ARCON

CONVERGED IDENTITY PLATFORM

Unified Identity Security Platform for

Human | Non-Human | Privileged | Non-Privileged

Predict | Protect | Prevent

www.arconnet.com

EXECUTIVE SUMMARY

Identity as the Security Perimeter

The enterprise perimeter has shifted. It is no longer defined by a firewall or a data center boundary. Today, every identity that connects to an application, a workload, a privileged account, or a cloud resource is an entry point — and a potential attack vector.

Organizations are accelerating cloud adoption, embracing hybrid workforces, deploying SaaS at scale, automating operations, and distributing infrastructure across multiple clouds. Every wave of modernization creates new identities: employees, administrators, contractors, vendors, service accounts, APIs, bots, cloud workloads, Kubernetes pods, and DevOps pipelines. Each one represents access. Each one represents risk.

Yet most enterprises still manage this identity landscape with a fragmented stack of disconnected tools — separate consoles for IAM, PAM, IGA, MFA, CIEM, and endpoint privilege. These siloed solutions create inconsistent policies, visibility gaps, governance blind spots, and growing operational complexity. The gaps between them are precisely where modern breaches occur.

> ***Over 80% of enterprise breaches involve compromised credentials or identity-related vulnerabilities. The answer is not more tools. It is a unified identity fabric.***

ARCON Converged Identity Platform is the answer to this challenge. It brings IAM, IGA, PAM, CIEM, MFA, EPM, digital vaulting, machine identity governance, behavioral analytics, and risk intelligence into one centralized platform — unified by a single control plane, a shared policy engine, and a consistent governance experience.

Unlike platforms assembled through acquisitions that bolt tools together, ARCON was architected from the ground up as a converged identity platform. Built on a cloud-native architecture with independently deployable microservices, ARCON delivers unified identity governance without the complexity of managing multiple vendors, multiple contracts, and multiple operational models.

The result is an identity security platform that reduces risk, accelerates compliance, lowers operational cost, and enables enterprises to modernize at their own pace — without ripping out existing investments.

THE CHALLENGE

The Identity Explosion

Modern enterprises no longer manage users. They manage identities — millions of them, spread across on-premises systems, cloud platforms, SaaS applications, and automated pipelines. Every identity is an access point. Every unmanaged identity is a risk.

Today's enterprise identity landscape has expanded far beyond the traditional workforce user. Understanding the full scope of what must be governed is the first step toward securing it.

Human Identities

Employees, administrators, contractors, vendors, remote workers, temporary staff, break-glass accounts, and third-party partners. These identities require lifecycle management from day one — provisioning at onboarding, modification at role change, and clean revocation at exit.

Privileged Identities

System administrators, database administrators, DevOps engineers, cloud operations teams, security personnel, and vendor support accounts. These identities have elevated access to critical systems and represent the highest-value targets for attackers.

Machine & Non-Human Identities

Service accounts, API keys, SSH keys, certificates, tokens, automation accounts, bots, robotic process automation (RPA) agents, and workload identities. Machine identities now outnumber human identities in most enterprises — and they are the fastest-growing and least-governed segment of the identity estate.

Cloud & Workload Identities

AWS IAM roles and users, Azure Managed Identities, GCP service accounts, OCI IAM identities, Kubernetes workloads, container identities, DevOps pipeline credentials, and SaaS application identities. Cloud identities are dynamic, ephemeral, and frequently over-provisioned.

> ***Every unmanaged identity is an open door. Every excessive entitlement is an unguarded window. The enterprise attack surface is now defined by the breadth and depth of its identity estate.***

As organizations expand across hybrid and multi-cloud environments, the challenges compound: identity visibility degrades, access governance becomes inconsistent, compliance reporting grows complex, and operational teams are overwhelmed managing disconnected tools.

The volume, velocity, and variety of modern enterprise identities demand a fundamentally different approach — one that converges governance, access control, and risk intelligence into a single operational framework.

THE PROBLEM

The Cost of Fragmented Identity Security

Most enterprise identity environments are not platforms. They are stacks — separate tools for IAM, PAM, IGA, MFA, CIEM, endpoint privilege, and secrets, each operating in isolation with its own console, its own policies, and its own data model.

The gaps between these disconnected tools are where governance breaks down, where attackers move laterally, and where compliance evidence is hardest to produce. Fragmented identity security does not just create operational complexity — it creates security risk.

Key Consequences of Identity Fragmentation

Disconnected identity context	No unified view across users, entitlements, sessions, workloads, and secrets
Inconsistent policy enforcement	Each tool enforces policies independently — access controls are never truly aligned
Increased operational complexity	Multiple consoles, workflows, and databases drain IAM team capacity
Higher integration overhead	Maintaining point-to-point integrations increases deployment and support costs
Limited identity visibility	Siloed architectures prevent unified risk visibility across all identity types
Audit and compliance gaps	Fragmented reporting complicates certification campaigns and regulatory audits
Expanded attack surface	Unmanaged identities, standing privileges, and shadow access create exploitable gaps
Poor lifecycle governance	Joiners, movers, and leavers fall through the cracks of disconnected systems

> ***The average enterprise manages identity risk across 7 or more disconnected tools. Each integration point is a potential failure point — operationally, financially, and from a security standpoint.***

The modern enterprise requires a converged identity strategy — one built on centralized governance, unified visibility, and a consistent policy engine that spans every identity type, every environment, and every access scenario.

THE SOLUTION

Introducing ARCON Converged Identity Platform

One platform. Every identity. Unified governance. ARCON Converged Identity Platform brings IAM, IGA, PAM, CIEM, EPM, MFA, vaulting, machine identity governance, behavioral analytics, and risk intelligence into a single operational framework.

Unlike fragmented identity environments that rely on multiple disconnected tools, ARCON Converged Identity Platform provides a unified control plane for identity lifecycle management, privileged access, governance, cloud entitlements, machine identities, authentication, and risk intelligence. Organizations gain centralized visibility, consistent policy enforcement, and modern identity security — without disruptive platform replacement.

> ***Built on a unified cloud-native platform architecture with independently deployable microservices, shared policy services, integrated identity intelligence, and a consistent operational experience.***

What ARCON Converges

Workforce IAM	Identity Governance & Administration	Privileged Access Management
Cloud Entitlement Management	Endpoint Privilege Management	Multi-Factor Authentication
Digital Vault & Secrets	Machine Identity Governance	Identity Intelligence & Analytics

Built for Progressive Identity Modernization

ARCON is designed for the real world — where enterprises have existing investments, ongoing programs, and cannot afford a complete platform rip-and-replace. Organizations can adopt ARCON incrementally:

- Start with a single module — PAM, IGA, or CIEM — and expand over time
- Coexist with existing IAM, MFA, or ITSM solutions
- Integrate ARCON's governance layer alongside current platforms
- Progressively consolidate identity operations as confidence grows
- Protect existing investments while adding new capabilities

This flexibility makes ARCON the right platform for organizations at every stage of their identity security journey — from first deployment to full convergence.

ARCHITECTURE PRINCIPLES

Principles That Shape Every Layer

ARCON Converged Identity Platform is not simply a collection of features. It is built on five architectural principles that ensure every capability — from authentication to vault to analytics — operates as part of a coherent, unified identity platform.

- **Unified Identity Fabric**

One control plane spanning human identities, privileged accounts, machine identities, cloud workloads, and SaaS applications. Every identity type is governed through a single operational framework — with shared workflows, unified policies, and consistent audit trails. No siloes. No context switching. No governance gaps.

- **Modular Microservices**

ARCON delivers capabilities through independently deployable microservices — IAM, PAM, IGA, CIEM, EPM, and analytics can be deployed as a complete platform or as individual services alongside existing tools. Each service scales independently, updates independently, and integrates cleanly with the shared control plane. Organizations get platform power with deployment flexibility.

- **Vault-First Security**

Every sensitive credential, secret, certificate, API key, and token is protected by cryptographic vaulting at its core. ARCON's vault architecture supports HSM integration, FIPS-aligned key handling, AES-256 encryption, and automated rotation — making secure credential management a foundation, not an afterthought.

- **Policy-Driven Access**

Access decisions across the platform are governed by declarative, versioned policies — RBAC, ABAC, Separation of Duties (SoD), and Just-In-Time (JIT) controls. Policies are defined once, applied consistently, and audited continuously. This eliminates the policy drift that emerges when governance rules are scattered across multiple tools.

- **Observability & Auditability**

Every identity action — authentication, authorization, privilege elevation, access request, or policy change — generates an evidence trail. ARCON provides end-to-end audit logging, session capture, SIEM forwarding, compliance dashboards, and evidence-ready reports. Compliance is not a project — it is a continuous byproduct of how the platform operates.

PLATFORM ARCHITECTURE

Multiple Layers. One Identity Fabric.

From identity consumers at the top to protected resources at the base — every layer of the ARCON architecture is decoupled, observable, and policy-aware. Together, they form a complete identity security stack for hybrid, cloud, and on-premises environments.

Platform Layer	Components
Identity Consumers	Business users · Privileged users · Third-party users · Machine identities · Cloud workloads · DevOps pipelines · Service accounts
Authentication & Access	SSO · MFA · Adaptive authentication · JIT · Secure web gateway · Secure remote access
Unified Control Plane	IAM engine · PAM engine · IGA engine · CIEM engine · EPM engine · Policy engine · Workflow engine
Intelligence & Governance	Knight Analytics · Risk scoring · Session monitoring · Access reviews · Governance campaigns · Compliance reporting
Vault & Integration Foundation	Password Vault · Digital Vault · My Vault · Secrets management · HSM integration · API gateway · Connector suite · SIEM / ITSM / DevOps
Protected Resources	Business apps · SaaS · Endpoints · Databases · Servers · Network devices · Cloud resources · Kubernetes · DevOps tools · OT / IoT

Security Architecture

Every layer is engineered for regulated environments. ARCON enforces defence-in-depth across cryptography, network, access, audit, and resilience:

- FIPS-aligned cryptography with HSM-backed key handling
- AES-256 encryption at rest and in transit
- End-to-end audit logging and session recording
- SIEM forwarding to Splunk, QRadar, ArcSight, and many more via Syslog and API.
- HA clustering, backup, and disaster recovery
- Secure APIs with role-based access controls

IDENTITY LIFECYCLE

The Identity Lifecycle, End to End

Every identity in the enterprise follows a lifecycle — from initial discovery through onboarding, authentication, authorization, governance, vaulting, monitoring, and reporting. ARCON governs that entire lifecycle through a single platform.

Most enterprises manage different lifecycle stages with different tools — creating handoff gaps, governance blind spots, and audit complexity. ARCON closes those gaps by governing the complete identity lifecycle in one operational framework.

Lifecycle Stage	ARCON Capabilities
DISCOVER	Identity & entitlement discovery · Shadow access surface mapping · Cloud identity visibility · Machine identity detection
ONBOARD	HRMS-driven JML automation · Role-based birthright access · Policy-driven provisioning · Automated account creation
AUTHENTICATE	SSO · MFA (OTP, biometric, push) · Adaptive authentication · Risk-based access signals
AUTHORIZE	RBAC / ABAC enforcement · JIT & approval workflows · SoD policy checks · Least-privilege controls
GOVERN	Access certifications · SoD & exception management · Role governance · Entitlement reviews
VAULT	Credential vaulting · Secrets management · Certificate lifecycle · Automated rotation & check-out
MONITOR	Session recording · Behavioural analytics · Anomaly detection · Privileged activity intelligence
REPORT	Compliance dashboards · Audit-ready evidence · Risk reporting · Governance campaign visibility

Discover → Onboard → Authenticate → Authorize → Govern → Vault → Monitor → Report. One continuous governance loop, across every identity in the enterprise.

UNIFIED WORKSPACE

Identity Hub — One Workspace for Every Persona

ARCON Identity Hub is the unified workspace that brings every identity experience into one consistent, role-aware surface. Employees, managers, approvers, administrators, and auditors each get a personalised view of the capabilities relevant to their role.

Traditional identity environments force users to navigate multiple portals, request through different channels, and find credentials across separate systems. Identity Hub eliminates that friction — delivering a single front-door for every identity-related task.

What Users Can Do in Identity Hub

Capability	What It Does	How It Works
My Apps	Access all authorised applications in one click	No password prompts, no navigation
Access Requests	Request access to apps, assets, or elevated rights	Tracked, routed, auto-approved or escalated
My Vault	Retrieve personal credentials, secure notes, and secrets	Vaulted, governed, and auditable
Sessions	Launch and monitor privileged sessions directly	Session control and recording built in
Reports	View personal access history, certifications, and usage	Compliance-ready evidence on demand
Profile	Manage authentication factors and access preferences	Self-service, IT-governed

Purpose-Built Consoles for Every Operator

- Identity Hub — Unified workspace for users: apps, requests, profile, and resources
- Administration Console — Single pane for policy management, role configuration, and workflow orchestration
- Password Vault — Enterprise vault for privileged credentials with rotation and check-out controls
- My Vault — User-level vault for personal credentials, secrets, and secure notes
- Digital Vault — Secure storage and sharing of files, certificates, and sensitive assets
- Knight Analytics Console — Behavioural and risk analytics across identity and access activity
- Console — Inspection-grade visibility into privileged sessions and commands

PLATFORM CAPABILITY — 01

Workforce Identity & Access Management

Every employee, contractor, and partner deserves frictionless access to the resources they need — and nothing more. ARCON Workforce IAM delivers seamless, secure access through SSO, adaptive MFA, and automated lifecycle management.

Workforce IAM is the foundation of enterprise identity security. When it works well, users move faster and IT operates smarter. When it fails, helpdesk calls mount, shadow IT grows, and security posture degrades. ARCON makes it work well.

Key Capabilities

Single Sign-On (SSO)

Centralized application access across web, cloud, and on-premises applications using SAML, OAuth, and OIDC. Users authenticate once and access everything they need — reducing password fatigue and support overhead while improving the user experience.

Multi-Factor Authentication (MFA)

OTP-based, push notification, biometric, QR-code, hardware token, and facial recognition — supporting every authentication scenario from mobile workforce to high-security system access. Third-party MFA integration supported where existing investments are in place.

Adaptive Authentication

Risk-based access decisions that consider device posture, geo-location, IP reputation, time of access, and user behaviour. When risk signals are elevated, ARCON automatically steps up authentication requirements — protecting assets without adding friction to normal access patterns.

Identity Lifecycle Management

HRMS-driven automation for Joiner-Mover-Leaver workflows. New users receive birthright access based on role models at onboarding. Role changes trigger access modifications automatically. Departing users are deprovisioned completely and immediately — eliminating orphaned accounts and access creep.

Runtime Access Control

Dynamic access controls that enforce entitlement boundaries at runtime — ensuring users can only access what they are currently authorised to access, based on current role, current context, and current risk posture.

> ***Business Outcome: Reduce helpdesk password tickets by 60%, accelerate onboarding from days to hours, and eliminate orphaned accounts that persist after employee exit.***

PLATFORM CAPABILITY — 02

Identity Governance & Administration

Governance is not a checkbox. It is the continuous discipline of ensuring every identity has the right access, for the right reason, for the right duration — and that every access decision can be proven to an auditor.

ARCON IGA automates Joiner-Mover-Leaver processes, orchestrates access requests and certifications, enforces role governance, and provides unified visibility across entitlements, roles, departments, and cloud access — all from a single governance platform.

Governance Capabilities

Identity Lifecycle Governance

Policy-driven provisioning and deprovisioning connected directly to HRMS. Access is granted based on role models, modified when roles change, and revoked automatically at exit — with full audit trail at every step.

Access Certification Campaigns

Periodic and event-driven access reviews where managers, application owners, and compliance teams certify whether existing access is still appropriate. ARCON tracks campaign progress, sends escalation reminders, and generates certification records ready for audit.

Workflow Orchestration

Low-code workflow builder for access request automation, multi-stage approval chains, escalation management, and policy-driven provisioning. Workflows connect to ServiceNow, Jira, BMC Remedy, and other ITSM systems for ticket-based governance.

Role & Department Governance

Dynamic role management, department-level access controls, entitlement mapping, and Separation of Duties (SoD) policy enforcement. Role mining capabilities help organizations identify toxic access combinations and remediate them before they become audit findings.

Governance Visibility

Unified correlation across users, roles, entitlements, assets, permissions, cloud access, and privileged accounts — giving governance teams and auditors a complete picture of who has access to what, and why.

> ***Business Outcome: Reduce access review effort by 70%, eliminate excessive entitlements identified during certification campaigns, and produce audit evidence in minutes rather than days.***

PLATFORM CAPABILITY — 03

Privileged Access Management

Privileged accounts are the most valuable targets in any enterprise. System administrators, database administrators, cloud operations teams, and vendor support accounts all hold the keys to critical systems. ARCON PAM ensures those keys are never left unguarded.

ARCON PAM secures privileged access across enterprise infrastructures, applications, databases, cloud platforms, and business-critical systems — combining credential vaulting, session monitoring, and AI-powered intelligence into a complete privileged access governance platform.

Core PAM Capabilities

Privileged Credential Vaulting

Every privileged credential is stored in an encrypted vault with automated password rotation, credential randomization, and time-limited check-out. No administrator ever needs to know the actual password — ARCON handles injection, rotation, and audit automatically.

Just-In-Time (JIT) Access

Eliminate standing privileges with time-bound, ephemeral access grants. Administrators request elevated access, ARCON provisions it for the required window, and access expires automatically. JIT access dramatically reduces the attack surface by ensuring no privileged account is permanently active.

Session Management & Monitoring

Every privileged session is recorded, monitored in real time, and stored for audit. Video recording, command logging, keystroke capture, and session analytics provide complete visibility into what every administrator did, when, and from where.

AI-Powered Session Intelligence

ARCON transforms session recordings into actionable intelligence. The platform generates AI-driven intent summaries that describe what a privileged user was doing during a session — enabling auditors to review hours of privileged activity in minutes. Behavioural baselining and anomaly detection flag unusual commands or access patterns for immediate investigation.

> ***AI Session Intelligence: ARCON automatically summarises privileged session activity — reducing audit review time by up to 80% and surfacing behavioural anomalies that manual review would miss.***

Secure Third-Party & Vendor Access

Browser-based privileged sessions for vendors and contractors — no VPN, no agent, no credential sharing. ARCON provides controlled, recorded, time-limited access to specific systems, with full audit trail and session termination capability at any point.

PLATFORM CAPABILITY — 04

Cloud Infrastructure Entitlement Management

Cloud environments create identity and entitlement sprawl at a scale that manual governance cannot keep pace with. IAM roles, permission policies, service accounts, and cloud-native identities multiply faster than they are reviewed — creating excessive entitlements that expand the attack surface.

ARCON CIEM gives organizations complete visibility into cloud identities and entitlements across AWS, Azure, GCP, and OCI — enabling right-sizing, risk reduction, and continuous cloud access governance.

CIEM Capabilities

Cloud Identity Discovery

Discover every IAM user, role, group, service account, managed identity, and workload identity across all connected cloud platforms. ARCON maps entitlements to resources, policies to identities, and access patterns to risk — providing the cloud identity visibility that most organizations currently lack.

Entitlement Right-Sizing

Identify excessive, unused, and over-provisioned permissions across cloud platforms. ARCON's AI/ML-based risk scoring highlights the highest-risk entitlements for immediate remediation — and recommends least-privilege configurations based on actual usage patterns.

Workload & Machine Identity Governance

Govern service identities, workload identities, tokens, and certificates operating within cloud environments. Map identity-to-workload relationships, track usage, and enforce governance policies across containerized and serverless architectures.

Multi-Cloud Governance

Unified entitlement visibility and governance across AWS, Azure, GCP, OCI, and Kubernetes — from a single dashboard. No more switching between cloud consoles to understand your cross-cloud identity posture.

JIT Cloud Privileges

Extend Just-In-Time access controls to cloud environments. Cloud privileges are granted on request, limited to the required duration and scope, and revoked automatically — eliminating standing cloud permissions that create unnecessary risk.

> ***Business Outcome: Reduce your cloud attack surface by eliminating over-provisioned permissions. Organizations using ARCON CIEM routinely right-size 40-60% of cloud entitlements in their first governance campaign.***

PLATFORM CAPABILITY — 05

Endpoint Privilege Management

Every endpoint is a potential entry point. Endpoints with excessive local administrator rights — workstations, servers, developer machines — are among the most common starting points for lateral movement and ransomware attacks.

ARCON EPM enforces least privilege across Windows, Linux, Unix, and macOS endpoints — removing standing local admin rights and replacing them with controlled, policy-driven privilege elevation that preserves productivity without sacrificing security.

Endpoint Governance Capabilities

Privilege Elevation & Delegation Management (PEDM)

Users can request temporary privilege elevation for specific applications or tasks — ARCON evaluates the request against policy, grants minimum necessary privileges, logs every action, and revokes elevation automatically when the task is complete. Administrators maintain control; users maintain productivity.

Application Control

Rule-based application allow-listing and block-listing enforced at the endpoint. Only approved applications can execute. Unapproved applications — including malware delivered through phishing or download — are blocked before execution, reducing ransomware risk dramatically.

Endpoint Visibility & Monitoring

Continuous monitoring of endpoint activity including privileged actions, application execution, and access attempts. Integration with ARCON PAM enables unified visibility across server and endpoint privileged activity in a single console.

Endpoint Password Vaulting

Local administrator account credentials are vaulted and rotated automatically — eliminating the risk of shared local admin passwords that attackers exploit for lateral movement across Windows environments.

File Integrity Monitoring

Detect unauthorized changes to critical system files, configurations, and registry settings — providing early warning of compromise and ensuring configuration compliance across the endpoint estate.

> ***Business Outcome: Eliminate standing local admin rights across the workstation estate without a single helpdesk call — replacing them with governed, auditable privilege elevation that users can self-serve in seconds.***

PLATFORM CAPABILITY — 06

Machine & Non-Human Identity Governance

Machine identities are the fastest-growing and least-governed segment of the enterprise identity estate. Service accounts, API keys, SSH keys, certificates, tokens, and workload identities now outnumber human identities in most organizations — and they are increasingly targeted by attackers who know they are rarely monitored.

ARCON extends identity governance beyond human users to include every machine identity, workload identity, and trust material in the enterprise — bringing the same visibility, lifecycle control, and governance discipline to non-human identities that IAM applies to people.

Machine Identity Governance Capabilities

Discovery & Visibility

Discover every service account, bot, API key, SSH key, certificate, token, automation account, and workload identity across on-premises, cloud, and hybrid environments. Many organizations are surprised to find they have three to five times more machine identities than they believed.

Trust Material Governance

Track and govern SSH keys, API keys, certificates, tokens, and secrets throughout their lifecycle. Identify certificates nearing expiry before they cause outages. Detect overprivileged service accounts before attackers exploit them.

Workload Identity Governance

Map identity-to-workload relationships across containerized environments, Kubernetes clusters, and cloud-native services. Understand which workloads have access to which resources — and enforce governance policies accordingly.

Machine Identity Analytics

Detect anomalous machine identity behaviour — unusual API call patterns, unexpected access to sensitive resources, or service accounts operating outside their normal scope. Machine identity analytics are essential for detecting compromised service accounts that have been hijacked for lateral movement.

> ***Securing the Fastest Growing Identity Attack Surface: 45% of identity-related breaches in 2024 involved non-human identities — service accounts, API keys, or certificates that were unmanaged, over-privileged, or never rotated.***

PLATFORM CAPABILITY — 07

Digital Vault & Secrets Management

Credentials that are not vaulted are credentials that are at risk. ARCON's vault architecture provides enterprise-grade protection for every sensitive asset — from privileged passwords and API keys to certificates, secrets, and application-to-application credentials.

ARCON operates a multi-tier vault architecture designed for different credential types, different user personas, and different security requirements — all governed by the same policy engine and audit infrastructure.

Vault Architecture

Password Vault

Enterprise vault for privileged credentials with automated rotation, check-out/check-in controls, dual-control access, and full audit trail. No administrator touches a credential directly — ARCON injects credentials into sessions automatically and rotates them after every use.

Digital Vault

Secure storage and encrypted sharing of files, certificates, sensitive documents, and digital assets. Supports secure file transfer between teams with access controls, version management, and audit logging.

My Vault

User-level vault for personal credentials, secure notes, and application passwords. Employees store and retrieve personal credentials securely — reducing the risk of passwords stored in browsers, spreadsheets, or sticky notes.

Secrets Management

Centralized management of application secrets, API keys, tokens, encryption keys, and application-to-application passwords. Secrets are versioned, rotated on schedule, and injected into applications dynamically — eliminating hard-coded credentials in code repositories and configuration files.

HSM Integration

Integration with Hardware Security Modules for FIPS 140-2 compliant key storage and cryptographic operations — meeting the most stringent regulatory requirements for financial services, government, and defence sectors.

> ***Business Outcome: Eliminate hard-coded secrets from code repositories, automate certificate renewal before outages occur, and provide auditors with complete evidence of every credential access event.***

PLATFORM CAPABILITY — 08

Identity Intelligence & Risk Analytics

Static identity security reacts to incidents after they happen. Intelligent identity security anticipates risk before it materialises. ARCON's integrated analytics engine — powered by Knight Analytics and — delivers continuous identity risk visibility, behavioural intelligence, and compliance insight.

Identity intelligence is not a separate product bolted onto ARCON. It is woven into every layer of the platform — surfacing risk signals from authentication, authorization, session activity, entitlement changes, and governance actions, and correlating them into actionable insight.

Analytics Capabilities

Knight Analytics — Identity Risk Intelligence

Behavioural analytics across the entire identity and access landscape. Knight Analytics baselines normal access patterns for every user, role, and identity type — and flags deviations that indicate potential compromise, insider threat, or governance drift. Risk scores are continuous, dynamic, and integrated into access decisions.

— Privileged Session Intelligence

Inspection-grade visibility into privileged sessions and commands. combines session recording with behavioral analysis to detect anomalous command sequences, unusual data access patterns, and suspicious administrative activity — then generates AI-powered summaries that reduce audit review time dramatically.

User Behaviour Analytics (UBA)

Continuous monitoring of access behaviour, login patterns, application usage, and data interaction — establishing behavioral baselines and detecting anomalies including impossible travel, after-hours access, bulk data downloads, and lateral movement indicators.

Identity Risk Scoring

Dynamic risk scores for every identity, role, and entitlement — updated continuously based on access behaviour, governance posture, and threat intelligence signals. Risk scores feed directly into adaptive authentication decisions, ensuring high-risk identities face stronger verification requirements.

Entitlement Analytics

Visibility into excessive permissions, dormant accounts, role mining results, and entitlement drift — enabling proactive governance before entitlements become audit findings or attack vectors.

> ***Business Outcome: Shift from reactive incident investigation to proactive risk reduction. ARCON's analytics layer surfaces the top 10% of risky identities and***

> ***entitlements — enabling security teams to focus governance effort where it matters most.***

PLATFORM CAPABILITY — 09

Identity-Centric Zero Trust Security

Zero Trust is not a product. It is an architectural philosophy: never trust, always verify. Identity is the foundation of every Zero Trust implementation — because every access decision starts with verifying who is asking, why they need it, and whether the risk is acceptable.

ARCON Converged Identity Platform is purpose-built to enable identity-centric Zero Trust. Every capability — from authentication to vaulting to session monitoring — contributes to a Zero Trust posture that is continuous, context-aware, and evidence-driven.

How ARCON Maps to Zero Trust Requirements

Zero Trust Requirement	ARCON Capability
Verify explicitly	MFA, adaptive authentication, and risk-based access decisions at every session
Use least privilege	RBAC, ABAC, JIT access, PEDM, and CIEM entitlement right-sizing
Assume breach	Session monitoring, behavioural analytics, anomaly detection, and SIEM integration
Reduce standing access	JIT grants, ephemeral privilege elevation, and automatic access expiry
Evaluate continuously	Knight Analytics risk scoring, governance reviews, and adaptive policy enforcement
Audit everything	Video logs, command logs, access reports, session recordings, and SIEM forwarding

Zero Trust in Practice

ARCON enables Zero Trust across every identity type — workforce users who authenticate through SSO and MFA, privileged administrators who access systems through JIT-controlled sessions, cloud workloads governed by CIEM entitlement policies, and machine identities managed through secrets governance.

Zero Trust is not a destination — it is a continuous posture. ARCON makes continuous verification, continuous governance, and continuous audit a natural byproduct of how the platform operates.

ENTERPRISE INTEGRATION

Connect Across Your Enterprise

Identity security does not operate in isolation. ARCON integrates natively with the directories, cloud platforms, ITSM systems, SIEM tools, DevOps pipelines, and enterprise applications that organisations already use.

ARCON's API-first integration architecture ensures that adding converged identity governance does not require replacing the existing enterprise ecosystem — it enhances it.

IDENTITY & DIRECTORY	CLOUD & INFRASTRUCTURE	ITSM & WORKFLOW
Active Directory	AWS	ServiceNow
Entra ID / Azure AD	Microsoft Azure	Jira
LDAP	Google Cloud Platform	BMC Remedy
Okta	Oracle Cloud (OCI)	Ticket-based approvals
Google Workspace	Kubernetes / OpenShift	Workflow automation
HRMS integrations	VMware / Hyper-V	

SIEM & MONITORING	DEVOPS & AUTOMATION	ENTERPRISE APPLICATIONS
Splunk	Jenkins	SAP
ArcSight	Ansible	Salesforce
IBM QRadar	Chef	Microsoft 365
RSA NetWitness	GitLab	Atlassian
Syslog	CI/CD pipelines	Databases
	Container orchestration	Web applications

ARCON supports SAML 2.0, OAuth 2.0, OIDC, REST APIs, SCIM, and Syslog/CEF for SIEM integration — enabling connectivity across virtually any enterprise technology stack.

DEPLOYMENT

Same Platform. Your Perimeter.

Every organization has a different infrastructure reality — regulatory constraints, cloud maturity, data residency requirements, and operational preferences. ARCON supports every deployment model, with the same platform capabilities regardless of where it is deployed.

Deployment Model	Characteristics & Best Fit
On-Premises	Full data and key control. AD/LDAP integration. HSM support. HA/DR control. Air-gapped environments supported. Best for: regulated enterprises, banking, government, defence, healthcare, and data-residency-restricted environments.
SaaS	Reduced infrastructure overhead. Faster deployment. Managed availability and updates. Built-in scalability. Best for: cloud-first organizations seeking fast time-to-value and minimal infrastructure management.
Hybrid	Vault and credential control retained on-premises. Governance and analytics extended to cloud. Consistent policy engine across both environments. Best for: enterprises in phased cloud migration with sensitive credential residency requirements.
Kubernetes	Microservices orchestration with auto-scaling, self-healing, and workload portability. Best for: large-scale, cloud-native, and containerized deployments requiring platform-level resilience and scalability.

The platform capabilities are identical across all deployment models. Organizations can begin with one model and transition to another as infrastructure strategies evolve — without re-licensing or re-implementing.

MODERNIZATION STRATEGY

Modernize Without Rip-and-Replace

The biggest barrier to identity transformation is not technology — it is disruption risk. Organizations have existing tools, active integrations, and ongoing programs. A platform that demands a complete replacement before delivering value is a platform that stays in the proof-of-concept stage indefinitely.

ARCON is designed for progressive adoption. Organizations can start with one capability, demonstrate value, expand over time, and gradually consolidate identity operations — without disrupting the systems users depend on today.

Four Adoption Journeys

PAM-First

Begin by securing privileged access — the highest-risk identity segment. Deploy credential vaulting, session monitoring, and JIT access. Demonstrate immediate risk reduction and audit capability. Expand to IGA, CIEM, and workforce IAM over time.

IGA-First

Start with identity lifecycle governance and access certification — ideal for organizations facing compliance deadlines or audit pressure. Deploy Joiner-Mover-Leaver automation and access review campaigns. Expand to PAM, CIEM, and analytics as governance matures.

CIEM-First

Begin by gaining visibility into cloud entitlements across AWS, Azure, GCP, and OCI. Right-size over-provisioned cloud permissions. Deploy cloud governance policies. Expand to PAM, IGA, and workforce IAM as cloud maturity grows.

Full Platform Transformation

Deploy the complete ARCON Converged Identity Platform as a unified identity security transformation — replacing fragmented tools with a single platform, consolidating governance into one control plane, and accelerating operational maturity across all identity types.

Coexistence Capability	How It Works
Coexist with existing IAM platforms	ARCON integrates alongside current tools — no forced replacement
Extend current PAM implementations	Add governance, analytics, and IGA alongside existing vault tools
Leverage ARCON IGA with existing IAM	Governance layer added without replacing authentication infrastructure
Protect existing investments	Connector ecosystem preserves integrations already built

Expand at your own pace	Capabilities activated progressively, not deployed all at once

INDUSTRY USE CASES

Purpose-Built Outcomes for Every Industry

Identity security is not one-size-fits-all. Banking regulators, healthcare standards bodies, government frameworks, and industrial security requirements each create distinct identity governance challenges. ARCON is deployed across regulated sectors worldwide.

Banking, Financial Services & Insurance (BFSI)

BFSI organizations face the most stringent regulatory requirements for privileged access, data governance, and audit readiness. ARCON delivers privileged access governance for banking operations, third-party access security for vendor management, cloud entitlement governance across AWS and Azure, and audit acceleration for PCI-DSS, SOX, and RBI compliance.

A major retail bank deployed ARCON PAM and CIEM across multi-cloud environments — unifying privileged access governance and entitlement right-sizing across AWS, Azure, and GCP in a single operational framework.

Government & Public Sector

Government organizations require centralized identity governance across multiple departments, strict Zero Trust implementation for sensitive systems, critical infrastructure protection for operational technology, and multi-agency access governance for shared platforms. ARCON supports NIST, ISO 27001, and government-specific identity security frameworks.

Healthcare & Pharmaceuticals

Healthcare organizations manage sensitive patient data, regulated clinical systems, and complex third-party access requirements. ARCON provides controlled privileged access to EHR and clinical systems, workforce identity management for nursing and administrative staff, and HIPAA-aligned access governance with real-time audit capabilities.

Telecom & Media

A national telecom operator replaced fragmented identity tooling with ARCON Converged Identity — unifying user lifecycle management, end-user password management, access governance, and analytics for business-critical applications. Automated JML lifecycle management, unified audit trail, and analytics-driven reporting delivered immediate operational improvement.

Manufacturing & Industrial

Manufacturing organizations manage distributed workforces across multiple sites, vendor access to operational technology (OT) environments, and growing industrial IoT identity requirements.

ARCON governs vendor access to OT systems, enforces least privilege across endpoints, and provides multi-site identity visibility from a single platform.

BUSINESS OUTCOMES

What Converged Identity Delivers

Identity convergence is not just a security initiative — it is an operational transformation. Organizations that consolidate identity governance onto a single platform reduce cost, accelerate compliance, strengthen security posture, and improve the user experience simultaneously.

Business Outcome	What It Means in Practice
Unified Identity Visibility	Centralized view of every human, privileged, machine, and cloud identity — with real-time risk intelligence
Reduced Attack Surface	Eliminate standing privileges, excessive entitlements, and unmanaged machine identities that attackers exploit
Faster Compliance Reporting	Evidence-by-default architecture produces audit-ready reports in minutes, not weeks
Lower Operational Cost	Consolidate 7+ identity tools into one platform — reducing licensing, integration, and administration overhead
Stronger Governance	Continuous access certifications, SoD enforcement, and lifecycle governance eliminate entitlement drift
Accelerated Onboarding	HRMS-driven automation delivers birthright access on day one — reducing onboarding time from days to hours
Better User Experience	Single Identity Hub for apps, access requests, vault, and sessions — eliminating portal proliferation
Zero Trust Readiness	Continuous verification, JIT access, and behavioral analytics provide the identity foundation for Zero Trust
Future-Ready Security	Machine identity governance, cloud entitlement control, and AI analytics extend coverage to emerging identity threats
Progressive ROI	Modular adoption means organizations see value from the first module — with ROI compounding as convergence grows

WHY ARCON

Why Organizations Choose ARCON

There are many identity security vendors. What makes ARCON different is not the list of capabilities — it is the architectural philosophy, the implementation philosophy, and the market track record.

Architected for Convergence from Day One

ARCON Converged Identity Platform was not assembled through acquisitions. It was designed from the ground up as a unified identity security platform — with a shared data model, shared policy engine, shared vault architecture, and shared analytics layer. There are no integration seams between capabilities, because the capabilities were never separate products.

20+ Years of Privileged Access Leadership

ARCON's privileged access management capability is built on two decades of enterprise deployment experience — across banking, government, healthcare, telecom, and critical infrastructure globally. That operational depth is embedded in every aspect of the platform architecture.

Progressive Modernization Without Risk

ARCON can be adopted incrementally alongside existing tools — protecting current investments while adding new governance capabilities. No other platform offers the same combination of convergence ambition and coexistence flexibility.

Compliance-Ready by Architecture

Audit trails, session recordings, certification records, and governance dashboards are generated automatically as the platform operates — not produced reactively in response to audit requests. Compliance readiness is a continuous byproduct, not a project.

Deployed at Scale in Regulated Sectors

ARCON is in production at scale across banking, financial services, government, healthcare, telecom, and manufacturing organizations globally — delivering convergence in the most demanding regulatory environments.

API-First Extensibility

ARCON's API-first architecture integrates with virtually any enterprise technology stack — directories, cloud platforms, ITSM, SIEM, DevOps, and enterprise applications — without requiring a forklift of the existing ecosystem.

> ***One platform. Multiple identity services. Shared intelligence. Unified governance. That is why organizations choose ARCON.***

Every Identity.

One Fabric.

Unified Governance.

Predict | Protect | Prevent

ARCON is helping enterprises build an identity-secure future.

Whether you are modernizing existing IAM ecosystems, strengthening privileged governance, improving cloud entitlement visibility, or building a Zero Trust architecture from the identity layer up —

ARCON provides the platform, the expertise, and the flexibility to get there.

www.arconnet.com