SpyCloud

SPYCLOUD.COM

Know the terrain

THE 2026 SPYCLOUD

IDENTITY THREAT REPORT

▶ BENCHMARKS, BLIND SPOTS, AND STRATEGIES FOR **DETECTING, REMEDIATING, AND REDUCING** IDENTITY THREATS ACROSS HUMAN AND NON-HUMAN IDENTITIES

CONTENTS

INTRODUCTION

MAPPING THE NEW IDENTITY TERRAIN

Identity exposure is measurable, operational, and fixable. Yet most organizations still struggle to manage it consistently.

Many security teams are navigating with an outdated map – one built for well-marked trails, not the sprawling backcountry attackers now operate in. The gap between what organizations can see and what attackers can reach is the terrain this report sets out to chart.

Today's identity attack surface extends far beyond traditional boundaries. It now stretches past employee credentials to session cookies and refresh tokens, non-human identities (NHIs) tied to AI agents and APIs, and third-party partners and ecosystems. As that terrain expands, attack prevention increasingly depends less on how well an organization knows its own camp and more on how it can identify exposed identity assets outside its perimeter – and remediate them before attackers take advantage.

Report findings are based on a survey of 750 cybersecurity leaders and practitioners across North America, the United Kingdom, and select European markets. This report benchmarks how organizations with 500 employees or more detect, remediate, and govern identity threats, where critical blind spots remain, and what distinguishes the most mature identity security programs.

THE LANDSCAPE ATTACKERS ARE EXPLORING TODAY

SpyCloud continuously recaptures identity assets circulating in the criminal underground, extending well beyond what most organizations can see in their existing tooling.

1+ TRILLION
recaptured identity assets

65.7 BILLION
distinct identity records

17+ BILLION
session cookies

63+ MILLION
recaptured API keys and tokens

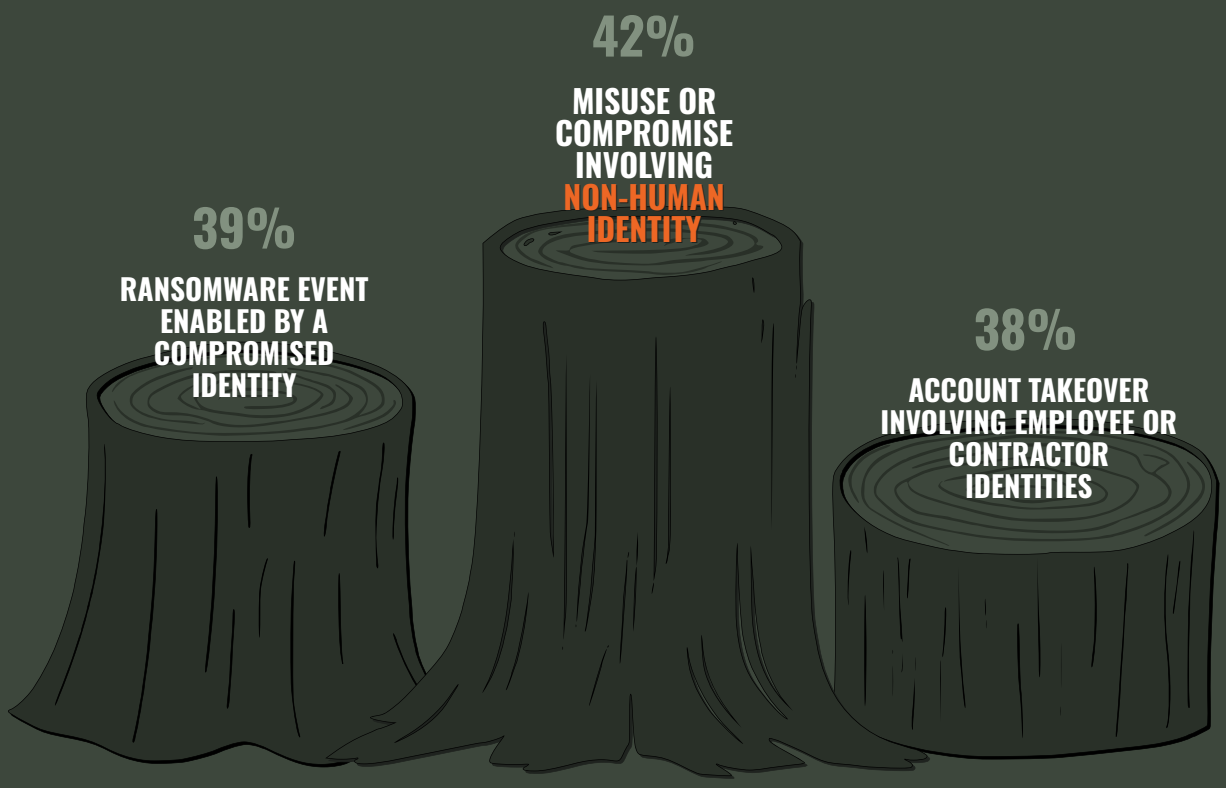
KEY TAKEAWAYS

01 IDENTITY-BASED EVENTS ARE NOW A ROUTINE REALITY

More than two-thirds (**68%**) of organizations experienced an identity-based event in the past year, with affected organizations **averaging eight events**, confirming that identity compromise has become an operational reality rather than an isolated incident.

02 NHIs ARE NOW THE LEADING ROUTE FOR INTIAL ACCESS

NHI-related misuse was the top reported identity-based event type (42%), followed by a ransomware event enabled by a compromise identity (**39%**) and account takeover involving employee or contractor identities (**38%**).



03 VISIBILITY GAPS LEAVE CRITICAL MARKERS UNSEEN

Organizations that experienced identity events were significantly less likely to have visibility into stolen session cookies (**37% vs. 50%**) and personal devices (**40% vs. 52%**), suggesting that blind spots continue to fuel successful attacks.

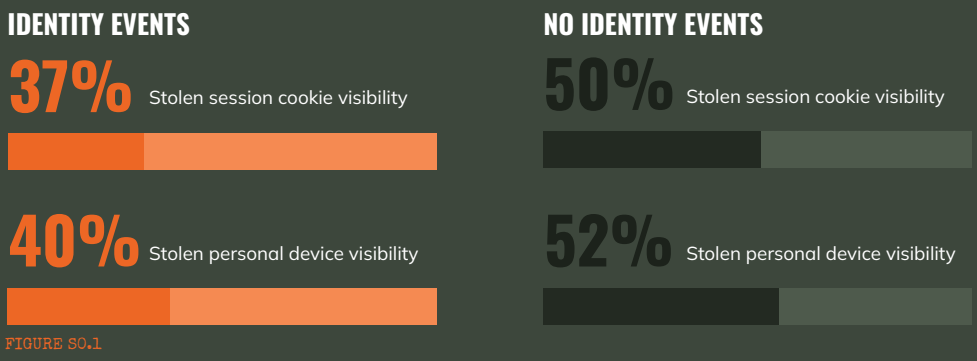
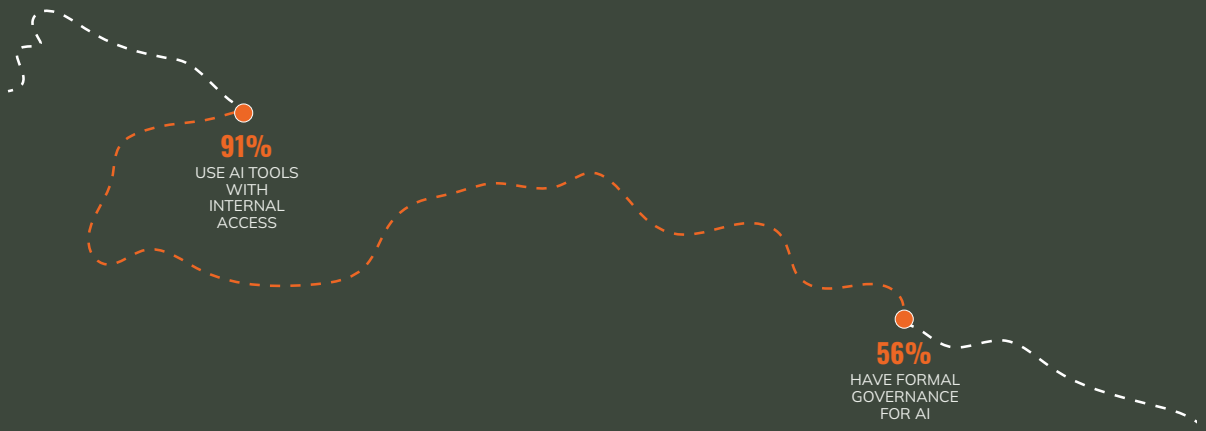


FIGURE SO.1

04 THE GOVERNANCE MAP HAS NOT KEPT PACE

Ninety-one percent (**91%**) of organizations use AI tools or agents with internal access, but only **56%** have formal governance and ownership for AI- and NHI-related privileges.



05 CONFIDENCE CAN HIDE THE BIGGEST BLIND SPOTS

C-suite leaders were far more confident in their NHI visibility than frontline operators (**66% vs. 50%**). While the U.S. and Canada largely tracked the global baseline, the **UK** reported the highest confidence (**53%**) despite experiencing the highest identity event rate (**77%**), demonstrating that confidence does not necessarily reflect coverage.

06 INDUSTRY DIFFERENCES REVEAL DIFFERENT FREQUENCY AND IMPACT OF IDENTITY EVENTS

The **Government** sector reported experiencing a much higher frequency of identity events (**92.3% vs. 68%** total), and government orgs reported the highest average event volume (**10 events vs. 8** total average). **Manufacturing** organizations, on the other hand, were significantly less likely to have experienced an identity-based event (**58% vs. 68%** total), but when they did, the fallout was worse, reporting customer or partner trust loss as a business impact (**56.9% vs. 40.2%** total) and higher average impacts across the board – a classic "fewer, but costlier" pattern.

07 THE TRAIL EXTENDS BEYOND ORGANIZATIONAL BOUNDARIES

Third-party malware infections **(23%)** and API key/application exposures **(22%)** were cited as the leading causes of supply chain identity events across respondents. Vendor remediation validation is uneven, even across technology-heavy sectors. **Telecommunications** leads with the highest active validation rate at **68%**, while **Technology / Software** organizations report the lowest rate at **38%**, revealing meaningful differences in third-party identity governance.

08 THE BEST ORGANIZATIONS PROVE WHAT'S POSSIBLE

Germany emerged as a benchmark for third-party identity governance, with **76%** of organizations actively confirming vendor remediation, demonstrating that stronger operational practices can substantially improve supply chain visibility.

09 SCALE INFLUENCES CONFIDENCE, BUT NOT CERTAINTY

Large enterprises (5,000+ employees) reported significantly higher confidence in their identity visibility than mid-market organizations, but confidence alone did not consistently translate into better outcomes.

10 MANUAL REMEDIATION CREATES COSTLY DETOURS

Organizations relying on manual remediation reported higher incident response costs (**39%**) and customer trust loss (**47%**) compared to their peers who report using high levels of automation (**32% and 36%**, respectively).

Know the terrain

SECTION 01

TRAILING AHEAD TO OPERATIONAL MATURITY

The data in this year's report suggests that operational maturity is more closely associated with resilience than company size, industry, or geography. **Organizations with more mature identity threat protection programs report lower identity-based event rates and stronger visibility, monitoring, remediation, governance, and automation practices.**

IN THIS SECTION

01.1

THE IDENTITY THREAT PROTECTION MATURITY TRAIL

To benchmark organizational readiness, respondents were grouped into four maturity tiers based on their identity exposure across visibility, monitoring, governance, automation, and remediation capabilities.

TIER	STATUS	SHARE OF RESPONDENTS
01	**REACTIVE** Limited visibility, manual processes, and inconsistent remediation	9%
02	**BUILDING** Building foundational processes but still challenged by visibility and operational consistency	37%
03	**OPERATIONAL** Repeatable workflows, measurable outcomes, and increasing use of automation	45%
04	**OPTIMIZED** Continuous monitoring, strong governance, and automated remediation across key identity workflows	9%

FIGURE S1.1

01.2

IDENTITY-BASED EVENT RATES BY MATURITY TIER

Building organizations experience the highest incident rate, likely reflecting greater visibility into identity exposures before mature processes and automation begin reducing risk. From there, the data shows a clear maturity effect: **identity-based event rates decline substantially as organizations move from Building to Operational and ultimately Optimized.**

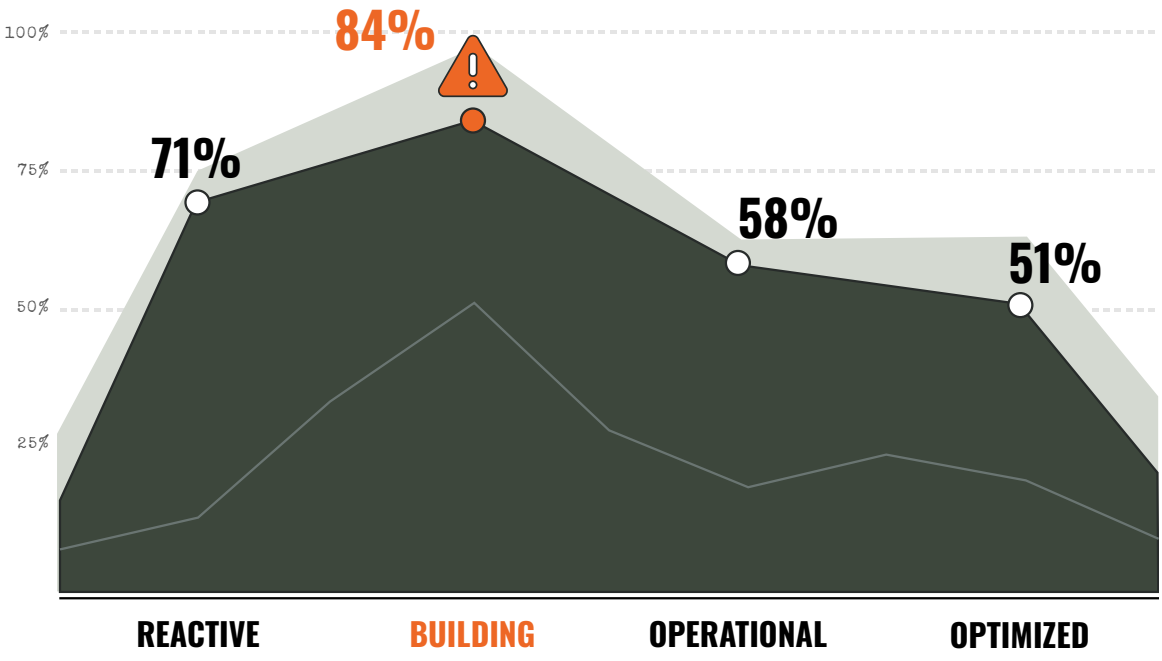


FIGURE S1.2 ▶ Organizations reduce identity risk as they progress along the maturity trail

WHAT SETS IDENTITY RESILIENCE LEADERS APART

Optimized organizations consistently outperform their peers by combining stronger visibility, continuous monitoring, automated remediation, and effective governance. Together, these capabilities help reduce identity exposure and lower the likelihood of identity-based incidents.

▸ TRAIL MARKER

MATURITY VARIES BY SECTOR

Industry alignment seemingly influences identity security maturity. **Telecommunications (18.4%)** – which has been on the receiving end of a growing number of targeted attacks in recent years – and **Retail & Ecommerce (13.4%)** have the highest concentration of organizations operating at the Optimized maturity level, while **Insurance** reports the highest share of Reactive programs **(17.7%)**, underscoring that some industries remain earlier in their operational journey.

RETAIL / ECOMM · OPTIMIZED
13.4%

TELECOM · OPTIMIZED
18.4%

INSURANCE · REACTIVE
17.7%

Know the terrain

SECTION 02

BLIND SPOTS BECOME INITIAL ACCESS VECTORS

Identity-based events are a recurring operational reality, not isolated incidents. **Sixty-eight percent (68%)** of organizations experienced an identity-based event in the past 12 months, and affected organizations averaged **8 identity-based events** annually, with nearly half **(49%)** experiencing **6-10 events**.

IN THIS SECTION

02.2

Despite the frequency of these events, organizations remain highly confident in their ability to identify identity exposures. Nearly half **(46%)** describe themselves as very confident in their visibility. Moreover, confidence increases with organizational seniority. **Two-thirds (66%)** of C-suite leaders believe they have adequate visibility into non-human identities NHIs, compared with **50%** of frontline security operators.

The disconnect becomes even more apparent when organizations look at the identity events they are actually experiencing. Rather than traditional employee account compromise, machine identities and other non-human identities now account for the most common identity-based events reported by security teams.

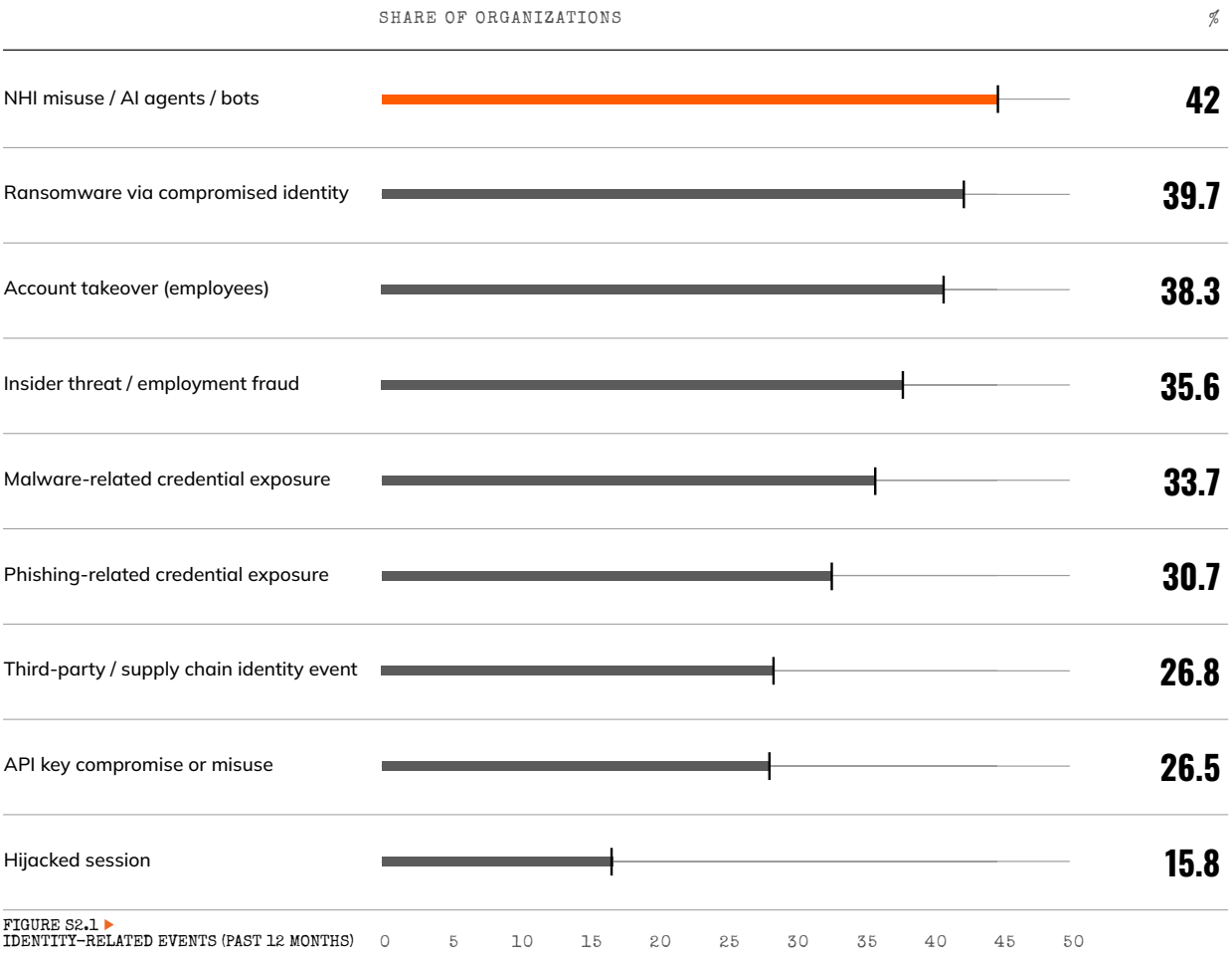


FIGURE S2.1 ▶
IDENTITY-RELATED EVENTS (PAST 12 MONTHS)

02.2

CONFIDENCE VS. IDENTITY-BASED EVENT RATE BY MARKET

Very confident in visibility (% of respondents) vs. experienced an identity-based event (past 12 months).

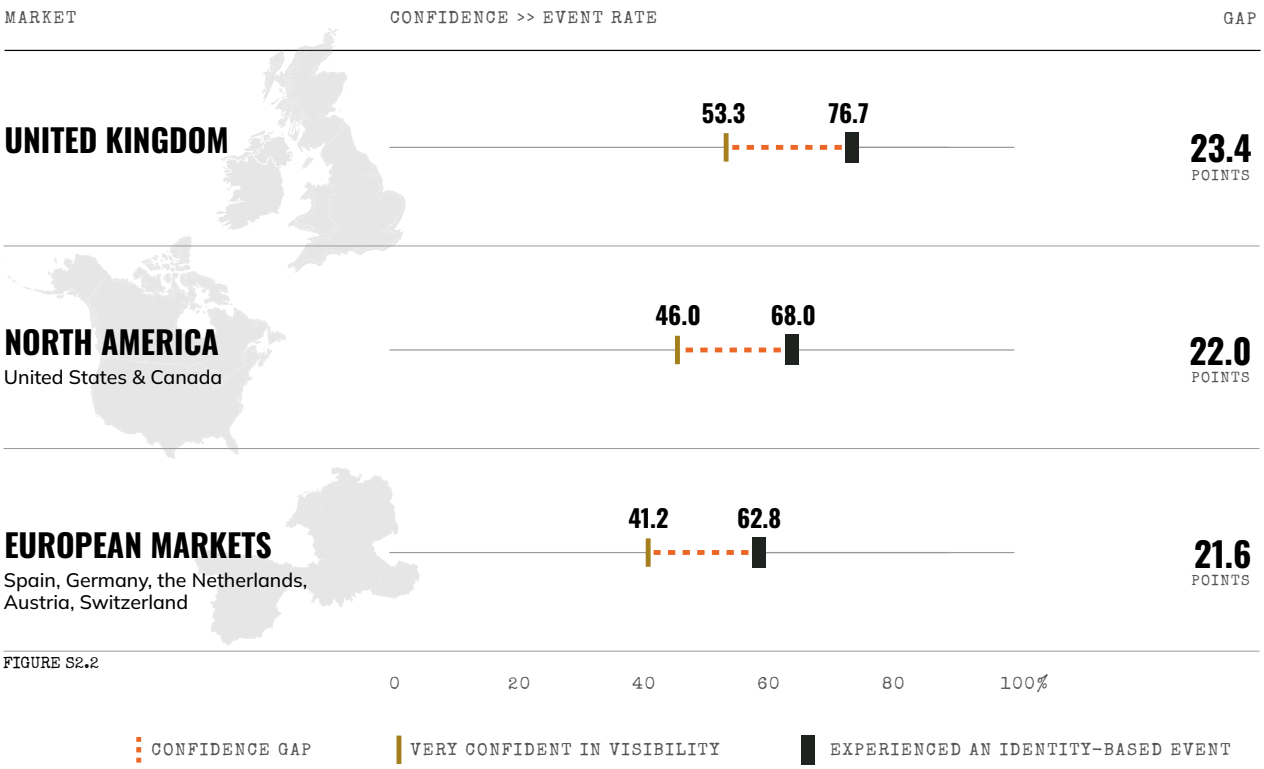


FIGURE S2.2

23.4
UK CONFIDENCE VS EVENT RATE GAP

HIGH CONFIDENCE DOESN'T ALWAYS MEAN LOWER RISK

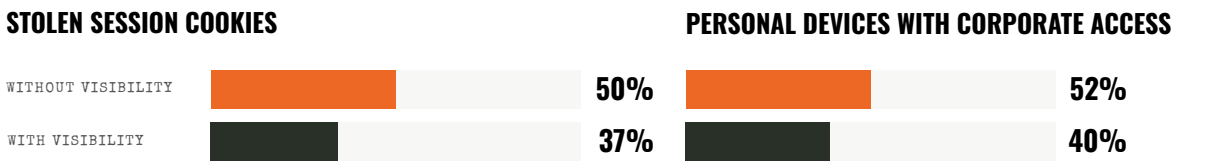
Across the regional segments shown, organizations report relatively high confidence in their visibility, yet identity-based events remain common. **The disconnect is most pronounced in the United Kingdom**, which reports both the **highest visibility confidence (53.3%)** and the **highest identity-based event rate (76.7%)**, reinforcing a central finding of this report: *confidence does not equal coverage*.

02.3

ATTACKERS EXPLOIT WHAT ORGANIZATIONS CAN'T SEE

Organizations that avoided identity-based events consistently monitored more exposure types than those that experienced incidents. Visibility into two areas stood out most in affecting whether an organization **experienced identity-based events:**

FIGURE S2.3

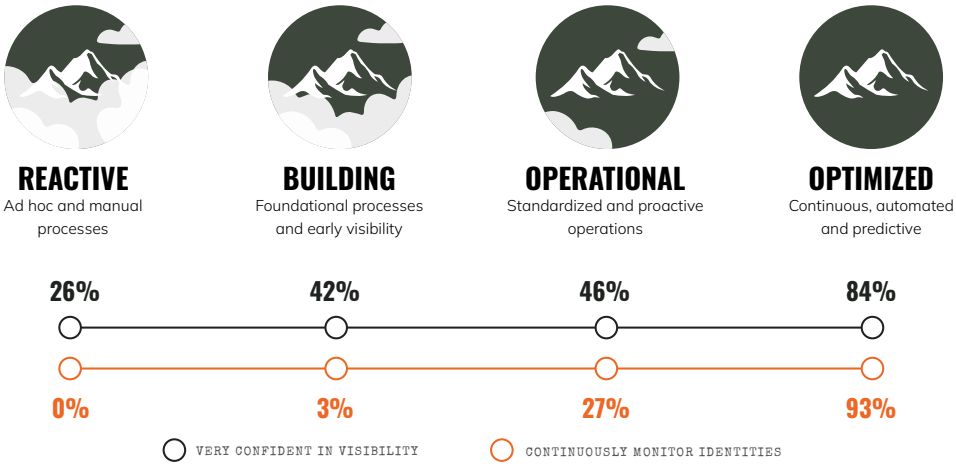


The findings reinforce a central theme of this report: attackers exploit what organizations cannot see.

WHAT SETS IDENTITY RESILIENCE LEADERS APART

Visibility and continuous monitoring improve dramatically as organizations progress along the Identity Threat Protection Maturity Trail. By the time organizations reach the **Optimized** tier, confidence in visibility and proactive monitoring become defining operational strengths.

FIGURE S2.4



The most mature organizations combine broad visibility with continuous monitoring, enabling them to identify and remediate identity exposure before it becomes an incident.

▸ TRAIL MARKER

PHISHING AND MALWARE REMAIN PERSISTENT ACCESS PATHS

Phishing and malware continue to create boundless opportunities for bad actors, providing them with stolen credentials, session cookies, refresh tokens, and more to carry out account takeover, session hijacking, ransomware, and other attacks.

THE STATE OF PHISHING & MALWARE FOR ENTERPRISES

PHISHING & SOCIAL ENGINEERING AS A COMMON ACCESS PATH
37%

INCOMPLETE VISIBILITY ON PHISHING EVENTS
40%

MALWARE EXPOSURE VISIBILITY ON MANAGED DEVICES *ONLY*
53%

Know the terrain

SECTION 03

THE ATTACK MAP EXTENDS BEYOND THE PERIMETER

AI tools, agents, applications, vendors, and partners are creating new identity paths into the business. As these connections expand, identity risk increasingly comes from privileged access that sits outside traditional governance and visibility.

IN THIS SECTION

03.1

AI ADOPTION HAS OUTPACED GOVERNANCE

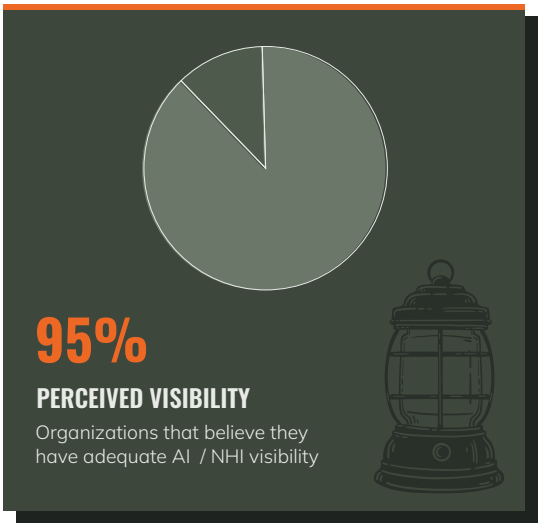
Nearly every organization (**91%**) now uses AI tools or agents with access to internal systems, applications, or data. Yet only **56%** have formal policy and clear ownership for managing AI- and NHI-related privileges. Another **41%** rely on informal processes or partial ownership.

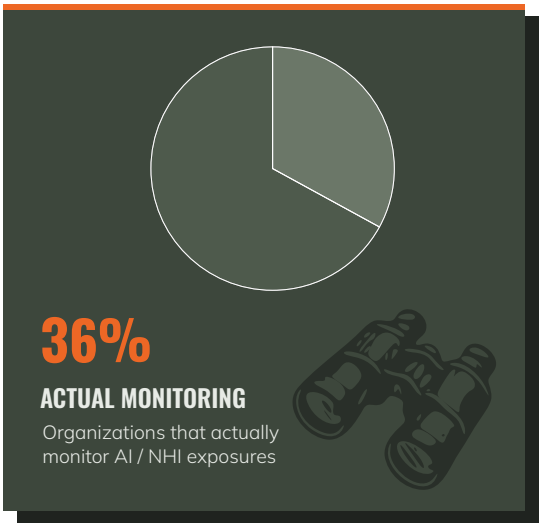
03.2

THE AI TRAIL IS HARDER TO TRACK THAN ORGANIZATIONS THINK

Organizations overwhelmingly believe they have visibility into AI-related identity exposure. Nearly all organizations (**95%**) agree they have adequate visibility into NHI exposures associated with AI tools, agents, service accounts, applications, or bots.

FIGURE S3.1





CONFIDENCE DOES NOT EQUAL COVERAGE

AI- and NHI-related exposures are the least-monitored category of risk in this study.

03.3

SURVEY SAYS:

NHIs ARE NOW THE LEADING ROUTE FOR INITIAL ACCESS

The visibility gap has real consequences. NHI-related misuse was the most commonly reported identity-based event **(42%)**. Meanwhile, **50%** of affected organizations cited exposed, compromised, or overprivileged NHIs, including API keys, tokens, and service accounts, as common access paths, and **31%** identified them as the single most common initial access vector.

The challenge is especially acute in the selected **European markets** surveyed, where **34%** of affected organizations identified exposed, compromised, or overprivileged NHIs as their most common initial access vector.

Perceived risk does not always track with actual events. While only **28%** of organizations overall consider misconfigured or overprivileged NHIs to be a high-risk threat, **Government** organizations are substantially more likely to do so at **41%**, suggesting heightened awareness of this emerging identity threat.

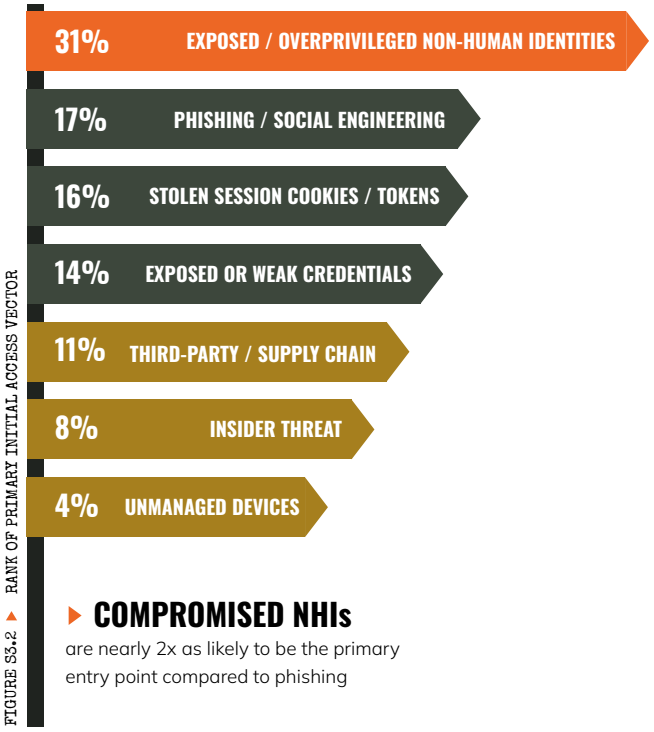


FIGURE 53.2

EUROPEAN MARKETS

34% of affected organizations identified NHIs as their most common initial access vector

Know the terrain

SECTION 04

EXPANDING IDENTITY ACCESS PATHS

Governance helps bring the trail into view.

Formal governance doesn't just assign ownership. It improves visibility across the broader identity ecosystem. For example, **49%** of organizations with formal AI governance have visibility into personal devices with corporate access, compared with 36% of organizations relying on informal governance.

IN THIS SECTION

▸ TRAIL MARKER

SHADOW ACCESS, NOT JUST SHADOW IT

As AI tools, agents, service accounts, and applications gain access to business systems, identity risk increasingly stems from shadow access: privileged connections that exist outside traditional governance and visibility.

Overprivileged NHIs are often less a technology problem than an operational one, reflecting unclear ownership, inconsistent governance, and identity hygiene gaps.

WHAT SETS IDENTITY RESILIENCE LEADERS APART

Leaders at **Optimized** organizations don't stop at identifying third-party identity exposures. They consistently verify that threats have been remediated, reducing the risk of unresolved exposures across their vendor ecosystem.

The maturity gap is substantial:

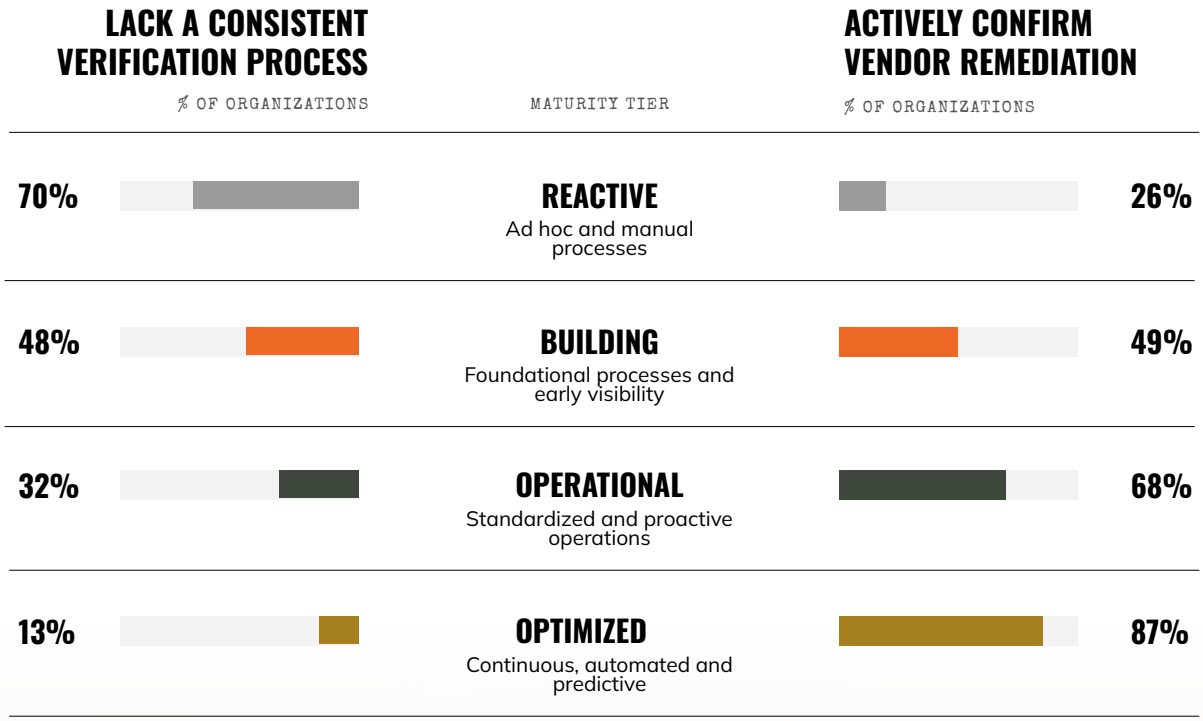


FIGURE S4.1

TRAIL MARKER

INDUSTRY BENCHMARKS CHALLENGE ASSUMPTIONS

Vendor remediation validation varies meaningfully by industry.

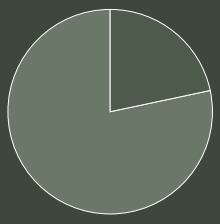
HIGHEST ACTIVE VALIDATION RATES	
TELECOMMUNICATIONS	68%
ENERGY, EXTRACTION & UTILITIES	63%
RETAIL & ECOMMERCE	62%

LOWEST ACTIVE VALIDATION RATES	
FEDERAL GOVERNMENT	52%
TRAVEL & HOSPITALITY	44%
TECHNOLOGY / SOFTWARE	38%

TRAIL MARKER

THE MALWARE-TO-SUPPLY-CHAIN PIPELINE

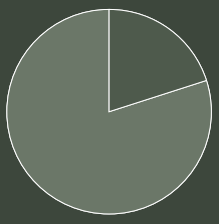
Many supply chain identity incidents begin with common exposure hygiene failures rather than sophisticated attacks.



23%

MALWARE-INFECTED THIRD PARTY DEVICES

as the leading cause of supply chain identity incidents



22%

EXPOSED API KEYS OR APP ACCESS

involving vendors or partners

Know the terrain

SECTION 05

THE COST OF A SLOWER PACE

Identity exposure creates an ongoing operational burden that extends far beyond the initial incident. **Nearly half (49%) of affected organizations experienced 6 to 10 identity-based events in the past year**, while another **13%** battled **11 to 25** events, making investigation, remediation, and validation a recurring demand on security teams.

How organizations respond to those exposures has a direct impact on business outcomes.

IN THIS SECTION

05.1

MANY ORGANIZATIONS ARE STILL TAKING THE LONG WAY AROUND

Organizations relying on manual or case-by-case remediation consistently report greater business impact than those with more automated workflows.

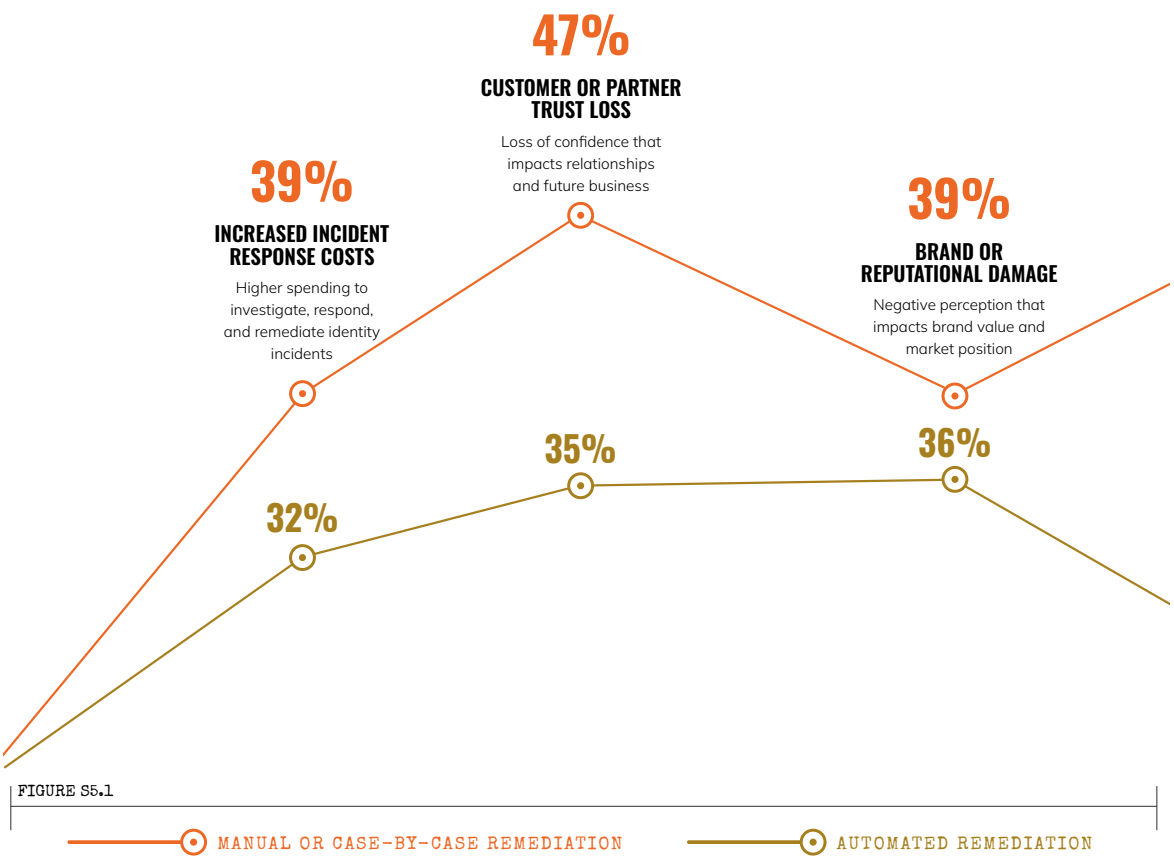


FIGURE S5.1

05.2

EVERY DETOUR ADDS PAIN

Despite the clear benefits of automation, most organizations remain in a transitional phase. While relatively few still rely entirely on manual processes, only about **one in five** have reached fully optimized remediation and investigation capabilities.

05.3

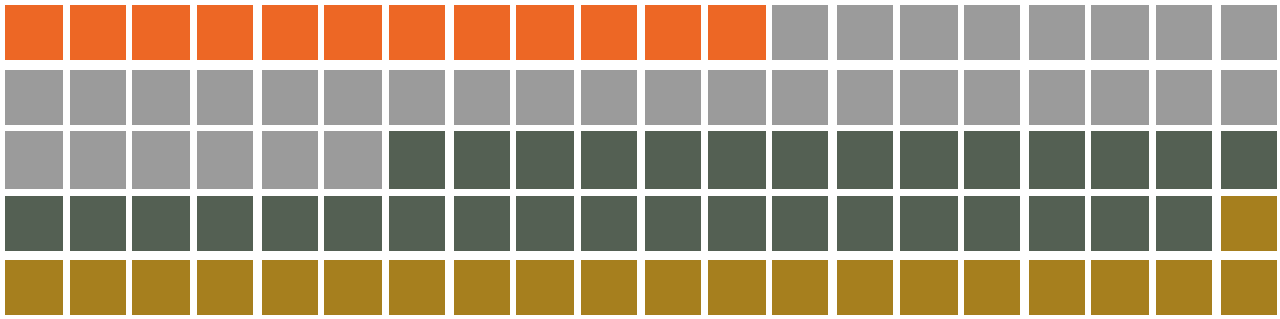
IDENTITY EXPOSURE REMEDIATION MATURITY

Organizations relying on manual or case-by-case remediation consistently report greater business impact than those with more automated workflows.

HOW ORGANIZATIONS REMEDIATE TODAY

ONE SQUARE = ONE ORGANIZATION OUT OF 100

FIGURE S5.2



67 OUT OF EVERY 100 COMPANIES ARE IN TRANSITION

LESS MATURE — MORE MATURE

12%	34%	33%	21%
REACTIVE	**BUILDING**	**OPERATIONAL**	**OPTIMIZED**
Respond case-by-case with no consistent process	Developing repeatable remediation workflows	Regularly remediate based on prioritized tasks	Automate and optimize remediation across systems

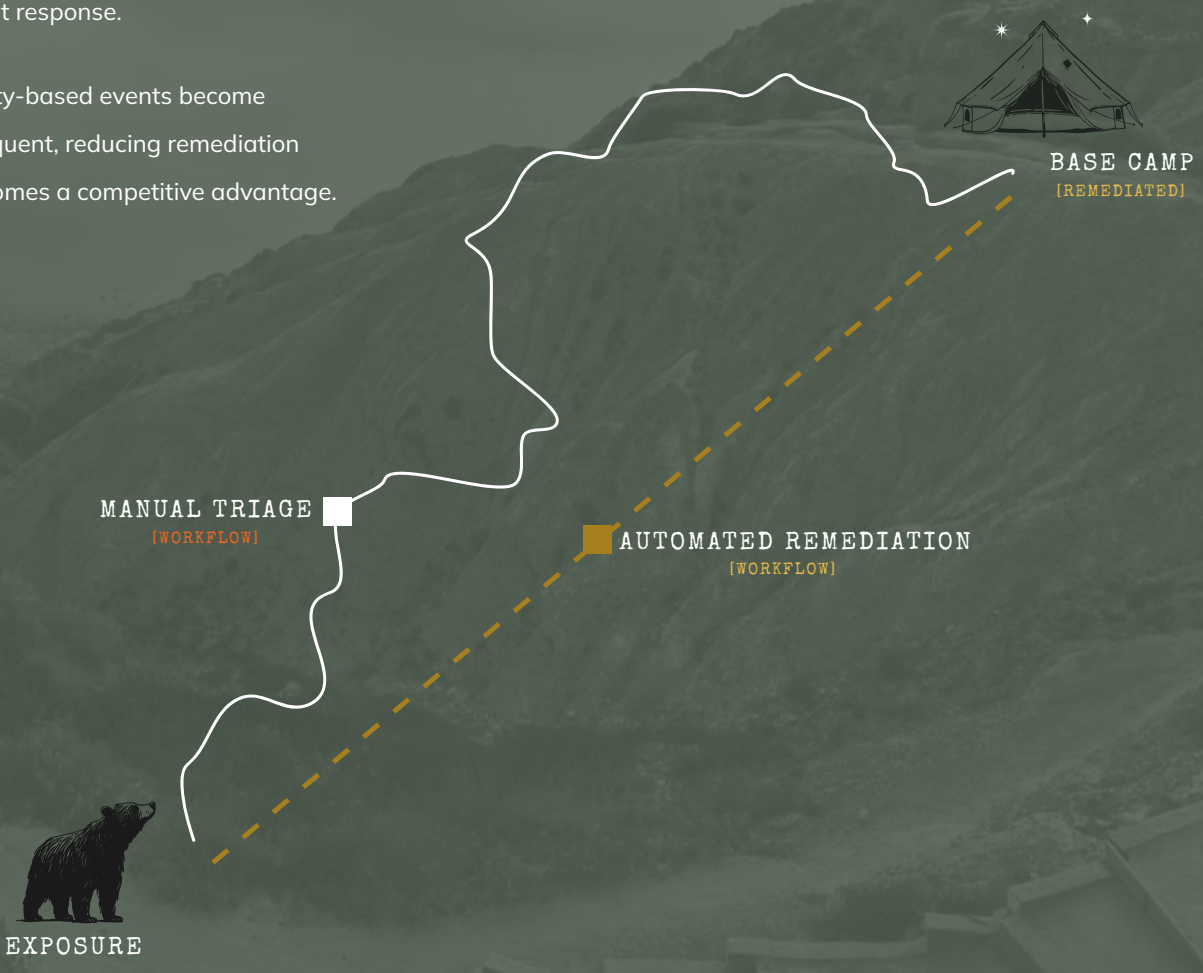
▸ TRAIL MARKER

THE REMEDIATION WINDOW COMPOUNDS RISK

Every hour between exposure and remediation is time attackers can use what they already have – especially for critical exposures like session cookies and tokens stolen by malware or in phishing attacks. Organizations with automated remediation workflows cut that window significantly and see lower incident response costs and customer trust loss as a result.

Automation doesn't simply improve efficiency. It reduces the time identity exposures remain available for attackers to exploit. Organizations with more automated remediation experience lower operational costs, fewer business impacts, and more consistent response.

As identity-based events become more frequent, reducing remediation time becomes a competitive advantage.



WHAT SETS IDENTITY RESILIENCE LEADERS APART

Automation is one of the clearest operational differences across the Identity Threat Protection Maturity Trail. As organizations mature, they move from manual, reactive workflows to fully automated and orchestrated remediation.

ORGANIZATIONS WITH FULLY AUTOMATED & ORCHESTRATED REMEDIATION WORKFLOWS BY TIER:

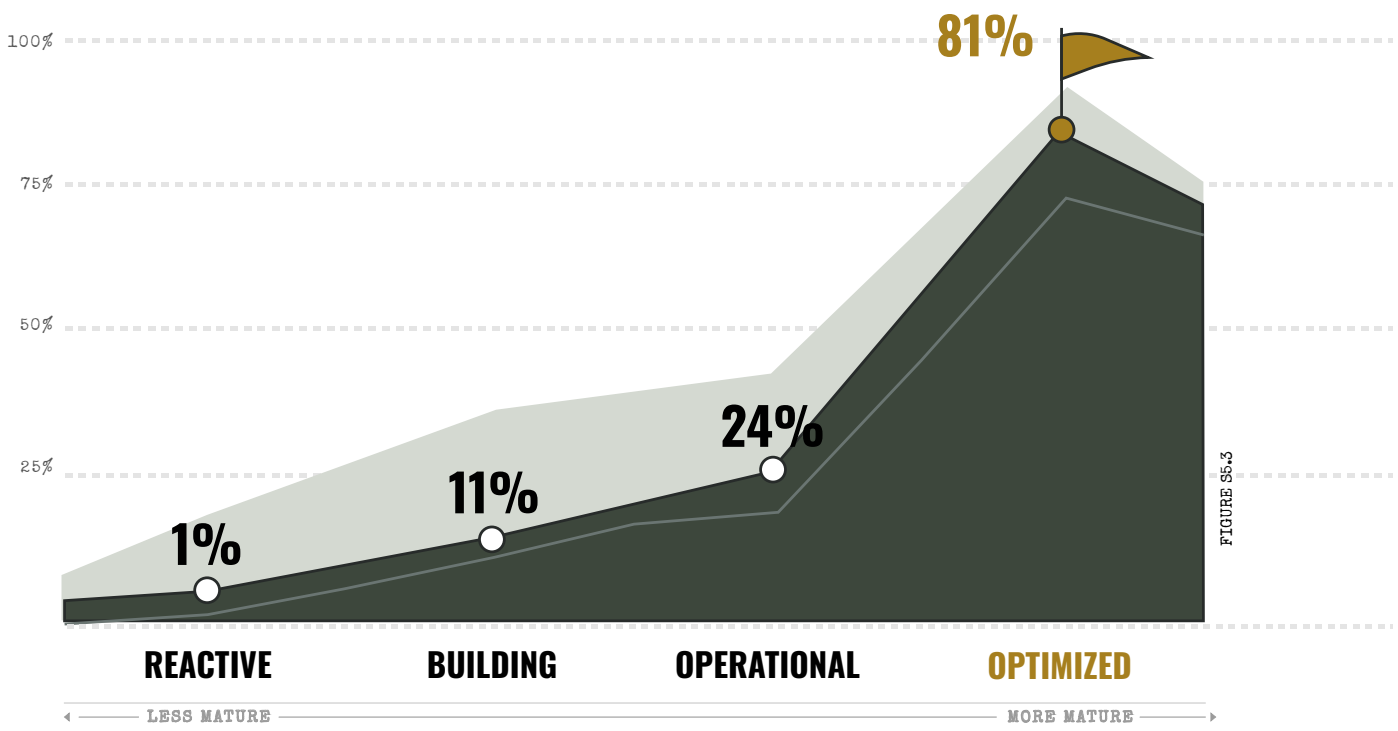


FIGURE 35.3

Fully automated remediation remains rare until organizations reach the Optimized tier. The sharp increase from **24%** of Operational organizations to **81%** of Optimized organizations highlights automation as one of the defining capabilities that separates trail leaders from the rest of the market.

Know the terrain

SECTION 06

CHARTING THE PATH FORWARD

Identity exposure can't be addressed through a single technology, process, or policy. The strongest programs build operational maturity over time, strengthening visibility, accelerating remediation, and validating outcomes across an expanding identity ecosystem.

IN THIS SECTION

06.1

The survey findings suggest organizations understand this challenge. The **top planned investments over the next 12–18 months** reflect a balanced approach rather than a search for a single solution.

- **35%** plan to automate identity-related incident response workflows.
- **32%** plan to enhance supply chain and vendor risk management.
- **31%** plan to reduce identity exposure across employees.

Together, these priorities point to a practical roadmap for reducing identity exposure. The organizations making the greatest progress focus on three operational priorities.

1. GET THE FULL PICTURE:
EXPAND VISIBILITY BEYOND THE PERIMETER

Leading organizations continuously monitor identity exposure across employees, vendors, any and all devices accessing work applications, session cookies and tokens, AI tools, and NHIs.

As the identity ecosystem expands, visibility must extend beyond traditional user accounts. Organizations that broaden visibility across these exposure types are better positioned to identify emerging risks before they become identity-based incidents.

2. SHORTEN THE TRAIL:
AUTOMATE RESPONSE & REMEDIATION

Visibility without action creates more alerts, not better outcomes. Trail leaders reduce exposure faster through automated investigation, remediation, and validation workflows, reducing the time attackers have to exploit exposed identities.

Key capabilities include:


CREDENTIAL ROTATION


SESSION & TOKEN REVOCATION


PRIVILEGE REDUCTION


AUTOMATED RESPONSE ORCHESTRATION

3. CLOSE THE LOOP:
VERIFY VENDOR REMEDIATION

Mature programs do not simply identify third-party exposure. They confirm it has been remediated.

Nearly **40%** of organizations lack a consistent process to verify vendor remediation, leaving them vulnerable to unresolved identity exposures across third-party ecosystems.

Verifying remediation closes the loop between detection and response, helping make sure identity risks are actually eliminated rather than simply identified.

WHAT IDENTITY RESILIENCE LEADERS DO CONSISTENTLY

Organizations reaching the Optimized tier consistently:

- **Maintain** broad visibility across human and non-human identities
- **Continuously monitor** identity exposure
- **Automate** investigation and remediation
- **Govern** AI and NHI access through formal ownership
- **Verify** remediation across third-party ecosystems

Together, these capabilities distinguish organizations that simply respond to identity exposure from those that manage it as a measurable, repeatable operational discipline.

Know the terrain

SECTION 07

THE JOURNEY AHEAD

The organizations performing best are not necessarily eliminating identity exposure. They are identifying exposures sooner, responding more consistently, and reducing the operational and business impact when incidents occur.

The difference is operational maturity. Organizations that **continuously improve visibility, remediation, governance, and validation** are better equipped to stay ahead of an expanding identity attack surface.

IN THIS SECTION

TRAIL MARKER

BENCHMARK YOUR POSITION ON THE TRAIL

Where are you on the Identity Threat Protection Maturity Trail? Assess your organization's capabilities across five key dimensions.

CAPABILITY	REACTIVE	BUILDING	OPERATIONAL	OPTIMIZED
VISIBILITY	☐	☐	☐	☐
MONITORING	☐	☐	☐	☐
GOVERNANCE	☐	☐	☐	☐
AUTOMATION	☐	☐	☐	☐
VENDOR REMEDIATION VERIFICATION	☐	☐	☐	☐

LESS MATURE — MORE MATURE

BENCHMARK YOUR MATURITY ▶
TAKE THE ASSESSMENT

08.1

METHODOLOGY

This report is based on a survey of **750 cybersecurity decision-makers and practitioners** conducted in **June 2026**. Results are reported at a **95% confidence level** with a **±3.58% margin of error**.

01 RESPONDENTS

Security architect or engineer: **23%** · Identity and access management (IAM) director, manager, or specialist: **22%** · Security director, manager, or team lead: **20%** · CIO, CISO, or IT security executive: **19%** · Security operator, analyst, or incident responder: **11%** · Security administrator: **3%** · Other role in IT security: **2%**

02 COMPANY SIZE

500–999 employees: **20%** · 1,000–4,999 employees: **42%** · 5,000–9,999 employees: **29%** · · 10,000–25,000 employees: **8%** · More than 25,000 employees: **1%**

03 GEOGRAPHY

United States: **27%** · Canada: **20%** · United Kingdom: **20%** · Select European markets (Spain, Germany, The Netherlands, Austria, Switzerland: **33%**

03 INDUSTRIES

Manufacturing: **13%** · Healthcare: **12%** · Energy, Extraction and Utilities: **11%** · Insurance: **11%** Retail & Ecommerce: **11%** · Financial Services / Banking: **10%** · Professional Services: **8%** · Technology / Software: **8%** · Telecommunications: **5%** · Education: **4%** · Government – Federal: **3%** · Government – State/Local: **2%** · Travel & Hospitality: **2%**

ABOUT SPYCLOUD

SpyCloud transforms recaptured identity data from the criminal underground into actionable intelligence that helps organizations prevent, detect, and respond to identity-based threats. Its automated identity threat protection solutions help stop ransomware and account takeover, detect insider threats, protect employee and consumer identities, and accelerate cybercrime investigations.

To learn more about SpyCloud's holistic approach to identity threat protection and see your organization's exposed identity data, visit **spycloud.com »**