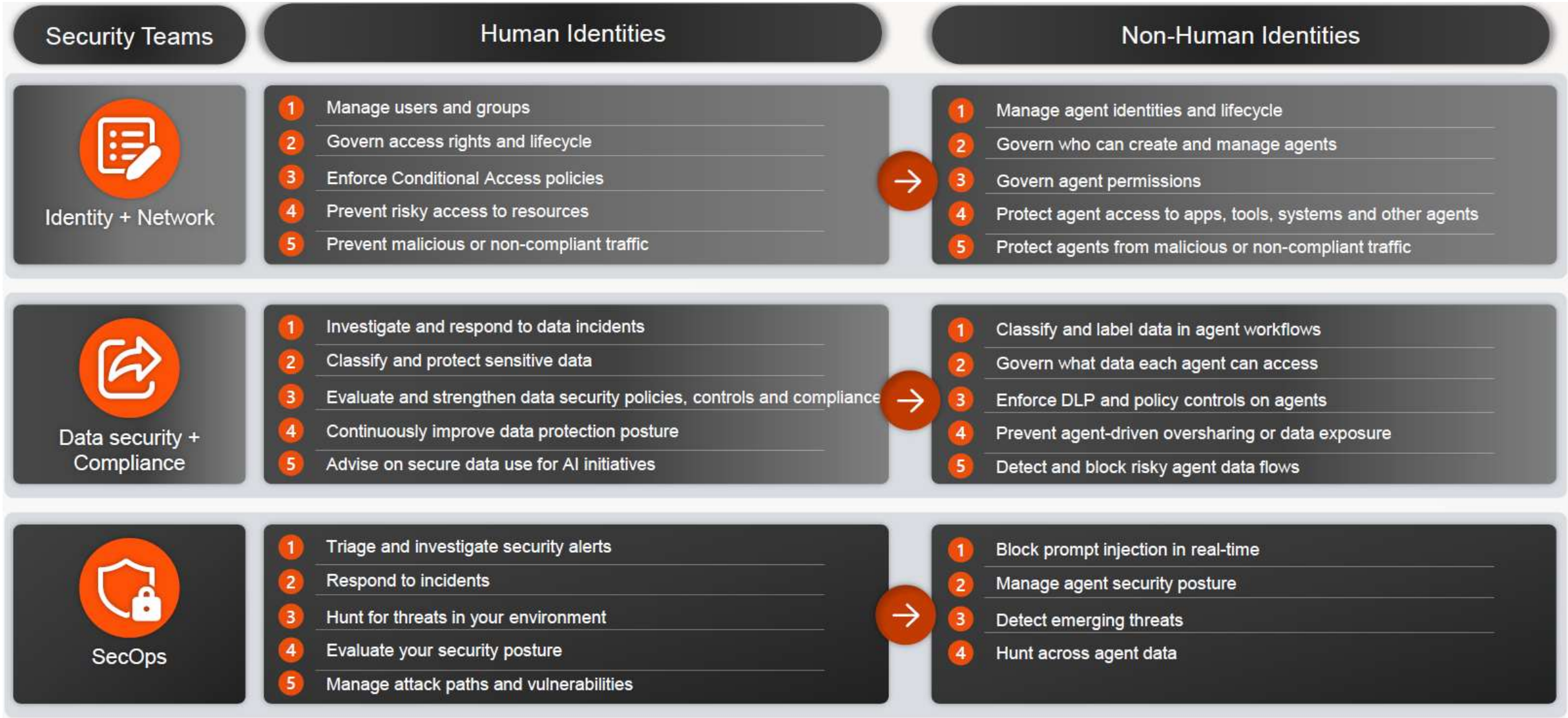
"Confidence depends on visibility, not optimism."

"It's hard to demonstrate control when everything is manual."

"Classification accuracy varies widely across teams."

"We don't have a natural point where data is reviewed or cleaned up."

Enabling your Security Teams and Solutions



Developing threat-led strategies to defend identities from compromise

How do you protect identities from compromise?

How do you detect compromised identities?

How do you respond to compromised identities?

- Secure Identity Architecture
- Strong Authentication
- Secure Administration Practices
- Secure Configuration and Hygiene
- Secure Service Account Lifecycle
- Logging and Monitoring of Identity Infrastructure
- Identity Detection and Response
- Anomaly Detection
- Automated Response Actions
- Security Testing (Red Team testing & Purple Team testing)

How do you recover identities?

- Automated Identity Recovery
- Identity Recovery Exercising

What It Takes to Secure the Future

An integrated view on Resilience.

Revisiting data security to prep for impact of AI.

Continued Best in Suite vs Best in Breed (Tech Simplification).

Expanded Identity & Access Universe

Understanding Shared Responsibility Models across PaaS and SaaS.

Thank you

pwc.com