CROSSIDENTITY
IAM CONVERGED

Cross Identity vs. Microsoft Entra

Identity Security: Bundle vs. Infrastructure

Table of Contents

1. Executive Summary

Identity has become the primary control plane for modern enterprise security. As organizations expand across cloud, hybrid, and SaaS environments, every user, workload, service account, and privileged role represents both an operational necessity and a potential risk surface.

Most enterprises begin their identity journey with Microsoft Entra. Its deep integration with Microsoft 365 and Azure, combined with broad identity and access capabilities, makes it a natural default choice. For organizations with a primarily Microsoft-centric environments and basic access control needs, this approach is often sufficient.

However, as identity programs mature, security leaders increasingly encounter a structural limitation: identity capabilities exist, but they do not operate as a single security system. Governance, privileged access, cloud entitlements, risk detection, and compliance are delivered through multiple services that must be integrated, orchestrated, and operated independently. Over time, this creates operational complexity, delayed enforcement, and fragmented risk visibility.

This report examines a fundamentally different approach.

Cross Identity was designed as a converged identity security infrastructure, not a bundle of identity tools. All core identity functions—Access Management, Identity Governance, Privileged Access Management, Cloud Infrastructure Entitlement Management, Identity Threat Detection and Response, Identity Security Posture Management, and Data & Privacy Compliance—operate on a single architectural core with one risk engine and one control plane.

The distinction explored in this report is not about feature parity. It is about architecture.

- Microsoft Entra represents an identity bundle model, optimized for ecosystem integration and breadth.
- Cross Identity represents an identity infrastructure model, optimized for unified control, real-time risk enforcement, and operational simplicity at scale.

This document provides an architectural comparison of these two approaches, examining how design choices impact security outcomes, operational efficiency, and enterprise readiness in hybrid and multi-cloud environments.

The objective is not to displace one platform with another, but to help organizations determine which identity model aligns with their security maturity, operating reality, and long-term risk posture.

2. Understanding Microsoft Entra

Microsoft Entra is Microsoft's enterprise identity platform, evolved from Azure Active Directory and positioned as a foundational enterprise identity platform component of Microsoft's broader security and productivity ecosystem. It plays a central role in how organizations authenticate users, control access to applications, and manage identities across Microsoft cloud services.

At its core, Microsoft Entra delivers robust identity and access management capabilities, including authentication, conditional access, single sign-on, and lifecycle management for workforce and external identities. Its tight integration with Microsoft 365, Azure, Windows, and the broader Microsoft security stack makes it a natural choice for organizations operating primarily within the Microsoft ecosystem.

Over time, Microsoft Entra has expanded to include additional identity-related capabilities, such as identity governance, privileged identity management, and cloud entitlement visibility. These capabilities are delivered through distinct services—often licensed and operated separately—but presented under the Entra product family.

This design reflects Entra's historical evolution rather than a single, unified architectural blueprint. Identity governance, privileged access, cloud permissions, threat detection, and compliance are provided through multiple engines that are connected through integrations and shared portals, rather than through a single converged core.

As a result, Microsoft Entra functions best as an identity platform—providing broad coverage and strong ecosystem alignment—rather than as a fully converged identity security infrastructure. Governance decisions, privilege controls, and risk signals may originate in different systems and require orchestration across tools to achieve end-to-end enforcement.

For many organizations, this model is effective and appropriate. Microsoft Entra offers a familiar operational experience, strong native capabilities, and significant value when identity security requirements are largely contained within Microsoft-managed environments.

However, as identity security requirements expand—particularly across hybrid, multi-cloud, and non-Microsoft systems—the architectural implications of a multi-engine identity model become more pronounced. These implications form the basis for the comparisons explored in the following sections of this report.

3. The Problem with Identity Bundles

Most modern identity platforms are positioned as “all-in-one” solutions, combining multiple identity and security capabilities under a single brand or licensing model. While this approach simplifies procurement and initial adoption, it often obscures an important architectural reality: many identity platforms are bundles of distinct systems rather than a single, unified security infrastructure.

In a bundle-based model, core identity functions—such as identity governance, privileged access management, cloud entitlement management, threat detection, and compliance—are delivered as separate services. These services may share a common portal or administrative experience, but they operate on independent engines, data models, and policy frameworks.

This separation introduces what many organizations experience as an Integration Tax.

The Integration Tax is not a one-time cost. It accumulates over time in the form of custom integrations, manual workflows, duplicated policies, and operational overhead. Security teams must invest significant effort to ensure that governance decisions propagate to privileged access controls, that cloud entitlement risks result in remediation, and that identity threat signals lead to enforceable action rather than isolated alerts.

More critically, identity bundles tend to fragment risk management. Identity risk is detected in one system, analyzed in another, and enforced in yet another. This delay between detection and action increases exposure and weakens security outcomes, particularly in environments where identity misuse can escalate rapidly.

From an operational perspective, bundled architectures often result in:

- Multiple consoles and operational roles for identity security
- Longer deployment timelines driven by integration dependencies
- Higher ongoing costs associated with managing and maintaining inter-system connections
- Slower response when identity incidents span governance, privilege, and cloud entitlements

From a security perspective, the greatest risk is not missing functionality, but the gaps between systems. Attackers do not exploit the absence of features; they exploit delays, inconsistencies, and blind spots created by fragmented control planes.

As identity becomes the primary security perimeter, these gaps become increasingly difficult to justify.

Addressing this challenge requires a shift in thinking—from assembling identity capabilities to operating identity as a unified security infrastructure. That shift is the foundation of the approach examined in the next section.

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

Cross Identity was designed to address the structural limitations of bundle-based identity platforms by taking a fundamentally different approach: treating identity Cybersecurity-as-an-Infrastructure, not as a collection of integrated tools.

Rather than assembling governance, privileged access, cloud entitlements, risk detection, and compliance as separate services, Cross Identity was built from the ground up on a single, converged architectural core. All identity functions operate within one system, share one data model, and are governed by one unified policy and risk framework.

In practical terms, this means that Access Management, Identity Governance (IGA and IAG), Privileged Access Management, Cloud Infrastructure Entitlement Management, Identity Threat Detection and Response, Identity Security Posture Management, and Data & Privacy Compliance are not modules stitched together after the fact. They are native capabilities of the same identity engine.

This architectural convergence eliminates the Integration Tax inherent in bundle-based models. There are no external workflows required to synchronize governance with privilege, no delays between risk detection and enforcement, and no dependency on third-party systems to translate identity insights into action.

At the center of this design is a single control plane and unified risk engine. Risk signals from posture analysis, behavioral monitoring, privilege usage, and cloud entitlements are continuously evaluated and enforced directly within the identity layer. Governance decisions can immediately impact privileged access, cloud permissions, and access policies without orchestration across multiple systems.

Because identity security functions operate as one system, Cross Identity enables a continuous control loop:

- Risk is identified across all identity types
- Decisions are made using a unified risk model
- Enforcement is applied natively and immediately
- Posture is reassessed in real time

This approach transforms identity security from a reactive process into an operational capability that scales with enterprise complexity.

Cross Identity was built to support the realities of modern enterprises: hybrid environments, multi-cloud infrastructure, human and non-human identities, and highly regulated operating models. By abstracting identity security away from any single ecosystem, it delivers consistent control and visibility across Azure, AWS, GCP, SaaS platforms, and on-prem systems.

The architectural implications of this design become most visible when the two approaches are compared directly. That comparison is the focus of the next section.

5. Architecture Comparison

Identity Bundle vs. Converged Identity Security Infrastructure:

The most significant difference between Microsoft Entra and Cross Identity is not the list of features each platform offers, but how those features are architected and operate together.

Architecture determines how quickly risk is identified, how consistently policies are enforced, and how much operational effort is required to maintain security over time.

Bundle-Based Architecture (Microsoft Entra)

Microsoft Entra follows a bundle model, where identity capabilities are delivered through multiple services that have evolved independently and are unified at the branding and portal level.

In this model:

- Core identity, governance, privileged access, cloud entitlements, threat detection, and compliance are implemented as separate engines
  Risk signals are generated and processed across different systems
- Enforcement often requires cross-service integration or orchestration
- Identity security outcomes depend on how well these components are configured and maintained together.

This approach prioritizes breadth and ecosystem integration. It works effectively when identity requirements are relatively contained and when organizations are willing to manage the operational complexity that comes with multiple systems.

However, as identity programs scale, architectural fragmentation becomes more visible. Governance decisions may not immediately impact privileged access. Cloud entitlement risks may surface without automated remediation. Identity threats may generate alerts without direct enforcement.

Converged Infrastructure Architecture (Cross Identity)

Cross Identity follows an infrastructure model, where all identity security capabilities are built into a single, unified system.

In this architecture:

- All identity functions share the same core engine and data model
- Governance, privilege, cloud entitlements, and risk are inherently linked
- Policy enforcement is atomic and immediate
- Risk evaluation and response occur within the identity layer itself

Because there are no external integrations required to connect identity functions, security decisions propagate instantly across the entire identity lifecycle. Governance actions directly affect privileged access. Risk posture influences access and entitlements in real time. Compliance policies are enforced as part of normal identity operations.

Architectural Implications

The difference between these two models has practical consequences:

- Speed: Unified architectures reduce delay between detection and enforcement
- Consistency: Policies are applied uniformly across identity types and environments
- Resilience: Fewer integration points reduce failure modes
- Operations: Teams manage one system instead of coordinating several

Bundle architectures optimize for modularity and ecosystem alignment. Infrastructure architectures optimize for cohesion, control, and security at scale.

As identity becomes the primary attack surface, these architectural choices increasingly determine whether security programs remain manageable—or become operationally fragile.

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

Architecture Comparison

Dimension	**Microsoft Entra (Bundle Model)**	**Cross Identity (Infrastructure Model)**
Core Architecture	Multiple services unified at portal level	Single converged identity engine
Policy Model	Distributed across services	Unified policy framework
Risk Processing	Fragmented across tools	Single native risk engine (Warchief™)
Enforcement	Often delayed, cross-system	Immediate, native enforcement
Governance ⇔ Privilege	Integrated via APIs	Atomic, same system
Cloud Entitlements	Separate service	Native, embedded
Compliance	External integration	Built-in, lifecycle-driven
Operations	Multiple consoles	Single control plane

6. Capability Comparison

Architecture ultimately determines how identity capabilities function in real-world enterprise environments. While both Microsoft Entra and Cross Identity provide broad identity security coverage, the depth, consistency, and operational effectiveness of those capabilities differ significantly due to their underlying design.

This section compares how each platform delivers core identity security functions, with emphasis on convergence, enforcement, and operational reality rather than feature checklists.

Access Management

Microsoft Entra provides strong authentication and conditional access capabilities, particularly within Microsoft-managed environments. Its access controls are tightly integrated with Microsoft 365, Azure, and Windows, making it effective for organizations operating primarily within that ecosystem.

Cross Identity delivers access management as part of a unified identity layer spanning SaaS, on-prem, and multi-cloud environments. Access decisions are evaluated in the context of governance state, privilege, posture, and risk, enabling more adaptive and consistent enforcement across all identity types.

Identity Governance

Identity governance in Microsoft Entra is delivered through Entra ID Governance, which operates as an add-on service. Governance processes are effective but remain logically separate from privileged access and cloud entitlement enforcement, often requiring additional configuration to ensure alignment.

Cross Identity provides native, enterprise-grade identity governance as a foundational capability. Lifecycle management, access reviews, segregation of duties, and entitlement controls are inherently linked to access and privilege, ensuring governance decisions are enforced immediately across the identity stack.

Privileged Access Management

Microsoft Entra's privileged access capabilities are centered on Privileged Identity Management (PIM), primarily focused on Azure and Entra roles. While effective within that scope, broader privileged access across non-Microsoft systems often requires additional tools.

Cross Identity delivers full-spectrum privileged access management covering cloud, on-prem infrastructure, applications, databases, and non-human identities. Privilege controls are governed by the same policies and risk engine that manage identity lifecycle and access.

Cloud Infrastructure Entitlement Management

In the Microsoft ecosystem, cloud entitlement management is delivered through a separate service. Visibility into permissions is strong, but remediation and governance alignment can require orchestration across systems.

Cross Identity embeds cloud entitlement management directly into identity governance and risk analysis. Cloud permissions are treated as identity attributes, enabling continuous assessment and automated enforcement as part of the normal identity lifecycle.

Identity Risk and Compliance

In Microsoft environments, identity risk detection, posture assessment, and compliance enforcement are distributed across multiple services. These components integrate, but they do not operate as a single decision system.

Cross Identity unifies identity risk detection, posture management, and compliance within the same infrastructure. Risk signals directly influence access, privilege, and governance decisions without reliance on external systems or manual workflows.

Summary Observation

Microsoft Entra delivers broad and capable identity functionality, particularly within Microsoft-centric environments. Cross Identity delivers a converged set of capabilities designed to operate as a single security system across complex, hybrid, and multi- cloud enterprises.

The next section focuses specifically on identity risk—where architectural convergence has the greatest impact on security outcomes.

Capability Comparison

Capability Area	Microsoft Entra	Cross Identity
Access Management	Strong within Microsoft ecosystem	Unified across SaaS, cloud, and on-prem
Identity Governance	Add-on service	Native, core capability
Privileged Access	Azure & Entra-focused	Full-spectrum PAM
Cloud Entitlements	Separate CIEM service	Embedded into governance & risk
Identity Risk	Distributed detection	Native detection + enforcement
Multi-Cloud	Azure-optimized	Cloud-agnostic
Operations	Integration-heavy	Converged

7. Identity Risk & Intelligence

As identity becomes the primary attack vector, the effectiveness of an identity security platform is defined by how well it can detect, correlate, and enforce risk as a single decision process. The critical distinction is not whether risk signals exist, but whether they are acted upon natively and immediately within the identity layer.

Distributed Risk Processing in Bundle-Based Platforms

In bundle-based identity architectures, identity risk is handled across multiple systems. Detection, correlation, and enforcement are performed by different services, each with its own policies, telemetry, and operational ownership.

Within the Microsoft ecosystem, identity risk signals may originate from identity protection services, threat detection platforms, analytics systems, or compliance tools. While these components integrate and exchange data, they function as independent engines rather than as a single command system.

This model introduces structural limitations:

- Risk detection and enforcement are decoupled
- Response often depends on manual workflows or external orchestration
- Identity posture and real-time threat signals are evaluated separately
- Mean time to respond increases as incidents span multiple systems

As a result, identity risk management often produces alerts and insights, but relies on downstream processes to translate intelligence into action.

Warchief™: Unified Risk Engine for Identity Infrastructure

Cross Identity addresses this challenge through Warchief™, its native identity risk engine built directly into the identity security infrastructure.

Warchief™ is not an external analytics layer or add-on service. It operates within the same core engine that governs identity lifecycle, access, privilege, and entitlements. This allows risk intelligence to function as an execution layer, not just an observation layer.

Warchief™ continuously correlates:

- Identity Security Posture Management (ISPM) — identifying structural and preventive risk before exploitation
- Identity Threat Detection and Response (ITDR) — detecting abnormal behavior, misuse, and active identity attacks

Because Warchief™ shares the same data model and control plane as IGA, PAM, CIEM, and access management, risk decisions are enforced immediately across the identity stack.

Risk as a Continuous Control Loop

With Warchief™, identity risk operates as a continuous decision loop:

- Risk is evaluated across all identity types (human and non-human)
- Signals from posture, behavior, privilege, and entitlements are correlated in real time
- Enforcement actions are executed natively at the identity layer

This eliminates the gap between detection and action that exists in multi-engine architectures.

Rather than escalating identity incidents through external systems or manual playbooks, Warchief™ executes policy-driven decisions directly—adjusting access, privilege, and entitlements in response to risk.

Security and Operational Impact

By unifying preventive and reactive identity security into a single engine, Cross Identity reduces:

- Mean time to respond to identity threats
- Blast radius of compromised identities
- Operational complexity in identity incident response

In an environment where identity attacks move faster than traditional security workflows, the ability to command identity risk from within the identity infrastructure itself becomes a decisive advantage.

The next section examines how this unified risk model performs across hybrid and multi-cloud environments, where consistency and enforcement are hardest to maintain.

8. Multi-Cloud & Hybrid Reality

Modern enterprises are inherently hybrid and increasingly multi-cloud. Business applications, infrastructure, and data are distributed across Azure, AWS, GCP, SaaS platforms, and on-premises systems. In this environment, identity security must operate as a consistent control layer across all environments, not as an extension of any single ecosystem.

Ecosystem-Optimized Identity Platforms

Microsoft Entra is deeply integrated with Azure and Microsoft 365, delivering strong identity controls within the Microsoft ecosystem. For organizations whose workloads, users, and governance requirements are largely confined to Microsoft-managed environments, this tight coupling can be highly effective.

However, in hybrid and multi-cloud environments, identity coverage becomes uneven:

- Azure receives the deepest native governance and privilege controls
- AWS and GCP rely more heavily on connectors and service-specific integrations
- Privileged access and entitlement management depth varies by environment
- Consistent policy enforcement often requires additional tooling and orchestration

As environments diversify, identity security posture can fragment, increasing both operational complexity and risk.

Cloud-Agnostic Identity Infrastructure

Cross Identity was designed as a cloud-agnostic identity security infrastructure, independent of any single provider's control plane. Identity governance, privilege, risk, and compliance are enforced using the same policies and decision logic, regardless of where identities or workloads reside.

From a single platform, organizations can:

- Apply consistent access and governance controls across Azure, AWS, GCP, SaaS, and on-prem systems
- Manage human, workload, and service identities uniformly
- Enforce the same privileged access and entitlement policies across environments
- Maintain centralized visibility into identity risk and posture

Because all environments are governed by the same infrastructure and risk engine, security outcomes remain consistent as the environment scales.

Why Consistency Matters

In multi-cloud environments, attackers exploit inconsistencies between platforms. Differences in privilege models, entitlement structures, and enforcement mechanisms create opportunities for lateral movement and escalation.

An infrastructure-level identity security model reduces this risk by eliminating ecosystem bias and enforcing uniform controls across all environments. Security teams no longer need to manage separate identity strategies for each cloud; instead, identity security becomes a stable, enterprise-wide control plane.

As organizations continue to adopt hybrid and multi-cloud architectures, the ability to operate identity security consistently across all environments becomes a foundational requirement rather than an optimization. The next section examines the operational impact of these architectural differences—specifically how they affect complexity, cost, and speed at scale.

9. Operational Impact

As identity programs mature, operational efficiency becomes as important as security coverage. The ability to deploy, operate, and scale identity security without excessive complexity directly influences long-term risk posture and total cost of ownership.

Operating Identity in a Bundle-Based Model

In bundle-based identity architectures, operational complexity tends to increase over time. While individual components may be straightforward to deploy, integrating governance, privileged access, cloud entitlements, risk detection, and compliance into a cohesive operating model requires sustained effort.

Common operational challenges include:

- Multiple administrative consoles and policy frameworks
- Specialized teams required to manage different identity services
- Extended deployment timelines driven by integration dependencies
- Higher ongoing costs associated with licensing, customization, and maintenance
  Slower response when identity incidents span governance, privilege, and cloud controls

As organizations scale, identity teams often spend more time maintaining integrations and workflows than improving security outcomes.

Operating Identity as Infrastructure

With a converged identity security infrastructure, operational complexity is reduced by design. All identity functions are managed through a single control plane, governed by one policy model, and enforced by one risk engine.

This operational model enables:

- A single team to manage the entire identity lifecycle
- Faster deployments with fewer integration points
- Immediate enforcement of governance and risk decisions
- Simplified audits and compliance reporting
  Lower administrative overhead as environments scale

Because identity capabilities activate together, organizations realize value earlier and with less operational friction.

Speed and Time-to-Value

Infrastructure-based identity platforms typically achieve faster time-to-value. Instead of deploying and integrating multiple services sequentially, governance, privilege, entitlements, and risk are enabled simultaneously as part of one system.

This reduces:

- Initial implementation timelines
- Configuration drift between identity services
- Dependency on custom automation or external orchestration

Security teams can focus on defining policy and managing risk, rather than maintaining the identity stack itself.

Long-Term Sustainability

Operational sustainability is a critical but often overlooked factor in identity security. Architectures that require continuous integration and coordination across tools tend to become fragile over time.

By contrast, infrastructure-level identity security provides a stable foundation that scales with enterprise growth, regulatory requirements, and cloud adoption—without proportionally increasing operational burden.

The next section examines how these architectural differences are validated by independent analysts and why external validation matters in enterprise identity decisions.

10. When Microsoft Entra Is Enough

Microsoft Entra is a capable and widely adopted identity platform. For many organizations, it meets identity and access requirements effectively and efficiently. Not every environment requires a converged identity security infrastructure, and recognizing where Entra is sufficient is an important part of making an informed decision.

Scenarios Where Microsoft Entra Fits Well

Microsoft Entra is often the right choice when:

- The organization is primarily Microsoft-centric, with most workloads in Azure and Microsoft 365
- Identity requirements focus on authentication, single sign-on, and conditional access
- Privileged access is largely limited to Azure and Entra roles
- Identity governance needs are moderate in scale and complexity
- Cloud infrastructure entitlements outside Azure are limited or non-critical
- Identity risk response can rely on alerts and manual intervention

In these scenarios, Entra's tight ecosystem integration, familiar operational model, and licensing alignment provide strong value with relatively low friction.

Why This Matters

Acknowledging when Entra is sufficient establishes an important baseline: the goal is not to replace Entra universally, but to understand the limits of a bundle-based identity model as complexity grows.

For organizations operating within a relatively contained environment, Entra can deliver effective identity security outcomes without the need for additional infrastructure.

Where the Model Begins to Strain

As environments evolve, some organizations encounter challenges that are architectural rather than configurational:

- Governance decisions do not immediately enforce across privileged access
- Cloud entitlement risks require manual remediation
- Identity risk detection produces alerts without native enforcement
- Identity operations become fragmented across multiple systems
- Hybrid and multi-cloud environments introduce uneven security posture

These challenges are not failures of implementation. They are natural consequences of operating identity as a set of integrated services rather than as a unified infrastructure.

Recognizing this inflection point is critical. It signals when identity security requirements have outgrown a bundle-based model and when an infrastructure-level approach becomes necessary.

The final section brings this comparison together by summarizing why organizations choose Cross Identity when they reach that point.

11. Why Organizations Choose Cross Identity

Organizations choose Cross Identity when identity security evolves from a functional requirement into a strategic infrastructure decision. This shift typically occurs as environments become more complex, attack surfaces expand, and operational friction begins to undermine security outcomes.

At this stage, the primary challenge is no longer access enablement, but control at scale.

Architectural Clarity

Cross Identity is selected by organizations that recognize the limits of bundle-based identity models and require a platform designed as a single system. A converged architecture enables governance, privileged access, cloud entitlements, risk, and compliance to operate as one continuous control layer rather than as coordinated services.

This architectural clarity reduces dependency on integration, orchestration, and manual intervention—allowing identity security to function predictably as complexity increases.

Unified Risk Execution

Organizations facing heightened identity risk choose Cross Identity for its ability to evaluate and enforce risk natively within the identity layer. By unifying identity posture management and threat detection through the Warchief™ risk engine, security teams gain the ability to act decisively rather than reactively.

Risk signals are not escalated across tools; they are executed directly through access, privilege, and entitlement controls. This reduces exposure time and limits the blast radius of identity compromise.

Consistency Across Hybrid and Multi-Cloud Environments

As enterprises expand beyond a single cloud provider, identity security must remain consistent regardless of where workloads and users reside. Cross Identity provides a cloud-agnostic control plane that enforces the same policies, governance models, and risk decisions across Azure, AWS, GCP, SaaS platforms, and on-prem systems.

This consistency simplifies operations and reduces the security gaps that arise from ecosystem-specific identity tooling.

Operational Sustainability

Organizations also choose Cross Identity to simplify identity operations. Managing identity as infrastructure reduces tool sprawl, accelerates deployment, and enables smaller teams to operate larger, more complex environments.

Over time, this translates into lower total cost of ownership, faster response to identity incidents, and a more sustainable security operating model.

Strategic Outcome: Cross Identity is not chosen to replace existing identity

platforms indiscriminately. It is adopted when organizations require identity security to operate as a foundational infrastructure layer—one that can scale with enterprise growth, adapt to evolving threats, and enforce control without increasing operational burden. In this context, Cross Identity represents a shift from managing identity tools to operating identity security as infrastructure.

12. Conclusion

Identity has become the defining security control plane for modern enterprises. As environments grow more distributed and attack surfaces expand, the effectiveness of identity security is determined less by feature availability and more by architectural coherence.

Microsoft Entra delivers strong identity capabilities, particularly within Microsoft-centric environments, and remains an appropriate solution for many organizations. Its bundle-based model provides broad coverage and ecosystem alignment, especially where identity requirements are relatively contained.

However, as identity security programs mature, organizations increasingly encounter challenges that stem from architectural fragmentation—delayed enforcement, operational complexity, and inconsistent risk response across hybrid and multi-cloud environments.

Cross Identity represents a fundamentally different approach. By operating identity security as a converged infrastructure with a unified control plane and native risk execution, it enables governance, privilege, access, and risk to function as a single system.

The decision between these models is not about replacing one platform with another. It is about choosing the identity architecture that aligns with an organization's scale, complexity, and security maturity.
For organizations operating at enterprise scale, where identity risk must be managed continuously and enforced consistently, identity security infrastructure is no longer optional—it is foundational.

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