CROSSIDENTITY
IAM CONVERGED

Cross Identity vs Arcon

Cybersecurity-as-an-Infrastructure VS Privileged Access Platforms

+91 901 926 6824 inquiry@crossidentity.com www.crossidentity.com

Table of contents

1. Executive Summary

Identity has become a foundational control plane for enterprise cybersecurity. As organizations operate across hybrid infrastructure, cloud platforms, SaaS applications, and automated systems, security effectiveness increasingly depends on how consistently identities are governed, monitored, and enforced.

ARCON is a well-established Privileged Access Management (PAM) platform, commonly adopted to secure administrative access, privileged sessions, and high-risk credentials. For organizations focused on controlling elevated access to critical systems, ARCON provides centralized credential management, session control, and audit capabilities.
However, modern identity risk extends beyond privileged credentials alone. Excessive access, cloud entitlements, dormant accounts, non-human identities, and lateral movement across identity boundaries often introduce exposure outside traditional PAM workflows. In PAM-centric architectures, governance, access management, and risk enforcement are typically addressed through adjacent systems or manual processes rather than as a unified control plane.

As identity environments scale and diversify, many organizations encounter a structural challenge: protecting privileged access does not inherently provide continuous identity security across the enterprise.

This document examines that architectural distinction.

ARCON represents a privileged access platform, optimized to protect elevated credentials and sessions. Cross Identity represents cybersecurity-as-an-infrastructure, where identity itself functions as a unified control plane governing access, privilege, entitlements, risk, and compliance.
The comparison in this report is not about feature parity or replacing PAM platforms. It is about understanding how identity security should operate at enterprise scale:

- ARCON is optimized for securing privileged access and administrator activity.
- Cross Identity is optimized for continuous, enterprise-wide identity security and enforcement.

The purpose of this document is to help organizations determine which architectural approach best aligns with their identity maturity, operational complexity, and risk posture—particularly in environments where identity risk must be managed continuously across hybrid, cloud, and non-human identity ecosystems.

2. Introduction: Privileged Access vs Enterprise Identity Security

2.1 The Expanding Identity Attack Surface

Enterprise identity environments have expanded well beyond administrators and privileged users. Modern organizations operate across on-premises systems, private infrastructure, multiple public clouds, SaaS platforms, APIs, and automated workloads. Human users, service accounts, bots, and machine identities all interact continuously with critical systems and data.

In this environment, identity security must function at scale. It must provide consistent governance, access control, and enforcement across heterogeneous infrastructure while adapting to rapid change in cloud services and deployment models.

Historically, many organizations approached identity security by focusing on privileged access—securing administrator credentials, controlling elevated sessions, and reducing standing privilege. This remains essential, as privileged identities represent a high-risk attack vector.
However, the identity attack surface has expanded. Identity risk now accumulates across:

- Excessive and inherited access
- Standing permissions outside PAM workflows
- Cloud infrastructure entitlements
- Dormant and orphaned identities
- Non-human and workload identities

These risks often exist without triggering privileged access controls, creating exposure that credential-centric security does not fully address.

2.2 From Privileged Control to Identity-Wide Enforcement

As identity environments become more complex, organizations face a fundamental architectural question:
Should identity security be enforced primarily at points of privilege, or continuously across the entire identity lifecycle?
Privileged access platforms are designed to secure elevated access through vaulting, session monitoring, and credential rotation. Governance, access management, cloud entitlement control, and risk detection are typically layered around these platforms through additional systems or manual processes.
While this model can be effective, it introduces coordination boundaries:

- Identity governance decisions may not immediately affect access or privilege
- Cloud entitlements are managed outside PAM enforcement
- Identity risk detection relies on external analytics and escalation
- Enforcement timing depends on orchestration across systems

As environments scale, these boundaries increase operational overhead and slow response.
This report explores that inflection point by comparing ARCON's PAM-centric model with Cross Identity's cybersecurity-as-an-infrastructure approach—examining how each performs as identity security shifts from isolated privileged controls to continuous, enterprise-wide enforcement across hybrid and cloud environments.

3. Understanding ARCON

3.1 ARCON's Role in Enterprise Security

ARCON is a Privileged Access Management (PAM) platform designed to secure elevated access to critical enterprise systems. It is commonly used to protect administrator accounts, privileged credentials, and high-risk sessions across on-premises and hybrid environments.

At its core, ARCON provides:

- Privileged credential vaulting and password management
- Privileged session control and monitoring
- Controlled access to critical servers, databases, and applications
- Audit logging and compliance reporting for privileged activity

ARCON's architecture reflects its focus on reducing exposure from privileged access misuse. By centralizing credential control and monitoring elevated sessions, the platform helps organizations limit standing privilege, improve accountability, and meet regulatory requirements related to administrator access.

For enterprises where securing privileged credentials is a primary security objective, ARCON serves as an important foundational control.

3.2 The PAM-Centric Security Model

ARCON operates within a PAM-centric security model, where identity protection is strongest at the point of privileged access. Security enforcement is focused on credential checkout, session initiation, and monitored interaction with critical systems.

In this model:

- Privileged identities are tightly controlled and audited
- Credential exposure is reduced through vaulting and rotation
- Session activity is monitored and recorded
- Compliance is demonstrated through privileged access logs

However, this model also defines the scope of the platform. Identity governance, access lifecycle management, cloud entitlements, and non-privileged identities typically exist outside the core PAM system and are addressed through separate IAM or security tools.

As a result:

- Identity governance decisions do not automatically enforce across all access types
- Cloud and SaaS permissions are managed outside PAM workflows
- Non-human identities are secured at the credential level, not governed holistically
- Identity risk detection often relies on external systems and manual escalation
-

These characteristics do not represent weaknesses in ARCON's PAM capabilities. Rather, they reflect the reality that ARCON was designed to secure privileged access, not to operate as a unified identity security control plane.

As identity security requirements expand beyond privileged sessions into continuous governance, entitlement control, and real-time risk enforcement, understanding the boundaries of a PAM-centric architecture becomes essential. The next section examines those limits in more detail.

4. The Limits of PAM-Centric Identity Architectures

4.1 Privilege Is Only One Dimension of Identity Risk

Privileged Access Management is a critical security control, but privileged credentials represent only a portion of the modern identity attack surface. In contemporary enterprise environments, identity risk often accumulates outside privileged sessions and administrator workflows.

Excessive access, inherited permissions, cloud entitlements, dormant accounts, and non-human identities frequently introduce exposure without triggering PAM controls. Attackers increasingly exploit these conditions to move laterally, escalate access incrementally, and establish persistence without immediately engaging privileged credentials.

In PAM-centric architectures, protection is strongest at points of privilege—credential checkout, session initiation, or command execution. Identity posture leading up to those events is often governed elsewhere, creating gaps between lifecycle management, entitlement control, and enforcement.

As a result:

- Identity risk can exist without privileged activity
- Lateral movement can occur below PAM visibility
- Excess access persists outside PAM enforcement
- Preventive controls are limited outside privileged paths

These gaps are architectural rather than operational. PAM platforms are optimized to protect high-risk access events, not to continuously govern the entire identity estate.

4.2 Coordination Overhead and Enforcement Gaps

To extend PAM platforms into broader identity security, organizations typically integrate additional systems for identity governance, access management, cloud entitlement control, and risk detection. While these integrations expand coverage, they also introduce coordination boundaries.

In practice:

- Governance decisions are evaluated separately from PAM enforcement
- Cloud entitlements are managed outside privileged workflows
- Identity risk detection relies on external analytics and alerts
- Enforcement actions require orchestration across systems

As environments scale across hybrid and multi-cloud infrastructure, these boundaries increase operational overhead and slow response. Identity incidents span multiple tools and teams, and risk detection is often decoupled from enforcement.
Most critically, the time between identifying identity risk and enforcing controls creates exposure that attackers can exploit.

These challenges do not reflect shortcomings in PAM technology. They reflect the limitations of architectures designed to secure specific access events, rather than to operate identity security as continuous cybersecurity infrastructure.

As identity environments grow more dynamic and non-human identities proliferate, many organizations reach an inflection point where PAM-centric controls remain necessary but no longer sufficient. The next section introduces Cross Identity's approach to addressing these challenges.

5. Cross Identity: Cybersecurity-as-an-Infrastructure

Cross Identity was designed as cybersecurity infrastructure, making identity the central control plane for continuous enforcement across the enterprise.

Recognized by leading analysts such as KuppingerCole as a Leader in IGA, IAG, and CIEM, Cross Identity delivers unified governance, access, and risk control across hybrid and cloud environments.

Infrastructure by Design

Cybersecurity infrastructure must operate deterministically at enterprise scale. In Cross Identity, identity security controls are not extended through integrations between PAM, IAM, and governance tools. They are embedded natively within a single, converged architecture governed by a shared data model and unified policy framework.

This design enables:

- Identity governance and access enforcement to operate as one system
- Privileged access to be inseparable from identity lifecycle and entitlement posture
- Cloud infrastructure permissions to be governed continuously
- Human and non-human identities to be treated consistently
- Risk signals to result in immediate enforcement

There is no dependency on downstream orchestration or manual coordination to translate identity insight into security action.

A Unified Identity Security Control Plane

At the core of Cross Identity is a single control plane that governs how identities interact with applications, infrastructure, and data. Preventive controls, real-time detection, and enforcement all operate through the same engine.

This enables a continuous security loop:

- Identity posture is assessed proactively
- Behavioral, entitlement, and privilege risk is evaluated in real time
- Enforcement decisions are executed immediately
- Posture is recalculated continuously

Identity security is no longer limited to protecting elevated access—it becomes an always-on enforcement layer across the entire identity estate.

Built for Modern Enterprise Environments

Cross Identity was built for today's enterprise realities: hybrid infrastructure, multi-cloud environments, SaaS platforms, APIs, and rapidly expanding populations of non-human and workload identities.

By treating identity security as infrastructure rather than as PAM-centric tooling, Cross Identity enables organizations to move beyond protecting isolated privileged access paths toward operating a stable, scalable identity security control plane that adapts as the enterprise evolves.

The next section compares these two architectural approaches directly, examining how PAM-centric platforms and identity security infrastructure differ in design, enforcement, and operational impact.

Comparison 2: Mid Enterprise

Dimension	ARCON (PAM-Centric Platform)	Cross Identity (Cybersecurity-as-an- Infrastructure)
Platform Model	PAM-first security deployment	All-in-one identity security foundation
Design Priority	Reducing exposure from admin accounts	Outcome-driven identity security
Configuration Model	Multiple components and policies	One engine, one configuration model
Policy Management	Privilege-focused policy definitions	Single policy layer across all identities
Governance Coverage	Limited outside privileged workflows	Built-in and enforced infrastructure-wide
Cloud & SaaS Coverage	Requires additional tools	Native coverage from day one
Risk Handling	Alerts require investigation	Automated enforcement within identity
Deployment Timeline	Incremental rollout over months	Weeks with minimal services
Operational Skillset	PAM specialists and administrators	Lean security teams
Security Operations	Multiple consoles and workflows	Single-pane identity security operations

What This Means in Practice

For large enterprises, PAM-centric platforms provide essential protection for high-risk access but require significant coordination to extend security across governance, cloud entitlements, and non-human identities.

For mid enterprises, PAM-centric architectures often introduce complexity early, as organizations must layer additional tools to achieve broader identity security coverage.
By contrast, cybersecurity-as-an-infrastructure delivers continuous enforcement, faster deployment, and lower operational friction at both scales by operating identity as a unified security control plane.

The next section examines how these architectural differences translate into capability delivery across access, privilege, cloud entitlements, and identity risk.

7. Capability Comparison

While architecture determines how identity security operates, organizations also evaluate platforms based on how effectively core capabilities are delivered in practice. This comparison focuses on coverage, convergence, and enforcement, rather than feature checklists.

Capability Comparison — Large Enterprise

Capability Area	ARCON	Cross Identity
Access Management	Addressed indirectly through privileged workflows	Unified access governed by identity, policy, and risk
Authentication	Not a core capability; relies on external IAM	Native authentication embedded into the identity control plane
Identity Lifecycle Management	Managed outside the PAM platform	Native lifecycle governance enforced infrastructure-wide
Identity Governance (IGA / IAG)	Requires external governance tools	Built-in governance with atomic enforcement
Privileged Access Management (PAM)	Core strength with credential and session control	Native PAM fully integrated with identity governance
Cloud Infrastructure Entitlements (CIEM)	Managed through adjacent tools	Embedded CIEM tied directly to access and governance
Identity Risk & Threat Detection	Relies on external analytics and escalation	Native detection and enforcement within the identity layer
Identity Security Posture (ISPM)	Assessed across multiple platforms	Continuous, always-on posture management
Non-Human & Workload Identities	Secured at credential level	Governed as first-class identities
Audit & Compliance	Privileged session logs and reports	Single authoritative audit trail
Operational Model	Coordinated operation of PAM and IAM tools	One converged identity security system

Capability Comparison — Mid Enterprise

Capability Area	ARCON	Cross Identity
Privileged Access Control	Strong PAM coverage for admin access	Access and privilege governed together
Time to Value	Slower due to staged PAM rollout	Weeks with minimal services
Identity Governance	Requires additional products	Included by default
Cloud & SaaS Entitlements	Requires extra tools and workflows	Built-in visibility and enforcement
Risk Detection & Response	Alerts require manual investigation	Automated enforcement through identity policies
Non-Human Identities	Managed as credentials	Managed natively as identities
Policy Management	Privilege-centric policies	Single policy layer across identities
Security Operations	Multiple consoles and workflows	Single-pane security operations
Staffing Requirements	Specialized PAM expertise	Lean security teams
Scalability	Scales with more tooling and admin effort	Scales as infrastructure

Key Observation

ARCON delivers strong privileged access protection and remains effective for securing administrator credentials and sessions. However, its capabilities are strongest within PAM-centric workflows and depend on adjacent systems to achieve identity-wide governance, cloud entitlement control, and continuous risk enforcement.

Cross Identity delivers identity security as cybersecurity-as-an-infrastructure, where governance, access, privilege, entitlements, and risk operate as a single system. As identity security requirements expand beyond privileged access into continuous enforcement across all identities, capability convergence becomes a decisive advantage.

The next section focuses on identity risk, privilege, and intelligence, where the operational impact of these differences is most visible.

8. Identity Risk, Privilege & Intelligence

As identity becomes the primary attack surface, the ability to detect, correlate, and enforce identity risk in real time is a defining cybersecurity capability. The contrast between PAM-centric platforms and cybersecurity-as-an-infrastructure is most evident in how identity risk is handled operationally.

Identity Risk in PAM-Centric Architectures

In PAM-centric models, identity risk is primarily evaluated at the point of privileged credential use or session initiation. Elevated access is closely monitored, and privileged activity is logged and audited.

However, identity risk often emerges outside privileged workflows. Excessive access, cloud entitlements, dormant identities, non-human accounts, and lateral movement typically accumulate without triggering PAM controls.

In this model:

- Risk signals are detected across multiple systems
- Correlation occurs outside the PAM platform
- Enforcement relies on escalation or manual intervention
- Identity posture and threat detection operate independently

While PAM-centric platforms provide strong visibility into privileged activity, they introduce delays between detection and enforcement when risk originates elsewhere in the identity estate.

Native Risk Execution in Identity Infrastructure

Cross Identity embeds identity risk and intelligence directly into its cybersecurity infrastructure. Risk is not treated as an external analytics output, but as an execution signal within the same engine that governs identity lifecycle, access, privilege, and entitlements.

This enables:

- Continuous assessment of identity posture across all identities
- Real-time correlation of entitlement, behavior, and privilege signals
- Immediate enforcement actions within the identity layer
- Continuous recalculation of posture after enforcement

Risk intelligence functions as an enforcement mechanism, not just an observation layer.

Continuous Identity Risk Enforcement

By converging governance, access, privilege, and risk within a single control plane, Cross Identity enables a continuous security loop:

- Identity posture is assessed proactively
- Risk signals are evaluated in real time
- Enforcement decisions are executed immediately
- Exposure is reduced before escalation

This eliminates the enforcement gap inherent in architectures where risk detection and response are decoupled from identity control.

Security and Operational Impact

Embedding identity risk intelligence directly into cybersecurity infrastructure enables organizations to:

- Respond faster to identity-based threats
- Reduce lateral movement and privilege escalation
- Eliminate manual escalation workflows
- Apply consistent risk controls across hybrid and multi-cloud environments

As identity attacks accelerate and non-human identities proliferate, the ability to execute identity risk natively—rather than observe and react—becomes essential.

The next section examines how these risk models perform across hybrid infrastructure, SaaS platforms, and non-human identity environment

9. Hybrid Infrastructure, SaaS & Non-Human Identities

Enterprise environments are no longer confined to on-premises systems and administrator access. Most organizations now operate across hybrid infrastructure, multiple public clouds, SaaS platforms, APIs, and automated workloads. Non-human identities—service accounts, bots, pipelines, and machine identities—often outnumber human users and change far more rapidly.

In this environment, identity security must function consistently across infrastructure, applications, and workloads, regardless of where identities originate or how frequently permissions change.

PAM-Centric Security in Hybrid and SaaS Environments
ARCON's PAM-centric architecture is effective at securing privileged access to critical systems, particularly in on-premises and hybrid environments where administrator control is a primary concern. Its credential vaulting and session monitoring capabilities help reduce risk associated with elevated access.

However, in SaaS- and cloud-heavy environments, PAM-centric models face structural challenges:

- Cloud and SaaS entitlements are managed outside PAM workflows
- Non-human identities are secured as credentials, not governed as identities
- Permissions change dynamically, often between PAM interactions
- Identity posture differs across infrastructure and SaaS platforms

As environments become more distributed and automated, maintaining consistent security outcomes requires increasing coordination across tools and teams.

Identity Infrastructure Across Environments
Cross Identity was designed to operate as cybersecurity-as-an-infrastructure, enforcing identity controls consistently across on-premises systems, cloud platforms, SaaS applications, APIs, and automated workloads.

With Cross Identity, organizations can:

- Govern access and entitlements across hybrid and multi-cloud environments in real time
- Apply uniform policies across infrastructure, SaaS, and APIs
- Treat non-human and workload identities as first-class entities
- Maintain continuous visibility into identity posture and risk

In hybrid and SaaS-driven environments, attackers exploit differences in entitlement models, privilege boundaries, and enforcement mechanisms between platforms. Inconsistent identity controls create opportunities for lateral movement, escalation, and persistence.

By operating identity security as infrastructure rather than as PAM-centric tooling, organizations reduce these gaps and establish a stable, environment-independent identity security control plane.

The next section examines when ARCON is enough, and where PAM-centric security remains an appropriate and effective choice.

10. When ARCON Is Enough— and When It's Not

ARCON is a capable and effective Privileged Access Management platform, particularly well suited for organizations whose primary identity security concern is controlling and auditing administrator and privileged access. Not every environment requires identity security to operate as full cybersecurity infrastructure.
Recognizing when a PAM-centric approach is sufficient is an important part of making an informed architectural decision.

Scenarios Where ARCON Fits Well
ARCON is often the right choice when:

- Protecting administrator credentials and privileged sessions is the dominant risk concern
- The environment is largely on-premises or hybrid with limited SaaS sprawl
- Privileged access paths are clearly defined and relatively stable
- Compliance requirements focus on auditability of privileged activity
- Identity governance and access lifecycle are handled through existing IAM tools
- Security teams are organized around PAM-centric operations

In these scenarios, ARCON provides strong centralized control over privileged credentials and sessions, significantly reducing exposure from credential misuse and unauthorized administrative access.

Why This Matters
Acknowledging when ARCON is sufficient establishes a necessary baseline. The goal is not to replace PAM platforms indiscriminately, but to understand where PAM-centric architectures reach their natural limits as identity environments evolve.
For organizations with constrained identity scope, limited cloud complexity, and a clear separation between IAM and PAM responsibilities, ARCON can deliver effective and appropriate security outcomes.

Where the Model Begins to Strain
As identity environments grow more dynamic, certain challenges emerge that are architectural rather than operational:

- Access risk accumulates outside privileged workflows
- Cloud and SaaS entitlements change faster than PAM controls can adapt
- Non-human identities grow beyond credential-centric management
- Identity risk detection produces alerts without native enforcement
- Operational overhead increases as integrations multiply

These challenges do not reflect deficiencies in ARCON's PAM capabilities. They reflect the realities of operating identity security through privileged-access controls rather than a unified identity control plane.

The next section explains why organizations choose Cross Identity when they reach that point.

11. Why Organizations Choose Cross Identity

Organizations choose Cross Identity when identity security must operate as a continuous, enterprise-wide cybersecurity control, rather than as a set of controls focused primarily on privileged access events.
This shift typically occurs as environments expand across cloud platforms, SaaS applications, APIs, and automated workloads, and as identity risk increasingly originates outside traditional PAM boundaries.

From Privileged Controls to Unified Identity Security
Cross Identity is adopted by organizations that require governance, access, privilege, cloud entitlements, risk, and compliance to function as one system, not as integrated but independent platforms.
By converging these capabilities into a single architecture, Cross Identity eliminates the need for manual coordination between PAM, IAM, and governance tools to achieve consistent security outcomes.
This architectural coherence allows identity security to remain effective as complexity increases.

Native Risk Enforcement
A primary driver for choosing Cross Identity is the ability to evaluate and enforce identity risk natively and immediately. Preventive posture management, entitlement analysis, behavioral signals, and privilege context operate within the same decision framework that governs access and identity lifecycle.
This enables organizations to move from alert-driven response to policy-driven execution, reducing exposure time and limiting the blast radius of identity compromise.

Consistency Across Hybrid, Cloud, and Non-Human Identities
As enterprises expand across on-premises infrastructure, multiple cloud providers, SaaS platforms, and automated workloads, identity security must remain consistent everywhere identity exists.
Cross Identity provides a cloud-agnostic identity security control plane that enforces the same policies across human and non-human identities alike—closing the gaps that PAM-centric architectures struggle to address.

Operational Sustainability
Organizations also choose Cross Identity to simplify long-term identity operations. Treating identity security as cybersecurity infrastructure enables lean teams to operate complex environments without proportional increases in tooling, integrations, or administrative overhead.
Over time, this results in:

- Faster deployments
- Reduced operational risk
- Lower total cost of ownership
- Greater resilience as identity environments evolves

The final section concludes the comparison by summarizing how architectural alignment determines long-term identity security outcomes.

12. Conclusion

Identity has become a central pillar of enterprise cybersecurity. As organizations operate across hybrid infrastructure, SaaS platforms, cloud services, and automated systems, the effectiveness of identity security depends less on individual point solutions and more on architectural alignment.

ARCON delivers strong and effective privileged access protection and remains an important control for securing administrator credentials and sessions. For many organizations, a PAM-centric approach provides meaningful risk reduction and remains a necessary part of the security stack.

However, as identity security requirements expand beyond privileged access into continuous governance, cloud entitlement control, non-human identity management, and real-time risk enforcement, the limitations of PAM-centric architectures become more visible. Coordinating identity posture, risk detection, and enforcement across multiple systems introduces delay, complexity, and exposure.

Cross Identity represents a different architectural model. By treating identity security as cybersecurity-as-an-infrastructure, it enables governance, access, privilege, entitlements, and risk to operate as a single, converged control plane—enforcing policy continuously across all identities and environments.

The choice between a PAM-centric platform and identity security infrastructure is not a question of replacement, but of fit. Organizations must evaluate their identity maturity, operational complexity, and risk tolerance to determine which model best supports their long-term security objectives.

As identity continues to define the enterprise security perimeter, architecture—not point controls—will determine resilience, consistency, and sustainability.

About Cross Identity

Elevate your identity security with Cross Identity, World's #1 converged IAM platform trusted by over 1,200 organizations to secure more than 70 million identities. More than just an IAM solution, Cross Identity unifies authentication, authorization, governance, and administration into a single, seamless experience. Our platform not only enhances security and compliance but also delivers an user experience and recommended by leading analysts that set the standard for the industry.

+91 901 926 6824

inquiry@crossidentity.com

www.crossidentity.com