EBOOK

The Guide to Identity Security Posture Management

An Identity-Centric Security Approach to Zero Trust and Least Privilege Access

plainID

Table of Contents

Introduction

In the ever-evolving landscape of cybersecurity, the shift from traditional perimeter-centric defenses to identity-centric security models is not just a trend but a necessity. With the digital transformation of businesses, the explosion in the number of digital identities, and the increasing sophistication of cyber threats, the focus of security efforts has shifted. Today, protecting digital identities is paramount. This is where Identity Security Posture Management (ISPM) comes into play, a comprehensive approach to safeguarding the digital identities and the data being accessed is integral to modern business operations.

This eBook delves into the concept of ISPM, exploring its significance, challenges, best practices, and future trends. Aimed at security and business leaders, this guide seeks to illuminate the path toward a more secure digital environment where identities are protected and managed with a strategic, holistic approach.

The Evolving Landscape of Cybersecurity

The world of cybersecurity has undergone significant transformations over the years. Initially, cybersecurity focused on fortifying the network perimeter - an organization's digital 'walls'. However, as technology evolved and business operations became increasingly digital and cloud-based, the concept of a fixed perimeter became obsolete.

Today, the security landscape is witnessing a paradigm shift towards identity-centric security. In this new paradigm, the identity - whether it be an employee, a partner, a customer, or a machine - becomes the central focus of security strategies. This shift acknowledges that the weakest link in security is often not the technology itself but the identities that interact with it.

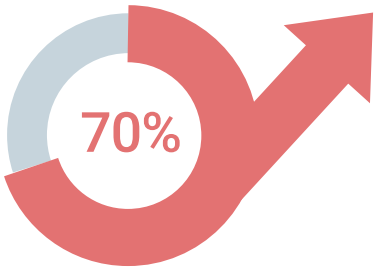
CHAPTER 1:

Understanding Identity Security Posture Management (ISPM)

Defining ISPM

Identity Security Posture Management, or ISPM, is a comprehensive approach to identifying identities and their digital interactions within an organization. It is a strategy that encompasses the identification, management, authorization and security of digital identities, ensuring that the right individuals have the appropriate access to digital resources, and more importantly, that unauthorized individuals do not.

ISPM is crucial in the modern cybersecurity landscape for several reasons. First, it addresses the complexity of the vast digital space identities operate in. Second, it helps organizations comply with increasing regulatory demands around zero-trust and least privileged access. Lastly, it plays a pivotal role in minimizing the risk of data breaches, often resulting from compromised identity credentials and over-privileged access.



of breaches are due to unauthorized access

*Source: https://www.ideagen.com/solutions/audit-and-risk/external-audit/trends-in-cybersecurity-breach-disclosures

Components of ISPM

The core components of ISPM include:

Discovery and visibility: This involves identifying all the digital identities within an organization and gaining visibility into their access rights and activities. It's about knowing your identity, 'who' is in your system, and 'what' they can do. It is critical to understand what policies and identities are associated with access to sensitive data to resolve and bridge gaps in access privileges.

Management and standardization: This aspect focuses on the administration of IAM-related life cycles and the automation of identity-related processes. It includes the management of access rights through authorization policies and identity roles, attributes, and entitlements, ensuring that identities have access to only what they need and nothing more.

Continuous and contextual enforcement: A robust ISPM strategy ensures dynamic and continuous risk-based authorization policy decisions are enforced consistently throughout the enterprise. Policies must be agile and responsive to real-time changes in user behavior, environment, and risk levels – adapting authorization responses for each access request. This ensures that access decisions are sensitive to the unique context of each interaction, maintaining a high level of assurance without compromising on user experience or operational efficiency.

In the next chapters, we will delve deeper into these components, exploring the challenges they present and the strategies to effectively manage them.

CHAPTER 2:

The Rise of Identity-Centric Security

Changing Paradigms in Cybersecurity

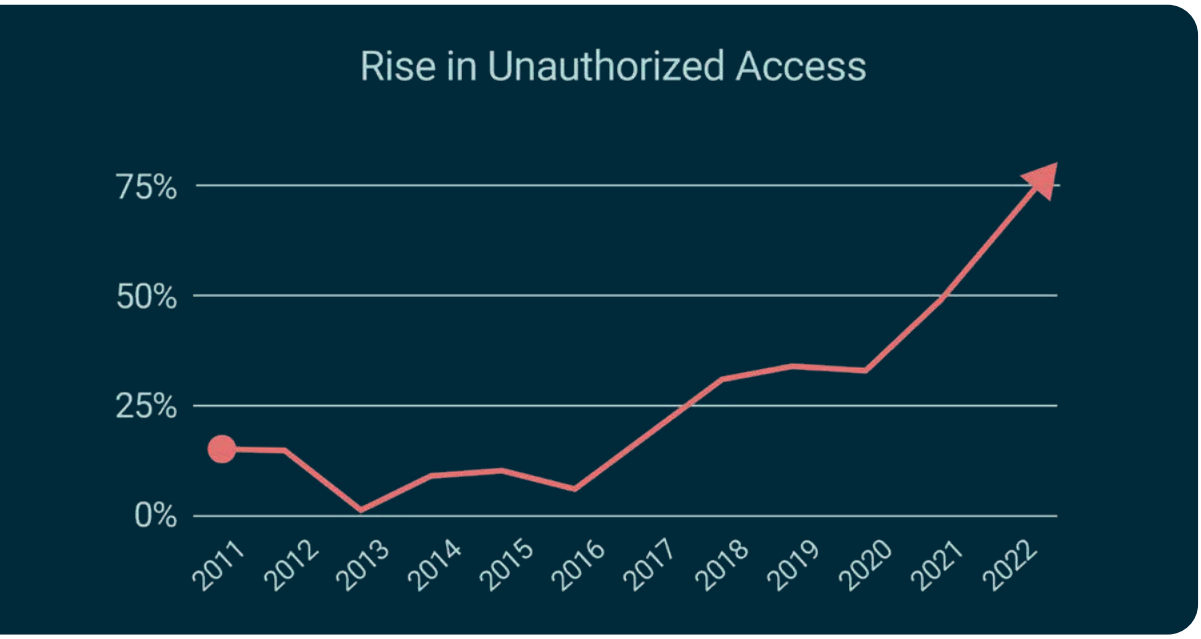
The cybersecurity landscape has been significantly redefined in recent years. The traditional focus on perimeter defense has given way to a more nuanced, identity-centric model. This shift recognizes that as digital ecosystems expand, organizations' access controls become fragmented across departments and functions, making it increasingly difficult to secure them through traditional means alone (e.g. role-based and attribute-based access controls, etc).

In an identity-centric security model, the primary focus is on securing identities within the organization, recognizing that each identity - whether it's an employee, a customer, or a system - potentially holds the key to vast swathes of sensitive data and resources.

The Role of Identity in Cybersecurity

An individual identity is like a master key. With the right credentials, one can access information via multiple layers: applications (i.e. SaaS and custom applications), APIs, microservices, and data platforms. This reality makes identities a prime target for external bad actors, and can also be exploited internally.

The increase in high-profile breaches and cyber-attacks where unauthorized access was the entry point highlights the importance of robust identity security measures.



*Source: https://www.ideagen.com/solutions/audit-and-risk/external-audit/trends-in-cybersecurity-breach-disclosures

CHAPTER 3:

Challenges in Identity Security

Common Challenges and Pitfalls

As organizations grow and evolve, they often grapple with complex identity environments. These challenges include managing many user accounts across various platforms, ensuring compliance with ever-changing regulatory landscapes, and the ongoing battle against sophisticated cyber threats.

One major challenge lies in the disparate nature of modern IT ecosystems. Organizations frequently employ a mix of on-premise and cloud-based solutions, each with its own set of rules and frameworks. This complexity can create gaps in security and increase the risk of breaches.

Unauthorized Access and Data Breaches

The statistics on data breaches paint a troubling picture. A significant portion of these incidents is attributable to unauthorized access, often facilitated by compromised or mismanaged identities. Nearly 70% of breaches in 2022[1] have been reported to be caused by unauthorized access. These breaches not only lead to immediate financial losses but also long-term reputational damage.

The root causes of these breaches vary but often include weak password policies, the lack of multifactor authentication, and poor access controls. These vulnerabilities highlight the need for a comprehensive approach to identity security that addresses the technical aspects and the human factors (e.g. manageability for administrators and user experience) involved.

[1] Trends in Cybersecurity Breach Disclosures A12-Year Review 2023

CHAPTER 4:

Implementing Effective ISPM

Best Practices in Identity Security

Implementing ISPM requires combining strategy, technology, and operational best practices. It begins with establishing a framework that lays the foundation for controlling and monitoring identity access within an organization.

1. Identity Hygiene: This involves defining and enforcing policies around identity management and access control. It includes regular audits of identity access privileges and ensuring that these privileges align with the current roles and responsibilities of the identity holder. Just like personal hygiene involves routines to maintain health and prevent disease, identity hygiene involves regular and systematic actions to secure digital identities and prevent unauthorized access. This is a crucial step in safeguarding sensitive data and systems from potential breaches.

2. Least Privilege Access: The principle of Least Privilege dictates that individuals or systems are granted only the minimum levels of access – or permissions – necessary to perform their roles or functions. In ISPM, this principle is crucial for minimizing the potential damage from security breaches, reducing the attack surface, and ensuring compliance with regulatory standards. By implementing Least Privilege Access, organizations can significantly diminish the risk of unauthorized access and data breaches, as users are restricted from accessing sensitive information or systems irrelevant to their specific roles and responsibilities.

3. Continuous, Contextual, and Consistent Access Decisioning: Effective ISPM is not a one-time activity but an ongoing process. The 3 C's approach[2] emphasizes the need for security systems to dynamically adapt and respond to ongoing changes in user context and environment, ensuring that access decisions are always relevant and appropriate to the current situation. By continuously evaluating and updating access permissions based on real-time data — such as user location, device security status, time of access, and typical behavior patterns — organizations can maintain a high level of security without hindering operational fluidity. Consistency in these decisions across all platforms and systems is key to maintaining an unbreachable and coherent security posture.

[2] Gartner, Identity-First Security Maximizes Cybersecurity Effectiveness, Rebecca Archambault, Felix Gaehtgens, James Hoover, Ant Allan, 7 December 2022

CHAPTER 4 CONTINUED:

Gaining Full Control with Access Policies

Effective Identity Security Posture Management (ISPM) is anchored in the comprehensive handling of access policies, encompassing their authoring, management, and enforcement. Each component plays a critical role in maintaining a secure and efficient digital environment:

1. Policy Authoring: The authoring of access policies is the foundational step in ISPM, where rules and criteria for access rights are crafted. This process involves defining clear, detailed, and context-aware policies that govern who can access what resources, and under what circumstances. Effective policy authoring ensures these rules align with organizational security requirements and business objectives, setting the stage for robust access control.

2. Policy Management: Managing and orchestrating access policies is an ongoing task that involves regular updates, reviews, and modifications to adapt to changing business needs, regulatory requirements, and evolving security threats. Effective management ensures policies remain relevant, efficient, and non-restrictive to legitimate business processes. This is especially critical for SaaS applications and platforms where high volumes of identities have access to massive amounts of data (e.g. proprietary business information, sensitive Personal Identifiable Information (PII), and other high-value data).

3. Policy Enforcement: The enforcement of access policies is the active application of these rules within the IT environment. It involves leveraging technology to ensure that all access decisions adhere strictly to the established policies. Effective enforcement requires robust and flexible security solutions capable of dynamic and real-time policy application, ensuring that unauthorized access attempts are identified and prevented.

The strength of an ISPM strategy lies in the synergy of these components, working together to create a secure, compliant, and efficient system for managing digital identities and access rights.

CHAPTER 5:

Solutions for Identity Security

Comparing Technologies Old and New, and Their Impact on ISPM

The evolution of Identity Security Posture Management (ISPM) marks a significant shift in the approach to Identity Security, especially when compared to traditional Identity Providers (IDPs), Identity Governance and Administration (IGA), and the emerging Identity Threat Detection and Response (ITDR) solution.

ISPM vs IDP: While IDP focuses on authenticating and providing identity to applications in a consumable manner (e.g. OAUTH, SAML, and authentication), ISPM goes a step further. ISPM continuously assesses and improves the security posture of identity infrastructure – discovering and alerting if identities are being provided to applications when they should not be, determining if access is too permissive, and discovering when specific identities are not protected appropriately (e.g. active MFA requirements, etc.) or under attack. It's proactive, using real-time data and analytics to identify potential vulnerabilities before they are exploited, and provides policy recommendations to bridge the security gap.

ISPM vs IGA: Identity Governance and Administration (IGA) and Identity Security Posture Management (ISPM) serve complementary roles in the broader context of identity security. IGA ensures that access rights. This includes roles management, access requests, and certification processes to manage and govern user access and is typically done at admin-time (i.e. focused on static definitions and lifecycles). In contrast, ISPM extends beyond these governance functionalities. It continuously assesses the security posture of an organization by monitoring identities and their activity (ie. identity activity), to determine how and where identity security posture is misaligned with security best practices. ISPM involves analyzing security configurations, identifying misconfigurations or policy deviations, and ensuring that identity and access controls are effectively mitigating risks.

CHAPTER 5 CONTINUED:

ISPM vs ITDR: The Identity Threat Detection and Response (ITDR) space is rapidly gaining attention for its focus on identifying and responding to threats against identity systems. ITDR is reactive, dealing with threats after they have been identified. In contrast, ISPM is proactive, focusing on preventing threats by maintaining a robust identity security posture by ensuring access policies are in place to mitigate unauthorized access and prevent breaches. Together, ISPM and ITDR create a comprehensive approach to identity security, covering both prevention and response.

ISPM represents a dynamic, intelligent, and comprehensive approach to identity security. It not only incorporates the foundational aspects of traditional IAM such as IDPs and IGA, but also complements the reactive strategies of ITDR by providing a visibility and auditing layer – therefore, creating a more resilient and adaptive identity security framework. As digital threats evolve, the role of ISPM will become increasingly vital in safeguarding identity data and infrastructure.

Conclusion

The Convergence of Identity and Security

The cybersecurity landscape has shifted from traditional perimeter-centric defenses to a more holistic, identity-centric approach. While there may be overlapping features and functionality across traditional and new solutions, ISPM plays a role in safeguarding digital identities and ensuring secure access to data – vital for modern business operations, driving revenue, and achieving data protection and privacy.

As enterprises embrace the convergence of Identity and security, it's clear that mastering ISPM is about more than grasping technical nuances. It's about adopting a mindset and framework that places Identity at the core of organizational security. In a digital world where digital identities increasingly serve as the primary gateway to critical resources and data, a strong ISPM strategy is essential.

To learn more about how PlainID can support your ISPM strategy, **contact us** today.

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.**