

## **SailPoint sorgt für Sicherheit und Echtzeitkontrolle in komplexen IT-Umgebungen**

Unternehmen weltweit müssen sich gegen Cyberbedrohungen aller Art wappnen – sowohl gegen Angriffe durch böswillige Angreifer als auch gegen solche, die von den eigenen Mitarbeitern ausgehen. Laut dem Bericht „2020 Cost of Insider Threats“, herausgegeben vom Ponemon Institute, haben [Betrugsfälle](#) seit 2016 [um 75 Prozent zugenommen](#). Eine Hauptursache ist die mangelnde Übersicht und Kontrolle über die Risiken für ERP-Systeme wie SAP, die häufig die kritischsten Geschäftsprozesse eines Unternehmens unterstützen und sensible Daten beherbergen.

Aufgrund der Komplexität der ERP-Sicherheitsstrukturen ist es extrem schwierig zu gewährleisten, dass jeweils nur Personen mit den entsprechenden Aufgabenbereichen auf bestimmte Daten zugreifen können. Nahezu unmöglich wird es, wenn Firmen versuchen, die Zugriffe manuell zu überwachen. Sind die Daten über mehrere ERPs und Anwendungen verteilt und mangelt es an Automatisierung, führen Unternehmen einen aussichtslosen Kampf, um sich zu schützen und Audit-Anforderungen zu erfüllen. SailPoint unterstützt Betriebe hier mit Identity Security. Als Teil des Identity Security Angebots ermöglicht SailPoint Access Risk Management eine breite Übersicht und Kontrolle über die Zugriffe im Unternehmen und vermittelt Verantwortlichen den detaillierten Einblick, den sie zur Minderung der Risiken brauchen, die von den heutigen komplexen ERP-Systemen ausgehen. SailPoint hilft Unternehmen, Risiken durch Zugriffe aller Art Herr zu werden, denn es ist die erste Verteidigungslinie. Es schützt den Perimeter und gestattet nur den richtigen Benutzern Zugang, wobei als zusätzlicher Schutz ein gesichertes Zugriffsverfahren angewendet wird. Gleichzeitig werden Firmen aber auch im Inneren geschützt. Dafür ist eine granulare Sicht und Kontrolle nötig, um – in Echtzeit – festzustellen, wer Zugriff hat, wer Zugriff haben sollte und was genau der Benutzer mit diesem Zugriff anfängt.