ENZOIC

2026

Credential Risk Report

From Password Hygiene to Continuous Credential Defense

Research by

Cybersecurity INSIDERS

Executive Overview

Compromised credentials turn authentication into an attack path. When an attacker signs in with a real username and password, the first move can look like ordinary access rather than a breach in progress. That gives attackers room to take over accounts, enter cloud and SaaS applications, escalate privileges, move laterally, and reach sensitive data before the organization confirms the login was malicious. Third-party breaches, infostealer malware, password reuse, and session theft keep a live supply of exposed credentials in circulation.

Based on a survey of 872 cybersecurity professionals, this report examines the operational gap at the center of credential security. Most organizations recognize compromised credentials as a primary attack vector. Far fewer can identify exposed active credentials and remediate them before attackers turn exposure into compromise.

Key findings:

- **Recognition of risk has outrun operational capability:**
  85% consider compromised credentials a primary attack path into the enterprise, yet only 19% continuously monitor active credentials and automatically remediate exposure. That is a 66-percentage-point gap between recognizing credential exposure as a material risk and operating a model that can contain it.
- **Exposed credentials are already inside:**
  73% have found their own workforce credentials in third-party breach data, dark-web sources, or infostealer logs in the past year, while 82% are concerned that previously compromised credentials may already be present in their environment.
- **Infostealer exposure remains under-monitored:**
  39% have found employee credentials in infostealer logs, yet 43% do not monitor that channel or are unsure whether they do.
- **MFA reduces misuse, but exposure remains:**
  66% remain concerned about MFA bypass, and 62% say their deployment still allows a password fallback. Only 13% believe MFA adequately addresses credential risk.
- **Investment is rising faster than ownership:**
  41% plan to add compromised-credential screening or monitoring, but only 29% treat automated credential abuse as a defined strategic priority.

Most credential-defense programs still operate as a collection of separate controls: breach monitoring in one place, password screening in another, identity detection and response in another workflow, and manual resets after exposure is found.

More mature organizations are treating these capabilities as one discipline: Continuous Credential Defense. They monitor active credentials, identify exposed ones while they are still usable, and automate remediation through the systems that grant access. In those programs, exposure is caught and closed before it becomes a compromise, containment no longer waits on a manual reset, and a valid login stops being a quiet way in.

Exposed Credentials Are Already Inside the Enterprise

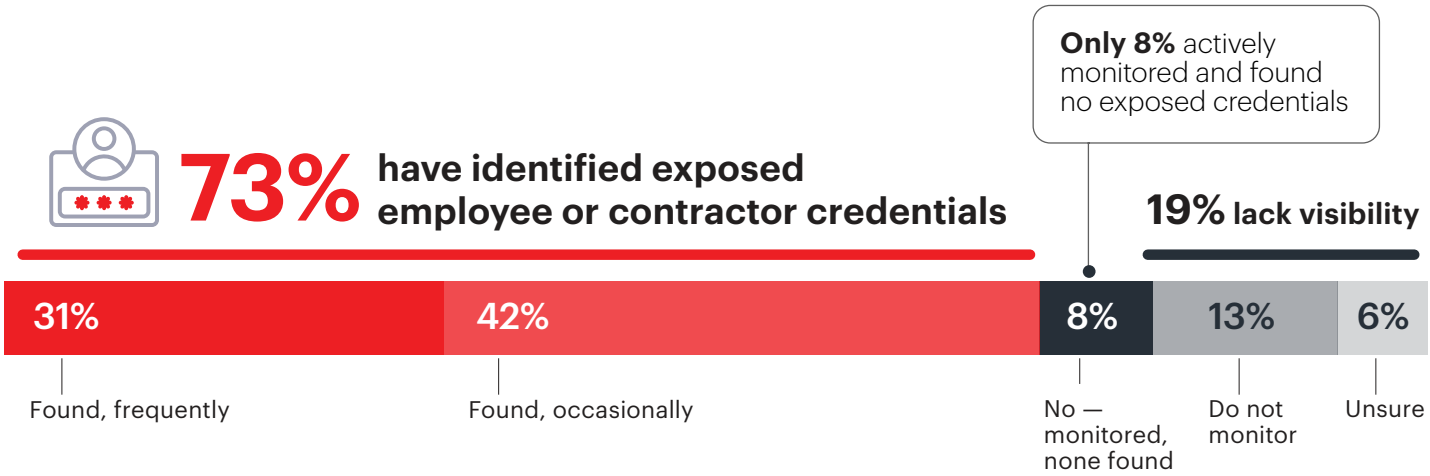
Credential exposure is not hypothetical. Most organizations have already found their own workforce credentials in breach, dark-web, or infostealer data - and that exposure is already connected to authentication-related incidents.

The evidence begins with what teams have already found in their own environments. 73% have identified employee or contractor credentials in third-party breach data, dark-web sources, or infostealer logs in the past year. Only 8% actively monitored and found no exposed credentials; 13% do not monitor for this exposure, and 6% are unsure whether they have any visibility at all. For many organizations, this is confirmed evidence that workforce credentials have appeared outside their control. It also explains why 82% are concerned that previously compromised credentials may already be present in their environment.

Credential exposure is already tied to active incidents. 71% experienced an authentication-related security incident in the past 12 months, and in 66% of the most recent incidents, attackers used valid credentials. The credentials found in breach data and the credentials used in incidents are not separate risk categories. They are part of the same operational chain: working logins that may remain trusted after they have appeared outside the organization's control. The operational question is who acts first: the team that finds and remediates the exposure, or the attacker who buys, tests, and uses the credentials.

Most Organizations Already Found Their Own Credentials Exposed

During the past 12 months, has your organization identified employee or contractor credentials exposed in third-party breach data, dark web sources, or infostealer-related datasets?



71% had an authentication-related incident in the past 12 months.

In **66%** of incidents, the attacker signed in with valid credentials.

Closing this gap starts with the assumption that credential exposure is already present. Organizations cannot remediate what they only find by chance. The first move is knowing which active credentials are exposed right now. Visibility is the prerequisite for every later control.

Infostealers Have Industrialized the Credential Supply Chain

Fresh stolen credentials keep entering attacker markets because infostealers have turned credential theft into a continuous supply chain. Stolen passwords, browser-stored access data, authentication tokens, and session material can move from an infected endpoint into criminal markets faster than reset and review cycles can respond.

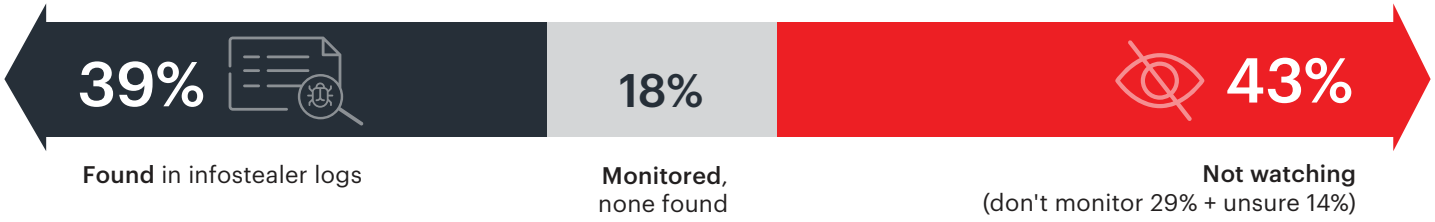
It often starts with one infected laptop. A single infection can capture saved browser passwords, authentication tokens, and session cookies, giving attackers more than a password to test. In some cases, a still-valid session cookie can be replayed to avoid the password prompt and the MFA challenge that a fresh login would trigger. The resulting logs can be sold while they are still useful, often before the victim knows the device was infected.

The 2026 Verizon Data Breach Investigations Report reinforces the timing problem. Among ransomware victims with an associated credential leak or infostealer event in the prior year, half experienced that event within 95 days before the ransomware attack.

Organizations only see this exposure when they monitor for it. 39% have already found employee credentials in infostealer logs tied to malware families such as Lumma, Vidar, and RedLine. Yet 43% either do not monitor that channel or are unsure whether they do. That leaves many organizations with limited visibility into one of the freshest sources of usable account material.

Teams Find Infostealer Exposure, but Many Are Not Monitoring

Have you identified employee credentials in infostealer malware logs (e.g., credential-harvesting malware such as Lumma, Vidar, or RedLine) in the past 12 months?



Infostealer involvement is also likely under-attributed. Only 12% named infostealer malware as the most likely initial access method in their most recent authentication-related incident, even though credentials stolen by infostealers may later be recorded as compromised-credential use, credential stuffing, MFA abuse, or unknown initial access.

Mature programs treat breach and infostealer feeds as live intelligence, not periodic research. The critical measure is freshness: how quickly the program can identify which credentials, cookies, or session artifacts have appeared outside the organization's control while they are still usable.

Source: Verizon, 2026 Data Breach Investigations Report, p. 44. https://www.verizon.com/business/resources/reports/dbir/

Credential Screening Still Happens at the Wrong Moment

Credential exposure often appears after a password is created, but most checks still occur when a password is set or reset. That timing mismatch leaves active credentials trusted after they have become exposed, creating the opening attackers exploit.

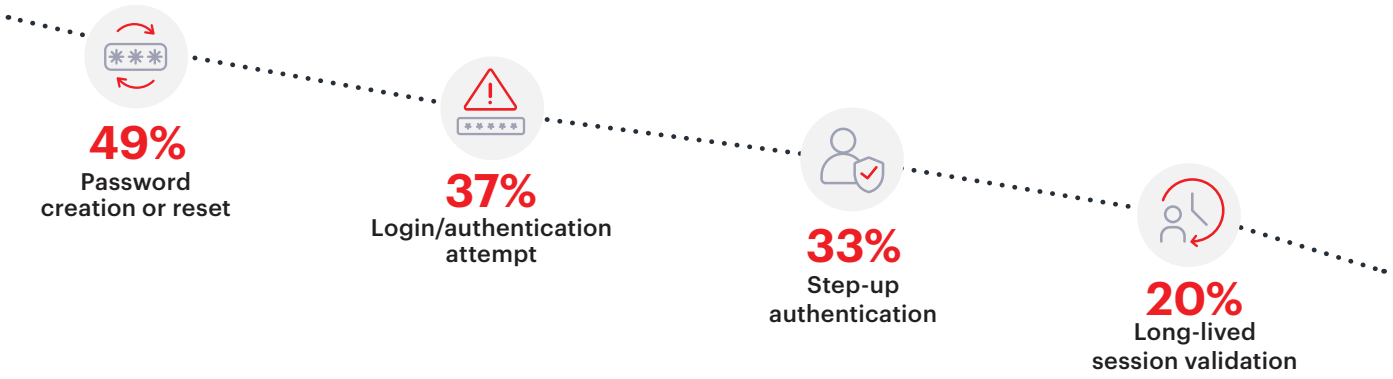
Teams check most heavily at the front of the lifecycle. 49% screen at password creation or reset, 37% at login, 33% at step-up authentication, and only 20% when a long-lived session re-authenticates. That is misaligned with how credential risk develops. After creation, credentials can be reused, captured through phishing, leaked in a third-party breach, or stolen from an infected endpoint while the account remains trusted. Yet monitoring drops off precisely after the credential enters active use.

NIST SP 800-63B reinforces the shift away from routine password expiration and toward password changes when there is evidence of compromise. That model depends on continuous evidence: teams have to keep checking active credentials after the password event. Today, too few do. Only 29% screen against live breach intelligence in real time or daily, and only 19% continuously monitor active credentials and automatically remediate exposure.

Active Directory makes the static-control problem concrete. 19% have not checked AD for compromised passwords at all. Across the full respondent base, 37% found 5% or more of AD accounts with compromised passwords, compared with 23% who found less than 5%, and another 13% found exposure they could not quantify. Even the lowest measured exposure group still found compromised passwords. Screening at creation answers only whether the password was safe at that moment. It does not answer whether the credential remains safe after days, weeks, or months of use.

Teams Check Most at Password Creation, Then Coverage Falls Off

At which points in the authentication lifecycle does your organization use credential-risk signals or compromised-credential checks?



More organizations found 5% or more of AD accounts with compromised passwords (37%) than found under 5% (23%). 19% have not checked AD for compromised passwords.

Teams getting this right no longer treat the password reset as the primary control point. Active credentials need continuous screening against live breach and infostealer intelligence, so exposure is found and remediated when it creates active risk, not only when a user eventually changes a password.

Detection Is Common. Confirmation and Response Lag

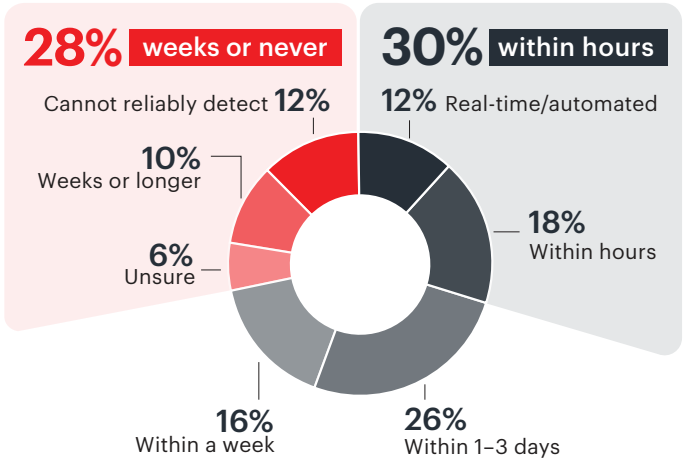
Most teams have some way to detect compromised credentials. The harder problem is speed: identifying exposure early, confirming whether the credential is still active, and containing the risk before a valid login becomes broader compromise.

Detection channels are common. Teams monitor dark-web and identity-breach feeds (56%), correlate alerts in the SIEM (52%), and run compromised-credential screening (42%). But having a detection channel does not mean exposure is found quickly. Only 30% can spot a newly exposed credential in real time or within hours, while 22% take weeks or cannot reliably detect it at all. Confidence reflects the same gap: only 14% are very confident they can identify compromised-credential use early in the authentication chain, while 47% are not confident or unsure.

Confirmation is where the clock keeps running. Among respondents answering about their most recent authentication-related incident, 49% determined within a week that compromised credentials were involved; 43% took longer or still cannot say. Response also remains heavily hands-on: forced password reset (61%), user notification (56%), and account investigation (53%) are the most common actions. Only 42% trigger automated alerting or case creation, and only 26% reduce privileges or restrict access pending review. Each manual handoff adds dwell-time risk. For teams that take more than a week, or never get a clear answer, that delay can become the attacker's operating window. It gives the attacker time to reuse the login, test privileges, and move from one valid account toward broader compromise before credentials are confirmed as the path in.

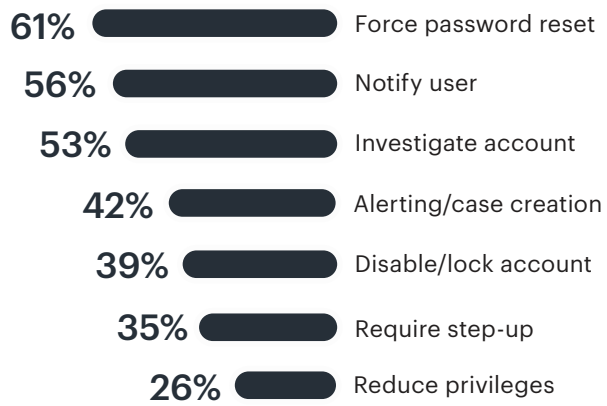
Only 30% Can Spot a Newly Exposed Credential Within Hours

How quickly can your organization detect newly exposed employee credentials from breach, dark web, or infostealer-related sources?



When Exposure Turns Up, the Response Is Still Mostly by Hand

When an employee's credentials are found to be exposed or compromised, what actions does your organization take?



After the most recent authentication-related incident, 49% confirmed credential involvement within a week. 43% took longer or still could not say.

Where this is working, teams connect detection, confirmation, and remediation into one workflow. They measure the time from credential exposure to containment. The shorter that window, the less time the attacker has to use the credential.

MFA Reduces Credential Misuse, but Exposure Remains

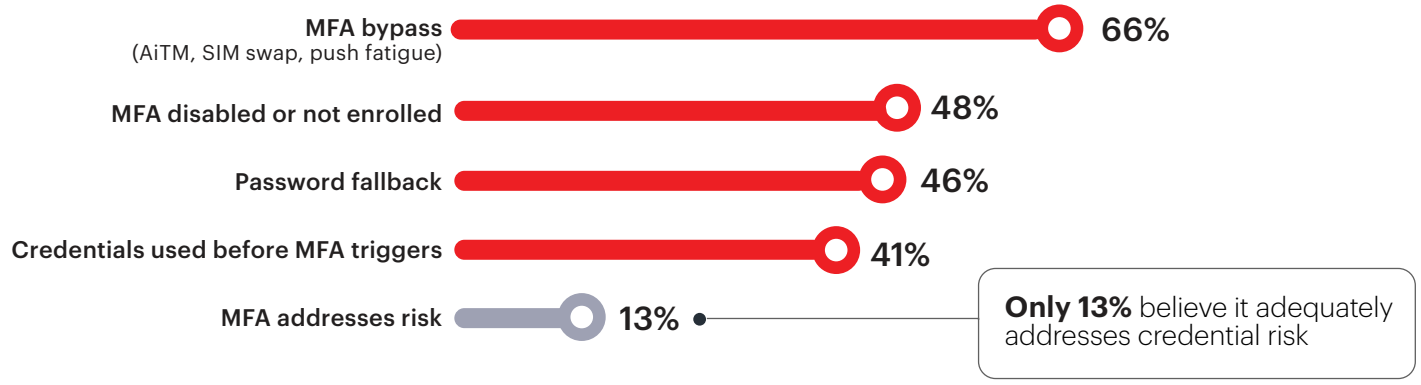
MFA makes a stolen password harder to use. The underlying credential exposure remains. Attackers exploit that gap.

The survey shows four gaps that keep exposed credentials relevant even when MFA is deployed. 66% remain concerned about bypass through adversary-in-the-middle kits, SIM swaps, and push fatigue. 48% worry about users who never enrolled or later disabled MFA. 46% point to password fallback, and 41% worry about credentials being used before MFA is triggered. These are operationally relevant attack paths. An adversary-in-the-middle proxy kit can sit between the user and a legitimate login, capturing session material after the user completes authentication. A stolen session cookie can sometimes be replayed later without a fresh password prompt or MFA challenge. Fallback paths keep passwords in play when stronger authentication is unavailable. Each route works differently, but the underlying issue is the same: the credential remains exposed even when MFA reduces its usefulness.

The data shows that most teams do not view MFA as sufficient on its own: only 13% believe it adequately addresses credential risk. Yet fallback remains common. 62% still allow password fallback when MFA is unavailable, and only 17% have eliminated that path. Overreliance on MFA also shows up in the obstacle data: 21% cite a belief that MFA removes the need for credential monitoring as a reason they have not started. MFA earns its place in the stack, but it was never designed to make exposed credentials disappear. Credential monitoring watches the layer beneath MFA: exposed username-password pairs and other reusable credential material, whether MFA is enabled or not.

Even with MFA, Four Credential Risk Gaps Remain

Even with MFA deployed, which credential-related risks remain a concern for your organization?



62% still allow a password fallback when MFA is unavailable. Only 17% have closed that path.

The strongest programs treat MFA and credential monitoring as complementary layers, not competing options. They close password-fallback paths and keep watching the credential layer beneath the prompt, so exposed passwords are found and remediated even while MFA reduces the chance of immediate misuse.

Credential Exposure Extends Beyond Core Workforce Accounts

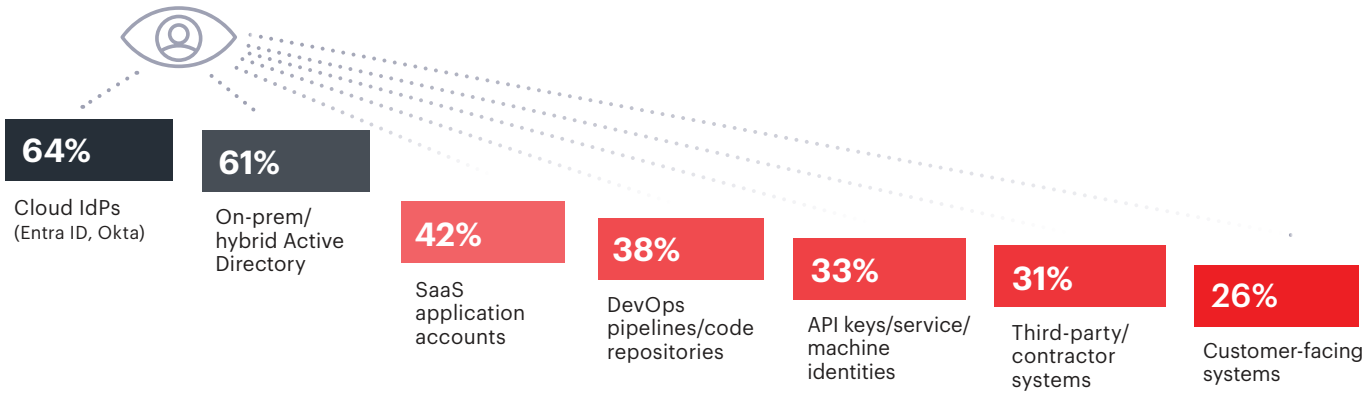
Most credential monitoring still focuses on core workforce identity systems, while many other identity types receive far less coverage. That matters because attackers can abuse exposed credentials, secrets, and access paths across SaaS accounts, service accounts, customer-facing authentication systems, and third-party environments.

Organizations monitor first where identity is easiest to govern. 64% monitor cloud identity providers such as Entra ID and Okta, and 61% monitor on-premises or hybrid Active Directory. Coverage drops quickly beyond that core: 42% monitor SaaS application accounts, 38% monitor DevOps pipelines or code repositories for secrets scanning, 33% monitor API keys, service accounts, or machine identities, 31% monitor third-party or contractor systems, and 26% monitor customer-facing or consumer authentication systems. Teams tend to cover the identities they control most directly, leaving other high-value access paths with thinner monitoring.

Coverage is weaker still for external identities. Only 18% monitor or enforce credential security for nearly all contractors, partners, vendors, and federated third parties. 42% cover only some high-risk external identities and 26% keep monitoring focused on full-time employees. These identities often reach core systems through access paths the security team controls less directly: a contractor account, a partner integration, a shared service account, or a machine credential tied to an automated workflow. Not all of these identities are privileged. Those that are can be especially valuable to attackers because they combine meaningful access with weaker visibility.

Credential Monitoring Is Strongest Where Identity Is Easiest to Govern

In which identity environments does your organization actively monitor for compromised or exposed credentials?



Only 18% cover all or nearly all external identities.
26% still monitor only full-time employees.

Coverage should follow access risk, not organizational convenience. Mature programs extend credential exposure monitoring beyond core employee accounts and prioritize the identities whose compromise would matter most: privileged users, service and machine credentials, third-party access paths, and customer-facing authentication systems.

Credential Defense Still Needs an Owner

Organizations are funding credential defense, but spending does not close the exposure gap by itself. A capability only matters once someone owns the workflow, integrates it into identity operations, and makes it part of daily response.

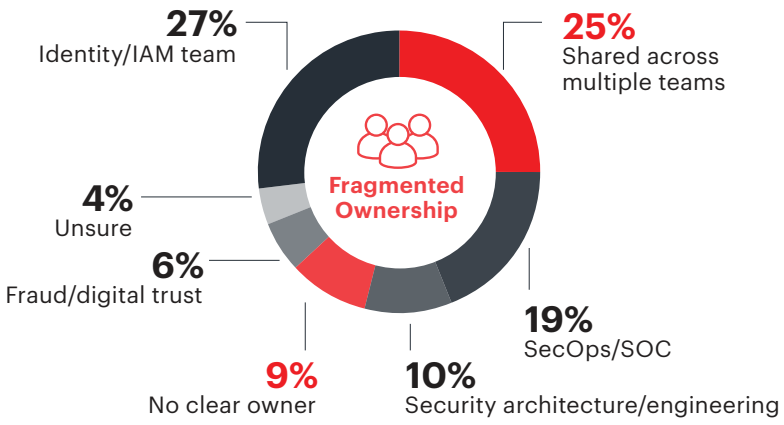
Organizations see the problem and are investing in adjacent controls. Over the next 12 months, 47% plan to expand or modernize MFA, 45% plan to invest in passwordless authentication, 43% in identity threat detection and response (ITDR), and 41% in compromised-credential screening or monitoring. The market is not ignoring credential exposure. The harder question is whether those investments become operating practice: continuous monitoring, automated remediation, and clear response workflows inside the identity systems where access is granted, changed, and revoked.

That is where programs stall. Credential exposure often has no single accountable home. IAM owns it in 27% of organizations, but 25% split responsibility across multiple teams and 9% report no clear owner at all. That fragmentation makes integration harder, which 40% cite as an obstacle, and keeps the issue from becoming a formal priority. Only 29% treat automated credential abuse at scale as a defined strategic priority. Competing priorities (49%) and budget or staffing constraints (44%) matter, but they are harder to overcome when no team owns the outcome. A capability without an accountable owner rarely becomes fully operational.

Standards can guide credential security practices, but they do not create operational accountability. NIST SP 800-63B is the most common standards influence, cited by 54% of respondents, but a standard cannot assign ownership, connect identity infrastructure, or automate remediation. Where credential exposure has an owner, the same workflow that closes risk also produces the evidence compliance and audit teams need: which credential was exposed, when it was found, what action was taken, and when the risk was contained. Until someone owns that workflow, the capability can exist on paper while exposed credentials remain active.

Ownership Splits Across Several Teams — or Goes Missing

Who primarily owns compromised credential risk management in your organization?



41%
plan to add compromised-credential screening or monitoring.

Only 29%
make automated credential abuse a defined priority.

Programs that close this gap pair capability with accountability. They assign one accountable owner for credential exposure, even when execution remains cross-functional, wire monitoring into the systems where remediation happens, and make automated credential abuse at scale a defined priority.

Continuous Credential Defense Maturity

The survey findings point to one operating pattern: credential programs rarely mature evenly. A team may monitor breach data but still rely on manual password resets. It may cover employee accounts well while leaving contractors, service accounts, and machine credentials under-monitored. The Continuous Credential Defense maturity model organizes those gaps into five dimensions and three levels, from Reactive to Adaptive, so teams can assess where their program operates today and what it needs to move toward continuous defense.

DIMENSION	REACTIVE	MANAGED	ADAPTIVE Continuous Credential Defense
Exposure Visibility	Checked only at password events; no visibility between events	Periodic breach and dark-web monitoring; exposure surfaced in days	Live breach and infostealer monitoring; exposure surfaced in real time
Screening & Enforcement	Complexity and expiration rules; no compromised-credential screening; MFA assumed sufficient	Known-compromised passwords blocked at creation or reset; limited screening after the password event	Continuous screening of active credentials; automated remediation
Detection & Response Speed	Ad hoc detection; manual response; credential involvement confirmed in weeks or never	Detection in place; response largely manual; involvement confirmed in about a week	Automated detection-to-remediation; involvement contained within hours
Identity Coverage	Limited to the full-time workforce in AD and cloud IdPs	Partial coverage of high-risk non-employee identities	Non-employee, non-human, and customer-facing identities prioritized by access risk
Governance & Ownership	No clear owner; credential abuse not prioritized; compliance checklist-driven	Ownership shared across teams; credential abuse acknowledged but not formally addressed	Clear owner; automated credential abuse a defined priority; standards drive practice

The Adaptive tier describes the target operating model: continuous visibility, active-credential screening, automated remediation, risk-based identity coverage, and clear ownership. The first four dimensions close technical gaps. Governance determines whether those capabilities are funded, integrated, assigned, and operated.

The survey findings suggest that most programs remain between the Reactive and Managed tiers. Only 19% monitor active credentials and remediate automatically. Only 30% can detect newly exposed credentials in real time or within hours. Only 18% cover all or nearly all external identities. Until more programs move toward Adaptive, exposed credentials remain usable for too long, giving attackers more time to turn a valid login into broader compromise.

What It Takes to Close the Exposure Gap

Most teams recognize compromised credentials as a primary attack path. Far fewer can continuously identify active credentials that have already been exposed, contain the risk, and remove those credentials from use before attackers turn exposure into compromise. The gap is operational. Closing it means moving from point-in-time password hygiene to Continuous Credential Defense.

1

See exposure while it is still useful to attackers

73% have already found their own credentials in third-party breach data, dark-web sources, or infostealer logs, yet 43% do not monitor infostealer exposure or are unsure whether they do. Start with continuous visibility into active credentials against live breach and infostealer intelligence. Measure freshness: how quickly the program can identify that a usable credential has appeared outside the organization's control.

2

Screen credentials already in use, not only new passwords

Only 29% screen against live breach intelligence in real time or daily, while 43% automatically block previously compromised passwords at creation or reset. That leaves too much control concentrated at the password event. Extend screening to active credentials across the lifecycle, and close password-fallback paths that keep exposed credentials useful even when MFA is deployed or passwordless adoption is underway.

3

Cut the window from detection to containment

Only 30% say they can detect a newly exposed credential in real time or within hours, and response still leans heavily on manual resets, user notifications, and account investigations. Connect detection, confirmation, and remediation into one workflow, then measure the time from exposure to containment. The goal is not simply to know that exposure exists. It is to invalidate, reset, restrict, or otherwise contain the credential before it becomes a path to broader compromise.

4

Cover the identities with the most access, not just the easiest ones

Only 18% monitor or enforce credential security for all or nearly all external identities. Coverage is thinnest across contractors, third parties, service accounts, machine identities, and customer-facing or consumer authentication systems. Extend monitoring beyond core employee accounts and prioritize by access risk: privileged users, service and machine credentials, third-party access paths, and any identity whose compromise would create material impact.

5

Assign an accountable owner

Only 29% treat automated credential abuse at scale as a defined strategic priority, and competing priorities remain the top obstacle. Assign one accountable owner, even where execution remains cross-functional, and integrate monitoring into the systems where remediation happens. Without ownership, visibility remains informational, response remains manual, and exposed credentials remain active longer than they should.

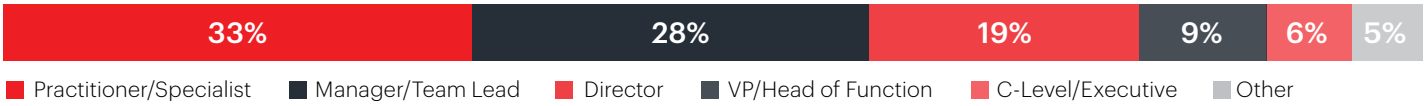
Together, these moves define Continuous Credential Defense: continuously monitoring active credentials, finding exposure while it is still actionable, and remediating through the systems that grant access. Where this discipline is in place, a successful login is not trusted simply because authentication succeeds. It is evaluated against credential exposure, abuse signals, and account context, so the organization can identify and contain risk before exposure turns into compromise.

Methodology and Demographics

This report is based on a survey of 872 cybersecurity professionals, fielded in mid-2026. Respondents include security practitioners, architects, managers, and executives with responsibility for identity, access, authentication, credential protection, and related security operations. The sample spans industries and organization sizes, with strong representation from mid-to-large enterprises: 86% of respondents work at organizations with 1,000 or more employees.

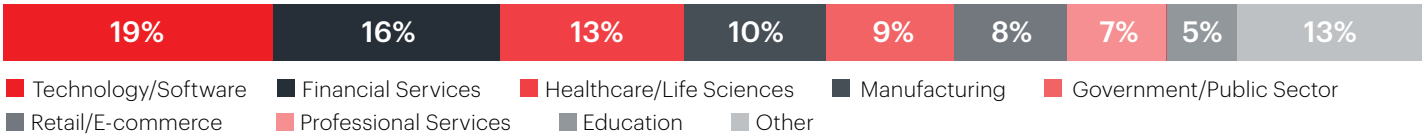
The research examines how organizations defend against compromised credentials across five areas: exposure visibility, credential screening and enforcement, detection and response speed, identity coverage, and governance ownership. The analysis centers on the operational gap between recognizing compromised credentials as a primary attack vector and continuously finding and remediating exposed active credentials before they are exploited.

RESPONDENT ROLE



FUNCTIONAL AREA

INDUSTRY



COMPANY SIZE

Percentages are based on the full respondent base unless otherwise noted. For select-all questions, response options are not mutually exclusive, so totals can exceed 100%. At a 95% confidence level, the full-sample margin of error is approximately ±3.3 percentage points.

Cybersecurity
INSIDERS

BENCHMARK YOUR SECURITY MATURITY

Independent cybersecurity research revealing the gaps that shape cybersecurity strategy

Cybersecurity Insiders produces independent research based on surveys of cybersecurity leaders and practitioners worldwide. Our reports reveal where security strategies break down in practice — helping organizations benchmark their maturity, identify capability gaps, and prioritize the actions needed to close them.

For more information, visit

cybersecurity-insiders.com

July 2026 // Version 1.5

ENZOIC

Enzoic is an enterprise-focused cybersecurity company committed to preventing account takeover and fraud through actionable Dark Web research. What sets Enzoic apart is the unique proactive approach to solving the problems that compromised passwords and credentials cause. By combining human intelligence with automated proprietary monitoring, Enzoic delivers the most current and complete threat research data.

Organizations can use Enzoic solutions to screen customer and employee accounts for exposed username and password combinations to identify at-risk accounts and mitigate unauthorized access. Enzoic's comprehensive approach to compromised password detection and its tailored solutions, like Enzoic for Active Directory, represent our company's unwavering commitment to protecting customer environments. Enzoic is a profitable, privately held company in Boulder, Colorado.

Email us at **info@enzoic.com** or visit **enzoic.com**