CROSSIDENTITY
IAM CONVERGED

Cross Identity vs. CyberArk

Cybersecurity-as-an-Infrastructure vs Privileged Access Platform

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

Table of contents

1. Executive Summary

Identity has become the primary control plane for enterprise cybersecurity. As organizations operate across hybrid infrastructure, multi-cloud platforms, SaaS applications, APIs, and automated workloads, security effectiveness depends on how comprehensively identities are governed, monitored, and enforced across the entire environment.

CyberArk is a long-established leader in Privileged Access Management (PAM). It is widely adopted to secure administrator credentials, privileged sessions, secrets, and high-risk access paths. For organizations whose primary concern is protecting elevated access and sensitive credentials, CyberArk delivers strong, proven security controls.

However, enterprise identity security has expanded beyond privileged access alone. Identity risk now emerges from excessive entitlements, dormant accounts, cloud permissions, non-human identities, and lateral movement across identity boundaries—often outside traditional PAM workflows. In privileged-first security architectures, governance, access, cloud entitlements, and risk enforcement are typically addressed through adjacent tools or integrations rather than as a single, unified system.

As identity attack surfaces grow, many organizations encounter a structural limitation: protecting privileged credentials does not inherently provide continuous control over the full identity lifecycle or real-time enforcement across all identities.

This document examines that architectural distinction.

CyberArk represents a privileged-first security model, optimized to protect high-risk credentials and sessions through specialized platforms. Cross Identity represents identity security as cybersecurity infrastructure, where governance, access, privilege, cloud entitlements, risk, and compliance operate as a single, converged control plane.

The comparison in this report is not about replacing PAM or diminishing its importance. It is about determining how identity security should operate at enterprise scale:

- **CyberArk** is optimized for securing privileged access within complex environments.
- **Cross Identity** is optimized for continuous, enterprise-wide identity control and enforcement.

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

2. Introduction: Identity Security Beyond Privilege

2.1 The Expanding Identity Attack Surface

Enterprise identity environments have evolved far beyond users and administrators. Modern organizations operate across on-premises systems, private infrastructure, multiple public clouds, SaaS platforms, APIs, and automated workloads. Human users, service accounts, bots, pipelines, and machine identities all interact continuously with sensitive 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, workloads, and deployment models.

Historically, many organizations approached identity security by focusing on high-risk access paths—particularly privileged credentials and administrator sessions. This approach remains essential, as privileged identities represent a critical attack vector.

However, the identity attack surface has expanded. Identity risk now accumulates across:

- Excessive access and entitlement sprawl
- Dormant and orphaned identities
- Non-human and workload identities
- Cloud infrastructure permissions
- Lateral movement across identity boundaries

These risks often emerge outside traditional privileged access workflows, creating exposure that is not fully addressed by credential-centric controls alone.

2.2 From Privileged Control to Identity-Wide Enforcement

As identity complexity increases, organizations face a key architectural challenge:
how to extend strong privileged controls into continuous, enterprise-wide identity enforcement.
Privileged-first security architectures are designed to secure elevated access through vaulting, session isolation, and credential rotation. Governance, access management, cloud entitlements, and risk detection are typically layered around this core through additional platforms, integrations, or operational processes.

While this model can be effective, it introduces coordination boundaries:

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

As environments scale, these boundaries can slow response and increase operational overhead.
This evolution introduces a critical question for modern enterprises:

Should identity security be enforced primarily at points of privilege, or continuously across the entire identity lifecycle?

This report explores that inflection point by comparing CyberArk's privileged-first architecture with Cross Identity's infrastructure-based approach—examining how each model performs as identity security becomes a foundational, always-on cybersecurity control across hybrid and multi-cloud environments.

3. Understanding CyberArk

3.1 CyberArk's Role in Enterprise Security

CyberArk is a long-established and widely trusted cybersecurity platform, best known for its leadership in Privileged Access Management (PAM). Its solutions are designed to protect the most sensitive identities, credentials, and access paths within enterprise environments—particularly administrator accounts, service accounts, and machine credentials.

At its core, CyberArk provides:

- Privileged credential vaulting and rotation
- Privileged session isolation and monitoring
- Secrets management for applications and workloads
- Endpoint privilege controls
- Strong audit and compliance capabilities

CyberArk's architecture reflects its origins in securing high-risk access. By focusing on privileged identities as the primary threat vector, CyberArk enables organizations to reduce the likelihood of credential theft, misuse, and unauthorized elevation.

For enterprises with complex infrastructure, regulatory requirements, and a need to tightly control administrative access, CyberArk remains a foundational security control and a critical component of many Zero Trust strategies.

3.2 The Privileged-First Security Model

CyberArk's approach is inherently privileged-first. Security enforcement is strongest at the point where identities transition into elevated access—such as credential checkout, session initiation, or secrets retrieval.

In this model:

- Privileged identities are tightly governed and monitored
- Credential exposure is minimized through vaulting and rotation
- Sessions are isolated and auditable
- Risk is reduced by limiting standing privilege

However, this architecture also defines the operational boundary of the platform. Identity governance, access decisions, cloud entitlements, and non-privileged identity lifecycle controls typically exist outside the core PAM system and are addressed through adjacent tools or integrations.

As a result:

- Identity governance operates independently from privileged enforcement
- Cloud permissions and entitlements are managed through separate workflows
- Non-human identities are secured at the credential level but not always governed holistically
- Identity risk detection often relies on external analytics and escalation

This does not reflect a weakness in CyberArk's PAM capabilities. Rather, it reflects the reality that CyberArk was designed to secure privilege, not to operate as a unified identity security control plane across all identities.

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

4. The Limits of Privileged-First Security Architectures

4.1 Privilege Is a Subset of Identity Risk

Privileged Access Management is a critical security control, but privilege represents only a portion of the modern identity attack surface. In contemporary enterprise environments, risk accumulates long before an identity attempts to access a privileged account or system.

Excessive entitlements, standing access, misconfigured cloud permissions, dormant accounts, and unmanaged non-human identities frequently create exposure without triggering privileged access controls. Attackers increasingly exploit these conditions to move laterally, escalate access incrementally, and establish persistence outside traditional PAM workflows.

In privileged-first security architectures, protection is strongest at points of elevation—credential checkout, session initiation, or secrets use. However, identity posture leading up to those events is often governed elsewhere, creating gaps between identity lifecycle, entitlement management, and enforcement.

As a result:

- Identity risk can exist without privileged activity
- Access accumulation may go undetected until escalation
- Lateral movement can occur below PAM visibility
- Preventive controls are limited outside privileged paths

This fragmentation is architectural rather than operational. Privileged-first platforms are optimized to secure high-risk access, not to continuously govern the full identity estate.

4.2 Coordination Overhead and Enforcement Gaps

To extend privileged-first platforms into broader identity security, organizations often integrate additional systems for governance, cloud entitlement management, identity analytics, and access control. While these integrations can provide coverage, they also introduce coordination boundaries.

In practice:

- Governance decisions are evaluated separately from privilege enforcement
- Cloud entitlements are reviewed on delayed or periodic cycles
- Identity risk detection depends on external analytics and escalation
- Enforcement actions require orchestration across systems

As environments scale across hybrid and multi-cloud infrastructure, these boundaries increase operational overhead and slow response. Security teams must manage policy consistency, data synchronization, and workflow reliability across multiple platforms.
Most critically, risk detection and enforcement become decoupled. Identity risk may be identified in one system, but enforcement occurs later—or elsewhere—allowing attackers time to exploit the gap.
These challenges do not reflect shortcomings in privileged access technology. They reflect the limitations of architectures designed to protect specific access events, rather than to operate identity security as a continuous, enterprise-wide control plane.

As identity attacks accelerate and non-human identities proliferate, many organizations reach an inflection point where privilege-centric controls are necessary but no longer sufficient. The next section introduces Cross Identity's approach to addressing these challenges by treating identity security as cybersecurity infrastructure.

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 function predictably at scale. In Cross Identity, identity security controls are not extended through integrations between discrete products; 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 external orchestration 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, eliminating the delay and fragmentation common in privileged-first and modular architectures.

This enables a continuous security loop:

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

Identity is no longer limited to protecting access events—it becomes an always-on enforcement layer for cybersecurity policy.

Built for Enterprise Complexity

Cross Identity was built for modern enterprise realities: hybrid infrastructure, multi-cloud environments, SaaS ecosystems, APIs, and rapidly growing populations of non-human and workload identities.

By treating identity security as infrastructure rather than as privilege-centric tooling, Cross Identity enables organizations to move beyond protecting isolated 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 privileged-first security and identity-centric infrastructure differ in design, enforcement, and operational impact.

6. Architecture Comparison

Privileged-First Security vs Identity Security Infrastructure

The most significant difference between CyberArk and Cross Identity is not the strength of individual controls, but how identity security is architected and operated as a whole. CyberArk is designed as a privileged-first security platform, where protection is centered on securing elevated credentials, sessions, and secrets. Identity governance, access management, cloud entitlements, and risk intelligence are typically layered around this core through integrations and adjacent systems.

Cross Identity is designed as identity security infrastructure, where identity itself functions as a unified cybersecurity control plane. Governance, access, privilege, cloud entitlements, risk, and compliance operate natively within a single, converged architecture.

Architectural Comparison: Privileged-First Platform vs Cybersecurity (Large Enterprise)

Dimension	CyberArk (Privileged-First Security)	Cross Identity Cybersecurity-as-an-Infrastructure)
Platform Model	Privileged access platform with multiple specialized modules	Single, converged identity security infrastructure
Design Focus	Securing high-risk credentials and sessions	Deterministic control across the entire identity estate
Core Engines	Separate engines for PAM, Secrets, Endpoint Privilege	One unified identity security engine
Policy Architecture	Privilege policies defined within PAM workflows	Centralized policy brain governing all identities
Governance ⇔ Enforcement	Coordinated through integrations and processes	Native, real-time enforcement with no latency
Privileged Access (PAM)	Primary security focus	Built-in, enterprise-grade PAM
Cloud Entitlements (CIEM)	Addressed through integrations or adjacent tooling	Native CIEM embedded into identity governance
Non-Human & Workload Identities	Secured primarily at the credential level	Governed as first-class identities
Risk Detection & Response	Detection and enforcement occur across systems	Immediate execution within the identity layer
Audit & Compliance	Evidence aggregated from multiple platforms	Single authoritative audit trail
Operational Model	Long-term platform coordination and upkeep	One identity-driven security control plane

Comparison 2: Mid Enterprise

Dimension	CyberArk (Privileged-First Security)	Cross Identity (Cybersecurity-as-an-Infrastructure)
Platform Model	PAM-centric platform expanded over time	All-in-one identity security foundation
Design Priority	Reducing exposure from privileged accounts	Outcome-driven identity security by default
Configuration Model	Multiple products to deploy and manage	One engine, one configuration model
Policy Management	Privilege-focused policies with extensions	Single policy layer across all access types
Governance Coverage	Partial, dependent on integrations	Built-in, enforced infrastructure-wide
Cloud & SaaS Coverage	Requires additional tools and workflows	Native coverage from day one
Risk Handling	Alerts require investigation and escalation	Automated enforcement within identity
Deployment Timeline	Incremental rollout over months	Weeks with minimal services
Operational Skillset	PAM specialists and platform admins	Lean security teams
Security Operations	Multiple consoles and workflows	Single-pane identity security operations

Key Observation

For large enterprises, privileged-first platforms provide strong protection for high-risk access but require significant coordination to extend security across governance, cloud entitlements, and identity risk. As environments scale, operational overhead increases.

For mid enterprises, privileged-first architectures often introduce complexity earlier than expected, as organizations must layer additional tools to achieve holistic identity security.
By contrast, an identity infrastructure model delivers consistent enforcement, faster deployment, and lower operational friction at both scales by operating identity as a unified cybersecurity control plane.

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

7. Capability Comparison

While architecture determines how identity security operates, organizations ultimately evaluate platforms based on how effectively core security capabilities are delivered in real-world environments. This comparison focuses on depth, convergence, and enforcement, rather than feature checklists.

Capability Comparison — Large Enterprise

Capability Area	CyberArk	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 through adjacent IAM or governance tools	Native lifecycle governance enforced infrastructure-wide
Identity Governance (IGA / IAG)	Integrated via third-party or partner solutions	Built-in, enterprise-grade governance with atomic enforcement
Privileged Access Management (PAM)	Core strength with deep credential and session control	Native PAM fully integrated with identity governance
Cloud Infrastructure Entitlements (CIEM)	Managed through integrations or external platforms	Embedded CIEM tied directly to access and governance
Identity Risk & Threat Detection	Relies on external analytics, SIEM, or SOAR	Native detection and execution within the identity layer
Identity Security Posture (ISPM)	Assessed across multiple tools	Continuous, always-on posture management
Non-Human & Workload Identities	Secured at secrets and credential level	Governed as first-class identities
Audit & Compliance	Evidence compiled across platforms	Single, authoritative audit trail
Operational Model	Coordinated operation of multiple security platforms	One converged identity security system

Capability Comparison — Mid Enterprise

Capability Area	CyberArk	Cross Identity
Access & Privilege Control	Strong privilege security, limited identity scope	Access and privilege governed together by default
Deployment Complexity	Incremental rollout with multiple components	Rapid deployment as a single platform
Identity Governance	Requires additional products and integration	Included by default, no add-ons
Cloud & SaaS Entitlements	Requires extra tooling and workflows	Built-in visibility and enforcement from day one
Risk Detection & Response	Alerts require investigation and escalation	Automated enforcement through identity policies
Non-Human Identities	Managed as secrets, not identities	Managed natively alongside human identities
Policy Management	Privilege-focused policies extended manually	One policy layer across all identity types
Security Operations	Multiple consoles and workflows	Single-pane security operations
Staffing Requirements	Specialized PAM expertise required	Managed by lean security teams
Time to Value	Months with staged adoption	Weeks with minimal services

Key Observation

CyberArk delivers industry-leading privileged access security and remains essential for protecting high-risk credentials in large enterprises. However, its capabilities are strongest within privilege-centric workflows and depend on adjacent systems to achieve identity-wide governance and enforcement.

Cross Identity delivers identity security as a converged capability set, where governance, access, privilege, cloud 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 critical differentiator.

The next section focuses on identity risk and intelligence, where the operational impact of these differences becomes 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 distinction between privileged-first platforms and identity security infrastructure becomes most apparent in how identity risk is handled operationally.

Identity Risk in Privileged-First Architectures

In privileged-first security models, identity risk is primarily evaluated at the point of credential use or session initiation. Privileged identities are closely monitored, and elevated access events are logged, controlled, and audited.

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

As a result:

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

While this approach can provide visibility into high-risk access events, it introduces delays between detection and enforcement and increases reliance on operational coordination during identity incidents.

Native Risk Execution in Identity Infrastructure

Cross Identity addresses these limitations by embedding identity risk and intelligence directly into the identity security infrastructure.

Rather than treating risk as an external analytics function, Cross Identity operates risk as an execution layer 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 behavioral, entitlement, and privilege signals
- Immediate enforcement actions within the identity layer
- Continuous recalculation of posture following enforcement

Identity risk is no longer observed and escalated—it is commanded and enforced.

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 occurs

This eliminates the enforcement gaps 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 paths
- Eliminate manual escalation workflows for identity incidents
- Enforce consistent risk controls across hybrid and multi-cloud environments

As identity threats 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 multi-cloud, hybrid, and workload-heavy environments, where consistency and enforcement are hardest to maintain.

9. Multi-Cloud, Workloads & Machine Identity

Enterprise environments are no longer defined by a single infrastructure model. Most organizations operate across a mix of on-premises systems, private infrastructure, multiple public cloud providers, SaaS platforms, APIs, and automated pipelines. Identity security must function consistently across all of these environments, regardless of where identities or workloads reside.

Privileged-First Security in Hybrid and Cloud Environments
CyberArk's privileged-first architecture has strong adoption in hybrid environments, particularly where protecting administrator access, service accounts, and sensitive credentials is a priority. Its vaulting, session control, and secrets management capabilities extend across on-premises and cloud infrastructure.
However, in multi-cloud and workload-driven environments, privileged-first models encounter practical limitations:

- Cloud entitlements are managed outside core PAM workflows
- Non-human identities are secured at the secret level but not governed holistically
- Identity posture differs across environments
- Risk response depends on coordination between platforms

As cloud services proliferate and permissions change dynamically, maintaining consistent enforcement requires increasing operational effort.

Identity Infrastructure Across Environments
Cross Identity was designed to operate as cloud-agnostic identity security infrastructure, enforcing consistent identity controls across all environments from a single control plane.
With Cross Identity, organizations can:

- Govern access, privilege, and entitlements across on-prem, private cloud, and public cloud environments
- Treat human, workload, and machine identities as first-class entities
- Apply uniform policies across SaaS, infrastructure, and APIs
- Maintain centralized visibility into identity posture and risk

Because governance, access, and enforcement are native to the infrastructure, security outcomes remain consistent regardless of deployment model or cloud provider.

Why Consistency Matters
In hybrid and multi-cloud environments, attackers exploit differences in entitlement models, privilege boundaries, and enforcement mechanisms between platforms. Inconsistent identity controls create opportunities for lateral movement, privilege escalation, and persistence.
By operating identity security as infrastructure rather than as a set of privilege-centric controls, organizations reduce these gaps and establish a stable, environment-independent identity security control plane.

The next section examines when CyberArk is enough, and where privileged-first security remains an appropriate and effective choice.

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

CyberArk is a mature and highly effective security platform, particularly for organizations where protecting privileged access is the primary identity security objective. Not every environment requires identity security to operate as a fully converged cybersecurity infrastructure. Recognizing when a privileged-first approach is sufficient is an important part of making an informed architectural decision.

Scenarios Where CyberArk Fits Well

CyberArk is often the right choice when:

- The organization's primary risk lies in administrator and privileged credential compromise
- Securing high-risk access paths is the dominant security requirement
- Privileged session monitoring and credential vaulting are core compliance needs
- The identity environment is relatively stable and changes are infrequent
- Identity governance, access management, and cloud entitlements are handled through existing IAM platforms
- Security teams are structured around PAM-centric operations

In these scenarios, CyberArk provides strong, focused controls that significantly reduce exposure from credential theft and misuse.

Why This Matters

Acknowledging when CyberArk is sufficient establishes an important baseline. The goal is not to replace privileged access platforms indiscriminately, but to understand where a privileged-first security model reaches its architectural limits as identity environments evolve.

For organizations with constrained identity scope, limited cloud complexity, and a clear separation between IAM and security operations, CyberArk can deliver effective outcomes.

Where the Model Begins to Strain

As identity security requirements expand, certain challenges emerge that are architectural rather than operational:

- Governance decisions do not automatically enforce across all access types
- Cloud infrastructure entitlements require separate tools and review cycles
- Non-human identities grow faster than credential-centric controls
- Identity risk detection produces alerts without native enforcement
- Operational complexity increases as integrations multiply

These challenges do not reflect deficiencies in CyberArk. They reflect the realities of operating identity security through privileged-first controls rather than a unified identity control plane. Understanding this inflection point helps organizations determine when identity security must evolve from protecting isolated access paths into operating as cybersecurity infrastructure.

The next section summarizes 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 collection of coordinated tools focused on specific access events.
This shift typically occurs as environments scale, cloud adoption accelerates, and the number of human and non-human identities grows beyond what privileged-first architectures were designed to manage holistically.

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 components. By converging these capabilities into a single architecture, Cross Identity removes the need for orchestration, synchronization, and manual coordination across identity and security platforms.
This architectural coherence enables identity security to remain predictable and enforceable as complexity increases.

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

Consistency Across Hybrid and Multi-Cloud Environments
As enterprises expand across on-premises infrastructure, private clouds, multiple public cloud providers, and SaaS platforms, identity security must remain consistent everywhere. Cross Identity provides a cloud-agnostic identity security control plane that enforces the same policies across all environments—human and non-human identities alike—eliminating gaps that attackers commonly exploit.

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

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

12. Conclusion

Identity has become a central pillar of enterprise cybersecurity. As organizations operate across increasingly complex and distributed environments, the effectiveness of identity security is determined less by individual controls and more by architectural coherence.

CyberArk delivers industry-leading privileged access security and remains a critical control for protecting high-risk credentials, sessions, and secrets. For many organizations, a privileged-first approach provides meaningful risk reduction and remains an essential 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 privileged-first architectures become more apparent. Coordinating identity posture, risk detection, and enforcement across multiple systems introduces delay, complexity, and gaps that adversaries increasingly exploit.

Cross Identity represents a different architectural model. By treating identity security as cybersecurity infrastructure, it enables governance, access, privilege, cloud entitlements, and risk to operate as a single, converged control plane. Enforcement becomes immediate, consistent, and scalable across hybrid and multi-cloud environments.

The choice between a privileged-first security platform and identity security infrastructure is not a question of replacement, but of alignment. 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 integration—will determine resilience, control, 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