

CATEGORY REPORT Q4 / 2026

Cybersecurity, Identity & Data Protection

Who can buyers trust to protect them now?



I *The Insight*
COLLECTIVE

LEAD GENERATION
FOR B2B TECHNOLOGY
BRANDS

The cybersecurity landscape is constantly evolving. Threats are becoming more frequent and severe, giving businesses less time to detect and contain them as attack surfaces continue to expand.

Regulators are also raising the bar, demanding greater evidence that security and compliance controls are not only in place, but effective.

That pressure is extending to vendors, as buyers demand greater transparency around what solutions can deliver, how they work, and how they perform when it matters.

This report explores what's driving these shifts across cybersecurity markets, how they vary by region, and what they mean for brands competing in a more demanding category.

\$4.99M

Record global average breach cost, up twelve percent in a year

IBM, 2026

31%

Breaches beginning with an exploited vulnerability, now the leading entry route

VERIZON, 2026

80 : 1

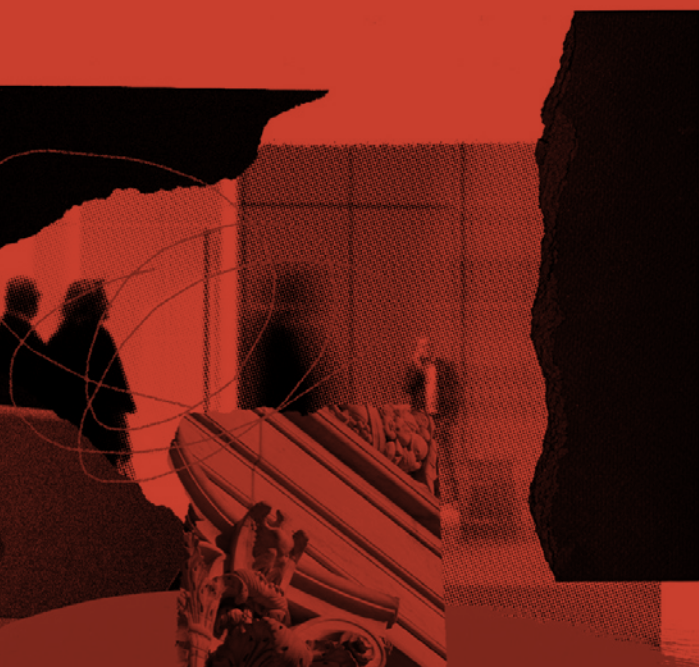
Machine identities for every human identity in the average enterprise

KPMG INTERNATIONAL, 2026

94%

Cyber leaders naming AI the most significant force reshaping their defenses

WORLD ECONOMIC FORUM, 2026



Four shifts reshaping the landscape.

85% of organizations raised their cybersecurity budget this year, and nearly nine in ten plan to raise it again in 2026 (Wiz, 2026). Yet more than half of those same leaders still don't believe that spending is enough to cover the risk they're carrying. The four measures below show where that gap is widening fastest.

REMIEDIATION CAPACITY

43 days

MEDIAN TIME TO FULLY PATCH A KNOWN VULNERABILITY

VERIZON, 2026

Patch backlogs are widening the attack surface

Only 26% of known, actively exploited flaws get fully patched, down from 38% a year earlier (Verizon, 2026). New vulnerabilities are being disclosed faster than most teams can triage them, while severity scores alone don't show whether a flaw creates a meaningful route to sensitive systems or data.

THIRD-PARTY RISK

48%

CONFIRMED BREACHES INVOLVING A THIRD-PARTY

VERIZON, 2026

The supply chain is becoming harder to control

Third-party involvement in breaches is up 60% in a year, and only 23% of third parties have even basic protections, like multi-factor authentication, in place on their cloud accounts. Supplier risk assessments often happen once, when a contract is signed, with limited visibility into how those risks change over time.

AI EXPOSURE

56%

YEAR-OVER-YEAR RISE IN AI-DRIVEN ATTACKS

IBM, 2026

AI has become a double-edged sword

AI-driven attacks now add roughly a million dollars to the average breach when they succeed, while AI tools employees weren't supposed to use appear in 43% of security incidents, more than double the year before (IBM, 2026). Deepfake impersonation is now the largest category of AI-enabled attack activity, yet most organizations still lack a formal process for approving which AI tools employees can use.

REGULATORY EVIDENCE

24 hrs

DEADLINE TO REPORT AN ACTIVELY EXPLOITED VULNERABILITY

EUROPEAN COMMISSION, 2026

Compliance has turned into an evidence-production problem

The 24-hour reporting deadline runs alongside 72-hour and 14-day filings, often to different authorities for the same event (European Commission, 2026). Similar rules already apply to businesses handling data from California (IAPP, 2026), putting greater pressure on controls to produce evidence on demand rather than simply operate in the background.

Identity management was built for *people*. Most identities today are *machines*.

Faster attacks and tighter compliance deadlines are only part of the change. The population security teams need to manage has changed too: machines, applications and AI agents now vastly outnumber the people traditional identity systems were designed around, creating new challenges around ownership, access, accountability and detection.

1

ORPHANED CREDENTIALS

Old machine credentials rarely get switched off

Machine identities can remain active long after they are needed, particularly when ownership is unclear. That leaves access in place without a clear reason or accountable owner.

2

RUNTIME ACCESS

What a program can access can change while it's running

Automated systems can make access decisions in real time, potentially going beyond what was approved in advance. That makes it harder for security teams to understand and control what an identity can actually reach.

3

ACCOUNTABILITY GAP

Every automated action needs a person's name attached to it

Auditors and insurers increasingly need to know who is responsible for automated activity, not simply that an action took place. For many organizations, connecting machine activity back to a responsible person or team remains difficult.

4

DETECTION BLIND SPOT

The old way of spotting suspicious activity doesn't work here

Detection built around working hours, familiar devices and human behavior doesn't translate neatly to software that operates continuously. Security teams need new ways to distinguish expected machine activity from behavior that warrants investigation.

250k

AVERAGE MACHINE IDENTITIES IN AN ENTERPRISE, UP FROM ROUGHLY 50,000 IN 2021

KPMG INTERNATIONAL, 2026

144:1

NON-HUMAN TO HUMAN IDENTITIES IN CLOUD-NATIVE ENVIRONMENTS

CLOUD SECURITY ALLIANCE, 2026

92%

TECHNOLOGY EXECUTIVES WHO EXPECT MANAGING AI AGENTS TO DEFINE SECURITY SKILL NEEDS WITHIN FIVE YEARS

KPMG INTERNATIONAL, 2026

What are buyers trying to resolve?

Research trends in this category point to two sets of questions: what buyers are trying to understand about their own environment, and what they need answered before they can choose a vendor. Four areas stand out.

OWNERSHIP GAP

Who owns each machine identity, and what can it reach?

Security teams can usually explain what their automated workloads and agents are designed to do. Fewer can say what those identities can access, when that access expires, or who is responsible for it. As machine identities multiply, keeping track of them becomes increasingly difficult.

VENDORS THAT CAN HELP BUYERS ESTABLISH VISIBILITY AND OWNERSHIP ARE BETTER PLACED TO ADDRESS A PROBLEM THEY ALREADY RECOGNIZE.

DATA VISIBILITY

Can we still say where sensitive data sits once AI tools are in the flow?

AI tools can now interact with sensitive data through prompts, retrieval systems and agent memory, creating visibility gaps for traditional data controls. Unauthorized tools add another layer of uncertainty, particularly where organizations lack clear processes for approving their use.

CLEAR VISIBILITY INTO HOW DATA MOVES THROUGH AI SYSTEMS IS BECOMING AN IMPORTANT PART OF THE BUYING CONVERSATION.

3x

RISE IN RESEARCH ACTIVITY AROUND IDENTITY LIFECYCLE MANAGEMENT LAST QUARTER

BOMBORA, 2026

2x

RISE IN RESEARCH DEMAND FOR DATA PRIVACY AND PROTECTION OVER THE SAME PERIOD

BOMBORA, 2026

PRIORITIZATION

We don't have enough people to close this backlog, so which gaps matter?

Remediation capacity has not kept pace with the volume of exposure teams are expected to manage, while specialist skills remain in short supply. Severity scores can help identify risk, but they don't always show which gaps deserve attention first.

BUYERS NEED MORE THAN ANOTHER LIST OF FINDINGS. THEY NEED A WAY TO UNDERSTAND WHICH RISKS DEMAND ACTION AND WHY.

RECOVERY PROOF

If we are hit, can we prove we can recover, and prove it to whom?

Ransomware continues to put recovery capabilities under pressure, shifting the focus from whether backups exist to whether recovery can actually be demonstrated. For buyers, that means being able to show that recovery works, that data remains intact, and that the process stands up to external scrutiny.

A DEMONSTRABLE RECOVERY PROCESS PROVIDES STRONGER ASSURANCE THAN BACKUP COVERAGE ALONE.

95% SECURITY TEAMS REPORTING AT LEAST ONE SKILLS GAP

ISC2, 2025

39% BREACHED ORGANIZATIONS REPORTING A RANSOMWARE ATTACK IN THE PAST YEAR

IBM, 2026



Three regions, three triggers.

Geography changes how buyers experience cybersecurity risk, as the regulatory and economic pressures behind it vary by market. Across the Americas, EMEA and APAC, those differences shape what buyers need to address and what they expect from vendors.

TOPIC	AMERICAS	EMEA	APAC
ECONOMIC PRESSURE	Breach costs are higher here than elsewhere, with the average US breach reaching \$11.5 million, more than double the global figure (IBM, 2026). That puts a clear financial value on reducing exposure and limiting the impact of incidents.	Ransomware remains the most financially disruptive cyber threat across the region, with supply chain routes accounting for a significant share of incidents (ENISA, 2025). That is putting greater focus on third-party assurance and resilience earlier in the buying process.	Australia recorded 1,205 breach notifications in 2025, an 8% increase, while data breaches are now the country's leading perceived privacy risk (OAIC, 2026). Public reporting is putting greater visibility on how organizations manage personal data and respond to incidents.
REGULATORY TRIGGER	Twenty states now have comprehensive privacy laws in force, while California's rules on annual audits, risk assessments and automated decision-making took effect in 2026 (IAPP, 2026). The result is a growing set of obligations for security and privacy teams to manage.	Product security reporting duties begin in September 2026 under the Cyber Resilience Act, with staged 24-hour, 72-hour and 14-day obligations alongside existing network security and data protection requirements (European Commission, 2026).	India's data protection rules are being phased in on a fixed schedule, with consent manager registration due in November 2026 and full compliance by May 2027 (Fisher Phillips, 2026). The framework also introduces significant penalties for non-compliance.
BUYER CONCERN	The challenge is keeping those obligations connected. Buyers need to understand which controls and systems support which requirements, and whether evidence gathered for one regime can support another.	Multiple reporting requirements create practical questions around ownership, timing and evidence. Buyers need to know who is responsible for each notification, which deadline applies, and how information remains consistent across authorities.	For organizations operating across the region, different consent, localization and breach-notification requirements create a complex compliance picture. Buyers need practical ways to translate those requirements into consistent processes across markets.

Where brands are active — and where the gaps are.

Content coverage varies significantly across the category. Established topics such as threat research are well served, while newer buying questions around machine identities, regulatory evidence and recovery assurance receive less practical guidance.

TOPIC	SCORE	CURRENT BRAND ANGLE	BRAND OPPORTUNITY
Threat research & adversary reporting	8/10	A well-established content area, with substantial investment in threat research and strong use of data to explain attacker behavior and tactics.	Move from describing the threat to helping buyers act on it: what to change, who owns it and how to measure whether the response is working.
Machine and agent identity governance	6/10	Coverage is fast-moving and often centered on new product capabilities, with less focus on managing the machine identities organizations already have.	Address the practical questions around inventory, ownership, access and retiring orphaned identities safely.
Data discovery, classification & AI data flow	6/10	Capability-level content is widespread, but much of the comparison material remains vendor-led, making it harder for buyers to assess claims objectively.	Give buyers a clear way to evaluate classification and data-flow controls using their own environments and requirements.
Recovery assurance & provable resilience	5/10	Recovery is well established as a capability, but content tends to focus on features, certifications and awards rather than the process of proving recovery works.	Focus on the practical side of resilience: test design, recovery times, integrity checks and the evidence needed for boards, insurers and regulators.
Regulatory evidencing & reporting readiness	3/10	One of the less developed areas of vendor content. Much of the practical guidance currently comes from legal and compliance specialists rather than technology providers.	Help buyers connect requirements to the systems, controls and evidence they already have, and identify what is still missing.
Consolidation, migration & switching economics	3/10	Consolidation is a significant buying theme, but content tends to make the case for fewer platforms rather than address the practicalities and risks of migration.	Address what happens during the transition: dependencies, overlap, migration timelines and how to retire legacy systems without creating new exposure.

The gaps are most apparent where buyers need practical guidance rather than another capability claim. Questions around prioritization, recovery, regulatory evidence and managing machine identities all require buyers to understand what to do, what to prove and who needs to own it.

What convinces a buyer changes at every stage.

The questions buyers ask change as they move closer to a decision, so the content they need changes with them. Early-stage buyers need to understand the problem; later-stage buyers need evidence that a solution will work in their environment and stand up to scrutiny.

STAGE	BUYER QUESTION	WHAT THEY NEED	FORMATS THAT WORK
Problem Awareness EARLY STAGE	"Are we exposed in ways we cannot currently see, and how would we know?"	A clear way to identify and size the problem before entering a product conversation, particularly around machine identities, unknown access and data paths they have not mapped.	SELF-ASSESSMENT DIAGNOSTICS THREAT RESEARCH WITH CONTROL IMPLICATIONS PEER BENCHMARKS BY SECTOR AND SIZE
Solution Exploration MID STAGE	"What are our options, and what does each one govern?"	Clear scope, boundaries and trade-offs. Buyers need to understand what different approaches address, where they stop, how they compare and what remains their responsibility.	ARCHITECTURE DECISION GUIDES EVALUATION CHECKLISTS COST-OF-OWNERSHIP MODELS
Vendor Evaluation LATE STAGE	"Can you prove this works in our environment, and what evidence will it produce?"	Evidence that stands up to scrutiny, from realistic proof of performance to a clear view of what the solution produces for audit, reporting and compliance.	PROOF-OF-CONCEPT FRAMEWORKS IMPLEMENTATION TIMELINES SAMPLE EVIDENCE AND AUDIT OUTPUT
Post-Purchase RETENTION & EXPANSION	"Are we getting the value we bought, and what should we consolidate or retire next?"	A way to measure value and maturity over time, alongside a clear path for expanding, consolidating or retiring technology without creating new gaps.	MATURITY BENCHMARKS CONSOLIDATION PLAYBOOKS COMPLIANCE READINESS REVIEWS

What's next for category marketers?

Across the regions and pain points explored in this report, buyers are looking for proof earlier in the process and more practical guidance around the decisions they need to make. For marketers, that creates an opportunity to build campaigns around the questions buyers are already asking rather than starting with the product.

- 
- 1 GIVE CAMPAIGNS MORE THAN ONE ENTRY POINT**
A single format and channel will not suit every buyer or every stage of research. Combine diagnostics, frameworks and practical examples with targeting and distribution that can reach buyers at different points in the journey.
 - 2 ADAPT THE MESSAGE TO WHO'S INVOLVED**
Identity and platform leads bring different questions to the buying process than security leadership. Tailor both content and targeting to those roles rather than treating the security function as a single audience, using the channels and communities each group already relies on.
 - 3 PUT PROOF AHEAD OF CAPABILITY**
Buyers increasingly want to know what a solution can demonstrate, not simply what it claims to do. Use late-stage objections and sales conversations to identify the evidence buyers need, then build that proof into web content, collateral and campaigns.
 - 4 CREATE RESEARCH BUYERS CAN USE INDEPENDENTLY**
Comparison content is largely vendor-authored, limiting its value when buyers are trying to make an objective assessment. Original research, benchmarks and evaluation frameworks can give buyers evidence they can apply to their own environment without relying on a vendor's preferred narrative.
 - 5 BUILD AROUND CONSOLIDATION MOMENTS**
Renewals and platform consolidation create natural points for buyers to reassess their technology estate. Campaigns aimed at these accounts can address the practical realities of switching – costs, dependencies, overlap and migration risk – rather than focusing only on the benefits of consolidation.

Sources:

IBM

Cost of a Data Breach Report 2026
2026

VERIZON

2026 Data Breach Investigations Report
2026

KPMG INTERNATIONAL

Cybersecurity Considerations 2026
2026

WORLD ECONOMIC FORUM

Global Cybersecurity Outlook 2026
2026

EUROPEAN COMMISSION

Cyber Resilience Act
2026

IAPP

New year, new rules: US state privacy requirements coming online as 2026 begins
2026

ENISA

ENISA Threat Landscape 2025
2025

OAIC

Data breach notifications increase to all-time high in 2025, new NDB stats show
2026

FISHER PHILLIPS

India's New Data Privacy Rules Are Here: 8 Steps for Businesses as Key Compliance Deadlines Approach
2026

CLOUD SECURITY ALLIANCE

Non-Human Identity and Agentic AI Governance
2026

ISC2

2025 ISC2 Cybersecurity Workforce Study
2025

IBM INSTITUTE FOR BUSINESS VALUE

Capturing the cybersecurity dividend: How security platforms generate business value
2025

BOMBORA

Company Surge intent data
2026

Better B2B marketing starts with better insight.

The Insight Collective is a specialist lead generation partner for B2B technology companies – applying marketing science to help you find, reach, and convert the right opportunities.



Next-Gen MQL

Identify accounts based on commercial fit, using your own customer data alongside market signals to focus on the opportunities most likely to convert.

2026 B2B Marketing Effectiveness Benchmark

Explore how 300 marketers globally are approaching confidence, measurement and the gap between strategy and proof.

Custom Category Reports

Commission a report built around your specific market, competitor set or priority buyer segment.



The Insight
COLLECTIVE

LEAD GENERATION
FOR B2B TECHNOLOGY
BRANDS

www.theinsightcollective.com