SaaS Authorization Management™ for Zscaler

Manage & Standardize on Authorization policies for SaaS Apps

Identity Security Challenges in SASE

In today's interconnected digital landscape, the pace of innovation is unprecedented, as we rapidly deploy new services and technologies to keep pace with the demands of business. From new applications and APIs to microservices and networks, the traditional *Edge* has long served as the guardian of our digital assets. However, relying solely on this tradition is no longer sufficient. In order for cybersecurity measures to be truly effective, every component of our security infrastructure must possess identity awareness.

Zscaler and other SASE (Secure Access Service Edge) solutions have made significant strides in integrating identity-aware controls into their authorization frameworks – marking a crucial step forward. However, more can be done to address a critical gap. It's imperative that any security enforcement point responsible for managing network connectivity must also align seamlessly with the broader Identity stack's security posture.

The efficacy of enterprise security measures hinges on the cohesive alignment of identity-aware controls across every facet of our security infrastructure. This holistic approach ensures not only the protection of our digital assets but also the preservation of our organization's overall security posture in an ever-evolving digital landscape.

Centralized Management for an Improved Security Posture

PlainID eliminates endpoint access challenges by externalizing authorization and centralizing its management. The **PlainID Authorizer™ for Zscaler,** available via **PlainID SaaS Authorization Management™**, centralizes policy management for Zscaler and industry-leading SaaS applications and tools.

PlainID Authorizers™ are available for applications, APIs, microservices, and data tools. The Platform is designed to help your organization adopt and proliferate authorization policies consistently at scale, with minimal effort.

Users are often given more permissions than their roles should allow due to oversights in security or lack of expertise in the reporting tools they use. Create policies in plain language that are simple to understand and can be applied anywhere and simplify auditing of access policies.

Full visibility and control of access policies across the ecosystem helps enterprises better protect PII and sensitive data. With PlainID, enterprises gain the necessary flexibility and agility to address the granularity of data privacy, and industry regulations both locally, and globally.

Business Impact

Streamline Access to Endpoints
Centralize and automate policy management to reduce manual efforts required to enforce policies across Zscaler and the ecosystem.

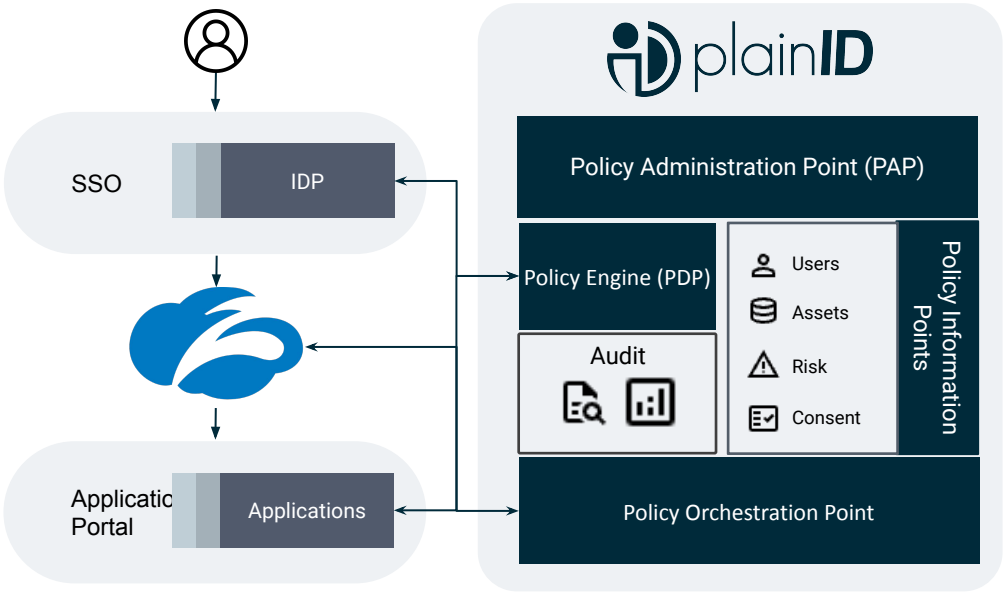
Minimize Security Gaps
Ensure policies are consistently applied across the enterprise with a Policy-based Access Control (PBAC) framework.

Gain Visibility & Monitoring
Track access policies from a single dashboard that provides reporting and alerting to inform administrators on policy changes.

Adapt to Evolving Requirements
Facilitate quick updates and adjustments to keep up with evolving business needs, security threats, or regulatory changes for compliance.

> *PlainID is excited to provide Identity-centric Security for Zscaler environments through our Authorizer which enables policy orchestration of Zscaler policies. Our customers can now increase their overall security posture, maintain data compliance, and extend their Zero Trust framework via an Identity-centric approach.*
>
> *Gal Helemski, CTO & CPO at PlainID*

How PlainID works with Zscaler



1. PlainID connects to Zscaler for Policy Orchestration, enabling PlainID to pull in and learn about all the access policies currently in Zscaler.
2. User request to access a critical application is directed to the Identity Provider (IDP).
3. The IDP sends an Authorization request to PlainID to determine user level of access.
4. PlainID verifies the user has approval, and the list of Fine-grained entitlements they are authorized for, based on the policies.
5. The IDP receives the response from PlainID and enriches the access token accordingly.
6. The token (i.e. enriched with fine-grained entitlements) is passed to Zscaler.
7. ZScaler connects the user to the critical application with *read-only* access rights.
8. *Optional*: Applications receives Dynamic and Fine-grained access control decisions from PlainID.

Future-proof Your Enterprise

The **PlainID Integration Hub** is designed to address the complex challenges of enterprise access control. By offering out-of-the-box Authorizers™ and Integrations, it allows for a standardized approach across varied and distributed infrastructures – unifying disparate access controls under one platform.

ForgeRock · PingIdentity · Google BigQuery · denodo · apigee · envoy · Open Policy Agent · okta · Azure Active Directory · trino · Starburst · Kong · HashiCorp Consul · snowflake · Power BI · Kuma · Istio

Visit PlainID.com/integration-hub for more information

ABOUT PLAINID

PlainID is the world's leading provider of enterprise Authorization, helping enterprises address the complex challenges of Identity Security. The PlainID Platform allows you to discover, manage, and authorize access control policies for enterprise applications and data. Our solution is architected to protect against identity-centric security threats powered by Policy-Based Access Control (PBAC). Visit PlainID.com for more information.

plainID