plainID

# Dynamic Authorization Service™ for a Complete Zero Trust Architecture

A Continuous, Risk-Based Approach to Access Control

# Table of Contents

# Introduction

Zero trust has emerged as a key security measure for organizations across all industries.

While it has gained significant attention as companies strive to maximize their defense against breaches, the increasing buzz around the term has led to a simplified understanding of its value, often resulting in misconceptions about its full scope and value.

Zero trust is not a product or solution that any individual vendor can provide. It is a cybersecurity philosophy that focuses on the paradigm and strategy of protecting digital assets. The philosophy's core concept is to trust no one and no thing, *because in the context of cybersecurity, trust is analogous to vulnerability.*

Crucially, this philosophy extends beyond authentication and safeguarding a network perimeter. We can no longer assume that a user's identity cannot be compromised just because a person is "inside the perimeter." Furthermore, our increasingly digital and distributed world makes a comprehensive zero trust approach all the more urgent. The new work-from-anywhere reality means that the perimeter is everywhere, which means a greater and ever-evolving attack surface. As Gartner has pointed out, security leaders must combine identity-first controls, policies and programs with decentralized and context-specific enforcement.[1]

> "Identity-first security has become a core concept of many security initiatives, such as zero-trust architecture, but traditional, siloed identity and access management (IAM) staffing models and tools were not designed for this type of distributed and fast-paced development approach."
>
> – Gartner Research (Gartner® "Predicts 2022: Identity-First Security Demands Decentralized Enforcement and Centralized Control," November 2021)

The world is adapting to this new reality. A majority of organizations have deployed or plan to deploy zero trust architecture[2] and a May 2021 **executive order** requires US federal agencies to shift to the architecture by 2024.

This ebook provides an overview of zero trust, including its past, present, and future; explaining how organizations can rethink their approach to zero trust to enforce protection throughout the digital journey between stakeholders and digital assets.

[1] Gartner, "Identity-First Security Demands Decentralized Enforcement and Centralized Control," 2022.
[2] Ponemon Institute, "2022 Global Study on Closing the IT Security Gaps," 2022.

# The Road to Zero Trust: NIST's 7 Tenets

While there are several ways to approach zero trust, the most widely recognized and understood method follows seven tenets established by the US National Institute of Standards and Technology (NIST)[3]. The tenets are:

1. All data sources and computing are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

The NIST special publication goes on to emphasize that, in order to function effectively, zero trust must be applied holistically. It cannot be an exclusive agent of the network alone. Rather, it must be applied to *all* assets and resources—including applications and assets *within* applications. Access (or "trust") is never granted implicitly. Quite the opposite: access is denied by default, which means that resources organized under a zero trust paradigm should always behave as if an attacker is present in every digital interaction.

> "With a zero trust mindset, organizations can protect themselves and their most critical assets even as security technologies and tools evolve."
>
> – John Kindervag, creator of the zero trust model, in The Wall Street Journal

[3] National Institute of Standards and Technology, SP 800-207: Zero Trust Architecture, 2020

Forrester has elaborated on this same premise, urging that threat prevention is best achieved by "only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices."

Zero trust, therefore, abides by three core principles:

1. All entities are untrusted by default
2. Least privilege access is enforced; and
3. Comprehensive security monitoring is implemented.

**Here's the bottom line:** The NIST Zero Trust Architecture (ZTA) is based on the principle of formulating access decisions dynamically based on policy. To achieve this, organizations must move beyond traditional identity and access control methods that fail to extend zero trust beyond authentication and network security. As digital environments continue to evolve in complexity, a new approach to Zero Trust is necessary for organizations to effectively safeguard their assets.

# Logical Components of a Zero Trust Architecture

A zero trust architecture that fully addresses each tenet described in the previous section must be comprised of the following logical components to enable continuous real-time access decision-making:

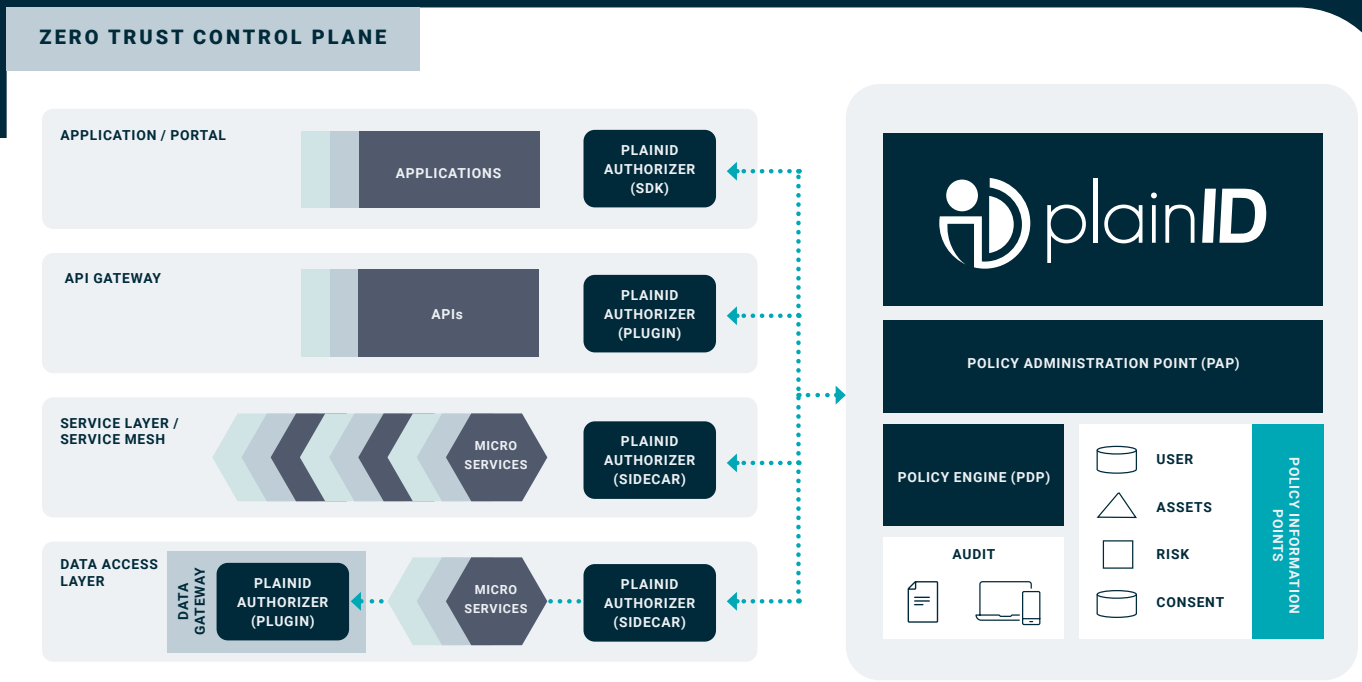


Figure 1. Zero Trust Control Plane

Complete ZTA hinges on the ability to leverage dynamic policies for turning untrusted access into trusted access. Components that drive these proactive access decisions include:

1. The policy information point (PIP) supports the policy decision with information from external sources and systems about identity, resources, risk signals, and more. As such, it serves the policy administration and the policy decision points.
2. The policy decision point (PDP) is powered by an authorization runtime engine to calculate the access rights needed in real-time. It should also handle permit/deny, user access tokens, and policy resolution requests according to the access policies defined and deployed by administrators.
3. The policy administration point (PAP) is where policy administrators manage the full policy management lifecycle: creating new policies, testing and troubleshooting existing policies, investigating policies, approving workflows, reviewing audit logs, viewing system analytics, and more.

In addition, the policy enforcement point (PEP) ensures that users and applications can only access or perform actions they are allowed to do, based on the defined policies. The PEP is commonly implemented close to the data and resources for optimal security and performance.

The most important job of a ZTA is making the decision about whether to grant, deny (and at what level), or revoke access to a resource. This is known as *authorization*.

On the left-hand side of the diagram, we see the different identity types that may have access to enterprise resources. And on the right, we see the resources they attempt to access—all of which lead to data. The flow of access between identity types and resources begins with the identity which, according to Zero Trust, is by definition an untrusted entity.

The identity moves through the decision flow based on the context of the access request: *who* the identity is, *what* they are trying to access, and *when* they are trying to access it. The decision is formulated in real time as defined by the policy. After the decision to grant access is made, the identity becomes trusted and may continue. It is important to emphasize that the access granted is contained for a specific request at the time of that request. Any new access request—for a new resource or at a different time—should be reevaluated through the same continuous process.

Finally, at the bottom, there are the systems that consume access-related information to deliver visibility and feed the analytics (as per the seventh tenet of the NIST framework).

# A Reference Architecture for Complete Zero Trust

Connecting identities to digital assets is a central challenge in modern business—dynamically, securely, and at scale.

Zero trust is a security paradigm and strategy that cannot be fully achieved by a single solution. Any claim by a vendor to provide a complete solution is false.

To achieve zero trust, organizations must implement an architecture consisting of different solutions responsible for establishing trust at each step of the digital journey between users and resources. These typically include identity management, authentication, endpoint device protection, and network and application access control.

However, without extending zero trust principles to the last mile of the user's journey to digital resources, the architecture is incomplete. This includes application objects, services, APIs, and data.

To address this, a complete zero trust reference architecture covering the entire digital journey is necessary. This architecture reflects industry standards, accepted principles, and the responsibility of each component. Note that this is a reference architecture and not an integration map between solutions.

## COMPONENTS OF ZERO TRUST ARCHITECTURE

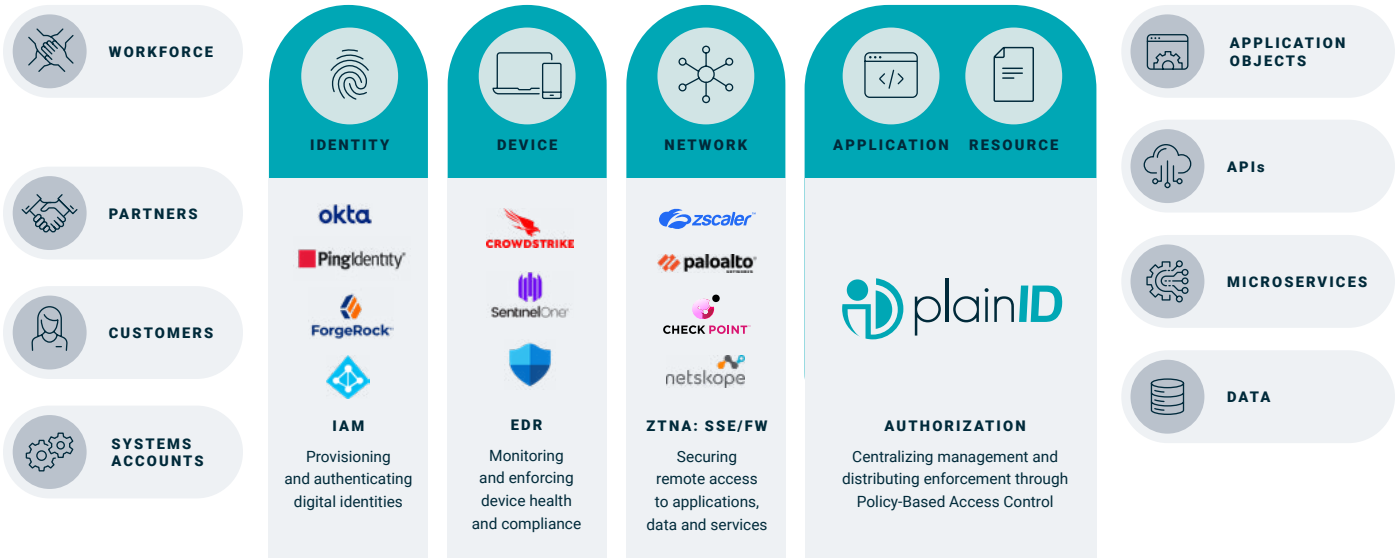


Figure 2. Examples of vendors that address different components of a Zero Trust Architecture

"A zero trust approach is primarily focused on data and service protection but can and should be expanded to include all enterprise assets (devices, infrastructure components, applications, virtual and cloud components) and subjects (end users, applications and other non-human entities that request information from resources)."

— NIST SP 800-207 Zero Trust Architecture

An Identity Security Posture Management (ISPM) platform provides the all-important missing links in a complete Zero Trust Architecture: establishing and enforcing granular, trusted access at the level of enterprises' most valuable digital assets.

An enterprise-grade ISPM platform should provide:

- Flexible deployment options: SaaS, Hybrid, On-Premises
- Dynamic, fine-grained authorization, with the ability to apply identity, context, and risk signals in real-time
- Policy-Based Access Control (PBAC) to define who can access what in natural language with a graphic representation
- Centralized policy management with distributed enforcement across the enterprise technology stack
- Full visibility and control of how identities (both human and machine) access digital resources
- Approval workflows and lifecycle management of policies to maintain management best practices and comply with audit requirements

# The Critical Importance of Authorization in Achieving Complete Zero Trust

Dynamic Authorization ensures consistent zero trust controls

To effectively implement a robust zero trust strategy across an enterprise, it is necessary to externalize authorization management and decision processing. Disparate handling of authorization by siloed applications will not result in proper implementation.

**Enter Authorization-as-a-Service.**

*Authorization-as-a-Service* (sometimes abbreviated to AuthZ-as-a-service) is a ready-to-use platform that can enable the externalization of authorization management. It combines advanced authorization capabilities and business-oriented processes to create end-to-end authorization that is extensible, secure, and scalable. This includes the central policy lifecycle management, workflows, auditing, and governance capabilities.

## Dynamic Authorization: Designed for Complete Zero Trust

Remember that the most fundamental premise of zero trust is that access is denied by default and each request is evaluated dynamically in real-time. Dynamic authorization (sometimes referred to as “run-time” or “real-time authorization”) satisfies this requirement by calculating the access decision based on the specific context of that session (who, what, how) in real-time, at the time of access.

This establishes and assures trust continuously. Requests are validated at every stage of the digital interaction. Trust must be established again and again to maintain security across a distributed digital environment.

> “Externalized runtime authorization enables zero trust architecture by implementing an identity perimeter using policy-based access control mechanisms. Security and risk management technical professionals should mitigate digital access risk by modernizing runtime authorization controls.”
>
> — Gartner®, Architecting Modern Policy-Based Runtime Authorization, 2020, by analyst Homan Farahmand

## Fine-Grained Authorization, At Runtime

In a zero trust paradigm, access should be granted in extremely narrow terms that correspond to a very specific purpose. Anything outside that scope should be denied. The access decision, in other words, should be fine-grained in the sense that it is responsive to many different attributes. Fine-grained authorization must also involve dynamic, real-time access decisions. Otherwise, trust will have been insecurely assumed.

Attributes that must be evaluated for making the decisions that drive complete zero trust are:

- User (e.g. group or role) level attributes, such as what is their current certification level, role and responsibilities, and whether they can access confidential and personally identifiable information (PII), among others.
- Asset attributes, such as data classification, location assignments, and any relevant metadata.
- The location (e.g. geolocation, IP, network address) and device that a user is authenticating from, including whether from an internal or an external system.
- The authentication factors being used, i.e., with single, two-factor, or multi-factor authentication.
- The time of day and day of the week at which the user is authenticating.
- Risk level or risk scores of the user that take identity-aware and risk-based contextual data into account.

A policy decision engine evaluates each of these and all other relevant attributes to make the decision at that point of access during runtime.

Furthermore, each time someone attempts access, a new decision is made in real time. This decision is driven by the highest levels of granularity possible, evaluating all the attributes that are updated to that specific point in time, as well as the real-time context and environment, rather than being based on attributes that are static or predefined by the application.

> "…the crux of the issue, which is the goal to prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible."
>
> — NIST, Zero Trust Architecture

## Policy-Based Access Control (PBAC)

As you can see, authorization is central to Zero Trust. Accordingly, it requires an authorization management framework that can enable its heavy lifting: Policy-Based Access Control (PBAC).

In spite of the name resemblance, PBAC doesn't replace RBAC or Attribute-Based Access Control (ABAC). A business-oriented approach to authorization, PBAC provides a comprehensive management framework that uses and orchestrates the full capabilities of the authorization toolkit: RBAC, ABAC, run-time decisions, fine-grained decisions, and coarse-grained decisions. An authorization policy defines who can do what and when, and a management UI makes it easy to reflect business logic with simple language to define the complex relationship between identities and assets.

PBAC fully externalizes authorization, allowing enterprises to achieve central policy management with distributed enforcement while maintaining consistent standards.

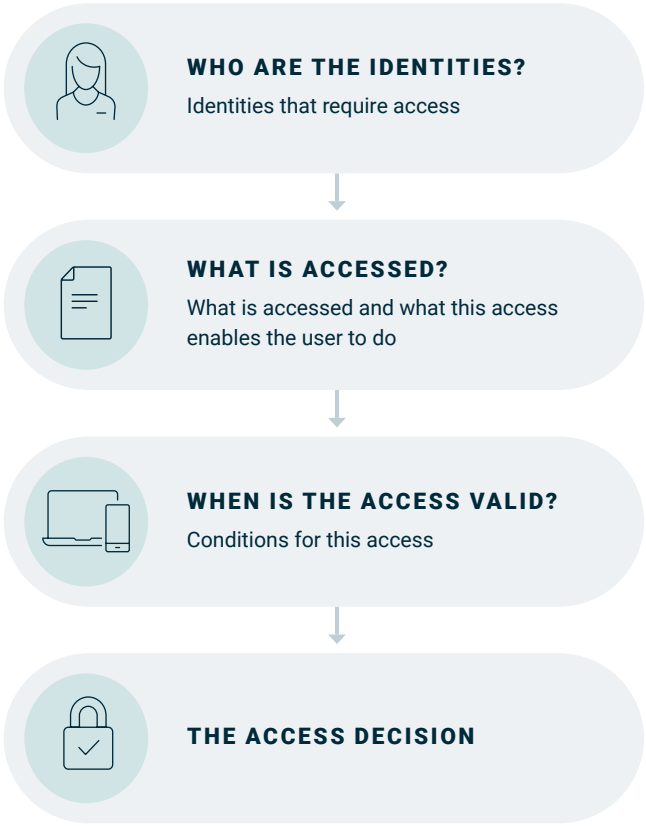


Figure 3. Access Decision-Making with PBAC

## Centralized Management with Distributed Enforcement

The combination of the processes above yields an Identity Security Posture Management platform that can scale to meet Zero Trust requirements. It maintains strict centralized management while also extending and enforcing last-mile trust to the very edge of a distributed technological environment.

PlainID created PlainID Authorizers to enable access decisions across the technical stack: the application, the API gateways, the microservices, and the data itself.

PlainID Authorizers are ready-to-use, specific integrations for distributing access decisions across all patterns in the enterprise, integrating “out-of-the-box” with the specific underlying enabling technologies.


Figure 4. Examples of PlainID Authorizers

# Zero Trust at Every Layer with Authorization

Ultimately, the core principle of zero trust is to start with a default deny approach and then dynamically evaluate each request in real-time. This is where dynamic authorization, also known as “run-time” or “real-time authorization,” comes in - it calculates the access decision based on the context of the session (such as who, what, and how) at the time of access.

By doing so, it establishes and maintains trust on an ongoing basis, ensuring that requests are verified at every step of the digital interaction. In a distributed digital environment, trust must be continuously re-established to maintain security.

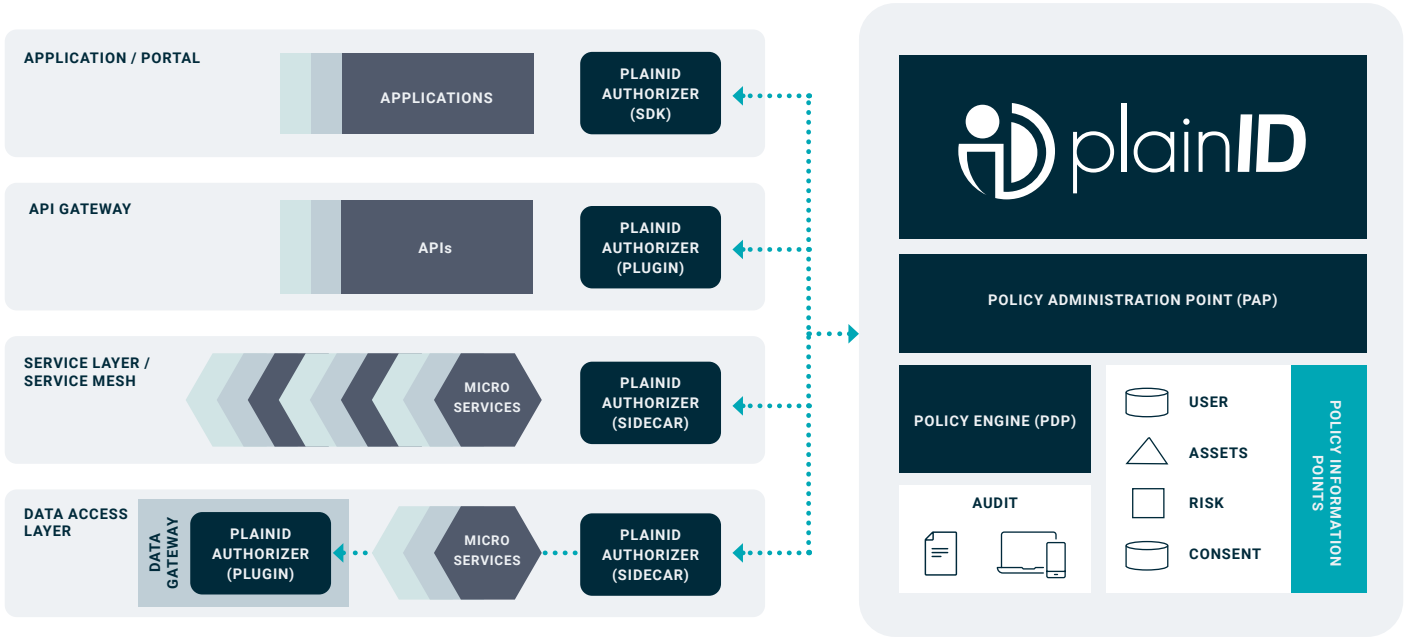


Figure 5. Zero Trust at Every Layer with Authorization

SUCCESS STORY

# Freddie Mac Modernizes Enterprise Architecture With PlainID Dynamic Authorization Service

## CHALLENGE

Freddie Mac needed a modern access control management approach that provided visibility and control to secure 400+ microservices for customer-facing loan approval processes, control access to 500+ AWS environments, and protect sensitive customer data used by the business intelligence (BI) analyst team.

## SOLUTION

The PlainID Dynamic Authorization Service aligned with Freddie Mac's need for consistency and centralized management of access policies for critical functions of the business, from application to APIs, microservices, and data assets, and ultimately enabled the enterprise to modernize its architecture for cloud-native applications and services.

## BENEFIT

With PlainID, Freddie Mac had the ability to implement PBAC to effectively address the needs of all types of deployment patterns and makes it simple for business and application teams to decouple authorization from application code.

By distributing policy enforcement closer to the data, Freddie Mac maintained stronger security, and improved application performance and productivity across multiple teams and projects.

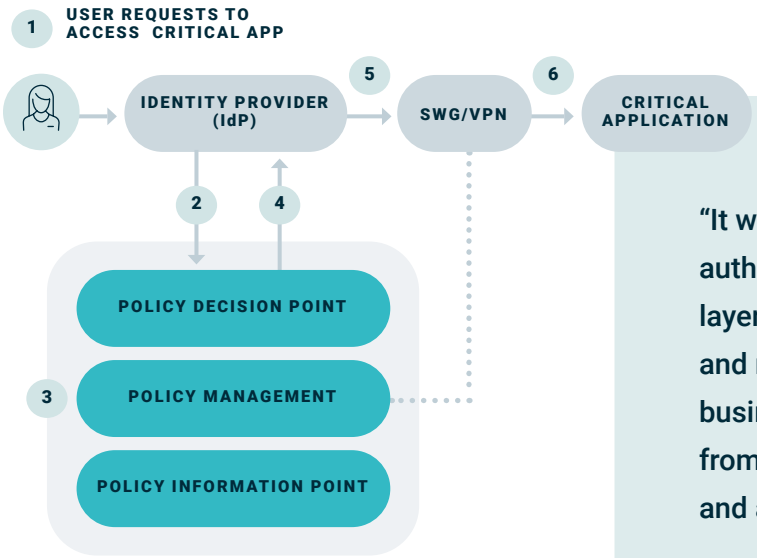


Figure 6. High-Level Implementation Architecture

**"It was important for us to have a single vision for how authorization is handled across multiple architecture layers. PlainID has made it simple for us to build and manage access policies that align security and business requirements across our technology stack—from legacy applications, to our modern cloud apps, and all the way to the data we collaborate on."**

-Dmitry Tepper, Senior IT Enterprise Architect

# ZTA and Identity-First Security: The New Power Couple

Zero trust is a proven and effective approach to reducing the risks and impact of security breaches. However, for organizations to fully achieve the benefits of a zero trust framework, it is critical to address access control beyond the network, including applications and intra-application assets. This requires an identity-first approach with modern access control capabilities such as dynamic authorization, authorization-as-a-service, authorizers, and PBAC.

To address this need, PlainID has developed the first complete and modern Identity Security Posture Management platform for Identity-First Security. This platform supports a zero trust architecture, providing dynamic authorization to the edge of the enterprise. It includes a SaaS-based management platform with PBAC as a framework and a range of authorization tools, a growing marketplace of PlainID Authorizers, and a reference architecture for centralized management with distributed enforcement.

**To learn how PlainID can help you be confident in the completeness of your Zero Trust environment, we invite you to reach out to us for a free trial.**

**REQUEST A DEMO**

## ABOUT PLAINID

PlainID is The Identity Security Company™. We help identity-centric enterprises defend themselves from adversaries who use identity-based attacks. Our Identity Security Posture Management Platform provides Identity Insights, SaaS Authorization Management, and Dynamic Authorization Services to create identity-centric security across SaaS, APIs, microservices, apps, and data powered by policy-based access control.

Visit PlainID.com for more information.