Securing Identity in the Age of AI

From Visibility to Continuous Control Across Human and Non-Human Access

An Independent Perspective from Trevonix

trevonix

Executive Summary

Organisations are undergoing a fundamental shift as key processes more and more rely on software, such as cloud workloads, APIs, robotic automation, and artificial intelligence systems, rather than human involvement.

This transformation has elevated identity to the primary control plane of the modern enterprise. Individuals are no longer the primary source of access risk. Service accounts, applications, integrations, and automated agents now handle more operational activities, often continuously and with elevated privileges.

Many organisations lack a complete understanding of:


Who or what has access to critical assets


How privileges accumulate over time


Whether access continues appropriately


Where toxic combinations of permissions exit


How automated system interact throughout environments

Without comprehensive visibility, governance is reactive, fragmented, and ineffective.
Trevonix's perspective is clear: Organisations cannot manage identity risk they cannot see.

Modern identity security, therefore, requires:


Complete visibility across all identities


Continuous governance rather than periodic review


Risk based prioritisation


Consistent controls across human and non-human access


Capability to support automation and AI safely

Converged identity platforms, provide the foundation for achieving this at enterprise scale.

trevonix

The Identity Challenge in a Digitally Driven World

From Workforce Access to Autonomous Operations
Conventional identity governance assumed employees were the primary actors in enterprise systems. Today, organisations operate in complex ecosystems in which software interacts with software at scale.

Examples include:

- Cloud-native applications and microservices
- Customer-facing digital applications
- Automated business workflows
- Data pipelines and analytics engines
- Third-party integrations
- AI-driven decision systems

Every engagement depends on identities that authenticate, authorise, and execute actions across systems. Automation and AI accelerate this shift by enabling autonomous agents to initiate transactions, access sensitive data, and modify systems without human involvement.

trevonix

The Visibility Gap

Why Fragmented Strategies Fail
Many organisations still rely on disconnected tools and processes to manage identity governance, privileged access, and cloud security.

Common challenges comprise:

- Incomplete inventory of identities.
- Limited visibility into cloud and SaaS environments.
- Week oversight of service accounts.
- Inconsistent policies across systems.
- Lack of context for risk decisions.
- Manual certification procedures.

These gaps create blind spots that undermine security, compliance, and functional resilience. A converged identity platform does this by providing a unified view of all identities and access relationships, enabling organisations to understand how permissions function across the enterprise.

trevonix

Non-Human Identities: The Fastest-Growing Attack Surface

Automation, digital transformation, and AI introduce large numbers of machine identities that commonly lack lifecycle management and accountability.

These include:

- AI agents
- Service accounts
- Application identities
- Workload credentials
- API keys and tokens
- Bots and automation accounts
- Integration identities

Since these identities operate continuously, they can rapidly accumulate privileges and remain active indefinitely.

Risk-based governance instead of static controls

Periodic access reviews cannot keep pace with dynamic environment. Modern identity governance must be continuous and contextual, focusing on exposures that materially threaten business operations.

Key capabilities include:

- Identification of toxic permission combinations
- Detection of segregation-of-duties conflicts
- Analysis of access paths across systems
- Prioritisation of remediation based on risk
- Automated enforcement of policies

This approach lets organisations reduce risk efficiently, rather than reviewing every access equally.

trevonix

Competent governance requires the ability to:

- Map relationships between identities and resources
- Discover non-human identities throughout environments
- Identify ownership and purpose
- Track lifecycle changes
- Detect orphaned or excessive access

Converged identity platforms enable organisations to manage these identities with the same rigour as they manage human identities.

Governing Privileged and High-Risk access

Privileged access presents disproportionate risk because it enables broad system control. Conventional models often grant persistent administrative rights, which create large attack surfaces. A modern approach substitutes standing privileges with time-Bond access granted only when required and automatically revoked afterwards.

Benefits include:

- Reduced exposure from compromised credentials
- Enforcement of least-privilege principles
- Improved accountability and traceability
- Sustaining productivity without sacrificing security

Platforms enable this through policy - driven elevation, approval, workflows, and monitoring capabilities.

trevonix

Securing External and Third-Party Access

Most organisations rely heavily on suppliers, contractors, partners, and service providers. External identities frequently fall outside traditional employee governance processes yet may still require access to sensitive systems.

Effective management includes:

- Structured onboarding and offboarding
- Risk-based provisioning
- Delegated administration where appropriate
- Continuous certification
- Automated removal of access when no longer required

This approach lowers supply-chain risk while enabling collaboration.

Continuous Compliance inside Dynamic Environments

Regulatory expectations increasingly require organisations to demonstrate ongoing control rather than periodic compliance.

Effective management includes:

- Live monitoring of access changes
- Automated certification campaigns
- Policy enforcement Consolidated
- Reporting
- Audit-ready evidence

This reduces audit effort and strengthens confidence in the effectiveness of controls.

Enabling Safe Adoption of Automation and AI

Automation and AI initiatives depend on broad access to data and systems. Without strong identity controls, these capabilities can introduce systemic risk.

Good governance enables organisations to:

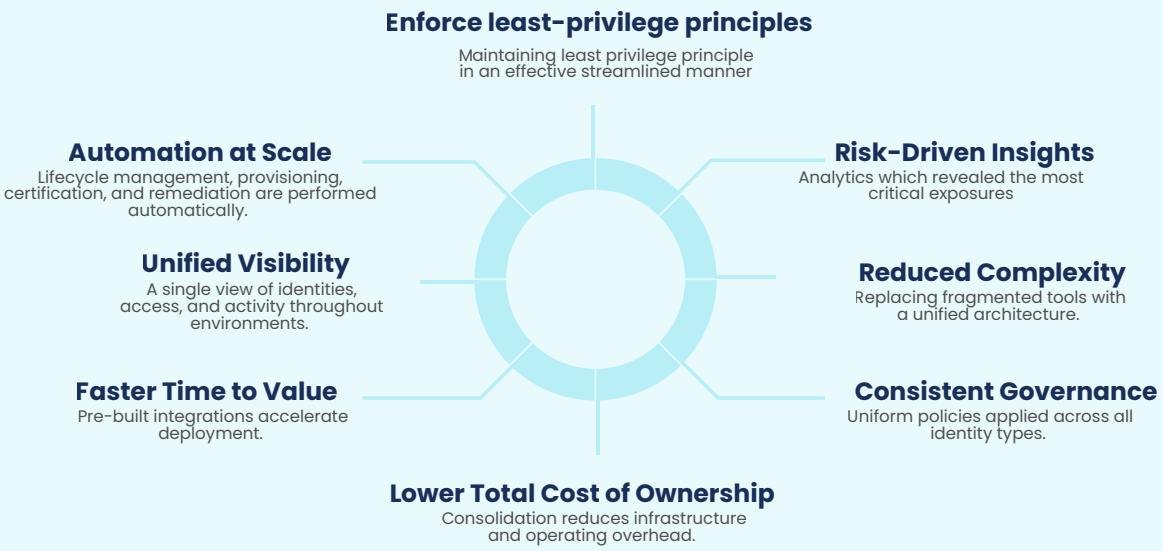
- Control what automated systems can access
- Enforce least-privilege principles
- Monitor autonomous actions
- Maintain accountability
- Secure sensitive data

Identity governance acts as the foundation for the responsible application of advanced technologies.

trevonix

The Value of a Converged Identity Platform

Managing modern identity risk requires more than using individual tools. A converged platform approach delivers:



A converged platform brings together governance, privileged access, and identity security capabilities within a single unified solution.

The Trevonix Perspective : Technology Plus Transformation

Technology alone does not deliver effective identity governance. Successful programmes require alignment across strategy, processes, operating models, organisational, accountability.

Trevonix supports organisations through:

- Identity maturity assessment
- Risk-aligned roadmaps
- Target operating model design
- Implementation guidance
- Adoption and change management
- Continuous improvement

trevonix

When appropriate, Trevonix facilitates engagement with platform specialists to explore feasible implementation approaches customised to each organisation's needs.

Conclusion

As organisations transition toward automated, digitally driven operations, identity governance becomes central to security, resilience, and trust. Converged identity platforms such as Saviynt Identity Cloud provide the visibility, control, and automation required to manage modern identity risk at scale.

Organisations that establish governance across all identities, human and non-human, will be more likely to innovate safely and maintain assurance for customers, regulators, and stakeholders. Those that do not risk operating with hidden vulnerabilities embedded within their own digital infrastructure.

Confidential Executive Briefing Offer

Trevonix offers organisations a confidential, no-obligation discussion to explore:

- Identity risks specific to your environment
- Practical approaches to improving governance
- Observed maturity patterns across industries
- How converged identity platforms are being used in practice

At your request, this discussion can include Saviynt specialists to provide technical perspectives and answer detailed questions.