

Buyer's Compass

Privileged Access Management

Commissioned by

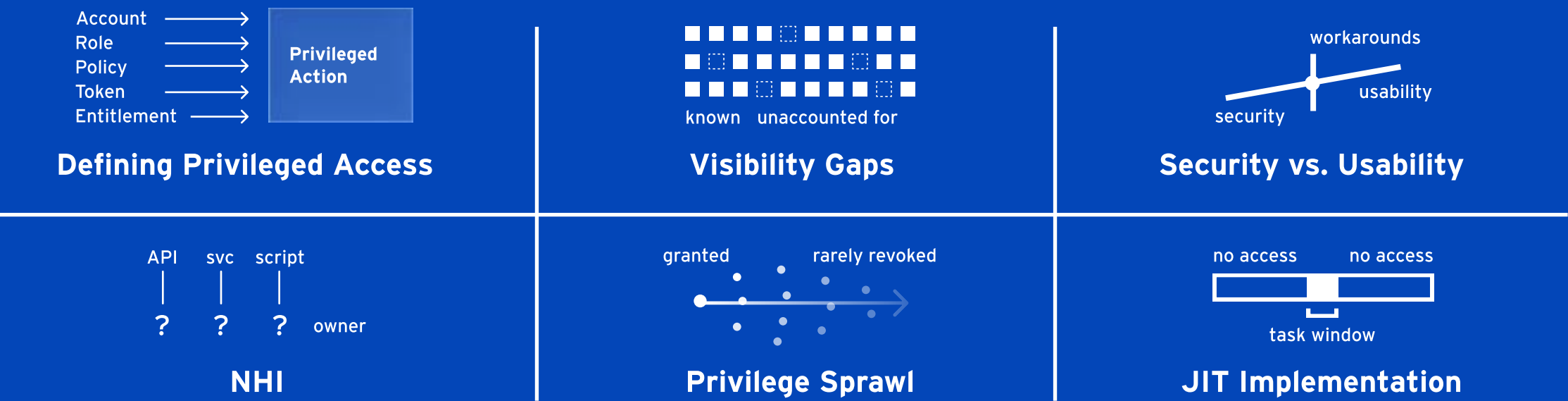
 **britive**

Privileged access remains one of the primary attack vectors in enterprise environments, yet organizations continue to struggle with defining, identifying, and controlling it effectively.

Privilege is no longer limited to a small set of administrator accounts but is distributed across human users, machine identities, applications, and automated processes. At the same time, infrastructure has become more dynamic, with access rights continuously created, modified, and revoked across systems and services. This combination of expanded scope and operational complexity makes it difficult to enforce consistent control over privileged actions.

The Challenge

The most common challenges organizations face in managing privileged access include:



Defining and Identifying Privileged Access

Privilege is increasingly tied to what an identity can do rather than the account it holds. This shifts the focus of Privileged Access Management (PAM) from managing specific identities to controlling high-impact actions, making it more complex to determine where and how PAM controls should be applied. Traditional approaches that focus on static administrator roles fail to capture the full range of privileged actions embedded in roles, policies, tokens, and application entitlements. As a result, organizations often underestimate their true privileged attack surface.

Balancing Security with Usability

PAM systems must enforce strong security measures (such as multi-factor authentication, session monitoring, and granular access control) without introducing unnecessary complexity for users. Striking the right balance between tight security and user-friendly access is a continuous challenge, as overly complex systems may lead to workarounds and risky behavior.

Managing Privilege Sprawl

Privileges accumulate over time as access is granted to support operational needs but rarely revoked when no longer required. This leads to excessive and persistent permissions across identities and systems. The gap between intended and actual access continues to widen, increasing the likelihood of misuse or exploitation by attackers.

Visibility Across Distributed Environments

Privileged access is spread across multiple systems, platforms, and services, each with its own access model and management tools. This fragmentation limits visibility into who or what has elevated permissions at any given time. Without a consolidated view, organizations struggle to assess risk, detect anomalies, or ensure that privileged access is aligned with business needs.

Securing Non-Human Identities (NHIs)

Service accounts, Application Programming Interface (APIs), automation scripts, and workloads now represent a significant portion of privileged activity. These identities often operate continuously, hold persistent permissions, and lack clear ownership or lifecycle management. Because they are not subject to the same controls as human users, they introduce substantial security exposure and are difficult to govern and monitor effectively.

Implementing Just-in-Time (JIT) Access

Reducing standing privileges requires shifting to on-demand access models where permissions are granted only when needed and for a limited duration. However, implementing JIT access across complex environments is operationally challenging without a purpose-built runtime platform. It requires integration with multiple systems, policy enforcement in real time, and coordination across teams, all of which can introduce friction if not handled carefully.

The Solution

PAM solutions are designed to secure, control, monitor, and govern access to systems, data, and services where elevated permissions are required. Rather than focusing solely on administrative accounts, PAM solutions address privilege as a set of capabilities that can be exercised by human users, applications, and machine identities.

These systems provide centralized mechanisms to discover privileged access, manage credentials and secrets, enforce policy-based authorization, and monitor privileged activity across distributed infrastructures. By limiting standing privileges and enabling context-aware access decisions, PAM supports the principle of least privilege and reduces the risk associated with compromised credentials or excessive permissions.



How the solution works

PAM solutions integrate with identity systems, infrastructure platforms, and applications to discover privileged identities and control how elevated access is granted and used. Credentials and secrets are secured in centralized vaults, while access requests are evaluated against policies that consider identity attributes, context, and risk signals. Access can be provisioned dynamically, often through JIT mechanisms, and all privileged sessions and actions are monitored, recorded, and analyzed. These capabilities allow organizations to maintain continuous visibility and control over privileged activity across both human and machine-driven operations.

Credential and Secrets Management

Reducing standing privileges requires shifting to on-demand access models where permissions are granted only when needed and for a limited duration. However, implementing JIT access across complex environments is operationally challenging without a purpose-built runtime platform. It requires integration with multiple systems, policy enforcement in real time, and coordination across teams, all of which can introduce friction if not handled carefully.

Discovery and Classification

PAM solutions continuously identify privileged accounts, roles, service accounts, and other identities across systems and platforms. This includes not only traditional administrator accounts but also application identities, APIs, and automated processes. By analyzing permissions, group memberships, and effective access, PAM systems determine which identities have elevated capabilities and classify them accordingly. This provides the foundation for applying consistent controls and reducing unmanaged or orphaned privileged access.

Policy-Based Access Control and Enforcement

Access to privileged resources is governed by centrally defined policies that determine who can access what, under which conditions, and for how long. These policies incorporate contextual information such as user role, device posture, location, time, and risk indicators. Enforcement mechanisms ensure that access is granted only when policy conditions are satisfied, replacing static entitlements with dynamic, context-aware authorization. This approach allows organizations to apply fine-grained control across diverse systems and services.

JIT Access and Privilege Elevation

PAM solutions reduce standing privileges by granting elevated access only when required. Through JIT mechanisms, users or processes request access for a specific task, which is approved and provisioned for a limited duration. Once the task is completed or the time window expires, privileges are automatically revoked. This minimizes the attack surface associated with persistent administrative rights and ensures that elevated permissions are tightly scoped and time-bound.

Privileged Activity Analytics and Risk Detection

PAM platforms analyze privileged activity to identify unusual patterns, misuse of access, or indicators of compromise. By correlating session data, identity context, and behavioral signals, these systems can detect deviations from expected activity and dynamically assign risk scores. Some solutions incorporate machine learning (ML) techniques to improve detection accuracy over time. This allows organizations to move beyond static monitoring toward continuous assessment of how privilege is exercised.

Third-Party Vendor Access Management

Reducing standing privileges requires shifting to on-demand access models where permissions are granted only when needed and for a limited duration. However, implementing JIT access across complex environments is operationally challenging without a purpose-built runtime platform. It requires integration with multiple systems, policy enforcement in real time, and coordination across teams, all of which can introduce friction if not handled carefully.

Session Management and Monitoring

Privileged sessions are proxied, monitored, and often recorded to provide visibility into how elevated access is used. PAM solutions can capture keystrokes, commands, and session activity across systems, enabling detailed audit trails. Real-time monitoring allows organizations to detect anomalous or unauthorized behavior during active sessions, and in some cases terminate sessions if risk thresholds are exceeded. This capability supports both security operations and compliance requirements.

Integration with Identity and Security Ecosystems

PAM solutions integrate with identity providers (IdPs), directory services, Identity and Governance Administration (IGA) platforms, and security tools such as Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), Identity Threat Detection and Response (ITDR), and endpoint protection systems. These integrations allow PAM to consume identity attributes, risk signals, and contextual data while sharing audit logs and activity insights with other systems. This interconnected approach ensures that privileged access controls operate as part of a broader identity and security architecture, supporting consistent enforcement, response, and visibility across environments.

Top Use Cases

1 Controlling Privileged Actions Across Identities

PAM is used to control what identities can do at the moment an action is executed. By enforcing policy-driven authorization and monitoring privileged activity in real time, organizations can prevent misuse of legitimate access and ensure that elevated capabilities are applied only within defined boundaries.

2 Reducing Standing Privileges Through JIT Access

Persistent administrative rights create unnecessary exposure. PAM enables organizations to replace standing privileges with time-bound, task-specific access that is granted only when required and automatically revoked after use. This approach limits the window of opportunity for attackers and reduces the overall attack surface without interrupting operational workflows.

3 Securing NHIs and Agentic AI

An increasingly significant proportion of privileged operations are executed by service accounts, workloads, scripts, APIs and AI agents. These identities often operate independently and hold broad permissions, making them difficult to govern with traditional controls. PAM provides visibility into these identities, manages their credentials and secrets, and enforces usage policies. This ensures that machine-driven privilege, including autonomous decision-making processes, is controlled, auditable, and aligned with least-privilege principles.

4 Protecting Credentials, Secrets, and Sessions

Privileged credentials, API keys, and cryptographic secrets remain a primary target for attackers. PAM solutions are used to securely store, rotate, and manage these sensitive assets while controlling how they are accessed and used. In parallel, session monitoring and recording provide visibility into privileged activities, allowing organizations to detect misuse, investigate incidents, and maintain a complete audit trail of administrative actions.

5 Discovering and Governing Privileged Access Exposure

Many organizations lack a clear understanding of where privilege exists and how it is distributed across systems and identities, particularly in cloud environments where access is defined through dynamic entitlements and policies. PAM, often in conjunction with Cloud Infrastructure Entitlement Management (CIEM) capabilities, is applied to discover privileged accounts, roles, and access paths, including orphaned or misconfigured permissions. By correlating identity, entitlement, and activity data across cloud platforms and enterprise systems, organizations can identify excessive privileges, enforce least privilege more consistently, and reduce the risk associated with hidden or unmanaged access.

Top Functional Selection Criteria

JIT Access

This category evaluates the vendor's capability to provide secure, on-demand access to privileged resources, which is activated only when needed, thereby minimizing the risks associated with prolonged or unnecessary access.

Credentials, Secrets, & Key Management

This measures the vendor's ability to securely store, manage, and rotate privileged credentials, including passwords, Secure Shell (SSH) keys, API tokens, and certificates. It includes vaulting, automated rotation, secure retrieval, and support for both human and machine credentials across hybrid environments.

Endpoint Privilege Management (EPM)

This evaluates the vendor's ability to control and enforce least privilege on endpoints and servers by removing standing administrative rights and enabling policy-based privilege elevation. It includes capabilities such as application-level elevation, command control, and cross-platform support (Windows, macOS, Linux) to manage privileged actions at the device level.

Identity Discovery & Visibility

This evaluates the vendor's ability to continuously discover, inventory, and provide visibility into identities, credentials, and access relationships across systems, including users, service accounts, workloads, and tokens. It ensures organizations can identify where privileged access exists, understand how it is used, and maintain ongoing oversight of access across hybrid and cloud environments.

Session Management & Monitoring

This evaluates the vendor's capabilities to establish, monitor, record, and control privileged sessions. It includes real-time session oversight, activity logging, session recording and playback, and the ability to intervene or terminate sessions to ensure accountability, auditability, and rapid incident response.

AI/ML Assistance

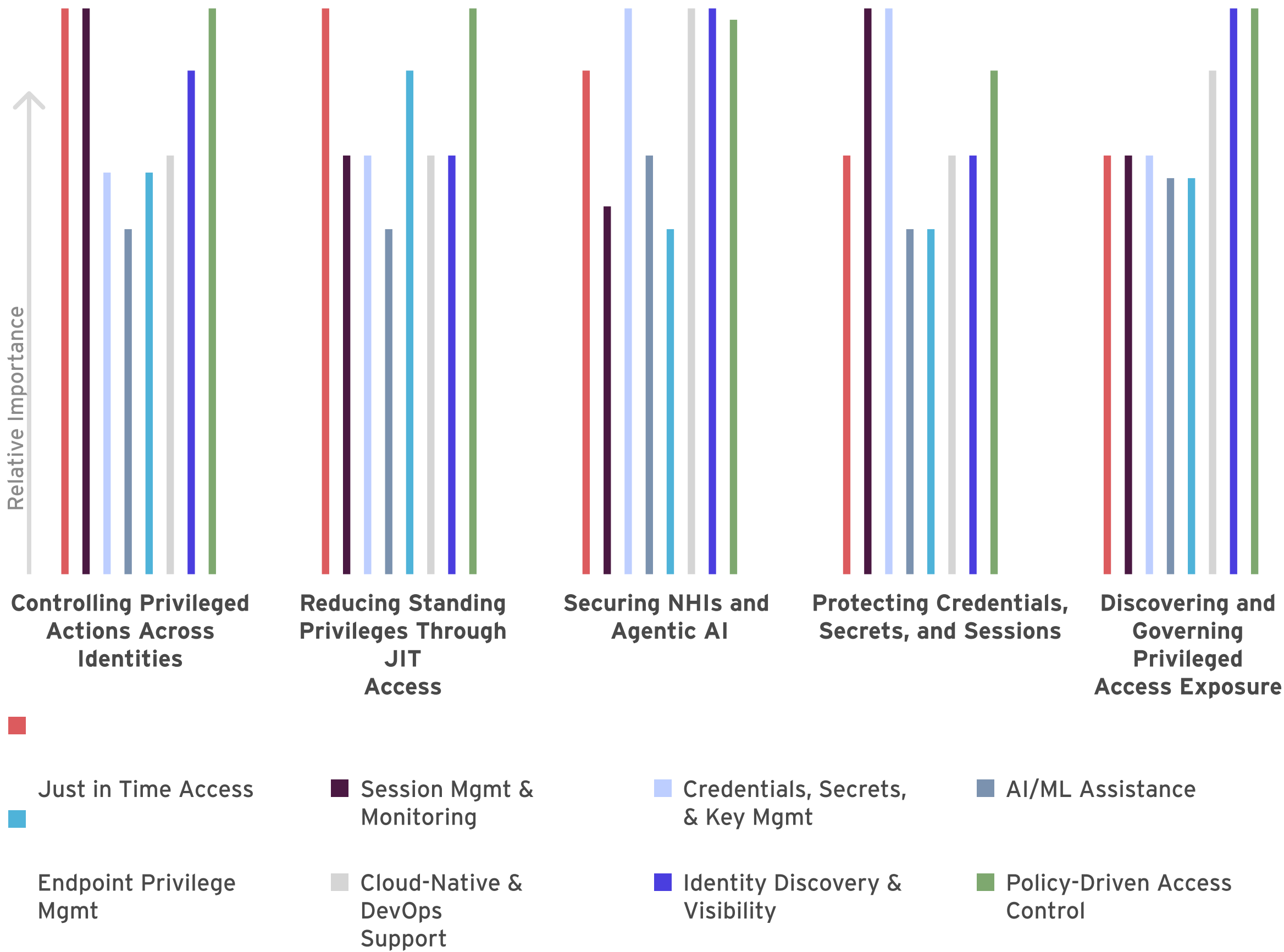
This evaluates the vendor's integration of AI and ML to enhance system functionalities, such as automating processes, usability, threat detection, predicting potential issues, and improving operational efficiency.

Cloud-Native & DevOps Support

This assesses the vendor's ability to secure privileged access across cloud and DevOps environments, including infrastructure-as-code, containers, and Continuous Integration and Continuous Delivery (CI/CD) pipelines. It covers integration with cloud platforms, support for dynamic and ephemeral workloads, and the management of privileges in modern, API-driven and automated environments.

Policy-Driven Privileged Access Control

This assesses the vendor's ability to enforce fine-grained, context-aware policies that govern when and how privileged access is granted. It includes JIT access, approval workflows, and dynamic authorization based on factors such as user, device, location, and risk, ensuring that privileged actions are tightly controlled and aligned with least privilege principles.



Vendor Spotlight

Established in 2018 and headquartered in Glendale, California, Britive is a privately held company focused on cloud-native PAM built around runtime authorization and access enforcement. Its core offering, the Britive Cloud Identity Security Platform, functions as a unified control plane for privileged access spanning human users, NHIs, and agentic identities.

The platform is delivered primarily as SaaS, with multitenant and dedicated deployment options, and extends into private environments through its lightweight Access Broker component. Britive is SOC 2 Type II compliant, licenses per managed identity, and targets mid-market and large enterprises with strong cloud footprints, concentrated mostly in North America, but with a growing presence in the EMEA and APAC region.



Founded

2018



Headquarter

Glendale, CA



Compliance

SOC 2 Type II



Core Offering

Britive Cloud Identity Security Platform



Target Market

North America, but growing in EMEA & APAC



Britive differentiates its approach from much of the PAM market by focusing on eliminating standing privileges altogether rather than optimizing how they are managed. According to the company, its approach extends beyond traditional vaulting, rotating, or gating of existing credentials through a checkout process. Instead, access is provisioned directly on the resource, at runtime, only when required and automatically revoked once the authorized task is complete, reflecting a Zero Standing Privilege (ZSP) model. Britive describes this as a foundational architectural principle that has shaped the platform since its inception, rather than a capability added in response to market demand. The platform's design is consistent with that claim. Each access request also carries a declared intent: the requesting identity, on whose behalf it acts, the task, the scope, and the duration.

Authorization evaluates the intent, not only the identity, and the same intent metadata flows through enforcement and audit.

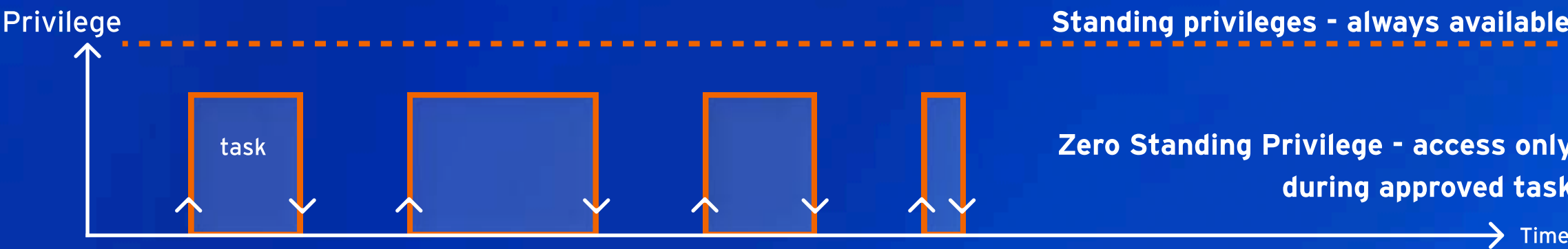
When access is requested, the platform evaluates policy and natively provisions the required permissions directly within the target cloud, SaaS, or on-premises environment. Those permissions exist only for the duration of the approved task, reducing reliance on persistent entitlements in favor of ephemeral, task-specific access while lowering the exposure associated with standing privileges and static credentials. For supported targets like AWS that support it, Britive temporarily assigns permissions within the target's native access model without provisioning a static local user. The identity assumes a role and receives short-lived, auto-expiring session credentials rather than a standing key. When access is checked in or the session expires, Britive removes the entitlement, leaving no standing assigned privilege behind.

Building on this runtime access model, Britive extends its authorization framework toward continuous authorization through the Shared Signals Framework (SSF). Rather than relying solely on the authorization decision made when privileges are granted, the platform can consume external risk signals during an active session and reevaluate authorization using attribute-based access control (ABAC) and policy-based access control (PBAC), allowing access to be adjusted or revoked as policy conditions change.

KuppingerCole Analysts believes that static authorization decisions are becoming insufficient for modern environments where risk changes continuously. Standards such as SSF provide the foundation for adaptive authorization by allowing security and identity systems to exchange risk signals in real-time. This enables access decisions to be reassessed as context changes, making continuous authorization an important capability for organizations pursuing mature Zero Trust architectures.

Britive treats every identity, non-human, agentic AI, and human, as a first-class citizen within the same policy model.

Organizations can register AI agents in Britive as local or federated identities. Federated identities authenticate through workload identity federation using SPIFFE, AWS STS, OIDC or SAML based providers. Britive also discovers agents and presents them with the permissions they hold so they can be onboarded as governed AI identities, beginning with agents created through the cloud providers' native agent platforms. Each agent carries metadata that includes its job function, business use, owner, and other custom attributes. Profile-based policies define which permissions an agent may request and, where applicable, which user privileges it may exercise on behalf of another identity.



The same policy model applies wherever the target system runs. Agents registered through a cloud agent platform routinely need to act on systems that sit outside it, including on-premises databases, data lakes, and applications that authenticate with credentials rather than tokens. Britive creates those permissions in the target system's own access model, keeps the underlying credential outside the agent's reach, and continues enforcing the granted scope at the resource, down to individual commands.

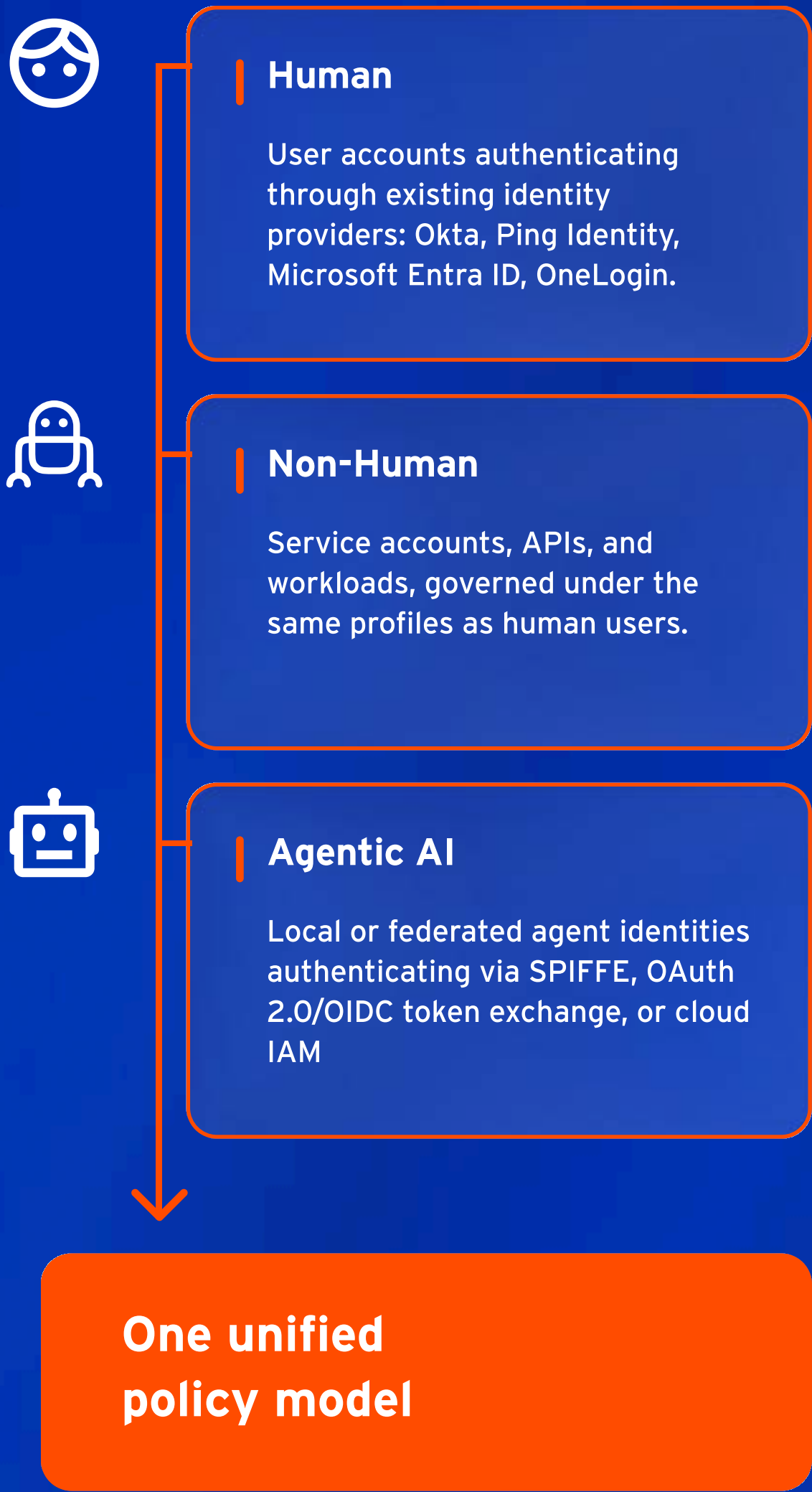
Britive extends this model to Model Context Protocol (MCP) traffic through the Britive MCP Gateway, a policy enforcement point deployed in the customer environment in front of an organization's MCP servers. Every tool call is evaluated against central policy at the moment of the call, with default deny: tools an identity is not entitled to are not visible to it, and a permitted call that requires privilege triggers a checkout that provisions the permission in the target system and revokes it when the task ends.

For targets that require credentials, the gateway holds and injects them at runtime, so the agent never receives a credential to hold or leak.

As data returns from the downstream server, the gateway can inspect every return payload, scanning for information that may be dangerous such as a hidden prompt-injections, blocklist URLs, obfuscation (zero-width characters, Unicode tag characters, Base64-encoded payloads), and secrets (AWS keys, application tokens, SSH keys, and similar). Flagged payloads are either sanitized or blocked from reaching the calling agent. Agents can also interact with the Britive platform itself, listing profiles and checking access out and in programmatically, through Britive's MCP server.

Sensitive operations can require human approval before access is granted, and permissions are automatically revoked once the task finishes. Every authorization decision, permission grant, and revocation is immutably logged and linked to the corresponding identity, creating a

comprehensive audit trail. For MCP tool calls, the audit record can also include the initiating prompt and the model's stated rationale for selecting the tool, as supplied by the client, alongside the arguments and outcome. This telemetry can be forwarded to external Security Information and Event Management (SIEM) systems for centralized monitoring and to Security Orchestration,



Automation, and Response (SOAR) platforms for automated response, while continuous trust evaluation tracks agent behavior for anomalous activity.

Moreover, the solution provides centralized dashboards and reporting capabilities that aggregate identity activity, entitlement usage, and audit trails into a single interface. Britive supports traditional PAM features while maintaining a modern architectural and deployment approach. Session management includes policy-based recording and monitoring of Secure Shell (SSH), Remote Desktop Protocol (RDP), database, and Kubernetes sessions, with playback, live monitoring, and session termination capabilities governed by policy. Administrators can also monitor sessions live, and database sessions can be replayed at the query level, with credentials and secrets masked in recordings. Crucially, sessions running through the MCP Gateway can also be monitored and recorded, providing human oversight and exact evidence of agentic activity in sensitive systems. Sessions can be established using native clients, such as RDP and SSH, or through a browser-based interface. The platform avoids thick proxies and endpoint agents while still supporting protocol-level command filtering and blocking. Credential and secret management is handled through an integrated vault supporting generation, rotation, versioning, and ephemeral credential issuance. The platform also extends to DevOps workflows, offering Terraform-based configuration and policy enforcement within pipelines. Britive also takes an agentless approach to Endpoint Privilege Management (EPM) by integrating directly with common EPM solutions such as CrowdStrike Falcon and Microsoft Defender.

Britive's API-first and agentless design allows direct integration with cloud providers, SaaS platforms, and infrastructure services without relying on proxies. Britive provides out-of-the-box integrations for major cloud providers, identity providers, SIEM/SOAR, and DevOps tools, though some environments may require more hands-on configuration than connector-based approaches. The platform integrates with existing identity providers such as Okta, Ping Identity, Microsoft Entra ID, Idira, and OneLogin for authentication, focusing instead on authorization and permission delivery.

This separation allows organizations to retain their existing IAM stack while introducing fine-grained, time-bound privilege control across diverse environments.

Looking ahead, Britive's roadmap is focused on expanding its support for the emerging agentic workforce. As described above, MCP support is delivered to Britive's customers through two components: the remote Britive MCP server, which exposes the platform's own operations as tools, and the Britive MCP Gateway.

Continued work extends the range of active security controls in the gateway and the authentication methods agents can use to reach it. This includes behavioral analysis for AI agents, where LLM-based techniques are intended to identify anomalous behavior or task misalignment during execution rather than relying solely on post-event analysis. It is also expanding lifecycle management for AI agents and other NHIs, which are created, modified, and retired far more dynamically than traditional user accounts.

Britive continues to extend its authorization model into on-premises environments through native protocol support and session recording for servers, databases, and network devices, with the goal of applying the same authorization framework across hybrid infrastructure. For organizations evaluating Britive, the key differentiator is not simply support for JIT access, an increasingly common capability across the PAM market, but its commitment to a ZSP architecture.

The platform assumes that privileges should not exist until they are needed, regardless of whether the requesting identity is human, machine, service, or AI agent.

As organizations adopt cloud-native architectures and autonomous AI systems, this architectural shift, runtime authorization and access enforcement under one unified control plane, is likely to become an increasingly important criterion for modern PAM use cases.



Considerations

Architectural considerations

Deployment

PAM solutions are delivered through a range of deployment models, reflecting the diversity of enterprise infrastructure and regulatory requirements. Many vendors provide SaaS-based offerings to simplify operations and enable scalability, while others support self-hosted deployments for organizations requiring greater control over sensitive systems and credentials. Appliance-based models also remain relevant, particularly where isolation of privileged access infrastructure is required. The choice of deployment model should align with operational practices, data residency obligations, and internal security policies.

Integrations and interoperability

To ensure seamless operation within an organization's broader security and IT environment, PAM solutions must integrate with a variety of systems, including Identity Governance, SIEM, DevOps, and IT service management (ITSM) tools. Most PAM platforms support RESTful APIs and offer built-in connectors for common platforms. Interoperability with these tools ensures smooth operations and enhances security controls.

Identity Fabrics alignment

PAM capabilities should be considered within the broader identity architecture rather than as a standalone control. Privileged access decisions depend on identity context, policy enforcement, and real-time signals from across the environment. Solutions that can both consume and contribute identity context through standardized interfaces allow privilege to be governed consistently across systems, identities, and workloads.

Pre-deployment considerations

Before deploying a PAM solution, organizations should assess their current privileged access risks, define their user roles, and map out their privileged accounts. It's also important to ensure that the PAM solution aligns with existing security policies, cloud infrastructure, and compliance requirements. Consideration should be given to how the PAM platform will integrate with current systems and processes.

At the same time, not all organizations operate highly dynamic or automation-driven environments. Many still require the foundational capabilities of traditional PAM, such as credential vaulting, session control, and administrative access governance, to address immediate risks and establish baseline control over privileged access.

Questions to Ask Vendors during RFPs

How does your solution support both traditional and evolving PAM use cases?

The solution should provide strong foundational capabilities such as credential vaulting, session monitoring, and access control, while also supporting newer requirements like managing NHIs and dynamic privilege assignment, enabling organizations to expand their PAM program over time without replacing core components.

How do you define privileged access in modern environments?

Privilege is increasingly tied to actions rather than identities. Understanding how a vendor defines privilege helps clarify the scope of protection, especially across human and machine-driven access.

How does your solution identify and discover privileged access across systems?

Many organizations lack visibility into what is truly privileged, especially as they continue to scale. Continuous discovery of accounts, credentials, and access paths is foundational to any PAM deployment.

How do you support JIT access and reduce standing privileges?

Reducing persistent access is central to modern PAM. Vendors should demonstrate how access is granted dynamically, time-bound, and automatically revoked.

Can privileged access be automatically approved based on policy and context?

Manual approval workflows do not scale. Policy-driven automation based on context (device, risk, location, etc.) is critical for operational efficiency and security.

How does your solution enforce control over privileged actions, not just access?

The core challenge is not granting access but controlling what can be done with it. Vendors should explain how they enforce restrictions at the point of action.

How does your solution support session monitoring and recording?

Session visibility is essential for audit and incident response. Real-time monitoring and the ability to terminate or control sessions are key capabilities.

How does your solution manage credentials, secrets, and machine access?

Modern environments rely heavily on non-human access. Vendors should demonstrate how they secure passwords, keys, tokens, workload identities, etc.

How does your solution support cloud-native and DevOps environments?

PAM must extend beyond traditional infrastructure. Support for APIs, CI/CD pipelines, containers, and cloud platforms is increasingly important.

How does your solution enforce policy-driven and context-aware access control?

Static roles are insufficient in dynamic environments. Vendors should support fine-grained, policy-based access decisions based on real-time conditions.

How does your solution integrate with identity, security, and IT operations tools?

PAM does not operate in isolation. Integration with IGA, SIEM, ITDR, SOAR, and cloud platforms is critical for end-to-end security and automation.

How does your solution support auditability and compliance requirements?

While compliance is not the primary driver, organizations still require strong audit trails and reporting to demonstrate control over privileged access.

What deployment models are supported, and how do they impact scalability and operations?

Deployment flexibility remains important, but organizations should focus on how deployment choices affect security, performance, and operational complexity.

What does the implementation and onboarding process look like?

Time-to-value is a key consideration. Vendors should provide clarity on deployment timelines, required resources, and ongoing support.

Can you provide reference customers with similar environments or requirements?

Real-world validation is critical. Speaking with customers helps assess how the solution performs in comparable use cases and operational contexts.

Recommendations



Prioritize a least privilege model with JIT access to reduce standing permissions and limit risk exposure.



Focus on cloud readiness and CIEM capabilities as environments become more cloud-centric.



Keep strong controls such as multifactor authentication and session monitoring in place for accountability and auditability.



Integrate PAM with the broader security and identity infrastructure, including IGA, SIEM and DevOps platforms.



Use automation and AI-driven analytics to improve efficiency and detect anomalous behavior.



Ensure the PAM strategy supports scalability, compliance and governance, with adequate user training and vendor support.

Contact Us

KuppingerCole Analysts AG

kuppingercole.com

info@kuppingercole.com

Visit [KuppingerCole.com](https://kuppingercole.com) ↗

Copyright

©2026 KuppingerCole Analysts AG. All rights reserved. Reproducing or distributing this publication in any form is prohibited without prior written permission. The conclusions, recommendations, and predictions in this document reflect KuppingerCole's initial views. As we gather more information and conduct deeper analysis, the positions presented here may undergo refinements or significant changes. KuppingerCole disclaims all warranties regarding the completeness, accuracy, and adequacy of this information. Although KuppingerCole research documents may discuss legal issues related to information security and technology, we do not provide legal services or advice, and our publications should not be used as such. KuppingerCole assumes no liability for errors or inadequacies in the information contained in this document. Any expressed opinion may change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Their use does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

For further information, please contact clients@kuppingercole.com.