SailPoint

eBook

Leitfaden zu Identity Security & Compliance

Durchgängige Compliance mit einem KI-gestützten Ansatz

Vorwort

Identity Security ist im heutigen digitalen Zeitalter ein wichtiger Faktor, um Compliance-Anforderungen zu erfüllen und die Sicherheit und das Vertrauen im Unternehmen zu stärken. Identity Security geht über die reine Einhaltung von Vorschriften hinaus. Vielmehr bietet sie einen strategischen, proaktiven Ansatz zur Compliance, indem sie die Sicherheit aller Identitäten und ihrer Zugriffsmöglichkeiten herstellt. Mit Identity Security können Unternehmen Zugriffsrechte verwalten, Nutzungsmuster nachverfolgen und Richtlinien für sämtliche Nutzer, Anwendungen und Daten durchsetzen, um die Erfüllung von Vorschriften zu automatisieren und die Einhaltung der sich ständig ändernden Bestimmungen nachzuweisen.

Wenn es Ihnen Herausforderungen bereitet, Compliance-Prozesse effektiv umzusetzen und in Ihre Systeme und Infrastruktur zu integrieren, ist eine moderne Identity-Security-Lösung auf Basis von KI der richtige Ansatzpunkt, um die Effektivität zu verbessern und die Kosten für eine nachhaltige und kontinuierliche Compliance zu senken.

Lassen Sie uns die dynamische Entwicklung von Compliance und Identity Security beleuchten und ihre Auswirkungen auf den Aufbau von Vertrauen, die Senkung von Risiken und Kosten, die Umsetzung von Geschäftsstrategien und die Bewältigung der komplexen Anforderungen des digitalen Zeitalters aufzeigen.

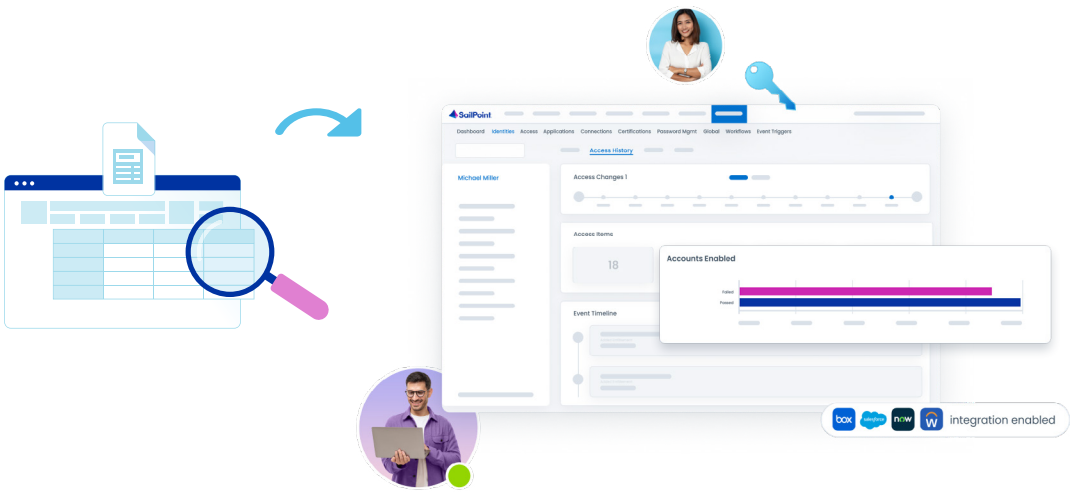
Von manuellen zu automatisierten Verfahren: Die Transformation der Compliance

Compliance kann komplex und aufwändig sein – und damit auch kostspielig. Die Einhaltung von branchenspezifischen und aufsichtsrechtlichen Vorgaben erfordert eine regelmäßige Überprüfung und Zertifizierung des Nutzerzugriffs. Das bedeutet für viele Unternehmen, dass sie ständig mit fehleranfälligen und ineffizienten Prozessen zu kämpfen haben, wie beispielsweise dem manuellen Erstellen von Zugriffsberichten, dem Abzeichnen von Zugriffsgenehmigungen und der manuellen Beseitigung unangemessener Zugriffsrechte für Nutzer.

Wenn Ihr Unternehmen mit einem der folgenden Probleme konfrontiert ist, ist es vielleicht an der Zeit, Ihre Compliance-Prozesse zu vereinfachen.

- Aufbau oder Nutzung von mehreren selbstentwickelten Lösungen zur Bewältigung von Audit- und Compliance-Anforderungen
- Anstellung von Vollzeitmitarbeitern oder Beratern zur Abwicklung von Compliance-Projekten wie Zugriffszertifizierungen und Durchsetzung von SoD-Richtlinien (Aufgabentrennung, Separation of Duty)
- Manuelles Exportieren und Formatieren von Daten für das nächste Audit durch Verantwortliche für Anwendungen
- Nutzung ineffizienter Tools wie Tabellenkalkulationen und E-Mails für manuelle Compliance-Prozesse
- Gleichbehandlung von Nutzern mit hohem und niedrigem Risiko, wobei Nutzern mit hohem Risiko nicht genügend Aufmerksamkeit oder Nutzern mit niedrigem Risiko zu viel Zeit und Mühe gewidmet wird

Um eine bessere Kontrolle über Ihre Identity-Daten zu erlangen, müssen Sie teure, fehleranfällige, papierbasierte manuelle Prozesse durch zentral definierte Richtlinien und automatisierte Zugriffszertifizierungsprozesse ersetzen. So können Sie nicht nur die Compliance-Kosten erheblich senken, sondern auch wiederholbare Verfahren für eine einheitlichere, prüfbare, zuverlässige, effiziente und leichter zu verwaltende Zugriffszertifizierung einführen.



Vier Schritte zur Vereinfachung von Compliance-Prozessen

Wenn Audit-Mängel und hohe Compliance-Kosten in Ihrem Unternehmen wichtige Herausforderungen darstellen, sollten Sie sich zunächst auf die Automatisierung der Compliance konzentrieren. Möglicherweise arbeiten Sie bereits an der Einführung eines „Least Privilege"-Zugriffsmodells, wie es zahlreiche rechtliche Rahmenwerke vorschreiben. Least Privilege ist zugleich ein zentrales Element bei der Durchsetzung eines „Zero Trust"-Ansatzes für Identity Security. Beim Least-Privilege-Prinzip stellen Sie sicher, dass jeder nur den Zugriff erhält, den er für die Erfüllung seiner Aufgaben benötigt. Wenn also eine Identität oder ein Konto kompromittiert wird, beschränkt sich die Gefährdung auf den Zugriff, den diese Person tatsächlich haben sollte, und nicht auf den überprivilegierten Zugriff, den Nutzer häufig haben – durch den es zu höheren Geldstrafen und einer stärkeren Exponierung kommen könnte.

Der Weg zu einem soliden Compliance-Rahmen beginnt mit vier grundlegenden Schritten zur Verbesserung der Transparenz, Sicherheit und Effizienz in Ihrem Unternehmen. Durch die Umsetzung dieser Strategien können Unternehmen ein solides Fundament für ein effektives Compliance-Management schaffen und KI nutzen, um Prozesse zu optimieren und Risiken zu mindern.

1. Einen zentralen Überblick erhalten

Der Ausgangspunkt jedes Compliance-Projekts sollte darin bestehen, sich ein Bild vom aktuellen Status der Nutzer zu machen, indem man sich einen zentralen Überblick über den Identity-Zugriff im gesamten Unternehmen verschafft. In dieser Phase wird ein zentrales Repository für Nutzer- und Zugriffsinformationen geschaffen, indem Daten aus Ihren maßgeblichen Quellen, wie etwa HR-Systemen und Auftragnehmer-Datenbanken, sowie Zielressourcen integriert und zusammengeführt werden.

2. Alle verwaisten Konten ermitteln und löschen

Der Ausgangspunkt jedes Compliance-Projekts sollte darin bestehen, sich ein Bild vom aktuellen Status der Nutzer zu machen, indem man sich einen zentralen Überblick über den Identity-Zugriff im gesamten Unternehmen verschafft. In dieser Phase wird ein zentrales Repository für Nutzer- und Zugriffsinformationen geschaffen, indem Daten aus Ihren maßgeblichen Quellen, wie etwa HR-Systemen und Auftragnehmer-Datenbanken, sowie Zielressourcen integriert und zusammengeführt werden.

3. Ausreißer identifizieren und beseitigen

Der nächste Schritt bei der Datenbereinigung liegt darin, Ausreißer zu bestimmen: Nutzer, deren Zugriff deutlich von den Erwartungen abweicht. Bei der Erstellung des Business Case für Ihr Identity-Security-Programm sollten Sie nach einer Lösung mit integrierter KI suchen, die Risikonutzer und Ausreißer bei Zugriffen erkennen und die Sicherheit deutlich erhöhen kann, indem sie die Ermittlung und Behebung von Schwachstellen unterstützt.

4. Zugriffszertifizierungen automatisieren

Generieren Sie anschließend eine Zertifizierungskampagne, mit der Sie die Zugriffsüberprüfungen für alle Nutzer automatisieren können. Heute können Ihnen dabei KI-gestützte Empfehlungen helfen, welche die Zertifizierungsprüfung vereinfachen und beschleunigen. So weiß Ihr Team ohne Weiteres, ob der Zugriff genehmigt oder verweigert werden sollte. Die Erstzertifizierung sollte dazu dienen, eine zuverlässige Datengrundlage zu schaffen.

Wenn die Grundlagen für die Einführung von Best Practices für die Compliance geschaffen sind, ist es wichtig, die rechtlichen Rahmenbedingungen zu verstehen, die diese Anforderungen bestimmen.

Daten in verschiedenen Branchen schützen

Die Orientierung in der Landschaft der Compliance-Vorschriften ist für Unternehmen in verschiedenen Branchen von entscheidender Bedeutung, insbesondere in stark regulierten Sektoren wie Finanzdienstleistungen, Gesundheitswesen, Behörden und Fertigung. Rechtsvorschriften dienen nicht nur dem Schutz sensibler Daten und der Wahrung der Privatsphäre, sondern auch der Aufrechterhaltung der Integrität und des Vertrauens von Unternehmen im digitalen Zeitalter.

Hier ein genauerer Blick auf einige der gängigsten Compliance-Vorschriften, -Rahmen und -Richtlinien:

NIST Cybersecurity Framework (CSF) 2.0: Bietet der Industrie, Regierungsbehörden und anderen Organisationen eine Anleitung zum Umgang mit Cybersicherheitsrisiken.

Der Digital Operations Resilience Act (DORA): Zielt darauf ab, die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in Unternehmen der Finanzbranche zu stärken. Es schreibt vor, dass EU-Finanzunternehmen strenge IT-Sicherheitsvorschriften einhalten müssen, damit das Finanzsystem im Falle einer schweren Betriebsstörung widerstandsfähig bleibt.

Datenschutz-Grundverordnung (DSGVO): Eine zentrale Verordnung in der EU, die den Standard für Datenschutz und die Wahrung der Privatsphäre setzt und sich auf Unternehmen weltweit auswirkt, die mit den Daten von EU-Bürgern arbeiten.

Federal Information Security Management Act (FISMA): Betrifft US-Bundesbehörden und schreibt den Schutz von Informationssystemen vor Bedrohungen vor.

Health Insurance Portability and Accountability Act (HIPAA): Regelt den Schutz sensibler Gesundheitsdaten von Patienten in den USA, der für Gesundheitsdienstleister und ihre Partner von entscheidender Bedeutung ist.

International Organization for Standardization (ISO) 27001: Bietet einen Rahmen für Informationssicherheitsmanagementsysteme (ISMS), der für Organisationen jeder Größe anwendbar ist.

Network and Information Systems Directive (NIS2, Richtlinie zur Netzwerk- und Informationssicherheit): Erweitert die ursprüngliche NIS-Richtlinie der EU und stärkt die Cybersicherheits-Resilienz bei wesentlichen Diensten (Energie, Verkehr, Banken, Gesundheit) und Anbietern digitaler Dienste (Cloud-Dienste, Suchmaschinen, Online-Marktplätze).

Payment Card Industry Data Security Standard (PCI DSS): Unerlässlich für Unternehmen, die Kreditkartentransaktionen abwickeln, da sie eine sichere Umgebung für die Daten der Karteninhaber aufrechterhalten müssen.

Sarbanes-Oxley Act (SOX): Erlegt Unternehmen in den USA strenge Audit- und Finanzvorschriften auf, um Gesellschafter und die Allgemeinheit vor Bilanzierungsfehlern und betrügerischen Praktiken zu schützen.

Das Verständnis und die Einhaltung dieser Vorschriften ist von grundlegender Bedeutung für die Integrität eines Unternehmens und den Aufbau von Vertrauen bei Interessengruppen, was die Notwendigkeit eines strategischen Ansatzes für Compliance und Identity Security unterstreicht.

So kann SailPoint Ihnen helfen

Unterstützt durch künstliche Intelligenz und maschinelles Lernen fördern die Identity Security-Lösungen von SailPoint mit ihrem umfassenden Ansatz zur Verwaltung und Sicherung digitaler Identitäten die Einhaltung der Vorschriften. Mittels Automatisierung von Zugriffsüberprüfungen, Rollen- und Richtlinienmanagement sowie Risikoerkennung trägt SailPoint dazu bei, die Einhaltung globaler gesetzlicher Vorschriften zu gewährleisten, da der Prozess der Erteilung, Änderung und des Entzugs von Zugriffsrechten optimiert wird – was letztlich das Risiko von zugriffsbezogenen Compliance-Verstößen verringert. Mit dieser proaktiven Ausrichtung auf Identity Governance können Unternehmen die Compliance vor dem Hintergrund sich ändernder Vorschriften und Bedrohungen deutlich stärken.

Die Vorteile unseres strategischen Ansatzes für Compliance und Identity Security liegen auf der Hand:

- **Optimierte Abläufe:** Automatisierte Workflows und intelligente Entscheidungsprozesse führen zu effizienteren Abläufen und einer deutlichen Reduzierung des manuellen Aufwands.
- **Gestärktes Sicherheitskonzept:** Die kontinuierliche Überwachung und anpassungsfähige Richtlinien tragen zu einer stärkeren Verteidigung gegen externe und interne Bedrohungen bei.
- **Kosteneinsparungen:** Durch die Abschaffung manuell ausgeführter Compliance-Aufgaben und die Automatisierung von Identity-Praktiken können Unternehmen ihre Gesamtbetriebskosten senken und eine schnellere Wertschöpfung erzielen.

Wenn Sie sich einen umfassenden Überblick darüber verschaffen wollen, wie SailPoint Ihre Compliance- und Identity-Security-Prozesse sichern und optimieren kann, vereinbaren Sie einen Beratungstermin mit einem Mitglied unseres Teams. Erleben Sie den Unterschied eines strategischen Compliance-Ansatzes für Ihr Unternehmen. Besuchen Sie **sailpoint.com/de/solutions/maintain-compliance,** um mehr zu erfahren.

SailPoint

Über SailPoint
SailPoint stattet das moderne Unternehmen für die nahtlose Verwaltung und Absicherung des Zugriffs auf Anwendungen und Daten aus – aus der Perspektive der Identity und mit Geschwindigkeit und in großem Umfang. Als einer der Marktführer in dieser Kategorie entwickeln wir die Identitätssicherheit als Grundlage für ein sicheres Unternehmen ständig weiter. SailPoint bietet eine einheitliche, intelligente und erweiterbare Plattform zur Abwehr der dynamischen, identitätszentrierten Cyber-Bedrohungen von heute und steigert gleichzeitig die Produktivität und Effizienz. SailPoint hilft vielen der komplexesten und anspruchsvollen Unternehmen auf der ganzen Welt, ein sicheres technologisches Ökosystem zu schaffen, das die Geschäftstransformation vorantreibt.