

HIRE

ONBOARD

RECOVER

OFFBOARD



A check leaves nothing behind for the next stage.

ONE CREDENTIAL, EVERY STAGE

One Identity Across the Enterprise

A single verified credential, from hire to offboard

Contents

01	The identity decision that happens before day one	3
-----------	---	---

02	Identity under attack at every stage	4
-----------	--------------------------------------	---

03	The check vs. the credential	6
-----------	------------------------------	---

04	The connected employee: one credential, every stage	7
-----------	---	---

05	The fragmentation problem	9
-----------	---------------------------	---

06	The trust infrastructure	10
-----------	--------------------------	----

07	What this means for your team	11
-----------	-------------------------------	----

08	Auditing your current posture	12
-----------	-------------------------------	----

09	Enterprise identity as infrastructure	14
-----------	---------------------------------------	----

The identity decision that happens before day one

When a new employee joins your organization, a background check vendor confirms they are who they claim to be on paper. Your HR system creates a record. Your identity provider provisions access. Your help desk gets a ticket to set up devices. The background check produces a historical summary, the identity provider produces credentials, and the help desk produces a ticket. Each system does its job without producing a persistent, verifiable record that the others can use. For most of the history of enterprise security, that fragmentation was manageable. Identity fraud was a retail problem,

and social engineering was an exception. The threat model assumed that someone who made it through hiring and onboarding was, broadly, who they said they were. That assumption no longer holds. The same technologies that have automated routine business operations have industrialized identity fraud across the full employee lifecycle: at hiring, through onboarding, across active employment, and at the moment of offboarding when access should stop but often doesn't. The result is a workforce identity surface that has expanded significantly faster than the infrastructure designed to secure it.

WHAT EACH SYSTEM PRODUCES TODAY

SYSTEM	OUTPUT	REUSABLE BY THE OTHERS
Background check vendor	A historical summary	No
Identity provider	Credentials for access	No
Help desk	A ticket	No

THE GAP

Each system does its job without producing a persistent, verifiable record that the others can use.

SECTION 02 IDENTITY UNDER ATTACK

Identity under attack at every stage

The workforce identity threat spans every stage of the employee lifecycle, and the gaps between those stages are where the most consequential vulnerabilities live.

At hiring

[By 2028, Gartner predicts 1 in 4 candidate profiles will be fake](#). The mechanisms are no longer speculative. Synthetic identities, personas constructed from real and fabricated data, are increasingly indistinguishable from legitimate applicants using conventional screening methods. Deepfake video interviews allow a fraudulent candidate to pass a live conversation with a human recruiter. AI-generated resumes, portfolios, and references clear automated filters designed to catch them. The stakes of a bad hire extend well beyond a compliance failure. As Gartner's research director in the human resources practice has noted, candidate fraud creates cybersecurity risks that can be far more serious than

making a poor hiring decision. An unverified identity granted enterprise access is an insider threat with a legitimate badge. The most operationalized version of this threat is nation-state. [North Korean IT worker infiltrations increased 220% over the past twelve months](#), with operatives submitting hundreds of thousands of job applications and successfully obtaining employment at major enterprises. [Nine security officials told Axios they had yet to encounter a Fortune 500 company that had not inadvertently hired a North Korean IT worker](#). These are the operational baseline for a program that has generated an estimated [\\$250 million to \\$600 million annually since 2018](#), according to UN estimates.

THE HIRING THREAT, IN NUMBERS

1 in 4

Candidate profiles predicted to be fake by 2028

Sources: Gartner; Axios; UN estimates.

220%

Increase in North Korean IT worker infiltrations over twelve months

\$250–600M

Estimated annual program revenue since 2018

During active employment

The threat does not end once an employee is onboarded. For most organizations, account recovery remains the most exploitable moment in the employee lifecycle: a help desk agent fielding a call from someone claiming to be an employee, working through security questions that can be answered by anyone with access to a dark web data broker. [Vishing attacks surged 442% between the first and second half of 2024](#),

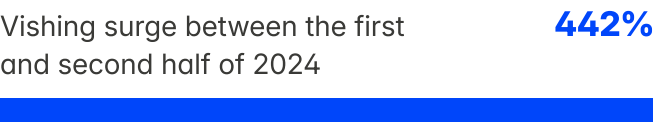
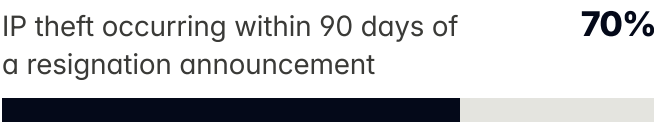
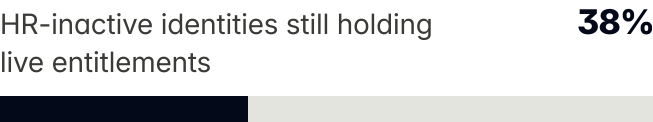
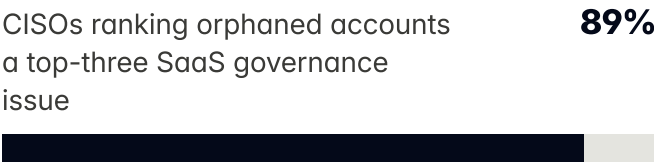
according to the CrowdStrike 2025 Global Threat Report. The Scattered Spider group that breached MGM Resorts and Caesars Entertainment in 2023 did not exploit a software vulnerability. They called the help desk, passed verification, and received credential resets that opened full system access. The vulnerability was the recovery process itself.

At offboarding

The moment an employee leaves is the moment their access should end. In practice, the gap between those two events is significant and measurable. [89% of enterprise CISOs now rank orphaned accounts as a top-three SaaS security governance issue](#). In one 2025 analysis, even when HR systems had flagged accounts as inactive, [38% of those identities continued to hold live entitlements in core business applications](#). Orphaned identities are increasing approximately 40% year over year. The

financial exposure is real. [70% of IP theft occurs within 90 days of an employee's resignation announcement](#), and the [average annual cost of insider risk reached \\$19.5 million in 2025](#), rising to \$24 million for North American organizations. [More than half of enterprises experienced an insider threat incident in the past year](#). The offboarding gap is a recurring cost, measured in breach forensics, legal exposure, and the time required to close access that should have closed automatically.

WHERE THE LIFECYCLE LEAKS



Sources: CrowdStrike 2025 Global Threat Report; CloudNuro; 2025 insider risk analyses.

\$19.5M

Average annual cost of insider risk, 2025

\$24M

North American organizations

~40%

Year-over-year growth in orphaned identities

The check vs. the credential

Every organization running a background check, an I-9 verification, or a knowledge-based authentication flow at account recovery is producing the same kind of output: a point-in-time check. The check answers a narrow question at a specific moment. It does not persist. It cannot be shared across systems. It carries no cryptographic weight. And it expires the moment circumstances change.

The distinction matters because of what checks cannot do.

A background check cannot tell you that the person presenting credentials three years after hire is still who the background check said they were. A knowledge-based verification at account recovery cannot confirm that the caller did not purchase the right answers for less than a dollar per record. An I-9 completed at onboarding cannot verify that the document presented was genuine rather than synthetic. A credential is categorically different. A

cryptographically signed credential binds a verified identity to a tamper-evident record at the moment of verification. It is reusable: the same verification event can be drawn upon at every subsequent identity moment without re-verifying from scratch. It is mathematically verifiable by any party, in any system, at any future time. And it does not degrade; the cryptographic signature either holds or it doesn't, regardless of how much time has passed.

WHAT A CHECK CANNOT DO

PROPERTY	A CHECK	A CREDENTIAL
Persistence	Answers a narrow question at a specific moment and does not persist.	Binds a verified identity to a tamper-evident record at the moment of verification.
Portability	Cannot be shared across systems.	Reusable at every subsequent identity moment without re-verifying from scratch.
Verifiability	Carries no cryptographic weight.	Mathematically verifiable by any party, in any system, at any future time.
Durability	Expires the moment circumstances change.	Does not degrade; the signature either holds or it doesn't.

SECTION 04 THE CONNECTED EMPLOYEE

The connected employee: one credential, every stage

The practical consequence of credential-based identity is that the employee experience changes at every stage of the lifecycle, and each stage compounds on the one before it.

Candidate screening

Verification at the point of application is the first moment where a persistent credential can be established. A candidate who submits a government-issued ID, passes liveness detection, and clears fraud signal analysis produces a record that goes beyond a background check summary: a cryptographically signed confirmation of who showed up to apply. That record

follows them forward. The I-9 penalty for non-compliance runs up to [\\$2,861 per violation](#) under current USCIS guidance, effective January 2025. The cost of hiring a nation-state operative who has cleared a conventional background check runs considerably higher, measured in system access, IP exposure, and the forensic cost of determining what they touched and when.

Onboarding

When a candidate who has been verified at hire moves into onboarding, the credential established at screening becomes the foundation for every downstream provisioning decision. Device enrollment, SSO configuration, and role-based access can each reference the same verified identity record rather than trusting that the person showing up on day one is

the same person who interviewed. Proof's own IT team built this directly: any employee receiving a new machine or being onboarded for the first time goes through identity verification before the process can proceed. The verification is embedded in the enrollment flow itself, so the identity decision happens at the moment it is actually consequential.

WHAT ONBOARDING REFERENCES, ONCE THE CREDENTIAL EXISTS

Device enrollment

Verification runs before a new machine is issued.

SSO configuration

Access is provisioned against the verified record.

Role-based access

Entitlements reference one identity, not an assumption.

Active employment and account recovery

The most significant advantage of a persistent credential becomes clear at the first account recovery event. When an employee loses access to their account and calls the help desk, the question the agent cannot reliably answer, whether this person is who they say they are, is one Proof has already answered. The credential established at hire is still valid. The verification does not need to happen again from scratch. This changes the

recovery process fundamentally. The agent's role shifts from making an identity judgment under pressure to routing a request to a process that can surface the existing credential. [The Verizon 2024 Data Breach Investigations Report](#) found that 68% of breaches involve a non-malicious human element, meaning a person made an error or fell for social engineering. The structural fix is removing the judgment call from the process entirely.

68% of breaches involve a non-malicious human element. The structural fix is removing the judgment call from the process entirely.



Offboarding and revocation

The lifecycle closes at offboarding, and this is where credential-based identity provides the most unambiguous advantage. A cryptographic credential can be revoked with mathematical precision. Deprovisioning an Okta account and revoking a cryptographic credential are different operations, and only the latter produces a record that

holds up under audit. With [38% of inactive identities still holding live entitlements](#) after HR flags them for deprovisioning, the gap between “HR says they left” and “the systems agree” is measurable and exploitable. A revoked credential closes that gap at the identity layer and produces a record that holds at every tier of the stack.

THE CREDENTIAL ACROSS FOUR STAGES

STAGE 01	STAGE 02	STAGE 03	STAGE 04
Screening	Onboarding	Recovery	Revocation
The credential is established at the point of application.	Provisioning references the same verified identity record.	The agent routes a request instead of making a judgment call.	The credential is revoked with mathematical precision.

The fragmentation problem

A typical enterprise today runs a different vendor at each stage of the employee identity lifecycle: a background check provider at pre-hire, a KYC or IDV vendor for contractors, an identity provider for SSO, an MFA vendor for authentication, a service desk platform for recovery, and an HRIS for offboarding. Each system does its job without producing a shared record that the others can reference. The audit trail is fragmented across systems that were

not designed to talk to each other, and the gaps between vendors are precisely where sophisticated adversaries operate. The cost is multiplicative: licensing, integration, and maintenance across five or six vendors, none of which eliminates the manual identity judgment that surfaces at every seam. And when a breach forensic investigation has to determine who had access, when, and on what basis, the answer spans systems that each tell a partial story.

ONE LIFECYCLE, SIX VENDORS			FIVE SEAMS, NO SHARED RECORD		
PRE-HIRE	CONTRACTORS	SSO	AUTHENTICATION	RECOVERY	OFFBOARDING
Background check provider	KYC or IDV vendor	Identity provider	MFA vendor	Service desk platform	HRIS
PRODUCES A historical summary	PRODUCES A verification result	PRODUCES Access credentials	PRODUCES An authentication event	PRODUCES A ticket	PRODUCES A termination record
SHARED WITH THE OTHERS No	SHARED WITH THE OTHERS No	SHARED WITH THE OTHERS No	SHARED WITH THE OTHERS No	SHARED WITH THE OTHERS No	SHARED WITH THE OTHERS No

Each dashed blue rule marks a seam: a handoff between systems that share no verifiable record.

SECTION 06 THE TRUST INFRASTRUCTURE

The trust infrastructure

The credential Proof produces is a cryptographically signed record issued by a [WebTrust-certified certificate authority](#) and listed on the [Adobe Approved Trust List \(AATL\)](#). WebTrust certification meets the same audit standard as the certificate authorities securing HTTPS globally; AATL is the separate trust store governing legally binding digital signatures on legal and financial documents.

AUDIT STANDARD

WebTrust

The same standard as the certificate authorities securing HTTPS globally.

TRUST STORE

AATL

Governs legally binding digital signatures on legal and financial documents.

This distinction matters in several contexts that CISOs and IAM directors encounter regularly.

Under regulatory scrutiny, the question is whether the identity determination was made by a defensible process. A risk score from a point-in-time check carries the weight of one vendor's methodology. A cryptographically signed credential issued by a WebTrust-audited CA carries the weight of independently audited, formally recognized trust infrastructure that any party can verify at any

time. Under legal dispute or incident forensics, the questions are: can the record be independently verified, and can it be repudiated? A cryptographic credential is mathematically verifiable by any party at any time, cannot be altered retroactively, and answers what was known about an identity, when it was known, and how it was established, with a precision that a log entry cannot match.

ELEVEN YEARS OF OPERATING RECORD

Proof has operated in some of the most regulated industries on earth for eleven years, securing more than \$200 billion in transactions annually with zero reversals.

The trust infrastructure behind the credential represents a measurable difference in what the credential means when it actually matters, a distinction no identity startup entering the market today can replicate.

11 years

Operating in the most regulated industries

\$200B+

Transactions secured annually

Zero

Reversals

SECTION 07 WHAT THIS MEANS FOR YOUR TEAM

What this means for your team

FOR THE CISO

Every stage of the employee lifecycle is a potential entry point, and most organizations have a different control at each stage producing a different kind of record with a different level of assurance. A credential infrastructure replaces that fragmentation with a single verifiable record that surfaces at each stage and closes each gap.

From an IAM architecture standpoint, credentials compound on each other: a system built on them reduces the surface area for social engineering, eliminates the manual judgment call at account recovery, and produces an audit trail that holds at the credential layer rather than only at the application layer. And critically, Proof augments Okta, Ping, and existing IAM investments rather than replacing them, so the rip-and-replace objection doesn't apply.

FOR HR AND PEOPLE OPS

The candidate fraud threat is one that background checks were never designed to solve. Background checks validate history, while identity verification validates the person presenting that history. The CISO Gartner interviewed on the 1-in-4 prediction noted that candidate fraud creates cybersecurity risks that can be far more serious than a bad hire, because a fraudulent identity that clears hiring carries full legitimate access from day one.

The I-9 compliance benefit is a secondary consideration. The primary one is that identity established at hire, carried through onboarding and active employment, and revoked cleanly at offboarding is a fundamentally different risk posture than identity managed separately at each stage by systems that do not share a record.

Background checks validate history. Identity verification validates the person presenting that history.



NO RIP AND REPLACE

Proof augments Okta, Ping, and existing IAM investments rather than replacing them.

SECTION 08 AUDITING YOUR CURRENT POSTURE

Auditing your current posture

Most enterprise identity programs have never been assessed as a lifecycle. They have been assessed by product: how mature is the IAM stack, how complete is MFA coverage, how robust is the SIEM.

The lifecycle view surfaces a different set of gaps, and it does not require a vendor to run. There are six diagnostic exercises worth doing before any evaluation or roadmap conversation.

01 Map your verification touchpoints.

At every stage of the employee lifecycle (application, onboarding, account recovery, role change, offboarding), identify who makes the identity decision, what information they use, and what the output is. A log

entry, a risk score, and a cryptographic credential carry very different weight under regulatory scrutiny and in breach forensics. Most organizations find that several stages produce no verifiable output at all.

02 Count your orphaned accounts.

Pull a list of accounts flagged as inactive in your HRIS and cross-reference it against live entitlements in your IDP. The accounts that appear in both columns

are your exposure. If you have not run this query, the [CloudNuro research on orphaned account prevalence](#) suggests the number will be larger than expected.

03 Red-team your help desk.

Have someone unfamiliar with your team call in and attempt a credential reset using only publicly available information: LinkedIn, company directories, previous data breach records. Record

how far they get. This exercise tends to be more clarifying than any audit report, because it makes abstract risk concrete in under ten minutes. Most organizations have never done it.

04 Benchmark your offboarding lag.

Calculate the average time from HR termination date to full access revocation across your five most sensitive systems. Hours, days, or weeks? For each system where the answer is

days or weeks, identify what's creating the delay: a manual process, a missing integration, or an absence of a shared identity record that the system can act on automatically.

05 Audit your I-9 and candidate verification process.

Determine whether your current hiring verification would catch a synthetic identity or a document submitted with AI-generated alterations. The specific question is: does your

verification confirm that the document is genuine, or only that the information on the document matches a database record? These are different questions with different answers.

06 Run the credential-versus-check inventory.

For every identity vendor in your current stack, answer one question: does this produce a check or a credential? A check answers a question at a single moment and expires. A credential persists, can be referenced by other systems,

and carries cryptographic weight. Map which vendor owns the identity decision at each stage of your lifecycle, and determine which stages have no credential output at all. The gaps in that inventory are the gaps in your program.

WHAT THE DIAGNOSTICS ARE LOOKING FOR

1 in 4	442%	38%	\$19.5M
Candidate profiles predicted fake by 2028 · exercise 05	Vishing surge across 2024 · exercise 03	HR-inactive identities still entitled · exercises 02 and 04	Average annual cost of insider risk · exercise 06

BEFORE YOU EVALUATE

None of these require a vendor. All of them will surface the shape of your current exposure with enough precision to inform a roadmap, a board conversation, or a budget justification.

SECTION 09 ENTERPRISE IDENTITY AS INFRASTRUCTURE

Enterprise identity as infrastructure

The organizations that will be best positioned in the next decade are treating identity as infrastructure today: as a persistent, verifiable, cryptographically secured foundation that every sensitive access decision can draw from, rather than as a feature of an identity provider, a capability of a background check vendor, or a problem routed to the help desk one ticket at a time.

- The candidate who verifies at screening.
- The employee who onboards with a credential.
- The worker who recovers access without a judgment call.
- The departing employee whose credential is revoked cleanly.

Enterprise identity is a lifecycle. The candidate who verifies at screening, the employee who onboards with a credential, the worker who recovers access without a judgment call, and the departing employee whose credential is revoked cleanly are one identity moving through

one infrastructure, producing one auditable record that holds at every stage. That is the standard Proof is built to deliver, and it is the standard that the threat landscape now requires. Ready to see what enterprise identity infrastructure looks like for your organization?

Talk to the Proof team to learn how organizations in financial services, insurance, and enterprise IT are closing the workforce identity gap across the full employee lifecycle.

Talk to Proof

About Us

Proof is the identity authorization company that verifies people and organizations, issues high-assurance cryptographic credentials and creates tamper-evident evidence of what they authorize—whether they act directly or through AI agents. Proof has secured more than \$640 billion in transactions for 10,000 organizations, including 16 of the Fortune 100. Learn more at proof.com.