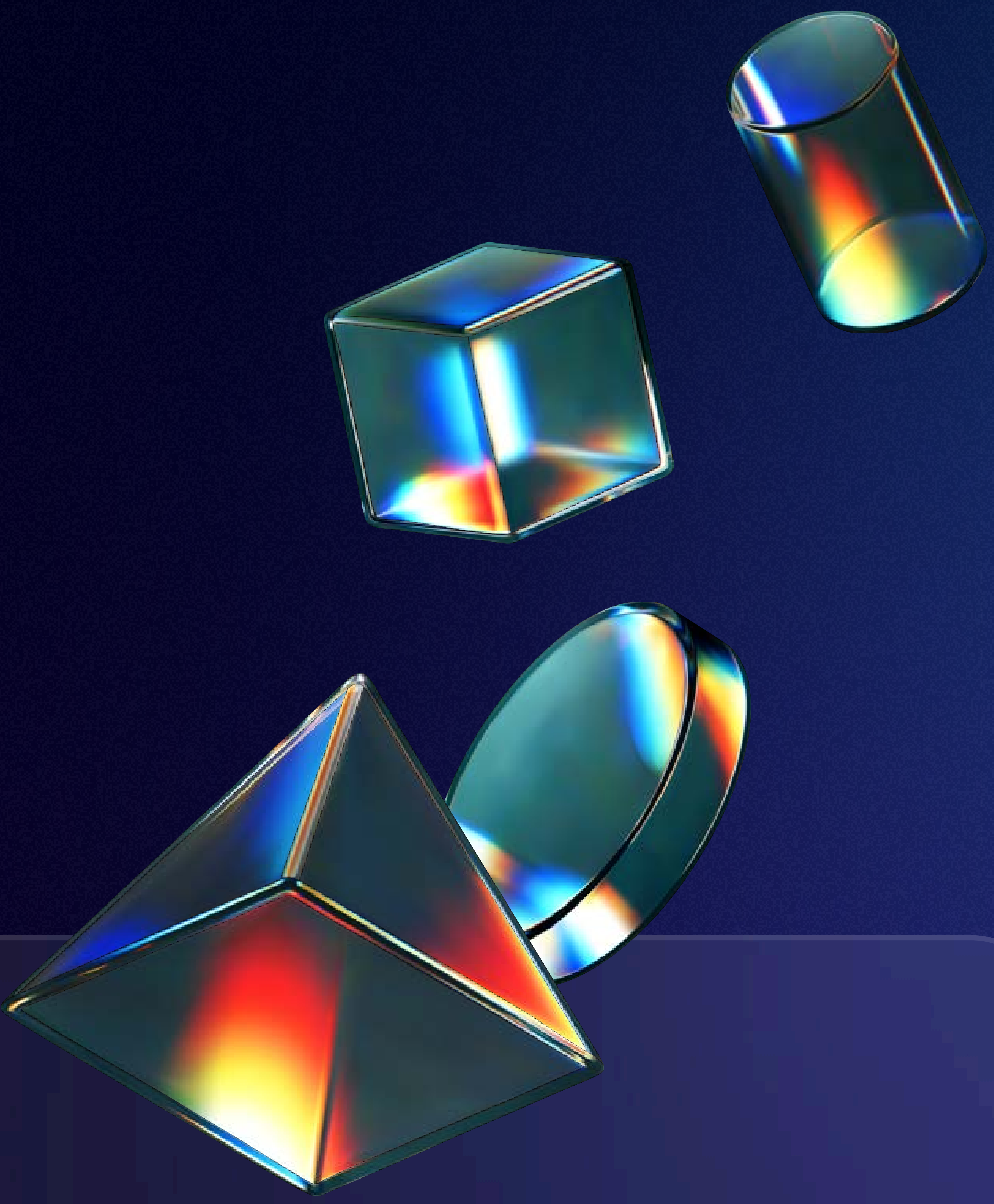
Securing Machine Identities in Modern Cloud Environments



THE NHI EXPLOSION IN CLOUD AUTOMATION

Cloud adoption has significantly increased the use of non-human identities (NHIs) —including machine identities, service accounts, and bots — across organizations. They're often used to drive automated processes, enhancing efficiency and reducing human error. However, they're also proliferating at a massive rate.

Machine identities greatly outnumber human identities, in some cases outnumbering human identities as much as 50 to 1. This widespread use of NHIs across multi-cloud environments presents critical security challenges, especially since securing these identities is often done differently to their human counterparts. For example, NHIs don't support multi-factor authentication (MFA), making it harder to secure.

Given the rise and prevalence of identity-based breaches, with compromised credentials reported as one of the most common attack vectors, unsecured NHIs represent a large potential attack vector. With their reliance on statically configured keys, tokens, certificates, and other authentication and permissioning methods, securing them alongside proliferating human identities across cloud platforms represents a risk that organizations need to tackle early on.

BEYOND HUMAN IDENTITIES

THE CHALLENGES IN SECURING THE MACHINE-DRIVEN FUTURE

While human identity management typically revolves around passwords, role-based access control (RBAC), and MFA, securing machine identities requires a fundamentally different approach because of the nature and configuration of their access.

NHIs are used to execute tasks like running scripts, patching systems, or deploying containers within the CI/CD pipeline. Since they're designed to run automatically at all hours and across entire systems, they typically operate independently of human interaction or control.

NHIs can be spun up and configured quickly across processes and different cloud environments as needed. If an organization doesn't have a strong policy on logging, managing, and monitoring these identities, the number of NHIs and their levels of access can become a large, un-regulated target for potential exploitation.

This often highlights and exacerbates the effects of a **lack of centralized visibility** into identities and permissions across the environment, which results in potential gaps in access management. This results in situations where NHIs are left running unchecked for fear of disrupting a process critical for day-to-day operations.

Legacy security approaches — such as vaulting and rotating static credentials — fail to account for the highly dynamic nature of machine identities in cloud environments. This results in over-provisioned identities, increased exposure to attack vectors, and unmanaged credentials embedded in code, making them difficult to update or secure.

Since NHIs often require elevated privileges to execute their set tasks, static permissions increase potential risk of a large-scale impact on an organization if their credentials are compromised.

This is where part of the demand for a more dynamic, cloud-native security solution stems from: eliminating standing access while automating privilege management to ensure minimal disruption in existing workflows for both human and non-human identities.

DYNAMIC PRIVILEGE MANAGEMENT

ZERO STANDING PRIVILEGES FOR NHIS

Machine identities, like human users, are often over-privileged because traditional security models tie authentication and authorization together. NHIs are often given static credentials with predefined permissions, leaving them susceptible to compromise.

This is where an organization's identity team can benefit from **decoupling authentication and authorization**.

Separating identities from the permissions they have access to allows organizations to provision identities with a true just-in-time (JIT) process, where permissions to sensitive or privileged resources are assigned and accessible only when needed.

Dynamic permissioning with ephemeral or temporarily assigned permissions goes beyond the principle of least privilege, where identities only have access to the absolute minimum privileges and permissions, they need to complete a given task.

True JIT permissioning opens the door for security and identity teams to implement zero standing privileges (ZSP), where identities in the environment exist without any inherent privileges attached. Using credentials directly will give access to these accounts, but there will be no permissions accessible without going through the JIT workflow.

In an environment with dynamic permissioning enabled, machine identities authenticate into the system they need access to, request the necessary permissions through a separate secure, trusted platform or system, and complete their tasks with short-lived access credentials that have a pre-configured expiration. Once the task is done, the credentials expire or are removed, eliminating the risk of standing privileges.

ACTIONABLE STRATEGIES FOR SECURING NHIS ACROSS THE CLOUD

To fully secure machine identities across dynamic cloud environments, organizations must adopt proactive strategies that scale with automation. The following techniques can mitigate the risks associated with machine identities:

Decouple Authentication & Authorization

This is the foundation of Zero Trust for machine identities. By separating credentials (authentication) from permissions (authorization), machine identities can authenticate to cloud environments without inheriting unnecessary privileges. Privileges are provisioned on demand and expire once the task is completed.

Centralize and Scale Privilege Management

Centralizing the management of machine identities across all cloud environments helps eliminate privilege sprawl and reduces reliance on static credentials. This process should be automated to align with cloud velocity, as manually managing identities is no longer scalable in environments with thousands of machine identities.

Gain Unified Access Visibility

Security teams need a holistic view of machine identity activity from a single platform. This should include a single source for detailed activity logs of identity and access data, including which identities accessed which resources, when, and with what permissions. This visibility ensures compliance and helps security teams identify over-provisioned or unused identities as well as spot anomalous NHI activity.

Build Secrets Governance into CI/CD Processes

Machine identities frequently handle sensitive secrets and credentials. Implementing JIT secret provisioning allows for secure, temporary access to sensitive information during the execution of specific tasks. Automatic secret rotation ensures that no static credentials remain in use, reducing the risk of exposure. Some cloud providers support taking this a step further with role assumption, allowing NHIs to perform their tasks while eliminating static credentials and logins entirely.

Automate Privilege Reviews

Frequent reviews of machine identities and their associated privileges should be automated to ensure that only necessary permissions are granted. This process can identify and remediate over-privileged identities before they become a liability. It can also spot changes to NHI permission grants which may warrant manual review.

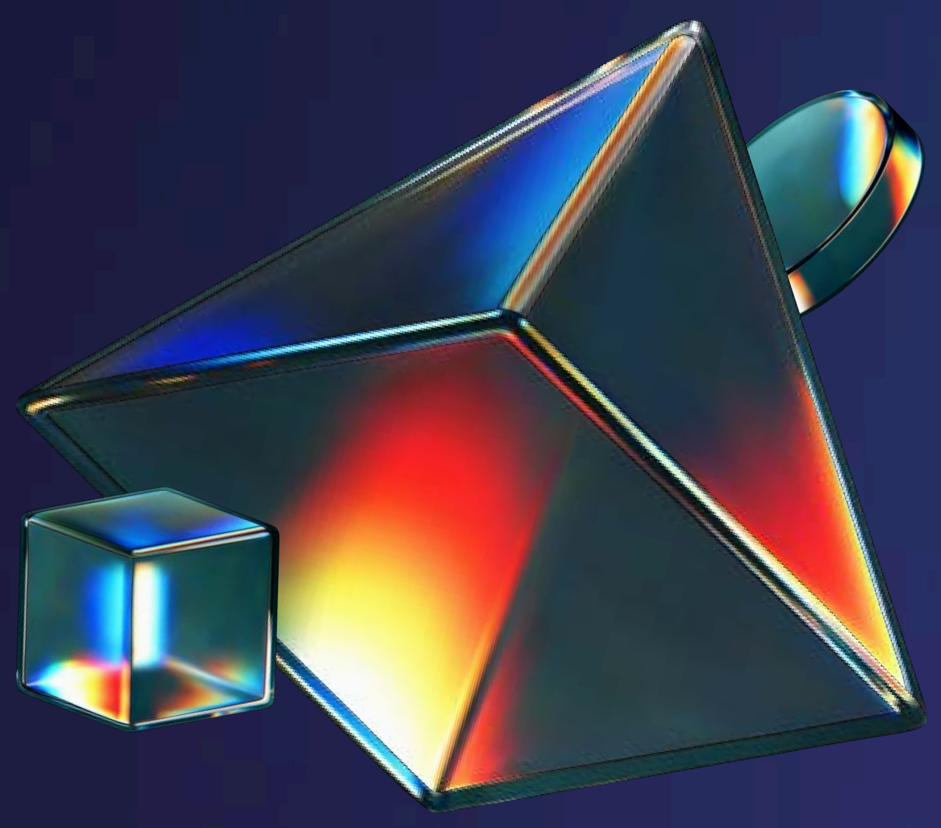
EMBRACING A SECURE, MACHINE-DRIVEN FUTURE

The rise of machine identities is a natural consequence of cloud automation, and the security risks they present cannot be ignored. By decoupling authentication from authorization, centralizing privilege management, and enforcing Zero Standing Privileges, organizations can secure NHIs while maintaining the speed and efficiency demanded by modern cloud environments.

britive

Britive's platform empowers organizations to meet these security challenges with adaptive, cloud-native solutions that ensure dynamic access management, comprehensive visibility, and full automation of privilege management processes.

> THE FUTURE IS MACHINE-DRIVEN—MAKE SURE YOUR SECURITY STRATEGY IS, TOO.



One Platform Across
All Cloud Environments.
Zero Standing Access.