WHITEPAPER

Enhancing Security for SaaS Applications

Remediate Risk & Protect SaaS Applications at Scale by Centralizing Policy Management

plainID

Table of Contents

Introduction

In the fast-paced Identity space, PlainID has consistently led the charge in Authorization. Recognized for its efficacy in controlling access within enterprise service stacks, PlainID now extends its capabilities to address a critical gap in Commercial Off-The-Shelf (COTS) SaaS applications. This whitepaper explores PlainID's latest offering, SaaS Authorization Management, and its impact on cybersecurity.

As we explore this topic, we'll unravel the reasons behind the strategic move to adapt authorization controls for the COTS SaaS world. PlainID's innovative solution enables the creation, management, and approval of policies within its framework, seamlessly translating and deploying them across a spectrum of COTS SaaS technologies.

The focus here is not on the intricacies of technology for its own sake but on understanding the tangible benefits. We will examine how this breakthrough enhances visibility and standardization, fortifying cybersecurity measures. The aim is to establish robust access controls and policies that cater to traditional service stacks and seamlessly integrate with the evolving landscape of COTS SaaS.

Let's explore the practical implications of PlainID's technology and its impact on modern cybersecurity challenges. Together, we'll uncover how this solution is crucial to building a more secure, standardized, and adaptable digital future for the enterprise ecosystem.

The Growing and Evolving Tech Stack

Over the past few years, there has been an unprecedented surge in the adoption of SaaS applications. The driving force behind this surge is the realization that investing time in constructing non-core elements of a business or offering is inefficient and unnecessary. Acquiring and adopting solutions from specialized companies catering to specific needs is more cost-effective and time-efficient. Consequently, COTS SaaS applications have evolved into indispensable technology within an enterprise's ecosystem.

While this strategic adoption has propelled business operations forward—whether in data analysis, storage, or diverse data presentation—it has exerted considerable pressure on security teams. The security challenge lies in ensuring the consistent security and protection of digital assets associated with or housed within these SaaS applications as digital identities journey through intricate layers of the tech stack.

Addressing this requires businesses to standardize their approach to managing access policies. Only through standardization can organizations achieve swifter, more comprehensive visibility, consistency, and security across their operations.

The security challenge lies in ensuring the consistent security and protection of digital assets associated with or housed within these SaaS applications as digital identities journey through intricate layers of the tech stack.

SaaS Authorization Management

PlainID's SaaS Authorization Management empowers organizations to manage their SaaS authorization landscape effectively, providing a centralized hub for viewing, managing, and auditing all access policies in a standardized manner. By adopting this centralized Policy-Based Access Control (PBAC) approach, organizations consistently enforce security measures across a diverse range of high-value and high-risk applications. It also offers enhanced visibility and comprehension for audit teams, streamlining compliance efforts. With PlainID, implementing the principle of Least Privilege Access has never been easier. PlainID Authorizers, integrations that orchestrate policies for different SaaS technologies, raise the security posture across the organization. Before we dive into the use cases, let's understand what Policy Orchestration is.

Policy Orchestration

Policy Orchestration is a comprehensive approach to managing and implementing policies across an organization's IT infrastructure. It involves integrating different systems, applications, and devices to ensure that policies are consistently applied, enforced, and monitored. Here are key aspects of Policy Orchestration:

Integration and Interoperability: Policy Orchestration requires integration with various IT components, such as identity and access management (IAM) systems. The goal is to create a unified framework where policies can be defined centrally and applied seamlessly across different parts of the IT environment.

Centralized Policy Management: Centralization of policy management enables organizations to define, view, and update policies from a single pane of glass. This ensures consistency and reduces the risk of policy misconfigurations or inconsistencies.

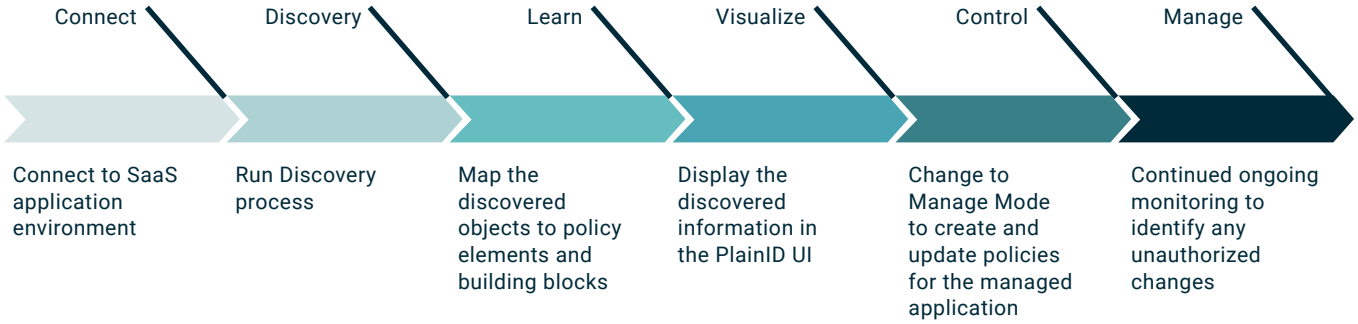
Automated Policy Enforcement: Automation plays a crucial role in Policy Orchestration. Automated enforcement of policies helps in real-time response to security incidents, access requests, or changes in the IT environment. For example, automated responses to security threats or unauthorized access attempts can be orchestrated to minimize the time between detection and mitigation.

Dynamic & Contextual Signals: Policies need to be adaptable to changing conditions. Policy Orchestration allows for dynamic adjustments based on factors such as changes in user roles, system configurations, or emerging security threats.

Compliance Management: Policy Orchestration facilitates compliance by ensuring policies align with regulatory requirements, industry standards, and internal guidelines. Continuous monitoring and reporting help organizations demonstrate and maintain compliance over time.

Risk Mitigation: By orchestrating policies, organizations can proactively address potential security risks. This includes automating responses to identified vulnerabilities, suspicious activities, or deviations from security baselines.

Audit and Reporting: Comprehensive audit logs and reporting capabilities are integral to Policy Orchestration. They provide visibility into policy-related activities, user access, and compliance status, aiding in post-event analysis and continuous improvement of securing access to digital assets.



Policy Orchestration begins with seamless integration with SaaS applications. Once connected to the target SaaS application, PlainID identifies existing objects and policies within the application environment. Subsequently, these elements are automatically translated into easy to manage objects and policies within PlainID's UI dashboard. This empowers organizations to utilize PlainID as a comprehensive reporting and auditing tool, facilitating clear insights for both security and business stakeholders. They gain a deep understanding of policy operations within the system, as well as visibility into identity-access relationships to organizational assets.

Upon activation of Manage Mode, organizations elevate PlainID as the authoritative source for all policies. Any policy updates are centrally managed within the dashboard, ensuring consistency and accuracy across the board. Attempting to modify policies directly within the target system triggers alerts within PlainID, notifying designated administrators. PlainID's proactive approach guarantees that security policies remain current and aligned with the company's Identity Security Posture at all times.

In summary, PlainID's SaaS Authorization Management solution empowers organizations to efficiently oversee their SaaS authorization landscape, offering a centralized platform for monitoring, managing, and auditing access policies in a standardized way. By embracing Policy-Based Access Control (PBAC) principles, organizations can uniformly enforce security measures across diverse and critical applications, enhancing visibility for audit teams and streamlining compliance efforts. With PlainID, implementing least privilege access is simplified, ensuring a robust security posture that scales throughout the organization. Through seamless integration and automated enforcement, Policy Orchestration enables organizations to dynamically adapt policies, mitigate risks, and maintain compliance while providing comprehensive audit and reporting capabilities. With PlainID serving as the central authority for policy management, organizations can ensure policy consistency and responsiveness to security incidents, safeguarding their Identity Security Posture effectively.

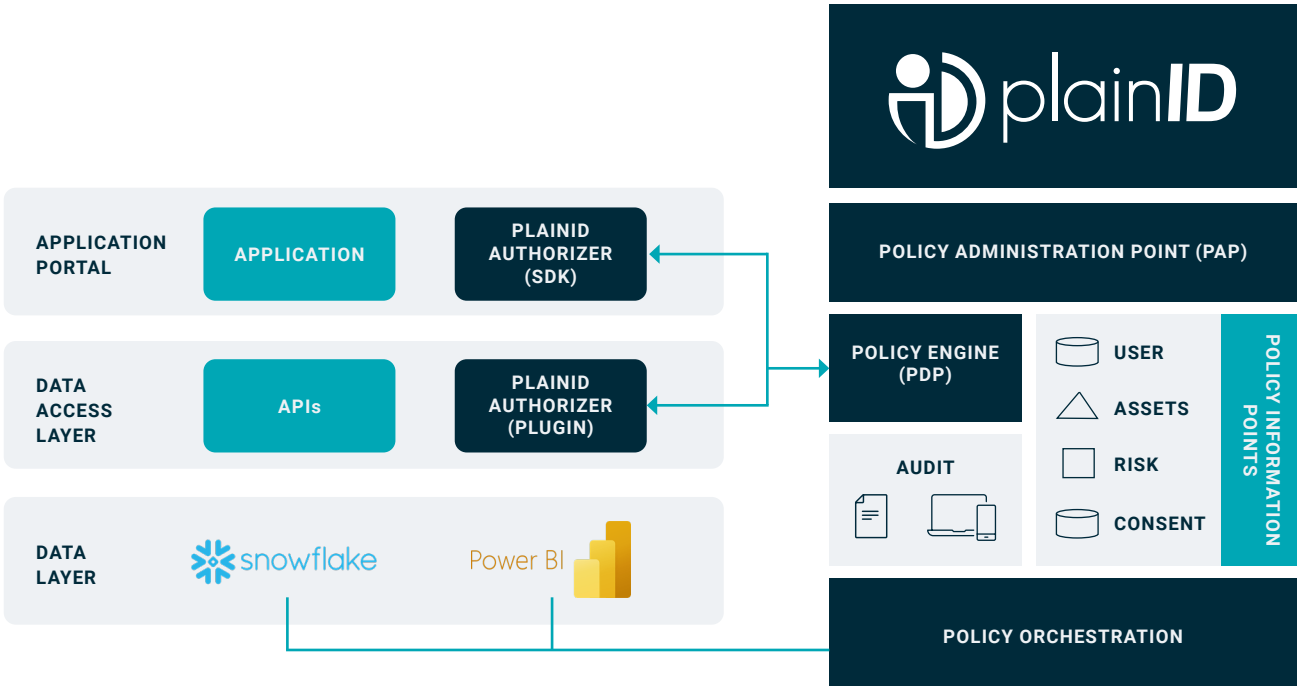
PlainID's proactive approach guarantees that security policies remain current and aligned with the company's Identity Security Posture at all times.

Use Cases

Zero Trust: Least Privilege Access

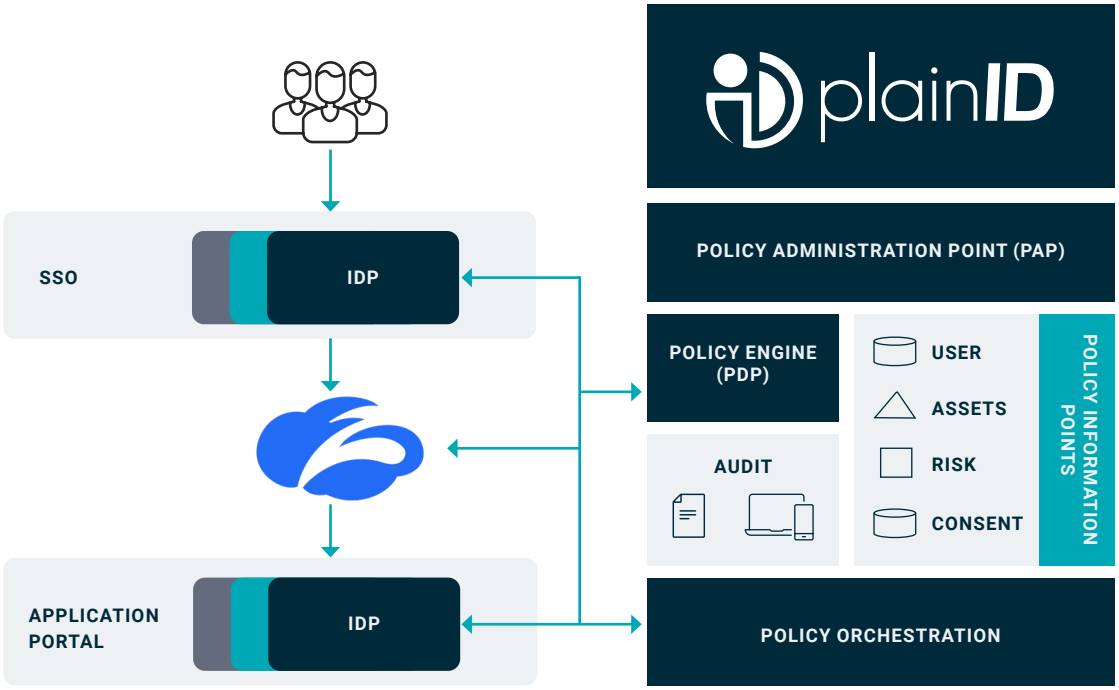
Policy Orchestration, achieved through centralized PBAC utilizing visibility and standardization of policies, supports the principle of least privilege access within organizations. By integrating different systems and applications into a unified framework, Policy Orchestration ensures that access policies are consistently enforced across the entire IT infrastructure. This centralization allows for the clear definition, management, and monitoring of access policies from a single point, simplifying the implementation of least privilege access.

For example, consider the deployment of Policy Orchestration for Power BI, a leading business analytics tool. With Policy Orchestration, organizations can define granular access policies within Power BI and ensure users only have access to the data and features necessary for their roles. Administrators can quickly review and update these access policies by centralizing policy management. Only authorized users can view sensitive reports or manipulate critical datasets. This reduces the risk of data breaches and enhances the efficiency of data governance efforts.



Similarly, integrating Policy Orchestration with Zscaler, a cloud security platform, enhances security posture and ensures least privilege access across web-based applications and services. Organizations can extend access policies defined within their internal systems to control access to web resources through Zscaler. Administrators can seamlessly enforce consistent access controls across internal and external applications by centralizing policy management.

This integration enhances security and simplifies policy management, ensuring access policies remain up-to-date and aligned with organizational security requirements. Ultimately, Policy Orchestration empowers organizations to proactively enforce least privilege access across their IT environment, mitigating security risks and enhancing data protection measures.



In the integration between PlainID and Zscaler, PlainID orchestrates access policies, ensuring seamless enforcement across the organization's IT landscape. When a user requests access to a critical application, the Identity Provider (IDP) forwards this request to PlainID for authorization. As the central authority for access policies, PlainID evaluates the user's request against the organization's policies to determine their level of access and specific entitlements.

Once PlainID verifies the user's access, it communicates the approved access and fine-grained entitlements back to the IDP. Subsequently, the IDP enriches the user's access token with this information. The enriched access token, containing the precise access permissions dictated by PlainID's policies, is then transmitted to Zscaler.

Zscaler utilizes the enriched access token to connect the user to the critical application with the appropriate level of access, ensuring adherence to the organization's access policies. This seamless orchestration by PlainID ensures that users only access resources for which they are authorized–enhancing security and compliance across the organization's IT infrastructure.

Audit and Compliance

Centralized, standardized, and visually represented Policy-Based Access Control (PBAC) not only enhances security measures but also significantly accelerates operations for audit, security, and compliance teams, ultimately benefiting business operations. By consolidating access policies into a centralized system organizations create a single source of truth for access management. This centralization streamlines the auditing process by providing audit teams with easy access to comprehensive and standardized policy information, allowing them to quickly assess the organization's security posture.

Furthermore, the business-driven representation of access policies via PlainID's Policy Mapping offers visibility into how access controls are configured across various applications and services. This visual representation enables security and compliance teams to identify potential gaps or inconsistencies in access policies more efficiently. By visualizing access policies, teams can rapidly pinpoint areas that require attention, facilitating prompt resolution of compliance issues and security vulnerabilities.

Moreover, the standardized approach to access policy management ensures consistency in enforcing access controls throughout the organization. Security and compliance teams can easily track and enforce standardized policies, reducing the risk of policy misconfigurations or non-compliance. This standardized approach not only strengthens security measures but also simplifies compliance efforts.

Overall, the centralized, standardized, and visually represented PBAC offered by ISPM platforms enables audit, security, and compliance teams to operate faster and more effectively. By providing easy access to comprehensive policy information, visual insights into access controls, and standardized policy enforcement, organizations can support faster business operations, streamline compliance efforts, and ultimately enhance their security posture.

Identity Security Posture Management

The integration of centralized, standardized, and visually represented Policy-Based Access Control (PBAC) solutions like PlainID, coupled with seamless orchestration across platforms such as Zscaler and Power BI, creates a defensive layer against identity-related breaches and significantly enhances Identity Security Posture Management (ISPM). By centralizing access policy management within PlainID, organizations establish a unified framework for defining, enforcing, and monitoring access controls across their IT infrastructure.

This comprehensive approach to access control not only simplifies the management of access policies but also strengthens security measures by ensuring that users are granted only the access they require, following the Zero Trust Principle of Least Privilege. PlainID's visualization capabilities provide security and compliance teams with clear insights into access policies, enabling them to identify and resolve potential security gaps or policy inconsistencies swiftly. This proactive approach to access management serves as a crucial prevention against identity-related breaches, minimizes the attack surface, and reduces the likelihood of unauthorized access.

Moreover, the orchestration of access policies to platforms such as Zscaler and Power BI through PlainID ensures that access decisions are consistently enforced across various technologies. By integrating PlainID's centralized policy management with Zscaler's cloud security platform, organizations can extend access controls to web-based applications, further fortifying their defenses against identity-related threats. Similarly, by enforcing granular access controls within Power BI, organizations can prevent unauthorized access to sensitive data and mitigate the risk of data breaches stemming from compromised user accounts.

The combined capabilities of centralized PBAC solutions, seamless Policy Orchestration across platforms, and visualization of access policies empower organizations to proactively manage their Identity Security Posture. By enforcing least privilege access, identifying and addressing security vulnerabilities, and ensuring consistent policy enforcement, these measures collectively contribute to a robust defense against identity-related breaches, safeguarding sensitive data and preserving the integrity of organizational systems.

Summary

Policy Orchestration powered by Policy-Based Access Control (PBAC) solutions such as PlainID enhances organizational security posture and mitigating identity-related breaches. By centralizing access policy management, PlainID facilitates the implementation of least privilege access across various platforms, including Zscaler and Power BI. This centralized approach not only streamlines access control but also ensures consistency and standardization, thereby reducing the risk of policy misconfigurations and compliance breaches.

The integration of PlainID with industry-leading solutions such as Zscaler and Power BI enables enterprises to enforce granular access controls and extend policy enforcement to web-based applications, strengthening defenses against identity-related threats. The visual representation of access policies within PlainID offers clear insights for security and compliance teams, enabling them to identify and resolve security gaps. This empowers organizations to proactively manage their Identity Security Posture. By enforcing least privilege access, identifying and addressing security vulnerabilities, and ensuring consistent policy enforcement, organizations can bolster their security defenses and safeguard sensitive data effectively.

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.