Deepening the ZPA Zero Trust framework with fine-grained access control

Integration highlights

- P0 Security extends Zscaler ZPA's network-level controls to just-enough, just-in-time access for private resources on-prem or in the cloud
- P0 automatically discovers sensitive resources without added infrastructure or operational overhead
- P0 AuthZ for ZPA delivers end-to-end audit trails and tamper-evident session recordings

The market challenge

Zscaler ZPA helps teams eliminate VPNs and enforce identity-based connectivity and segmentation to private environments. But many organizations struggle to scale least-privileged access control across private environments spanning on-premises infrastructure and cloud platforms. Customers still need action-level authorization inside platforms where resources, roles and permissions change constantly. Mapping private infrastructure and cloud resources as endpoints and maintaining ZPA segments becomes operationally heavy as environments change.

Without that layer, teams often fall back on persistent IAM roles, shared credentials, or broad SSH paths that expand blast radius when something goes wrong.

Teams need a practical way to replace standing permissions with time-bound access for private applications, infrastructure access (SSH/RDP), and cloud-native services such as IAM roles, RDS and S3.

The solution

P0 AuthZ for ZPA brings modern privileged access management to the network, delivering identity-first authorization control with just-in-time access to private resources. This integration redefines how enterprises securely connect their users, workloads, and devices to applications in a hybrid world.

ZPA secures how identities connect to private applications and environments. P0 secures what those identities are allowed to do once connected, down to specific actions on specific resources. P0 automatically discovers privileged resources, supports approval workflows, provisions temporary access and enforces time limits so access expires when it should.

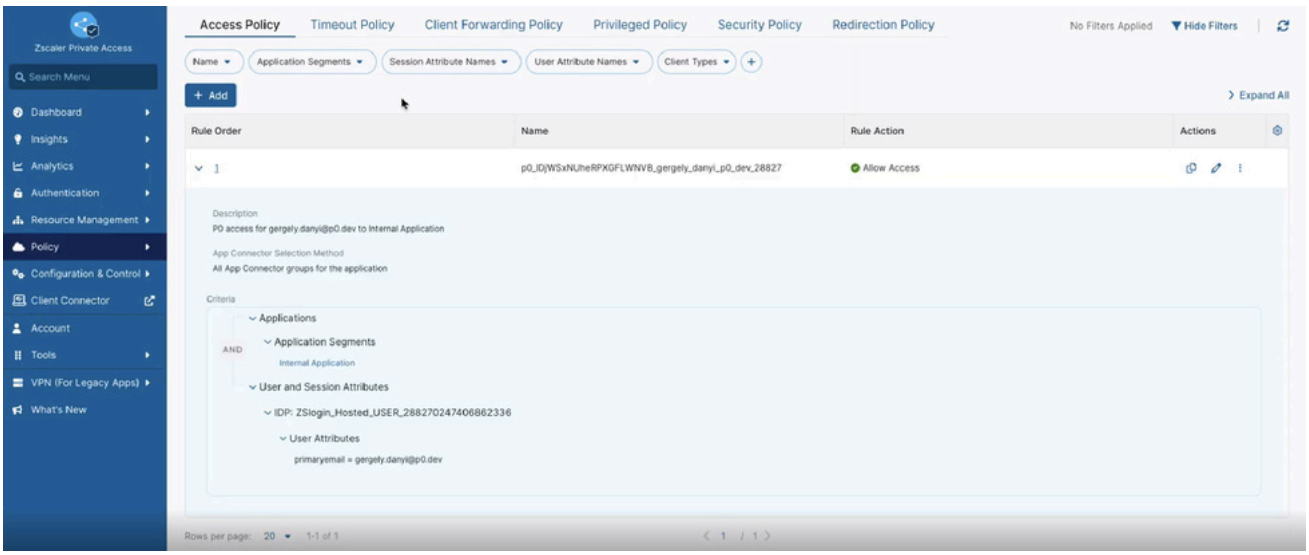
Together, customers can enforce Zero Trust end-to-end—from connectivity to authorization—with Zero Standing Privilege (ZSP). ZPA governs access to the environment, and P0 governs authorization within cloud services and IAM for the duration of each session.

Solution components deep dive

Achieving end-to-end Zero Trust requires both secure connectivity and least-privileged authorization. ZPA authenticates identity, evaluates device posture and establishes the secure connection. P0 evaluates access policies, orchestrates approvals when required, provisions ephemeral permissions and revokes them automatically.

- **Zscaler ZPA:** The network gatekeeper. It validates user identity via IdP integration, assesses device posture, and provisions encrypted tunnels to the target environment.
- **P0 Security Authz Control Plane:** The orchestrator for resource discovery and fine-grained authorization. It manages JIT workflows, evaluates posture policies against risk signals, provisions short-lived, least-privilege credentials or session permissions for the approved action.
- **P0 AuthZ for ZPA:** A lightweight component installed in the target environment (e.g., a VM) that handles fine-grain provisioning. Rather than relying on static IPs and manual segment maintenance, the agent uses labels and metadata to associate resources to ZPA application segments. That keeps segmentation aligned with dynamic infrastructure and supports a "policy-as-code" model.

The integration dramatically streamlines developer access by enabling requests within existing Slack, Teams, or CLI tooling—replacing manual ticketing processes with automated, policy-driven approvals.



Here, P0 AuthZ for ZPA dynamically provisions Zscaler rules to enable secure access to application segments.

Key use cases

Automate least-privileged access to private resources

Teams can grant just-enough, just-in-time access to Zscaler Private Access applications through SSH and RDP, eliminating static credentials and shared accounts. Access requests can be initiated through embedded workflows and are authorized via policy driven automations, with permissions that expire dynamically based on context or preset time durations.

Transition from break-glass access to Zero Standing Privilege

Achieving Zero Standing Privilege (ZSP) doesn't happen overnight. For organizations that still rely on break-glass access, P0 helps automate these workflows with ephemeral, owner-attributed access that is audit-ready by design. This enables teams to support legacy configurations while incrementally and sustainably eliminating shared accounts and static credentials.

Zscaler + P0 Security benefits

Action	Description
Automate cloud resource discovery and remove maintenance overhead	P0 continuously identifies and maps access to compute, databases, storage services, and identity roles across private infrastructure and cloud services without requiring manual endpoint configuration in ZPA.
Extend Zero Trust to cloud entitlements	Use ZPA for identity-based connectivity and add P0 for fine-grained authorization to private infrastructure in AWS, GCP and Azure
Replace standing privilege with just-in-time access	Automated time-bound and scoped access approval workflows for infrastructure authorization so access is least-privileged by default
Dynamically enforce policy based on real-time context	Access requests are evaluated and provisioned at runtime based on identity, device posture, risk signals and resource sensitivity.
Simplify investigations and audit preparation	Logs can be correlated from session start through approved permissions and executed actions and sent to Zscaler or the customer SIEM.

Conclusion

Zscaler ZPA and P0 Security help organizations eliminate VPNs and standing privilege, bringing modern privileged access management to the network.

Together, they combine ZPA's identity-based connectivity with P0's fine-grained authorization and automated resource discovery to make access to private applications safer, faster, and audit ready by default.

Beyond this ZPA integration, P0 supports ZSP governance and access management for service accounts, workloads and AI agents, applying consistent policy, ownership and audit trails for scalable control.

Want to see this integration in action?

Visit the Demo hub on www.p0.dev to get a quick overview of the Zscaler integration.

Better yet, click here to get a live demo and talk through how this would work in your environment.

About P0 Security

P0 Security is the central Authz Control Plane for modern production environments. P0 helps enterprises meet evolving privileged access demands by delivering secure, auditable and agile access across multi-cloud and hybrid infrastructure.

The central platform governs all identity types including human users, machines, workloads and AI agents. By managing the full privilege lifecycle from discovery through audit, P0 enables customers to programmatically replace broad access and static credentials with just-enough-privilege and just-time access.

Zero standing privilege. Zero added friction. Because threats to your production infrastructure must be priority zero.
Learn more at www.p0.dev.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure.

The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location.

Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform.

Learn more at zscaler.com.