APONO

Solution Brief

Apono: The Access Solution for Modern DevOps

The cost of standing access

In fast-moving engineering environments, engineers often require elevated privileges to develop, troubleshoot, and deploy solutions. This direct access is essential for configuring systems, diagnosing issues, and iterating on code. However, **standing access – blanket, persistent access – creates a wide attack surface and introduces unnecessary friction into daily workflows**. The result? Compromised security, hindered productivity, and a significant drain on valuable engineering and operational resources. Manual privilege escalation creates bottlenecks.

Traditional privilege escalation processes force engineers to submit tickets and wait in queues. This creates frustrating bottlenecks that delay:

- **Deployment**
- **Troubleshooting and Break-glass**
- **Innovation through the adoption technologies and services**

These delays aren't just minor inconveniences; they add up, leading to hours of lost engineering velocity and friction between development and cloud security teams.

Apono by the Numbers

96% Access risk reduction on average

3,796 Hours saved of waiting for access

zero Manual work from security, IAM and DevOps teams

Blanket privileged access creates risk

However, the alternative - granting blanket privileged access - creates an elevated security risk. Credentials tied to persistent privileges are a prime target for attackers, particularly in production environments.

Standing access transforms every developer or administrator account into a potential backdoor

Once compromised, attackers can use privileged credentials to move laterally through the network, **exfiltrate data, and disrupt critical services.**

The most alarming part? They can do all of this without triggering traditional perimeter-based defenses. Essentially, standing access transforms every developer or administrator account into a potential backdoor.

Identity isn't the new perimeter; context is

In today's cloud-native, API-driven environments, static identity access in traditional IAM solutions is insufficient. Traditional access management systems lack contextual awareness. They fail to consider crucial factors like:

- **Intentions**
- **Location**
- **Time of access**
- **Anomalies**

This oversight is critical because attackers aren't breaking in anymore; they're logging in using stolen or leaked credentials. Identity is **not** the new perimeter. **Context is**. Intrusions frequently hinge on stolen or compromised credentials; only context-based access permissions can prevent them.

The AI-imperative

According to the 2025 Verizon DBIR, credential abuse is the most common initial attack vector, playing a role in 22% of non-error, non-misuse breaches. This is likely due to the increasing role AI plays in two kinds of pervasive attacks:

- **Phishing:** Attackers now leverage AI to gather publicly available information and craft highly personalized and convincing phishing emails, making them harder to detect and increasing success rates.
- **Credential Stuffing:** Cybercriminals exploit vast databases of stolen credentials to gain unauthorized access. The scale and automation of these attacks mean that attackers can pull off substantial breaches even with low success rates.

Standing access exacerbates these risks: compromised credentials tied to persistent privileges can grant attackers prolonged and undetected access to privileged systems.

This is a particularly pressing problem in agile development environments. Here, the rapid deployment of containerized microservices contrasts sharply with the slower pace of traditional access reviews.

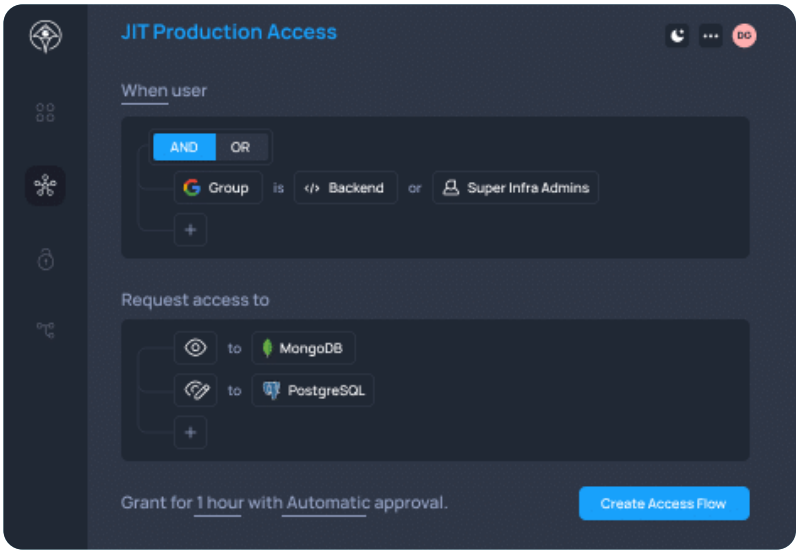
Compromised credentials tied to persistent privileges can grant attackers prolonged and undetected access to privileged systems

While services can be redeployed in seconds, access permissions are often infrequently reviewed, creating a cloud-speed gap that widens mean-time-to-response (MTTR) and exposure windows.

The rapid pace of development in cloud environments often outpaces traditional access management systems. This leads to an increased attack surface as access permissions remain static, despite constant infrastructure changes.

The Apono advantage

To close the cloud-speed gap and reduce the risks of standing access, you need an access model that's dynamic, contextual, and built for automation. That's where Apono comes in.



96% access risk reduction

Apono uses Just-in-Time (JIT) and Just-Enough-Privilege (JEP) access controls to reduce unnecessary standing privileges and ensure users have precisely the access they need, exactly when they need it. The result? Up to 96% reduction in access-related risk.

94% attack surface reduction

By replacing persistent access rights with time-bound JIT tokens, Apono reduces your attack surface by 94%. This method limits window of attack opportunity, significantly enhancing your overall security posture.

Automated access lifecycle management

Apono automates the access lifestyle management process, substantially reducing the manual workload for Security, IAM, and DevOps teams. We automate approvals and revocations, granting and rescinding access rights promptly and in line with the principle of least privilege.

Enhanced security and compliance

Security is at the core of our architecture. The Apono platform doesn't store customer keys, significantly reducing the risk of sensitive data exposure.

We provide comprehensive audit trails and integrate them seamlessly with existing identity providers, ensuring compliance with the regulatory requirements your organization is subject to.

Solution Deep-Dive

Just-in-Time (JIT) access

Apono's JIT access model replaces persistent permissions with scope-limited, time-bound rules. Access is granted only for the duration of a specific task or workflow and automatically revoked when that task is completed or times out.

This minimizes risk windows and eliminates the need for manual revocation, dramatically reducing the exposure created by standing privileges.

Just-Enough Privilege (JEP)

Instead of granting broad role assignments, Apono continuously maps actual permission usage across your environment. The recommendation engine suggests right-sized access policies based on observed behavior, ensuring users only get the exact permissions they need to do their jobs and nothing more.

Deploy Access Privileges at Scale

Streamline deployment and management for enterprise-scale via Terraform, CloudFormation, and more, saving time and ensuring that access policies are always up to date.

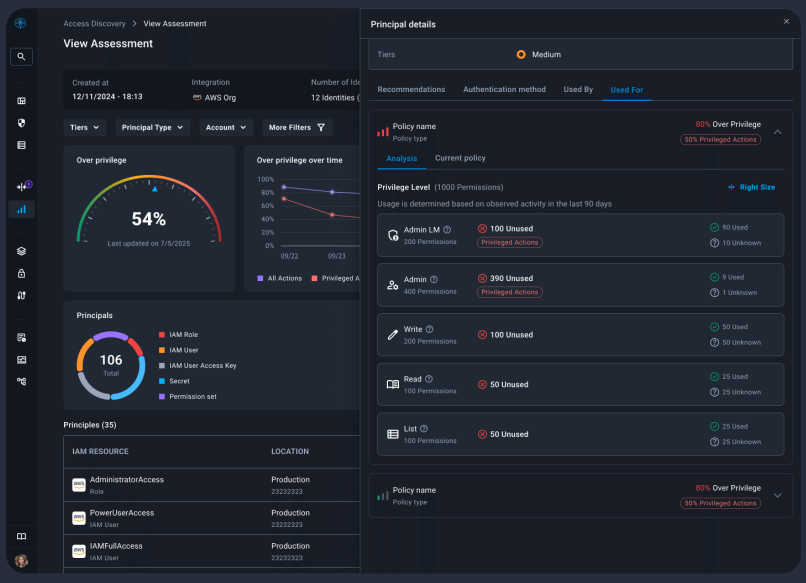
Access Discovery and Remediation of Risk

Apono's automated, audited, and intelligent Cloud Access platform empowers security teams to gain total visibility over cloud access privileges used by all human to non-human identities. It enables them to remediate risks efficiently by moving risky identities to a just-in-time and just-enough access model.

Continuous auditing

The Apono platform provides continuous auditing by logging every access request, approval, and revocation in real time. You can stream these logs directly to your SIEM to demonstrate compliance with regulations such as SOC 2, PCI-DSS, and HIPAA.

Additionally, Apono offers automated reporting and streams your activity details to communication platforms like Slack, enhancing transparency and facilitating rapid incident response.



Ready to benchmark your current attack-surface score and strengthen your security posture?

→ Book a demo now

Apono helps you eliminate standing risk and shrink your attack surface with:

- **Automated JIT access:** Grant access only when and where it's needed
- **Zero customer key storage:** Your secrets remain yours
- **Built-in compliance reporting:** Simplify audits for SOC 2, PCI-DSS, and HIPAA

Start enhancing your security and achieving compliance today.

> "Apono cuts the manual provisioning phase and optimizes daily work for R&D, ops, and security teams."
>
> — Alan Idelson, CISO, Cyberreason

APONO

Discover, manage, and monitor cloud access on a single platform

AICPA SOC 2 GDPR

Trusted partners

Hewlett Packard Enterprise · MATTEL · monday.com · Rho · tomorrow.io · bloomreach · bigpanda

About Apono

Founded in 2022 by Rom Carmel and Ofir Stein, Apono is redefining cloud security with its Cloud Privileged Access Platform.
With decades of expertise in cybersecurity and DevOps, Apono enables organizations to adopt just-in-time, just-enough privilege access, seamlessly bridging the gap between security and engineering teams. Trusted by Fortune 500 companies, Apono's platform empowers enterprises to enhance operational efficiency while maintaining robust security controls. Recognized in Gartner's Magic Quadrant for Privileged Access Management for two consecutive years, Apono is at the forefront of innovation in secure cloud access management.