

Sponsored content | White paper

The new era of executive risk: Why identity security must be continuous

A guide to managing risk and supporting audit readiness across all human and non-human identities



CSO

Sponsored by



Securing identities has become significantly more complex over the last several years. Organizations are no longer only managing employee identities. Contractors, vendors, partners, service accounts, machine identities, and AI agents all require access to business systems, creating a larger and more dynamic identity ecosystem than security teams have managed in the past.

At the same time, the burden on CISOs, CSOs, and risk and compliance officers continues to intensify. Boards and regulators expect these leaders to reduce cyber and compliance risk. To deliver on these mandates, they must prove that access to critical systems and data is strictly governed and that policies are consistently enforced.

Meeting those mandates has become increasingly complex as human and non-human identities are constantly provisioned and modified across cloud platforms, SaaS applications, and hybrid environments, often far faster than manual processes can track.

Identity is now the center of executive accountability

As executive accountability for cybersecurity continues to grow, security leaders are increasingly expected to demonstrate that identity governance is operating effectively — not simply that policies exist on paper. The ability to show who has access to critical systems, why that access was granted, and how access is continuously governed provides evidence of the oversight and due diligence expected by boards, regulators, and other stakeholders.

This is no longer just about organizational risk but may also involve personal and professional liability. A growing vulnerability now lies in agentic and non-human identities, which have become the primary attack vectors

for breaches that result in executive-level consequences. When a breach occurs, regulators and boards are increasingly holding the C-suite and security leaders directly accountable.

Traditional governance processes are not enough to reduce risk because they were designed for a different operating model. Periodic access reviews, manual certifications, and point-in-time audits provide only a snapshot of an environment that may change substantially days — or even hours — after the review is complete. These siloed tasks create visibility gaps that will likely increase as organizations add more non-employee and non-human identities.

Identity has always been a foundational component of security. Today, it has also become a central element of governance and organizational risk management. Modern enterprises depend on identities to connect employees, contractors, partners, applications, cloud workloads, APIs, service accounts, and AI-powered systems to the resources they need. Every one of these identities represents both a business enabler and a potential security risk.

The expansion of identity types has fundamentally changed the scope of the governance challenge:

- Employee identities may not be centrally governed.
- Third-party users may be managed through procurement systems, spreadsheets, or local directories.
- Machine identities may be created automatically as applications scale.
- AI agents introduce another layer of complexity as organizations begin assigning autonomous systems access to enterprise data and business processes.

As identity ecosystems become more distributed, governance can no longer focus on just employee identities. Security leaders need consistent visibility across identities operating within the enterprise.

All this growing complexity helps explain why identity security remains a top cybersecurity priority for security leaders. They increasingly recognize that security, compliance, and operational resilience all depend on understanding and governing access across an expanding identity landscape. **Non-human and agentic identities must be governed with the same rigor, visibility, and control as human users.**

Why point-in-time governance struggles to keep pace

Many organizations still approach governance through periodic review cycles, relying on a disruptive snapshot model. Managers must often certify access during frantic, point-in-time sprints on a quarterly or annual basis. This not only creates certification fatigue for business leaders but also leaves visibility gaps between audit periods where access can drift out of compliance.

These review activities remain necessary. The challenge is that identity environments rarely remain static between review cycles:

- Employees change roles.
- Contractors complete projects.
- Vendors gain temporary access to support new initiatives.
- Cloud applications are deployed by individual business units.
- Service accounts are created to support automation.
- Machine identities and AI agents are provisioned as new services come online.

Every change introduces an opportunity for access to drift from governance and compliance requirements.

Manual governance processes often struggle to keep pace with the rapid rate of change. By the time access is reviewed again, unnecessary privileges may have accumulated, orphaned accounts may remain active, or inconsistent policies may exist across different business systems.

The governance challenge becomes even greater when identity information is fragmented across multiple platforms. Organizations may have visibility into employee identities through HR systems while managing contractors via separate processes and machine identities through application teams. Without a unified view, security teams may struggle to understand the full scope of access across the enterprise.

Shift to continuous identity security

In today's regulatory environment, having the tools to support continuous visibility and governance is essential for executive leaders to demonstrate due diligence.



The issue extends beyond audit preparation. Security leaders increasingly need to demonstrate that governance processes are operating continuously, adapting to new changes, rather than simply documenting that reviews occurred at scheduled intervals.

Governance must also keep pace with the business itself. Security teams need controls that can nimbly support changes without creating unnecessary friction.

To help achieve continuous compliance, organizations must move away from static permissions and embrace adaptive identity security, an approach that dynamically adjusts to changing business requirements and risk signals while maintaining appropriate oversight.

Adaptive identity security addresses these challenges by shifting governance from a scheduled compliance activity to an ongoing operational discipline. Rather than relying on periodic reviews alone, organizations continuously validate access decisions, automate governance policies where appropriate, and maintain the visibility needed to demonstrate effective oversight as the environment changes. **The result is stronger security, improved audit readiness, and greater confidence that governance processes can withstand both internal scrutiny and external review.**

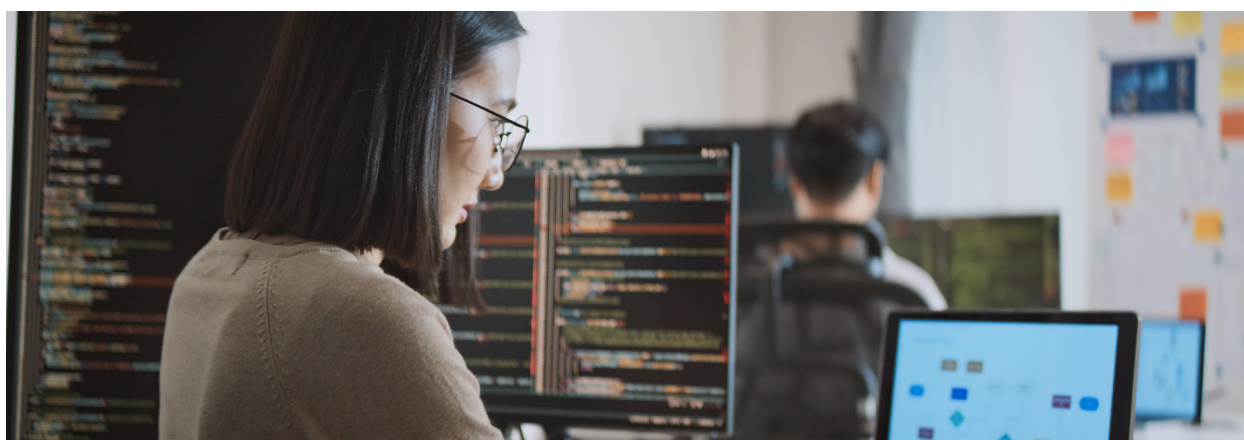
What continuous identity security looks like

Automated compliance evidence builds governance into day-to-day operations rather than treating it primarily as a compliance event.

Instead of waiting for periodic certification campaigns, organizations maintain ongoing visibility into identities and access relationships across enterprise systems. Access decisions can be automatically validated as business conditions change, helping reduce the time between a governance issue emerging and corrective action being taken.

Continuous governance also produces a more complete record of governance activity. Security leaders can demonstrate not only who has access to critical resources, but also how access was approved, when changes occurred, and whether governance policies were consistently applied.

AI-powered automation plays a foundational role in this process. Instead of forcing human managers to manually review every entitlement, an adaptive identity security program uses AI to analyze access trends, automate low-risk approvals, and dynamically flag high-risk anomalies as user contexts change.



A framework to see and govern all identities

Organizations that successfully transition from periodic to continuous governance often share three common capabilities:

1. Discover and unify identities. Effective governance begins with visibility — including the ability to discover and maintain visibility into employee, contractor, partner, machine, and AI identities across the enterprise. Bringing those identities together into a unified governance model provides security teams with a more complete understanding of who — or what — has access to business resources. Without that visibility, governance decisions are based on incomplete information, making it more difficult to identify unnecessary access or demonstrate effective oversight

2. Govern continuously. Lifecycle management, policy enforcement, access validation, and least-privilege controls become ongoing operational activities rather than periodic projects. Governance decisions occur as identities change, helping organizations reduce the window between business change and governance response. This approach also helps reduce the administrative burden associated with large-scale manual certification efforts while improving consistency across the enterprise.

3. Demonstrate and respond. Continuous governance helps organizations maintain up-to-date governance records, identify policy exceptions earlier, and document how access decisions are made. That evidence supports both internal decision-making and external regulatory or audit requirements while helping to identify potential issues before they become larger security events.

5 questions every CISO should be prepared to answer

As identity environments continue to evolve, security leaders should be able to answer several fundamental governance questions:

- ☐ **Can we centrally identify every identity operating across our environment?**
- ☐ **Can we demonstrate who — or what — has access to critical systems at any given time?**
- ☐ **Is our approach to access static, or is it truly adaptive?**
- ☐ **Can we quickly produce the evidence auditors and regulators require?**
- ☐ **Do we have the unified identity security foundation needed to adapt to evolving regulations?**

The ability to consistently answer “yes” to these questions is becoming an important measure of governance maturity.

Build a foundation for continuous governance

Identity security is no longer limited to supporting compliance initiatives. It enables organizations to manage security risk across increasingly complex identity ecosystems while demonstrating the oversight expected by executive leadership.

As organizations continue to expand their use of cloud services, automation, machine identities, and AI, their governance processes

must also evolve. Point-in-time reviews remain an important component of governance, but they are most effective when supported by continuous visibility, policy enforcement, and ongoing validation of access decisions.

The SailPoint Platform provides the adaptive identity security required to bring human, third-party, machine, and AI identities under a single control plane. SailPoint enables organizations to replace fragmented, reactive audits with automated, continuous compliance evidence, providing definitive, real-time proof of exactly who — or what — has access at any given moment.

Through continuous visibility, AI-driven automation, and dynamic policy enforcement, organizations can build a centralized system of record designed to strengthen security and support your organization's continuous, audit-ready compliance goals.



Test your readiness

[Download the full guide](#), “5 identity security questions CISOs must be ready to answer” to help uncover your hidden access gaps. Use the guide to help determine your organization's audit readiness and identify identity security gaps to help reduce executive risk.

DISCLAIMER: THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY, AND NOTHING CONVEYED IN THIS DOCUMENT IS INTENDED TO CONSTITUTE ANY FORM OF LEGAL ADVICE. SAILPOINT CANNOT GIVE SUCH ADVICE AND RECOMMENDS THAT YOU CONTACT LEGAL COUNSEL REGARDING APPLICABLE LEGAL ISSUES.