REPORT

Definition von Identity Security Posture Management (ISPM): Ein Rahmenwerk zur Sicherung der modernen Identitätslandschaft

Identity Security Posture Management (ISPM) entwickelt sich zu einer neuen strategischen Cybersicherheitsdisziplin, die es Unternehmen ermöglicht, Risiken zu managen, Richtlinien durchzusetzen und die Compliance in zunehmend komplexen Umgebungen zu stärken. ISPM bietet Transparenz, Kontext und kontinuierliche Überwachung identitätsbezogener Risiken in hybriden Umgebungen.

Während andere gerade erst mit der Definition von ISPM beginnen, setzt RSA bereits alles daran. RSA Governance & Lifecycle bietet die IGA-Funktionen, die Unternehmen zum Management von Identitätsrisiken benötigen. Seit kurzem verfügt die Lösung über neue, erweiterte Dashboards auf Basis von ISPM-Prinzipien, die Unternehmen dabei helfen, die Oberfläche von Identitätsrisiken zu reduzieren, Compliance und Auditbereitschaft zu stärken, Risiken im Zusammenhang mit Cloud-Berechtigungen zu minimieren und vieles mehr.

Dieser Bericht definiert die Kernprinzipien von ISPM, skizziert die grundlegenden Fähigkeiten, die zu seiner Umsetzung erforderlich sind, und hilft Unternehmen dabei, ihre Bereitschaft zur Einführung einer ISPM-Strategie zu beurteilen, die eine langfristige Zero-Trust-Reife unterstützt.

Warum ISPM jetzt wichtig ist: Das Risiko der Untätigkeit

Wenn es Unternehmen nicht gelingt, Identitäten zu schützen, sind sie anfällig für eine Vielzahl von Bedrohungen. Falsch konfigurierter Zugriff, überdimensionierte Konten, schwache Authentifizierung und Schatten-IT sind nur einige der identitätsbezogenen Risiken, die Angreifer ausnutzen. Ohne effektiven Identitätsschutz sind Unternehmen erheblichen Risiken von Datenlecks, Insider-Missbrauch, Verstößen gegen Vorschriften, verzögerten Audits, Ransomware-Angriffen oder sogar einem Reputationsverlust ausgesetzt. Der Missbrauch privilegierter Zugriffe oder unentdeckte laterale Bewegungen bleiben oft monatelang unbemerkt und gefährden kritische Systeme und sensible Daten. In der heutigen Bedrohungslandschaft nehmen identitätsbasierte Angriffe nicht nur zu, sie sind auch die Hauptursache für Sicherheitsverletzungen in Unternehmen: 80 % der Sicherheitsverletzungen betrafen die Verwendung gestohlener Anmeldeinformationen.

ISPM wurde entwickelt, um diesen wachsenden Risiken entgegenzuwirken. Effektiv implementierte ISPM-Strategien bieten Unternehmen Echtzeit-Transparenz und verwertbare Informationen, um identitätsbezogene Risiken im großen Maßstab zu reduzieren. Das Ergebnis ist eine stärkere Sicherheitslage, verbesserte Widerstandsfähigkeit und mehr Vertrauen in die Einhaltung von Compliance-Anforderungen.

Die Herausforderungen, die ISPM löst

Die Identitätslandschaft ist zu weitläufig, fragmentiert und komplex geworden, als dass herkömmliche Kontrollmechanismen sie effektiv verwalten könnten. Da Unternehmen zunehmend Cloud-Dienste nutzen, Drittanbieter einbinden und Geschäftsprozesse automatisieren, steigt die Anzahl der Identitäten – und damit auch die Risiken. ISPM befasst sich mit den operativen und sicherheitstechnischen Schwachstellen, die sich aus diesem Wachstum ergeben. Dazu gehören:

- **Identitätsausbreitung:** bezeichnet die beschleunigte Zunahme von Benutzer-, Geräte-, Service- und Maschinenkonten. Mehr Identitäten führen zu überlappenden, verwaisten und Schattenkonten, die Angreifer ausnutzen können. Über die Hälfte (57 %) der Unternehmen erachten die Verwaltung der Identitätsausbreitung als einen wichtigen Schwerpunkt, was ihre Bedeutung in der aktuellen Sicherheitslandschaft unterstreicht.

- **Fehlkonfigurationen und inkonsistente Richtlinien** erschweren die Durchsetzung von Zugriffskontrollen und erhöhen die Wahrscheinlichkeit eines Privilegienmissbrauchs. Die Verbreitung hybrider Umgebungen (von 70 % der Organisationen gemeldet) erschwert die Durchsetzung von Identitätsrichtlinien über verschiedene Systeme hinweg zusätzlich.

- **Nicht verwaltete Berechtigungen** ermöglichen es Benutzern, Zugriffsrechte zu behalten, die nicht mehr ihren Verantwortlichkeiten entsprechen. Wenn der Zugriff nicht regelmäßig überprüft wird oder auf dem Prinzip der geringsten Berechtigungen basiert, erhöhen nicht verwaltete Berechtigungen die Wahrscheinlichkeit, dass übermäßige oder schädliche Kombinationen unbemerkt bleiben. Diese Lücken können direkt zu Sicherheitsvorfällen beitragen.
- **Eingeschränkte Sichtbarkeit** von privilegierten oder risikoreichen Konten verlangsamt die Erkennung böswilliger Aktivitäten und Insider-Bedrohungen. Mehr als 20 % der Unternehmen schätzten, dass identitätsbezogene Verstöße sie über **10 Millionen** US-Dollar kosteten. Insgesamt gaben 44 % an, dass diese Verstöße teurer seien als allgemeine Datenschutzverletzungen.
- **Schatten-IT** entsteht, wenn Geschäftseinheiten oder Mitarbeiter nicht autorisierte Anwendungen oder Systeme außerhalb des Zuständigkeitsbereichs der IT übernehmen. Diesen nicht genehmigten Technologien mangelt es oft an einer angemessenen Sicherheitsüberwachung, was das Risiko von Datenverlust, Fehlkonfigurationen und Compliance-Verstößen erhöht.

Diese Probleme sind nicht nur lästig. Sie schaffen auch echtes Risiko. Ohne klares Verständnis darüber, wer worauf Zugriff hat und ob dieser Zugriff angemessen ist, kommt es bei Audits zu Verzögerungen, die Einhaltung von Compliance-Vorgaben fällt schwer und die Zero-Trust-Ziele werden nicht erreicht. Überdimensionierte Konten, toxische Zugriffskombinationen und verzögerte Reaktion auf Vorfälle können zu Verstößen, Strafen und Vertrauensverlust führen.

ISPM bietet Sicherheitsteams die Transparenz und den Kontext, die sie benötigen, um diese wachsenden Herausforderungen zu bewältigen und die Angriffsfläche zu reduzieren. Es verlagert das Identitätsmanagement von der reaktiven Bereinigung zur proaktiven Risikominderung und bringt so das Identitätsrisiko in Cloud-, Hybrid- und lokalen Umgebungen unter Kontrolle.

Die acht Säulen des ISPM

ISPM ist proaktiv, nicht reaktiv konzipiert. Es hilft Unternehmen, kleine Risiken zu erkennen und zu adressieren, bevor sie zu größeren Sicherheitsvorfällen werden. Anstatt zu warten, bis Compliance-Verstöße, Sicherheitslücken oder Audit-Fehler Identitätsschwächen aufdecken, bietet ISPM kontinuierliches Posture Management, das Risiken langfristig reduziert. Diese zukunftsorientierte Strategie unterscheidet ISPM von herkömmlichen Ansätzen zur Identitätssicherheit. Die folgenden Säulen stellen die wichtigsten Ergebnisse dar, die Unternehmen von einem ausgereiften ISPM-Ansatz erwarten können. Sie werden jeweils mit Screenshots aus den RSA Governance & Lifecycle Advanced Dashboards illustriert, um zu zeigen, wie diese Ergebnisse in der Praxis erreicht werden:

1. Reduzierung der Identitätsrisikofläche

ISPM reduziert die wachsende Identitätsrisikofläche, die durch Identitätswildwuchs und überberechtigte Benutzer entsteht. Durch die kontinuierliche Transparenz des Benutzerzugriffs über alle Systeme hinweg trägt ISPM dazu bei, die Gefährdung von Anmeldeinformationen, laterale Bewegungen und übermäßige Privilegien zu begrenzen.

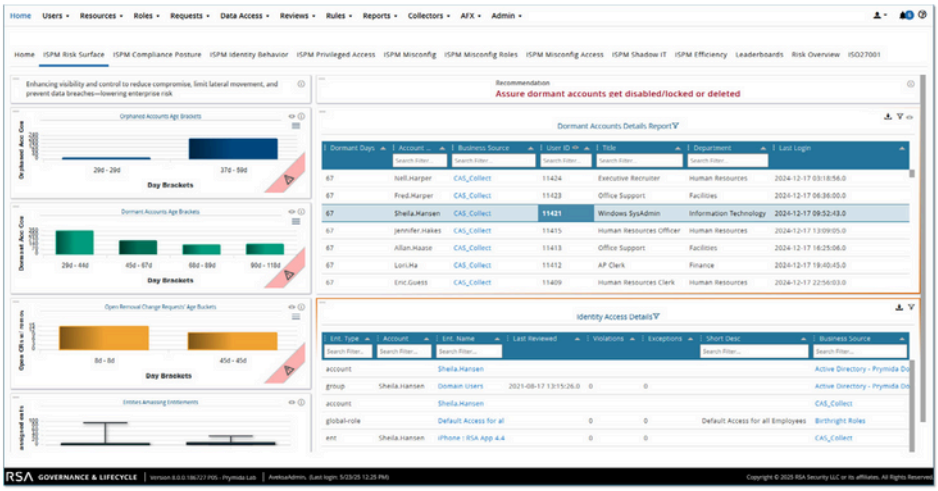

Abbildung 1: Das Risk Surface-Dashboard verbessert die Sichtbarkeit und Kontrolle, um unbefugten Zugriff zu verhindern, seitliche Bewegungen einzuschränken und Datenschutzverletzungen zu stoppen und gleichzeitig das Gesamtrisiko des Unternehmens zu reduzieren.

2. Stärkung der Compliance und Auditbereitschaft

ISPM automatisiert Zugriffsprüfungen, erkennt Richtlinienverstöße und liefert Echtzeitnachweise für die Einhaltung von Vorschriften wie DSGVO, DORA, HIPAA, PCI-DSS und vielen anderen. Dies reduziert Kosten und Aufwand für Auditzyklen.

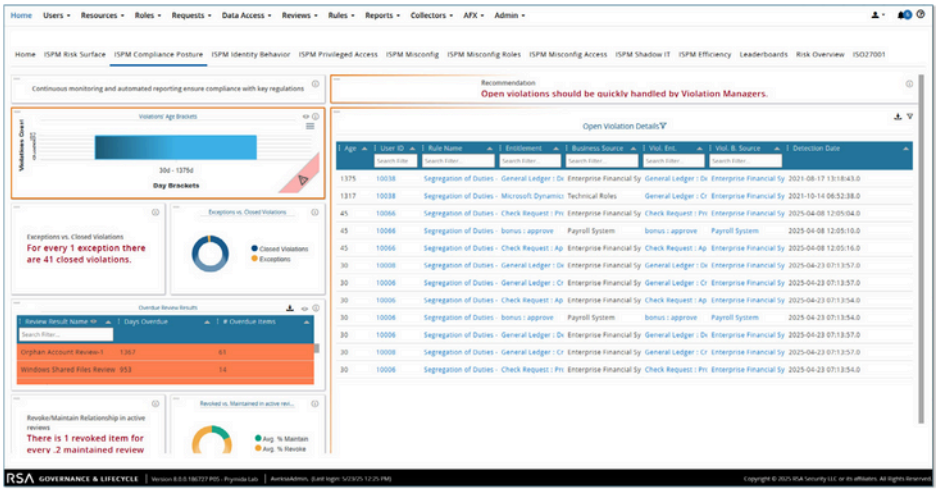

Abbildung 2: Das Compliance Posture-Dashboard bietet kontinuierliche Überwachung und automatisierte Berichterstattung, um die Einhaltung wichtiger Vorschriften sicherzustellen.

3. Minderung der Cloud-Berechtigungsrisiken

Wenn Unternehmen in die Cloud migrieren, berücksichtigt ISPM die Komplexität der Berechtigungsverwaltung in dynamischen Multi-Cloud-Umgebungen. Es verhindert Überbereitstellung und gewährleistet den Zugriff auf Cloud-Ressourcen mit den geringsten Berechtigungen.

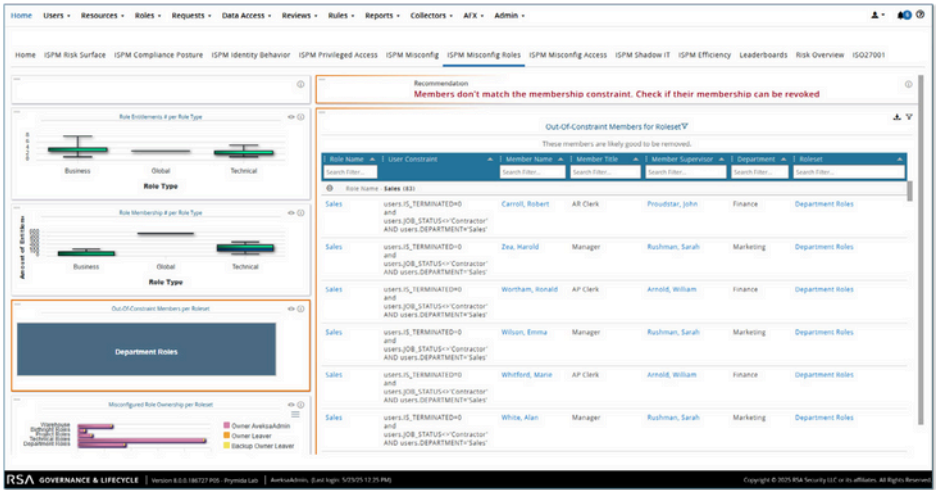

Abbildung 3: Das Dashboard „Fehlkonfigurierte Rollen“ identifiziert und behebt falsch konfigurierte Rollen, um eine Überbereitstellung zu reduzieren und den Zugriff mit den geringsten Berechtigungen in Cloud-, Hybrid- und lokalen Umgebungen durchzusetzen.

4. Erkennung identitätsbasierter Bedrohungen

ISPM hilft dabei, abnormales Verhalten wie Privilegienerweiterung oder Missbrauch von Anmeldeinformationen durch die Anwendung von Identitätsanalysen und Verhaltensüberwachung zu erkennen.

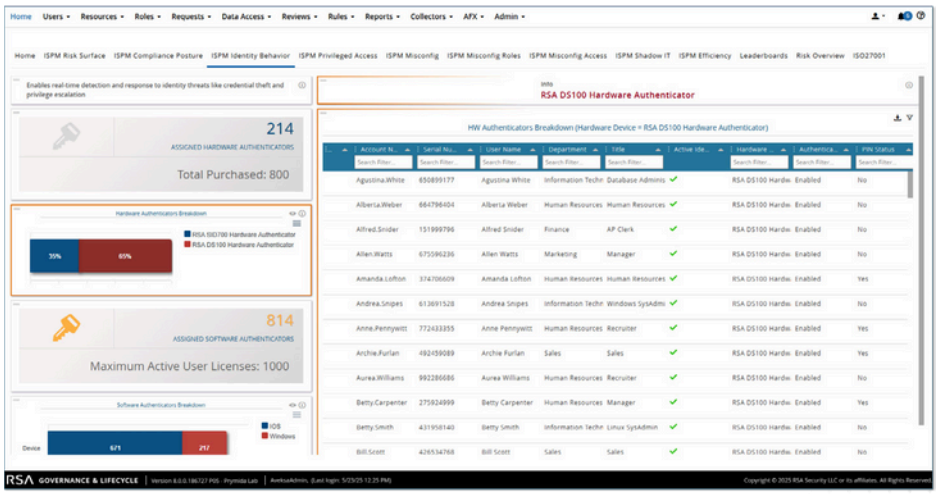

Abbildung 4: Ermöglichen Sie die Erkennung und Reaktion in Echtzeit auf Identitätsbedrohungen wie Anmeldeinformationsdiebstahl und Rechteausweitung.

5. Kontrolle des privilegierten Zugriffs

ISPM bietet Einblick in die Nutzung privilegierter Konten und unterstützt die Durchsetzung des Prinzips der geringsten Privilegien, indem es riskante Konten hervorhebt und die Richtliniendurchsetzung automatisiert.

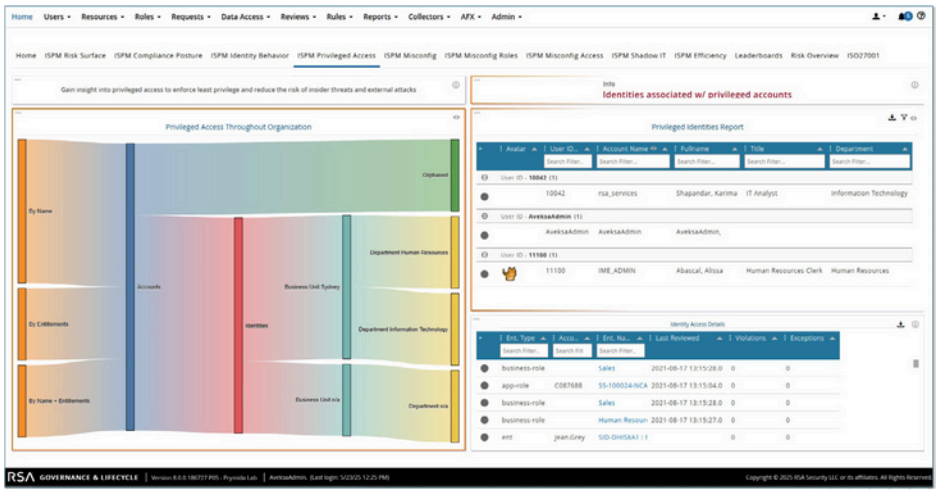

Abbildung 5: Erhalten Sie Einblick in den privilegierten Zugriff, um das Prinzip der geringsten Privilegien durchzusetzen und das Risiko von Insider-Bedrohungen und externen Angriffen zu reduzieren.

6. Beheben von Identitätsfehlkonfigurationen

Von der schwachen Durchsetzung der Multi-Faktor-Authentifizierung (MFA) bis hin zu übermäßigem Zugriff identifiziert ISPM Fehlkonfigurationen und leitet die Behebung an, um Sicherheitslücken zu schließen.

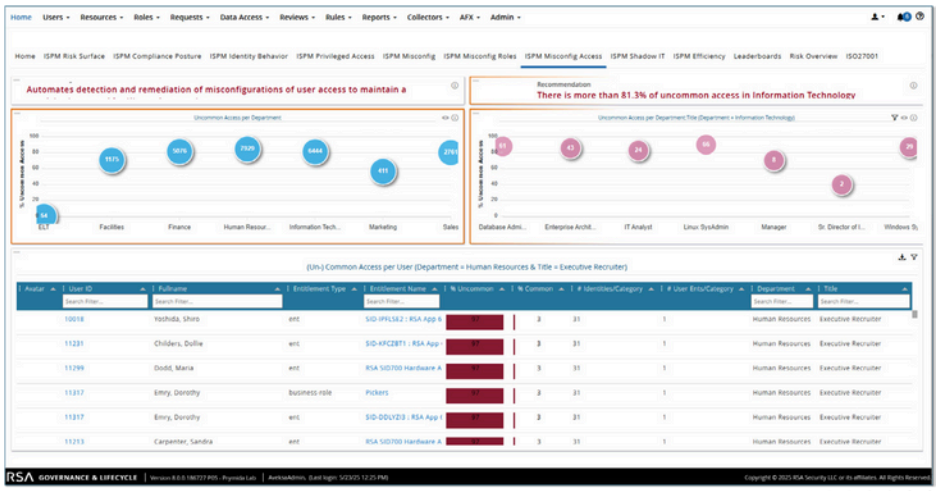

Abbildung 6: Die automatische Erkennung und Behebung von Fehlkonfigurationen des Benutzerzugriffs trägt zur Aufrechterhaltung einer konsistenten, sicheren Identitätsumgebung bei.

7. Beseitigung des Schattenzugriffs

ISPM erkennt und kontrolliert nicht autorisierte oder unbekannte Benutzer, Konten oder Anwendungen, die außerhalb formaler Identitätssysteme operieren.

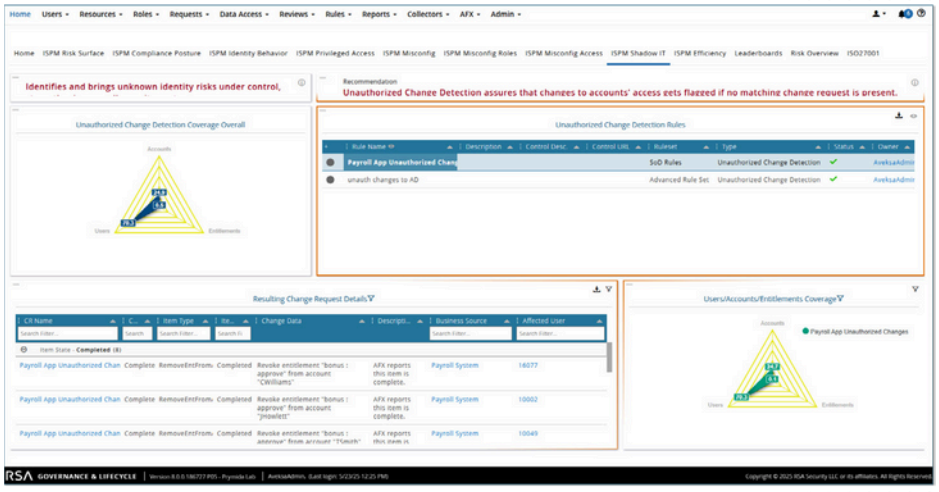

Abbildung 7: Dieses Dashboard bietet Einblick in die Abdeckung von Benutzern, Konten und Berechtigungen, um unbekannte Identitätsrisiken zu erkennen und unter Kontrolle zu bringen.

8. Steigerung der Betriebseffizienz

Durch die Automatisierung der routinemäßigen Erkennung von Identitätsrisiken und der Durchsetzung von Richtlinien ermöglicht ISPM den Sicherheitsteams, sich auf strategische Initiativen zu konzentrieren.

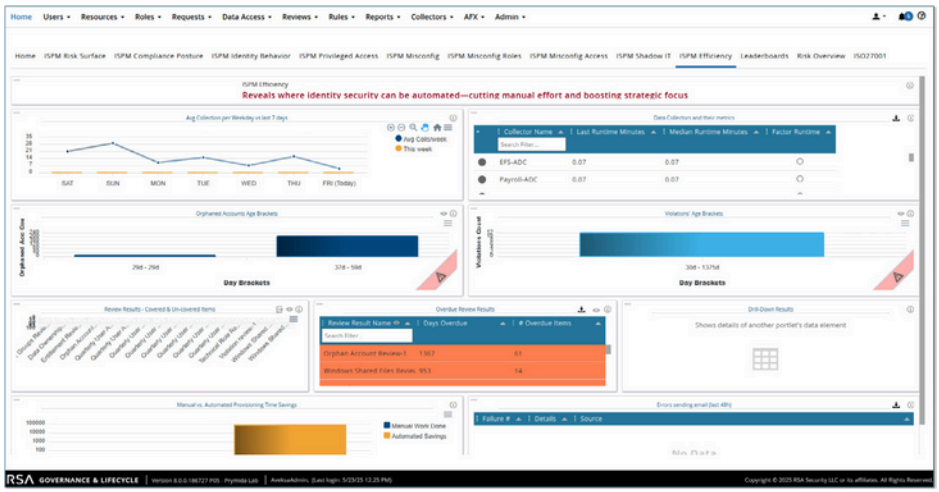

Abbildung 8: Dieses ISPM-Effizienz-Dashboard zeigt, wo die Identitätssicherheit automatisiert werden kann, um den manuellen Aufwand zu reduzieren und den strategischen Fokus zu stärken.

Für ISPM erforderliche Kernkompetenzen

ISPM ist kein einzelnes Tool oder Dashboard. Es handelt sich um einen strategischen Ansatz, der auf integrierten Identitätssicherheitstechnologien basiert. Diese Funktionen müssen zusammenarbeiten, um die Identitätslage kontinuierlich zu bewerten, Richtlinien durchzusetzen und Abhilfemaßnahmen zu steuern. Unternehmen, die ISPM implementieren möchten, sollten Folgendes sicherstellen:

- **Identitätsverwaltung und -administration:** Kernfunktionen wie Richtliniendurchsetzung, Zugriffszertifizierung, Rollenverwaltung und Lebenszykluskontrollen.
- **Identitätserkennung und -transparenz:** Tools zur Inventarisierung von Benutzern, Berechtigungen und Konten in der Cloud, On-premise, und Hybridumgebungen.
- **Überwachung und Analyse:** Erweiterte Analysefunktionen zur Verfolgung des Verhaltens, Erkennung von Anomalien und Priorisierung der Identität und der damit verbundenen Risiken.
- **Zugriffsverwaltung und starke Authentifizierung:** Kontextabhängige Zugriffsrichtlinien, MFA und moderne Authentifizierungsmethoden wie passwortlose und biometrische Anmeldung.
- **Überwachung privilegierter Zugriffe:** Funktionen zum Erkennen, Überwachen und Verwalten privilegierter und risikoreicher Konten.
- **SaaS- und Schatten-IT-Schutz:** Einblick in die Nutzung von SaaS-Apps und Mechanismen zur Kontrolle unbefugter oder nicht verwalteter Zugriff.
- **Integration über Identitätstools hinweg:** Eine einheitliche Architektur oder ein offenes Integrationsframework, das diese Funktionen zur Gewährleistung kontinuierlicher Transparenz und Richtliniendurchsetzung verbindet .

Fähigkeiten in eine schlüssige Cybersicherheitsstrategie umwandeln

Für ein effektives ISPM-Programm benötigen Unternehmen mehr als eine Checkliste mit einzelnen Funktionen. Sie benötigen vielmehr eine Plattform, die verschiedene Cybersicherheitskomponenten zu einer schlüssigen Lösung vereint. Eine einheitliche Identitätsplattform (UIP) vereint Governance, Zugriff und Authentifizierung in einer Architektur und ermöglicht so bessere Transparenz, stärkere Kontrollen und fundiertere Entscheidungen im gesamten Identitätsökosystem.

RSA ist eines der wenigen Unternehmen mit einer UIP, die Governance, Zugriff und Authentifizierung vollständig integriert. RSA Governance & Lifecycle bietet Governance und Transparenz. RSA ID Plus bietet Zugriff und Authentifizierung. RSA-Analyse-Engines verknüpfen Erkenntnisse plattformübergreifend. Nur wenige andere Anbieter bieten diese Kernkomponenten als Teil einer wirklich einheitlichen Architektur an.

Zero Trust und ISPM verstehen

Zero Trust ist ein Sicherheitsrahmen, der davon ausgeht, dass keinem Benutzer oder System standardmäßig vertraut werden sollte, auch nicht innerhalb des Netzwerks. Es erfordert kontinuierliche Identitätsprüfung, strenge Zugriffskontrollen und die Durchsetzung des Prinzips der geringsten Rechte. Wenn Zero Trust das Ziel ist, ist ISPM die Methode, um dieses Ziel zu erreichen. ISPM operationalisiert Zero Trust, indem es die erforderlichen Transparenz-, Analyse- und Durchsetzungsfunktionen bietet, um identitätsbezogene Kontrollen im Laufe der Zeit zu bewerten und zu verbessern.

Der Weg nach vorn

ISPM ist die Zukunft der Identitätssicherheit. Angesichts sich ständig weiterentwickelnder Bedrohungen und zunehmenden regulatorischen Drucks benötigen Unternehmen einen neuen Ansatz für das Management von Identitätsrisiken. Dieser Report bietet eine Grundlage für das Verständnis von ISPM, seinen wichtigsten Säulen und den Voraussetzungen für dessen Implementierung. Mit der RSA Unified Identity Platform können Unternehmen eine führende Rolle bei der Sicherung der Identitätslandschaft übernehmen und eine nachhaltige, Zero-Trust-orientierte Zukunft aufbauen.

Über RSA

RSA bietet unternehmenskritische Cybersicherheitslösungen zum Schutz sicherheitskritischer Organisationen weltweit. Die RSA Unified Identity Platform bietet echte passwortlose Identitätssicherheit, risikobasierten Zugriff, automatisierte Identitätsintelligenz und umfassende Identitätsverwaltung in Cloud-, Hybrid- und lokalen Umgebungen. Mehr als 9.000 Hochsicherheitsorganisationen vertrauen RSA bei der Verwaltung von über 60 Millionen Identitäten, der Erkennung von Bedrohungen, dem sicheren Zugriff und der Einhaltung von Compliance-Vorgaben. Weitere Informationen finden Sie auf unserer Website. Kontaktieren Sie unseren Vertrieb, finden Sie einen Partner oder erfahren Sie mehr über RSA.