



THE

IDENTITY ACCELERATION IMPERATIVE

A practical framework for securing human, machine & AI identities

ONE PLATFORM

Identity, Access and AI

Connect legacy and modern environments. Automate identity operations. Detect access changes. Govern every identity.

Secure Identities. Simplify Access. Scale Faster.

BRIDGESOFT

Executive Summary

Identity is now a platform-level capability - not a collection of disconnected IAM projects.

Identity has become foundational infrastructure for the modern enterprise. Organizations manage workforce identities alongside applications, APIs, service accounts, cloud workloads, machine identities, bots and AI agents while continuing to operate legacy systems, cloud platforms and SaaS environments.

The challenge is to strengthen security, governance and accountability without making every transformation initiative wait on identity integration and manual operational work. Identity acceleration addresses this by creating a repeatable operating model that connects, automates, observes, governs and extends identity capabilities.

CONNECT Integrate ecosystems	AUTOMATE Operate at scale	DETECT Observe changes	GOVERN Control access	ADAPT Extend identity
--	-------------------------------------	----------------------------------	---------------------------------	---------------------------------

CONNECT Connect legacy and modern identity ecosystems through an integration and orchestration layer.	AUTOMATE Automate lifecycle, access and governance operations, while accelerating IAM testing and deployment.
DETECT Continuously identify application-level access changes, anomalies and governance blind spots.	GOVERN Turn visibility into explainable, reviewable and accountable access decisions.
ADAPT Extend identity controls to human, machine and AI identities, including AI agents and automated workloads.	OUTCOME Modernize progressively without requiring wholesale replacement of existing identity investments.

The Identity Landscape Has Changed

The enterprise identity estate now spans human, machine and AI actors across hybrid environments.

A typical enterprise identity environment includes employees, contractors, partners and customers, but also applications, APIs, service accounts, cloud workloads, containers, devices, bots, machine identities and AI agents.

22% VERIZON 2025 DBIR Compromised credentials were an initial access vector in reviewed breaches.	30% IBM X-FORCE 2025 Abuse of user identities occurred in cases examined.	97% MICROSOFT 2025 Identity attacks observed by Microsoft were password spray attacks.
--	--	---

These figures come from different datasets, populations and methodologies. They should be interpreted individually rather than combined into one comparable population.

HUMAN Employees, contractors, partners and customers	MACHINE Service accounts, workloads, applications, APIs, devices and bots
AI AI agents, AI applications and autonomous workflows	HYBRID ESTATE Legacy systems, cloud platforms, SaaS and existing security investments

Identity therefore becomes a central control point for both transformation and cyber resilience: the more systems and digital actors an enterprise connects, the more important it becomes to make identity integration, lifecycle, visibility and governance repeatable.

Research references: Verizon 2025 DBIR; IBM X-Force Threat Intelligence Index 2025; Microsoft Digital Defense Report 2025; NIST SP 800-63-4 (2025).

Identity Can Become a Transformation Bottleneck

Enterprise identity programs often carry the integration and governance complexity of every application, platform and workflow they support.

LEGACY APPLICATIONS Limited integration options and inconsistent identity interfaces can slow onboarding.	MULTIPLE REPOSITORIES Identity data and access relationships may be distributed across directories, applications and security platforms.
MANUAL OPERATIONS Provisioning, approvals, reviews and exception handling can create delays and administrative effort.	INCONSISTENT ACCESS MODELS Different systems may use different roles, entitlements and authorization patterns.
CUSTOM INTEGRATION DEPENDENCIES One-off connectors and scripts increase engineering dependency and maintenance overhead.	GOVERNANCE COMPLEXITY Organizations need continuous visibility and defensible decisions across changing environments.

Identity modernization should be measured by business outcomes as well as technical completion.

- Faster application onboarding
- Reduced provisioning and deprovisioning time
- Greater governance and compliance coverage
- Lower administrative effort and better operational efficiency
- Faster detection and response to access changes

TRADITIONAL IAM VS. IDENTITY ACCELERATION

TRADITIONAL IAM	IDENTITY ACCELERATION
Project-centric implementation	Platform/capability-centric architecture
Heavy reliance on custom integrations	Reusable integration and orchestration patterns
Manual operational effort	Automated identity operations
Periodic reviews and governance	Continuous visibility and governance
Workforce-focused controls	Human, machine and AI identity governance
Limited application-level change visibility	Native and AI-enabled change detection
Slow application onboarding	Accelerated onboarding and modernization

What an Identity Acceleration Platform Should Look Like

A platform-centric architecture connects identity capabilities into one operating model for the enterprise.

Before technology choices are made, the target operating model should be clear: identity acceleration works when integration, reusable patterns, lifecycle automation, continuous visibility and governance operate as one connected capability - across human, machine and AI identities.

ENTERPRISE IDENTITY ECOSYSTEM	IDENTITY ACCELERATION PLATFORM	BUSINESS BENEFITS
Legacy applications Cloud / SaaS Directories / HR ERP / CRM Databases / APIs Existing IAM	Platform-centric architecture Reusable integration patterns Automated lifecycle governance Continuous visibility & governance Human, machine & AI identity governance Native change detection Accelerated onboarding	Cost Efficiency Productivity Security

1. CONNECT Bring systems and identity sources together	2. AUTOMATE Standardize repeatable lifecycle operations	3. DETECT See application and access changes continuously	4. GOVERN Apply policy, role, review and accountability	5. ADAPT Extend controls to machine and AI identities
6. CONNECTED CAPABILITIES Bring platform-centric architecture, reusable integration patterns, lifecycle automation, continuous visibility, identity governance, change detection and accelerated onboarding together.				

The result is a repeatable identity foundation that supports business transformation while maintaining security, governance and accountability.

From Platform Model to Bridgesoft Solution

Bridgesoft brings the identity acceleration capabilities together so enterprises can modernize progressively and execute faster.

FRAMEWORK	BRIDGESOFT CAPABILITY	WHAT IT ENABLES
CONNECT	Bridgesoft Identity Gateway (BIG)	Identity integration and orchestration across IAM platforms, governance systems, directories, applications, databases, APIs and legacy environments.
AUTOMATE	IAM / IGA + IAG Automation Suite	Lifecycle, access and governance workflows; IAM testing, validation, deployment acceleration and operational automation.
DETECT	Native Change Detection + AI-enabled Change Detection	Application-level access change visibility, anomaly detection, monitoring and governance risk insights.
GOVERN	IGA + Access Recon + Role Analytics	Lifecycle governance, certifications, audit readiness, role and entitlement analysis, least privilege and compliance.
ADAPT	NHI + AI Identity Governance	Discovery, ownership, authorization, monitoring, risk and lifecycle controls for AI agents and non-human identities.
SECURE ACCESS	SSO + MFA + Advanced Authentication	Stronger access assurance across critical enterprise resources.
IMPLEMENT	IAM / IGA Implementation + Cloud IAM Services	Plan, deploy, integrate, configure, optimize and support identity capabilities.

Implementation acceleration comes from reducing custom engineering, reusing proven integration and workflow patterns, automating repeatable tasks, and validating changes earlier in the delivery cycle.

40%

PLATFORM BENEFIT: FASTER IAM IMPLEMENTATION TIMELINES

A key platform benefit is the ability to accelerate IAM implementation timelines by up to 40%, helping teams move from integration and deployment effort toward business outcomes sooner. Results vary by scope, environment and implementation complexity.

CONNECT + AUTOMATE

Connect the ecosystem before you replace it. Then automate the identity operations that run across it.

Bridgesoft Identity Gateway provides the integration and orchestration layer between modern identity platforms and complex enterprise environments. The goal is not to eliminate every existing system; it is to create controlled movement of identity data and access processes across them.

BRIDGESOFT IDENTITY GATEWAY (BIG) Universal identity connectivity, reusable integration patterns, API-based orchestration, identity synchronization and accelerated application onboarding across cloud, on-premises and hybrid environments.	IAM / IGA LIFECYCLE AUTOMATION Provisioning, deprovisioning, access requests, approvals, role assignment, access reviews and exception handling.
IAG AUTOMATION SUITE IAM testing, validation, deployment acceleration and operational process automation to reduce deployment risk and improve consistency.	CONNECT BEFORE YOU REPLACE Extend and modernize existing investments progressively instead of forcing a wholesale replacement program.

REQUEST Access or identity action	POLICY Evaluate rules and context	APPROVE Route decisions	PROVISION Automate fulfillment	VERIFY Validate outcome	GOVERN Review continuously
---	---	-----------------------------------	--	-----------------------------------	--------------------------------------

The architecture becomes reusable: each new application, identity source or workflow can follow established patterns instead of becoming a new one-off implementation.

ADAPT - Govern Human, Machine & AI Identities

Identity controls must extend beyond people to every digital actor that can reach enterprise resources.

Bridgesoft extends governance to AI agents, service accounts, RPA bots, machine identities, application accounts, APIs and automated workloads. This creates one governance model for digital actors with different lifecycles, permissions and risk profiles.

HUMAN Employees, contractors, partners and customers	AI AGENTS Autonomous agents that can initiate tasks, call tools and access enterprise resources	SERVICE ACCOUNTS Application and system identities used by automated processes
RPA BOTS Bots executing repeatable workflows and transactions	MACHINE IDENTITIES Workloads, devices, certificates and application identities	APIs & WORKLOADS Technical identities that enable machine-to-machine activity

AI AGENT TRACKING: WHAT IS MONITORED?

CONTROL	CONTINUOUS MONITORING
Access boundaries	Which applications, APIs, data services and enterprise resources the agent is permitted to access.
Session duration	When a session starts, how long the agent remains active, and whether the duration aligns with the expected task.
Session exit	Whether the agent terminates access as expected, how the session ends, and whether residual access remains.
Behavior & changes	Changes in permissions, unusual access patterns, unexpected destinations or activity outside the approved boundary.

This turns “AI agent monitoring” into an operational control: define the boundary, observe activity within it, evaluate duration, monitor exit and trigger review when behavior moves outside the expected pattern.

Track the Identity, the Access Boundary and the Session

Effective AI-agent governance requires visibility into what the agent can reach and how its access behaves over time.

A non-human identity governance model should answer not only “who or what is this identity?” but also “what is it allowed to reach, what did it actually reach, how long did it remain active, and did the session end as expected?”

DISCOVER Find agents, service accounts, bots and workloads	REGISTER Assign owner, purpose and identity	BOUNDARY Define applications, APIs and resources in scope	AUTHORIZE Apply least privilege and policy	MONITOR Observe access and session activity	EXIT Confirm session termination and residual access	REVIEW Investigate exceptions and certify controls
--	---	---	--	---	--	--

AI AGENT CONTROL	WHAT TO CAPTURE	WHY IT MATTERS
Identity & ownership	Agent identity, owner, business purpose, environment	Creates accountability for every autonomous actor.
Application boundary	Allowed applications, actions and data zones	Limits where the agent can operate.
API boundary	Permitted APIs, endpoints, scopes and methods	Controls machine-to-machine reach.
Session duration	Start time, elapsed duration, inactivity and task window	Identifies overlong or unexpected sessions.
Session exit	Exit event, token/session termination, residual access	Confirms access is closed when work is complete.
Behavior	Expected vs. observed access and sequence	Highlights anomalies and potential misuse.
Change detection	Permission, role, configuration and access changes	Makes governance responsive to application-level changes.

CONTROL LOOP

CONTINUOUS AI AGENT GOVERNANCE
Discover → Define boundaries → Authorize → Monitor → Check duration → Confirm session exit → Detect changes → Review / remediate.

AI Identities Require Governance, Not Just Access

AI models, applications and autonomous agents can access enterprise systems - so their identities need lifecycle, policy, monitoring and accountability.

AI identity governance should combine registration and ownership with controlled access, continuous activity monitoring and measurable risk management. The objective is to make autonomous access explainable and auditable without preventing useful automation.

CAPABILITY	HOW IT WORKS	GOVERNANCE OUTCOME
AI agent discovery	Identify AI agents and the enterprise resources they interact with.	Known AI identity population.
Identity registration	Register the agent, owner, purpose and environment.	Accountability and lifecycle ownership.
Access approval	Route access requests through policy and approval workflows.	Controlled authorization.
Boundary enforcement	Limit access to approved applications, APIs, data and actions.	Least-privilege operating envelope.
Activity monitoring	Continuously observe access behavior, session duration and session exit.	Operational visibility.
Risk assessment	Identify unusual behavior, excessive access and policy exceptions.	Prioritized remediation.
Compliance reporting	Produce evidence for reviews, audits and policy checks.	Audit readiness.
Policy enforcement	Apply changes, revoke access or require review when conditions are violated.	Responsive governance.

SSO Simplify and secure access across applications with centralized authentication.	MFA Strengthen access assurance with adaptive multi-factor authentication.
GOVERNANCE Extend IGA, NHI and AI governance beyond the login event into lifecycle, policy and review.	ONE PLATFORM Bring identity governance, access management, integration and non-human identity controls together across hybrid environments.

The broader principle is simple: every identity that can access an enterprise resource should have an understandable lifecycle, accountable ownership, appropriate authorization and observable activity.

Measure Identity Acceleration With an Operational Scorecard

Identity modernization becomes meaningful when architecture improvements translate into measurable outcomes.

METRIC	WHAT TO TRACK
Integration time	Time to onboard applications and connect identity sources.
Provisioning / deprovisioning	Elapsed time, automation rate and manual intervention.
Automation rate	Percentage of recurring identity operations handled through workflows.
Change detection time	Time between an application-level access change and its detection / review.
Application coverage	Applications and identity sources connected to governance and monitoring.
Review completion	Access certification and governance review completion.
Manual effort	Hours or tasks requiring repetitive administrative work.
Machine identity coverage	Percentage of identified non-human identities with ownership, governance and lifecycle controls.
AI identity coverage	AI agents / identities discovered, registered, governed and monitored.
Exception rate	Unresolved policy exceptions, unmanaged access or control gaps.

PRACTICAL MATURITY PATH

CONNECT Connect priority systems	AUTOMATE Standardize operations	DETECT Add change visibility	GOVERN Expand certification and control	ADAPT Govern machine and AI
--	---	--	---	---------------------------------------

EXECUTIVE EVALUATION QUESTIONS

- Which identity sources and applications remain disconnected?
- Which lifecycle steps remain manual and how much effort do they consume?
- How quickly can application-level access changes be detected and reviewed?
- Which roles and entitlements are difficult to explain or certify?
- How much of the machine and AI identity population is known, owned and governed?

Modernize Without Losing Momentum

Identity acceleration is both an architecture model and a delivery model.

The delivery model starts with the target state and then moves through integration, configuration, validation and optimization. Existing investments remain part of the architecture while reusable patterns and automation reduce the amount of work required for every new initiative.

PLAN Priorities, dependencies, roadmap	DEPLOY Solution deployment	INTEGRATE Systems, apps, identity sources	CONFIGURE Policies, roles, workflows	OPTIMIZE Performance, governance, adoption	SUPPORT Ongoing operations and improvement
--	--------------------------------------	--	---	---	---

THE FUTURE OF IDENTITY IS HUMAN + MACHINE + AI

Enterprise identity environments are converging across legacy systems, cloud platforms, SaaS applications, APIs, workloads and AI. The operating model is moving from manual and periodic activity toward automated, continuous and context-aware identity controls.

CONNECT Integrate	AUTOMATE Operate	DETECT Observe	GOVERN Control	ADAPT Extend
-----------------------------	----------------------------	--------------------------	--------------------------	------------------------

The practical sequence is straightforward: connect the ecosystem, automate identity operations, detect changes, govern access and adapt controls to human, machine and AI identities.

Bridgesoft - One Platform for Identity, Access and AI

Secure identity foundations for modern, hybrid enterprise environments.

Bridgesoft helps enterprises simplify complex identity environments by connecting, automating and governing identity across legacy systems, modern applications and emerging digital environments.

IDENTITY GATEWAY Connect IAM platforms, governance systems, directories, applications, databases, APIs and legacy systems across hybrid environments.	IAM / IGA Automate identity lifecycle, access governance, approvals, reviews, roles, policy and compliance processes.
CHANGE DETECTION Use Native Change Detection and AI-enabled change detection to improve visibility into application-level changes and anomalies.	ROLE & GOVERNANCE INTELLIGENCE Use Access Recon and Role Analytics to support certifications, audit preparation, role analysis, least privilege and compliance.
NHI & AI IDENTITY Govern AI agents, service accounts, bots, machine identities, application accounts, APIs and workloads.	ACCESS & SERVICES Strengthen SSO/MFA and use implementation and Cloud IAM services to deploy, integrate, configure and optimize identity capabilities.

READY?

ACCELERATE YOUR IDENTITY TRANSFORMATION
Connect legacy and modern environments. Automate identity operations. Detect access changes. Govern every identity.

ONE PLATFORM FOR IDENTITY, ACCESS AND AI

BOOK A FREE DEMO | Talk with an IAM architect about your infrastructure, priorities and deployment timeline.

REFERENCES & RESEARCH

- NIST: SP 800-63-4 - Digital Identity Guidelines (2025).
- CISA: Zero Trust Maturity Model, Version 2.0.
- Gartner: 2025 research on machine identity and IAM for AI agents.
- Microsoft: Digital Defense Report 2025.
- IBM: X-Force Threat Intelligence Index 2025.
- Verizon: 2025 Data Breach Investigations Report.
- Google Cloud: security guidance and research on AI-agent governance, agent identities, access controls and non-human identities.

Statistics should be interpreted according to the methodology, population and definitions used by each source.