RSA

REPORT

Defining Identity Security Posture Management (ISPM): A Framework for Securing the Modern Identity Landscape

Identity security posture management (ISPM) is emerging as a new strategic cybersecurity discipline that enables organizations to manage risk, enforce policy, and strengthen compliance across increasingly complex environments. ISPM provides visibility, context, and continuous monitoring of identity-related risk across hybrid environments.

While others are just beginning to define ISPM, RSA is already delivering on it. RSA Governance & Lifecycle provides the IGA capabilities organizations need to manage identity risks; recently the solution added new advanced dashboards built on ISPM principles that help organizations reduce the identity risk surface, strengthen compliance and audit readiness, mitigate cloud entitlement risks, and more.

This report defines the core principles of ISPM, outlines the foundational capabilities required to enable it, and helps organizations assess their readiness to adopt an ISPM strategy that supports long-term Zero Trust maturity.

Why ISPM matters now: the risk of inaction

Failing to secure identities leaves organizations vulnerable to a wide range of threats. Misconfigured access, over-provisioned accounts, weak authentication, and shadow IT are just a few of the identity-related risks that attackers exploit. Without effective identity security, organizations will face significant risks of data breaches, insider abuse, regulatory violations, stalled audits, ransomware attacks, or even reputational collapse. Privileged access misuse or undetected lateral movement can often go unnoticed for months, compromising critical systems and sensitive data. In today's threat landscape, identity-based attacks are not only increasing, they are the leading cause of enterprise breaches: 80% of breaches involved the use of stolen credentials.

ISPM was created to counter these growing risks. When implemented effectively, ISPM strategies give organizations real-time visibility and actionable intelligence to reduce identity-related risk at scale. The result is a stronger security posture, improved resilience, and greater confidence in meeting compliance requirements.

The challenges ISPM solves

The identity landscape has become too sprawling, fragmented, and complex for traditional controls to manage effectively. As organizations adopt more cloud services, bring in third-party users, and automate business processes, the number of identities grows—and so do the risks. ISPM addresses the operational and security blind spots that result from this growth. These include:

- **Identity sprawl** is the accelerated growth of human, device, service, and machine accounts. More identities leads to overlapping, orphaned, and shadow accounts that attackers can exploit. Over half (57%) of organizations consider managing identity sprawl a major focus, highlighting its significance in the current security landscape.
- **Misconfigurations and inconsistent policies** make it harder to enforce access controls and increase the likelihood of privilege misuse. The prevalence of hybrid environments (reported by 70% of organizations) further complicates identity policy enforcement across different systems.

- **Unmanaged entitlements** allow users to retain access that no longer reflects their responsibilities. When access is not regularly reviewed or based on least-privilege principles, unmanaged entitlements increase the chance of excessive or toxic combinations going unnoticed. These gaps can directly contribute to security incidents.
- **Limited visibility into privileged or high-risk accounts** slows detection of malicious activity and insider threats. More than 20% of organizations estimated that identity-related breaches cost them over $10 million. In total, 44% said these breaches were more expensive than general data breaches.
- **Shadow IT** occurs when business units or employees adopt unauthorized applications or systems outside the purview of IT. These unsanctioned technologies often lack proper security oversight, increasing the risk of data exposure, misconfigurations, and compliance violations.

These issues are not just inconvenient. They create real exposure. Without a clear understanding of who has access to what, and whether that access is appropriate, organizations face delays during audits, struggle to meet compliance mandates, and fall short of Zero Trust goals. Over-provisioned accounts, toxic access combinations, and delayed incident response can result in breaches, penalties, and loss of public trust.

ISPM gives security teams the visibility and context they need to address these growing challenges and reduce the attack surface. It shifts identity management from reactive cleanup to proactive risk reduction, bringing identity risk under control across cloud, hybrid, and on-premises environments.

The eight pillars of ISPM

ISPM is designed to be proactive, not reactive. It helps organizations identify and address small risks before they become major security events. Rather than waiting for a compliance violation, breach, or audit failure to expose identity weaknesses, ISPM delivers continuous posture management that reduces risk over time. This forward-looking strategy is what separates ISPM from traditional identity security approaches. The following pillars represent the core outcomes organizations should expect from a mature ISPM approach, each illustrated with screenshots from RSA Governance & Lifecycle Advanced Dashboards to show how these outcomes are achieved in practice:

1. Reducing the identity risk surface

ISPM reduces the expanding identity risk surface caused by identity sprawl and over-entitled users. By providing continuous visibility into user access across all systems, ISPM helps limit credential compromise, lateral movement, and excessive privilege.

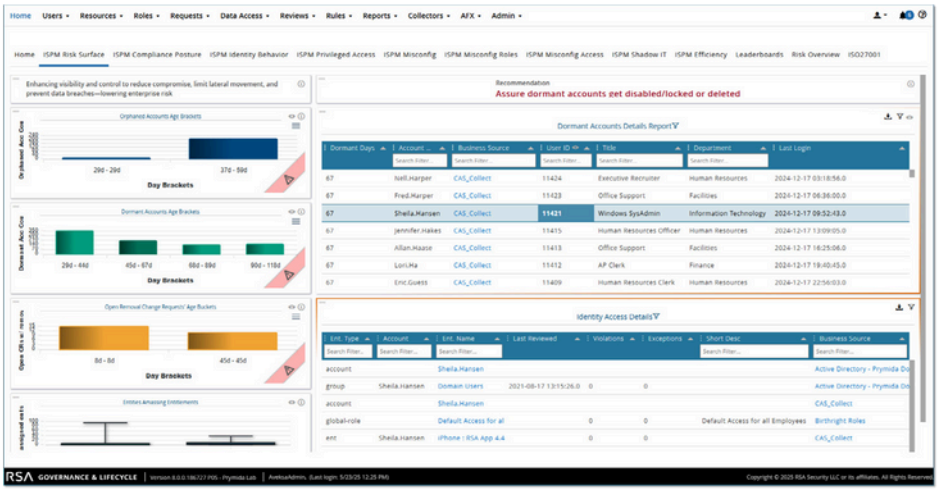

Figure 1: Risk Surface dashboard enhances visibility and control to prevent unauthorized access, limit lateral movement, and stop data breaches while reducing overall enterprise risk.

2. Strengthening compliance and audit readiness

ISPM automates access reviews, detects policy violations, and provides real-time evidence of compliance with regulations like GDPR, DORA, HIPAA, PCI-DSS, and many others. This reduces the cost and effort of audit cycles.

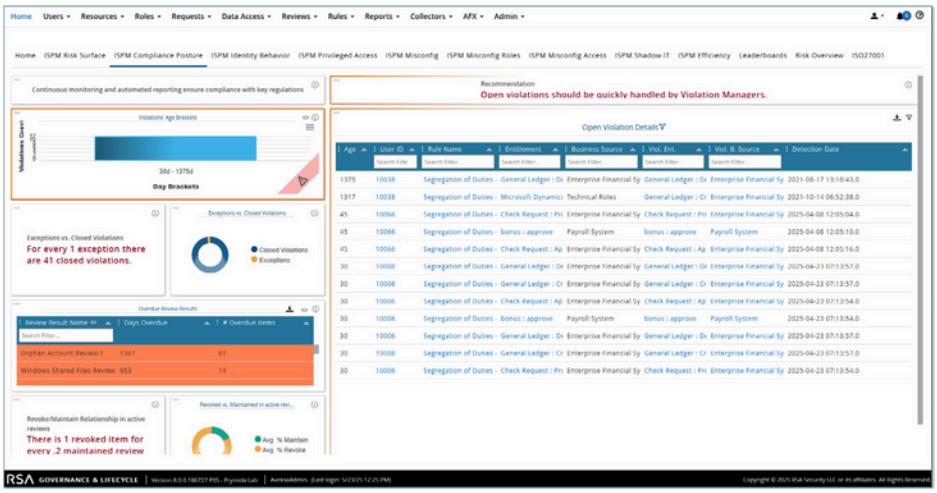

Figure 2: Compliance Posture dashboard provides continuous monitoring and automated reporting to ensure compliance with key regulations.

3. Mitigating cloud entitlement risks

As organizations move to the cloud, ISPM addresses the complexity of managing entitlements in dynamic, multi-cloud environments. It prevents over-provisioning and ensures least-privilege access to cloud resources.

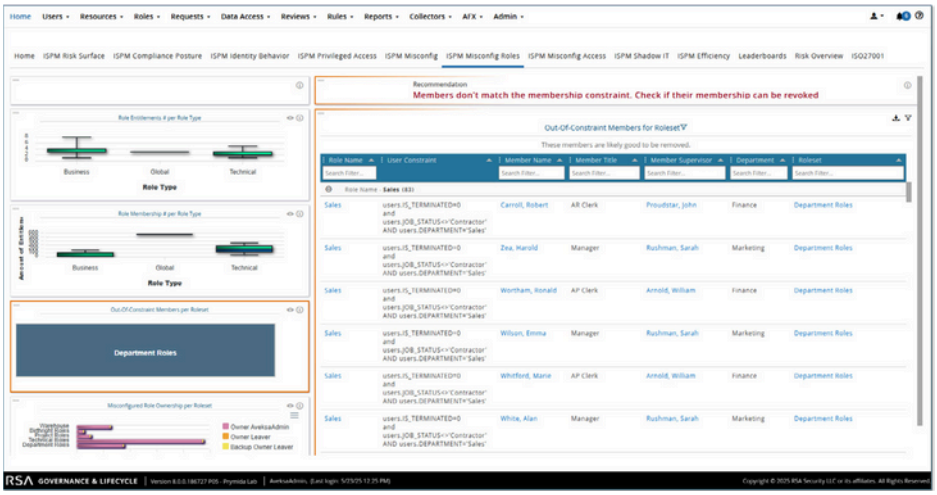

Figure 3: Misconfigured Roles dashboard identifies and resolves misconfigured roles to reduce over-provisioning and enforce least-privilege access across cloud, hybrid, and on-premises environments.

4. Detecting identity-based threats

ISPM helps detect abnormal behavior such as privilege escalation or credential misuse by applying identity analytics and behavioral monitoring.

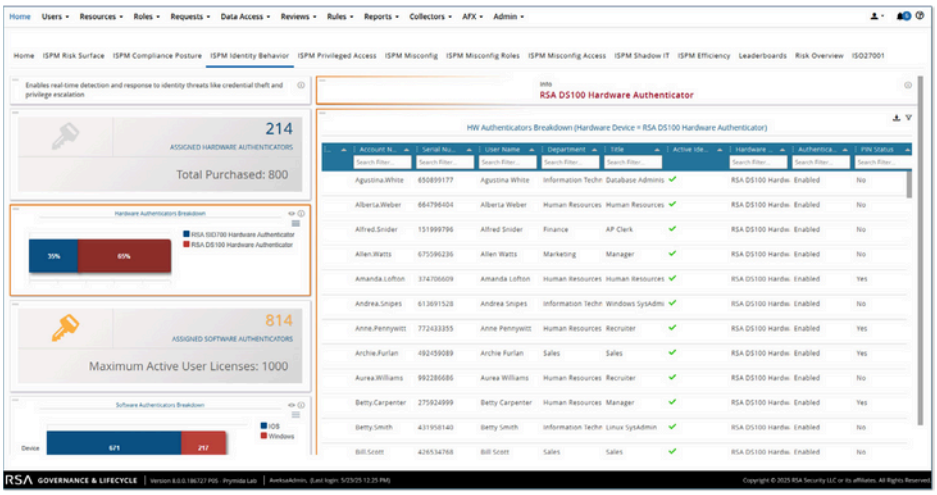

Figure 4: Enable real-time detection and response to identity threats like credential theft and privilege escalation.

5. Controlling privileged access

ISPM delivers visibility into privileged account usage and helps enforce least privilege by highlighting risky accounts and automating policy enforcement.

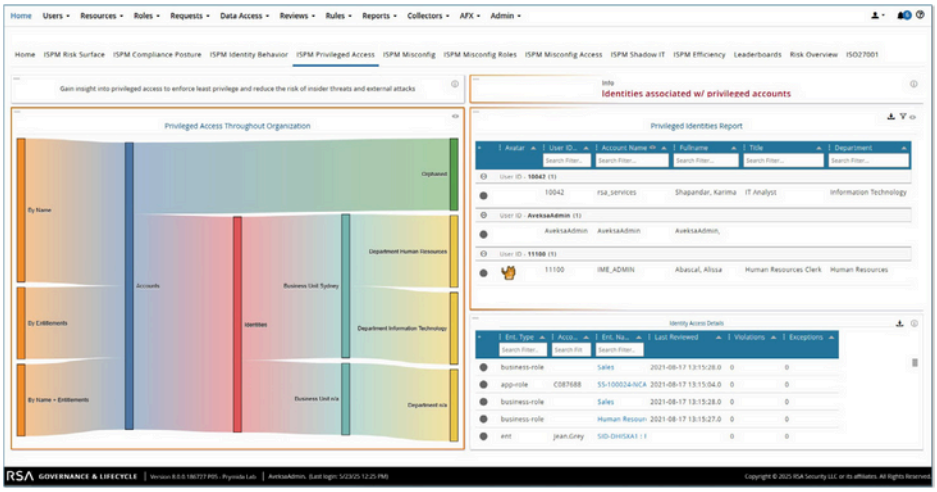

Figure 5: Gain insight into privileged access to enforce least privilege and reduce the risk of insider threats and external attacks.

6. Fixing identity misconfigurations

From weak multi-factor authentication (MFA) enforcement to excessive access, ISPM identifies misconfigurations and guides remediation to close security gaps.

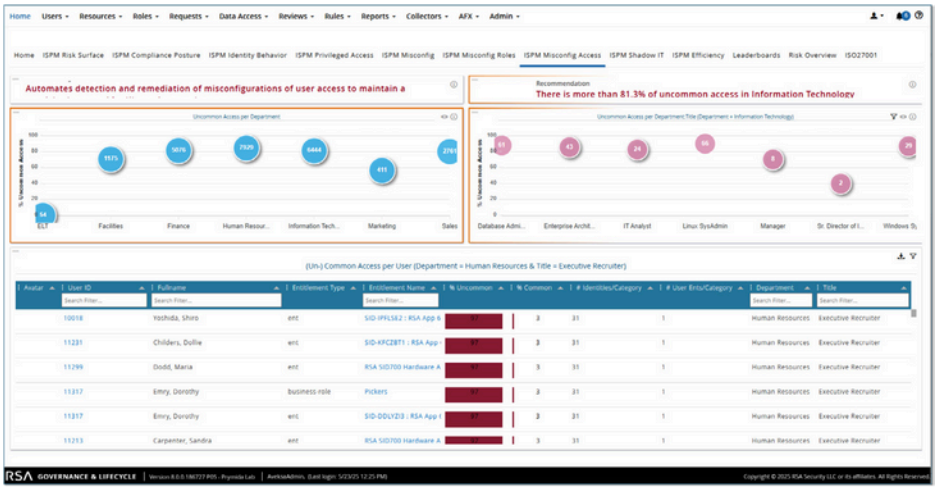

Figure 6: Automated detection and remediation of misconfigurations of user access help maintain a consistent, secure identity environment.

7. Eliminating shadow access

ISPM discovers and controls unauthorized or unknown users, accounts, or applications that operate outside formal identity systems.

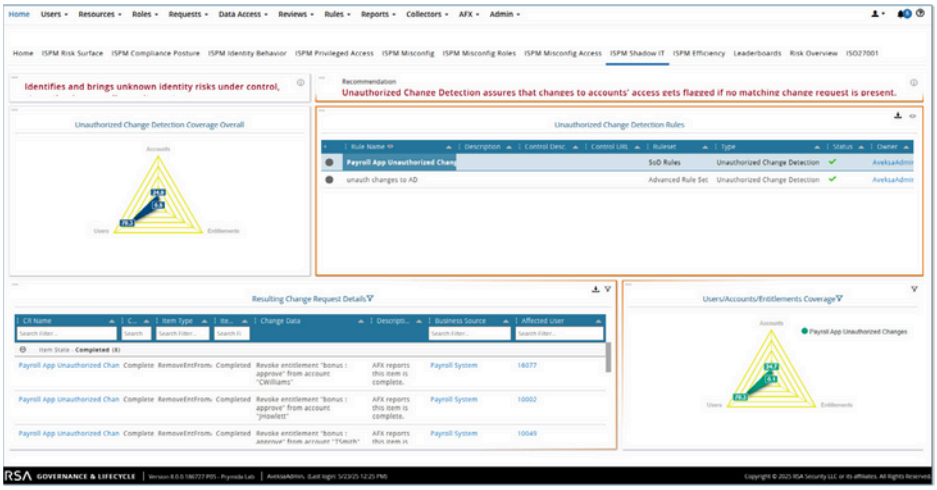

Figure 7: This dashboard provides visibility into users, accounts, and entitlements coverage to identify and bring unknown identity risks under control.

8. Increasing operational efficiency

By automating routine identity risk detection and policy enforcement, ISPM allows security teams to focus on strategic initiatives.

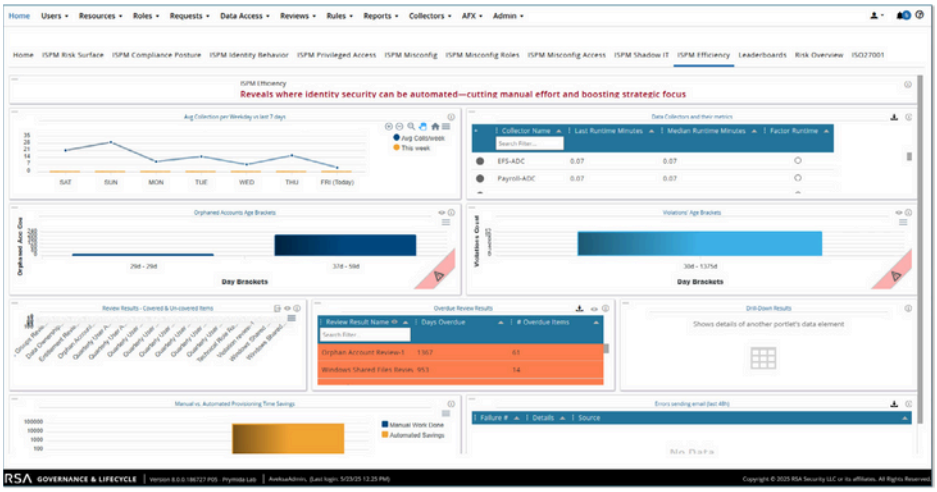

Figure 8: This ISPM Efficiency dashboard reveals where identity security can be automated to cut manual effort and boost strategic focus.

Core capabilities required for ISPM

ISPM is not a single tool or dashboard. It is a strategic approach built on a foundation of integrated identity security technologies. These capabilities must work together to continuously evaluate identity posture, enforce policy, and guide remediation. Organizations seeking to implement ISPM should ensure they have the following:

- **Identity governance and administration:** Core capabilities such as policy enforcement, access certification, role management, and lifecycle controls.
- **Identity discovery and visibility:** Tools to inventory users, entitlements, and accounts across cloud, on-premises, and hybrid environments.
- **Monitoring and analytics:** Advanced analytics to track behavior, detect anomalies, and prioritize identity-related risks.
- **Access management and strong authentication:** Context-aware access policies, MFA, and modern authentication methods such as passwordless and biometric login.
- **Privileged access oversight:** Capabilities to discover, monitor, and govern privileged and high-risk accounts.
- **SaaS and shadow IT protection:** Visibility into SaaS app usage and mechanisms to control unauthorized or unmanaged access.
- **Integration across identity tools:** A unified architecture or open integration framework that connects these capabilities to ensure continuous visibility and policy enforcement.

Turning capabilities into a cohesive cybersecurity strategy

To achieve an effective ISPM program, organizations need more than a checklist of individual capabilities. Instead, they need a platform that unifies distinct cybersecurity components into a cohesive solution. A unified identity platform (UIP) brings governance, access, and authentication together under one architecture, enabling better visibility, stronger controls, and more informed decisions across the identity ecosystem.

RSA is one of the only companies with a UIP that fully integrates governance, access, and authentication. RSA Governance & Lifecycle delivers governance and visibility. RSA ID Plus provides access and authentication. RSA analytics engines connect insights across the platform. Few, if any, other vendors offer these core components as part of a truly unified architecture.

Understanding Zero Trust and ISPM

Zero Trust is a security framework that assumes no user or system should be trusted by default, even inside the network. It requires continuous verification of identity, strict access controls, and least-privilege enforcement. If Zero Trust is the goal, then ISPM is the method to get there. ISPM operationalizes Zero Trust by providing the visibility, analytics, and enforcement capabilities needed to evaluate and improve identity-related controls over time.

The path forward

ISPM is the future of identity security. As threats continue to evolve and regulatory pressure increases, organizations need a new approach to managing identity risk. This report provides a foundation for understanding ISPM, its key pillars, and what is required to implement it. With the RSA Unified Identity Platform, organizations can take a leadership role in securing the identity landscape and building a sustainable, Zero Trust-aligned future.

About RSA

RSA provides mission-critical cybersecurity solutions that protect the world's most security-sensitive organizations. The RSA Unified Identity Platform provides true passwordless identity security, risk-based access, automated identity intelligence, and comprehensive identity governance across cloud, hybrid, and on-premises environments. More than 9,000 high-security organizations trust RSA to manage more than 60 million identities, detect threats, secure access, and enable compliance. For additional information, visit our website to contact sales, find a partner, or learn more about RSA.

RSA

©2025 RSA Security USA LLC or its affiliates. All rights reserved. RSA and the RSA logo are registered trademarks or trademarks of RSA Security USA LLC or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 06/25 Report