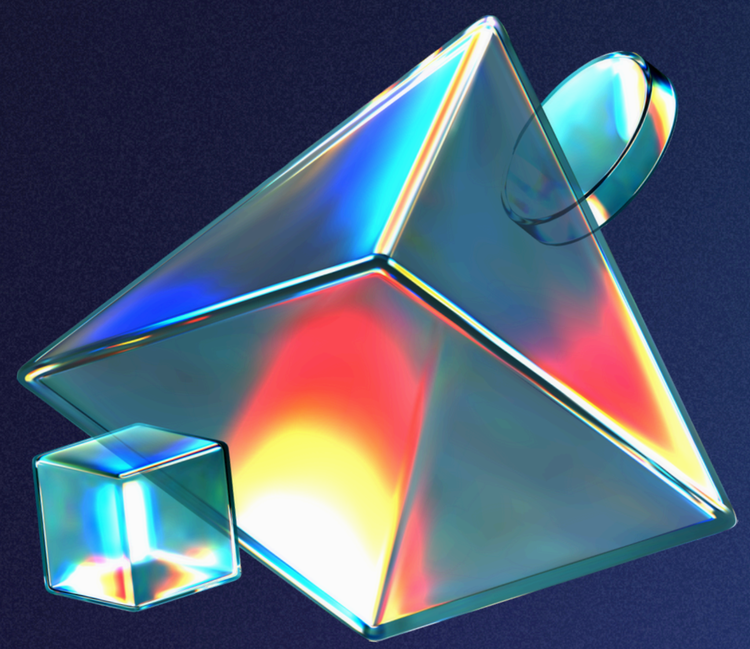
britive

>_ WHITEPAPER

Zero Trust in the Cloud Era

A Blueprint for Secure Identity Lifecycle Management



SUMMARY

As organizations adopt cloud-first strategies and multi-cloud environments, implementing Zero Trust principles has become essential for securing modern, distributed ecosystems. The Zero Trust model challenges traditional security approaches by eliminating implicit trust and enforcing continuous validation of users and devices. This whitepaper explores the foundational principles of Zero Trust, the role of modern Privileged Access Management (PAM) platforms in its implementation, and actionable strategies to enhance security and scalability through identity lifecycle management.

HIGHLIGHTS

Zero Trust Fundamentals	At its core, Zero Trust operates under the principle of “never trust, always verify,” emphasizing granular access control, least privilege, just-in-time permissions, and continuous authentication to mitigate threats.
Critical Role of PAM in Zero Trust	Cloud-native PAM platforms are a foundational part of zero trust architectures by enabling centralized, dynamic access management across diverse environments, supporting seamless integration with existing tools and ensuring robust compliance and visibility.
Actionable Strategies for Implementation	From inventorying identities and automating access lifecycle processes to adopting just-in-time credentials and securing non-human identities (NHIs), this guide offers practical steps to align with Zero Trust objectives.
Non-Human Identity Management	As NHIs proliferate in modern cloud ecosystems, their secure management is critical for reducing attack surfaces and ensuring operational efficiency.

UNDERSTANDING THE CORE ELEMENTS OF ZERO TRUST SECURITY

Fundamental Principles	Zero Trust operates under the principle of "never trust, always verify," emphasizing granular access control, least privilege, zero standing privileges, and continuous authentication to mitigate threats.
PAM Integration	Cloud native Privileged Access Management platforms enable centralized, dynamic access management across diverse multi-cloud and hybrid environments, supporting seamless integration with existing tools and maintaining robust compliance.
Implementation Framework	This guide provides practical steps for inventorying identities, automating access lifecycle processes, adopting just-in-time credentials, and securing non-human identities (NHIs).
Identity-Centric Security	As organizations shift to cloud environments, securing all identities—human and non-human—throughout their lifecycle becomes critical for reducing attack surfaces and maintaining operational efficiency.

WHY ZERO TRUST IS CRITICAL TODAY

The transition to cloud-first strategies, multi-cloud architectures, and hybrid environments has fundamentally transformed organizational operations. This evolution brings with it an increasingly sophisticated threat landscape, where the lack of traditional perimeters amplifies identity-related vulnerabilities.

Traditional approaches to identity management using static credentials, overprovisioned access, and siloed identity management no longer adequately protect sensitive data while meeting the demands of modern, cloud-forward teams. It is insufficient to protect access only to resources inside the network—especially as team members, devices, and segments are increasingly dispersed across multiple cloud tools, infrastructures, and geographies.

While the concept of Zero Trust has been around for years, only recently has interest really accelerated. This is because Zero Trust is a critical framework designed specifically for these contemporary challenges. By treating no user or system as inherently trustworthy, Zero Trust requires granular access control, continuous verification, and adaptive security measures to minimize risk.

CORE PRINCIPLES OF ZERO TRUST

Zero Trust is essentially a security model that requires all users and devices to be authenticated, authorized, and validated before being granted any permissions to resources or data—regardless of whether the request comes from inside or outside the organization's network.

The goal is to minimize risk by enforcing accurate, least privilege per-request access decisions across information systems and services. A major side benefit of this approach is a reduced blast radius in the event of an identity compromise. Segmenting privileges and verifying identity and authorization at each step means the access an attacker uses to get into one part of the network does not give them automatic access to systems and data in the network or access to other network segments.

Never Trust, Always Verify

The goal is to minimize risk by enforcing accurate, least privilege per-request access decisions across information systems and services. A major side benefit of this approach is a reduced blast radius in the event of an identity compromise. Segmenting privileges and verifying identity and authorization at each step means the access an attacker uses to get into one part of the network does not give them automatic access to systems and data in the network or access to other network segments.

Apply Least-Privileged Access (LPA)

Users and systems receive only the minimum access required for their specific tasks, with permissions dynamically assigned and revoked. Reducing or eliminating static privileges and moving to a JIT model limits potential privilege misuse as well as impact of any potential credential breach.

Assume Breach

Organizations must operate under the assumption that systems are already compromised and work to limit potential damage through reduced attack surfaces and granular access controls. JIT privileges with LPA are complementary, proactive risk mitigation approaches that can significantly reduce your attack surface.

WHY CLOUD-NATIVE PAM PLATFORMS ARE CRITICAL FOR ZERO TRUST IN MODERN CLOUD ENVIRONMENTS

Modern Privileged Access Management platforms, designed for multi-cloud ecosystems, serve as the foundation for implementing Zero Trust Architecture (ZTA).

These platforms should be capable of:

Unified Identity and Access Management

- Provide centralized control across AWS, Azure, GCP, and other cloud infrastructure and on-premises environments.
- Consistent security policy enforcement.
- Reduction of risk due to configuration errors or policy inconsistency.

Granular, Context-Aware Access Control and Enforcement

- Implement least privilege and zero standing privileges (ZSP) across environments.
- Grant access based on comprehensive contextual factors such as role, task, time of day, and location.
- Control access at deeper workload and application levels for consistent enforcement.

Dynamic, Just-in-Time Access and Credential Management

- Eliminate persistent credentials through short-lived, task-specific permissions.
- Minimize the impact of potential credential compromise.
- Support just-in-time (JIT) access provisioning.

Seamless Enterprise Tool Integrations

- Integrate with CI/CD pipelines, Kubernetes clusters, SaaS applications, and other tools through deep API capabilities.
- Enable continuous security monitoring with seamless data transfer through existing tools
- Maintain operational workflow efficiency with minimal disruption and manual effort.

Scalable Compliance and Visibility

- Centralize logging and audit trails for regulatory compliance with regulations like SOC 2, PCI DSS, and others.
- Provide real-time access pattern visibility in combination with other detection and visibility tools.
- Enable proactive threat detection and response within the full security suite.

By leveraging a multi-cloud native PAM platform, organizations can effectively implement Zero Trust principles, ensuring that every access request is validated and every identity is secured.

ACTIONABLE STRATEGIES FOR IMPLEMENTING ZERO TRUST

Inventory and Analyze All Identities

A comprehensive understanding of all identities, from standard human users to automations and other non-human identities (NHIs), is foundational for Zero Trust. Without an accurate inventory, it's impossible to manage access effectively or mitigate risks.

SUGGESTED ACTIONS

- Conduct an audit of all human identities and NHIs, including service accounts, API tokens, and robotic process automation (RPA) accounts.
- Use discovery tools to identify shadow IT and unmanaged identities across environments.
- Classify and prioritize identities based on risk levels and privilege scope. Prioritize security of high-risk identities with excessive privileges.

Implement Least-Privilege Access or Zero Standing Privileges (ZSP) for all Identities

Static permissions present significant security risks—especially when accessed with static, long-lived credentials. Dynamic access management removes static, reducing the attack surface to achieve zero standing privileges. Least-privilege access removes unnecessary, high-risk permissions, reducing the attack surface and risk from accidents.

SUGGESTED ACTIONS

- Transition from static, long-lived credentials for both human accounts and NHIs. Replace hardcoded secrets in scripts and automations with ephemeral credentials.
- Move static privileges, where possible, to just-in-time (JIT) privilege delivery. Privileges are automatically revoked after a set period for zero standing privileges.
- Regularly review and adjust roles and permissions to eliminate unnecessary privileges. Implement automated review and adjustment processes where possible.
- Enforce role-based and attribute-based access control (RBAC/ABAC) for granular permission management and automated NHI access management.

Adopt Granular, Policy-Driven, Identity-Centric Controls

Precise access management controls reduce risk exposure and improve overall security posture. By utilizing contextual identity and other data, access aligns with organizational security policies without hindering operations.

SUGGESTED ACTIONS

- Define attribute-based policies that incorporate contextual factors such as role, location, time of access, device, and others.
- Enhance security by implementing conditional access rules such as on call verification for break glass access or step-up MFA for high-risk privileges.
- Validate policy effectiveness through regular and continuous testing.

Centralize Identity Management Across Environments

Unified management ensures consistent policy enforcement across environments, simplifying oversight and maintenance.

SUGGESTED ACTIONS

- Deploy an identity control plane to manage permissions across cloud platforms, SaaS tools, Kubernetes clusters, and on-prem systems.
- Deploy a centralized identity platform to manage permissions for all identities across all platforms in the environment.
- Leverage integrations with existing security and operational tools such as identity governance and administration (IGA) systems, identity providers (IdPs), CI/CD pipelines, and others.
- Implement comprehensive access monitoring and analysis for real-time, high-context identity insights and posture management.

Automate Identity Lifecycle Management and Security Policy Enforcement

Manual processes are error-prone and resource-intensive. Automation of access provisioning, modification, and deprovisioning ensures accuracy and scalability across operations.

SUGGESTED ACTIONS

- Automate established workflows for onboarding, offboarding, and role changes to minimize or eliminate manual intervention.
- Implement automatic access revocation for inactive or orphaned accounts to reduce unnecessary exposure.
- Integrate with governance tools to streamline compliance reviews against internal and external policies.

Enhance Authentication Security

Reduce reliance and risk from static credentials by adding additional authentication protections such as Multi-Factor authentication (MFA) and establish limited-scope trust relationships.

SUGGESTED ACTIONS

- Require MFA for high-risk operations, such as accessing sensitive data or making configuration changes.
- When using technologies like OIDC, define narrow trust relationships between systems providing non-human identities like APIs and CI/CD workloads and their consuming systems to reduce the risk of unauthorized NHI access and behavior.
- Deploy adaptive authentication based on contextual risk factors to mitigate risk of compromise. For example, require step-up MFA for access outside normal business hours.

Align Access Management with Compliance Needs

Regulatory compliance often drives security requirements and business operations. Zero Trust practices will strongly support and enable meeting compliance needs.

SUGGESTED ACTIONS

- Implement centralized logging to track all access requests, approvals, and activities.
- Generate automated compliance reporting tailored to chosen regulatory frameworks.
- Create and enforce standardized policy templates aligned with these compliance frameworks.

Regular Zero Trust Strategy Assessment

Security requirements evolve continuously with new threats and technologies. An effective Zero Trust strategy must respond and change accordingly.

SUGGESTED ACTIONS

- Conduct regular penetration tests, review access logs, and refine policies to adapt to changing business conditions and emerging threats.
- Conduct regular tests to identify any weaknesses in access controls.
- Review access patterns and audit logs to ensure compliance and identify any emerging trends.
- Update security policies based on new threats or identified challenges.

THE PATH FORWARD

COMBINING ZERO TRUST WITH MODERN IDENTITY AND ACCESS TOOLS

Achieving Zero Trust can't be done with a single product or tool, but through a strategic framework implemented across your identity, network, and workloads.

Finding and integrating a cloud-native PAM designed specifically to meet the needs of modern multi-cloud and hybrid environments allows organizations to seamlessly integrate Zero Trust principles into their operations, reducing risk while enabling scalability and innovation.

KEY TAKEAWAYS

Identity is the New Perimeter

Security must be considered for every identity — human and non-human — at every stage of its lifecycle.

Dynamic Access is Essential

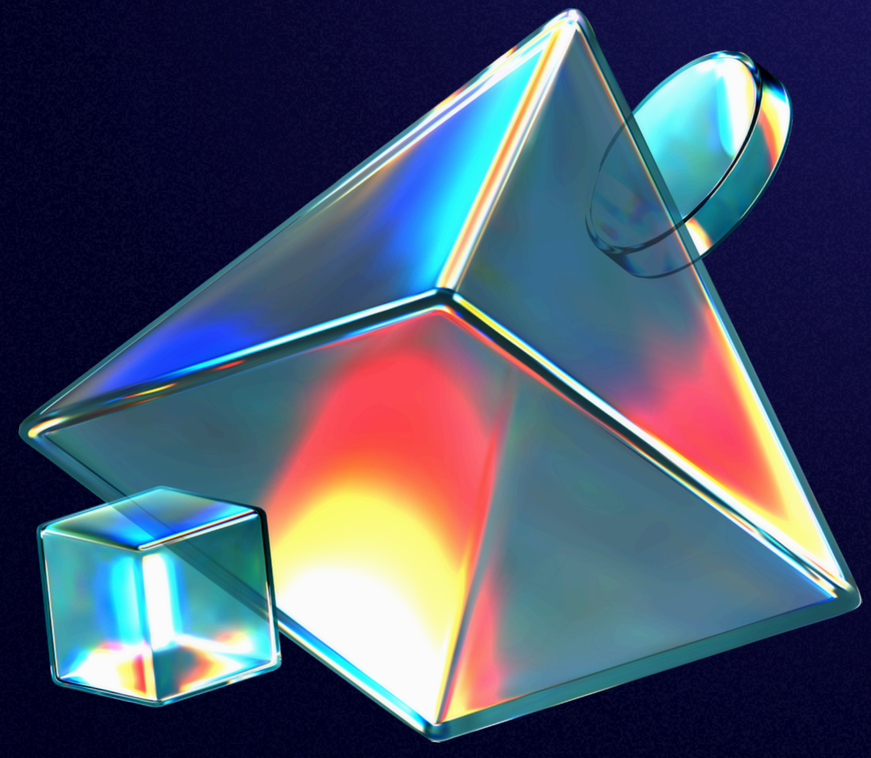
Static credentials must be replaced with temporary, task-specific access across the environment.

Unify and Automate

Central identity management and automated processes ensure scalability and efficiency.

Stay Adaptive

Regularly review and evolve your strategy to address new threats and operational requirements.

By adopting these strategies and leveraging modern PAM platforms, organizations can align their security practices with Zero Trust principles, enabling robust security, regulatory compliance, and operational efficiency across today's complex cloud landscape.

Learn More ↳