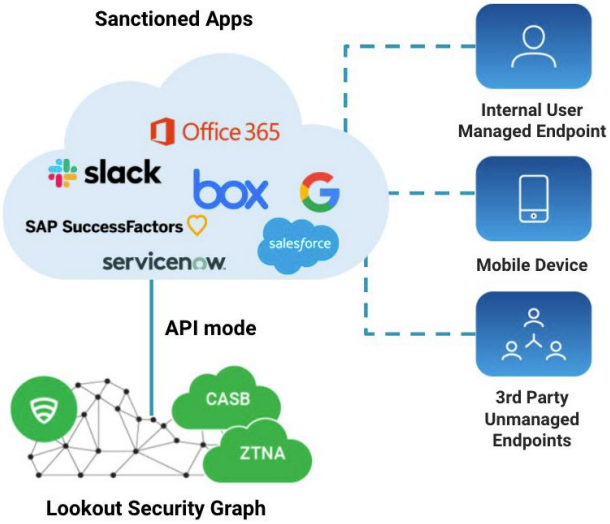
Lookout SaaS Risk Assessment

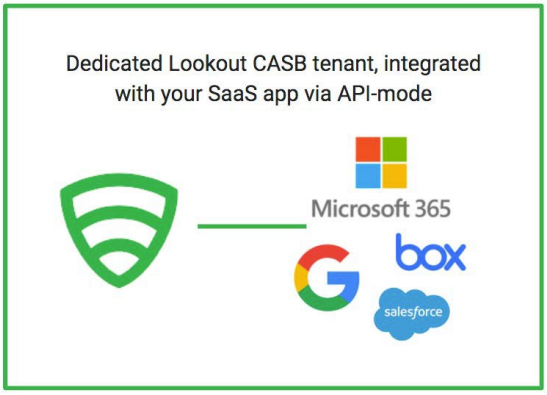
Jeden Tag nutzen Ihre Mitarbeiter von Ihnen bereitgestellte SaaS-Anwendungen wie Office 365, Google Workspace, Salesforce, Slack, ServiceNow oder andere. Sie laden Dateien hoch, Sie laden Dateien runter, Sie teilen Daten mit internen und externen Personen. Dieser Austausch stellt ein ständiges Risiko durch Datenlecks, unbefugte Weitergabe, Verstöße gegen gesetzliche Vorschriften oder das Eindringen von Malware dar. Das Lookout SaaS Risk Assessment bietet einen detaillierten Einblick in unerlaubtes Nutzerverhalten und potenzielle Datenlecks und ermöglicht Ihnen Risiken in Zusammenhang mit Ihren SaaS-Anwendungen zu identifizieren.



Wie funktioniert es?

Das Lookout SaaS Risk Assessment prüft einen bestehenden SaaS-Dienst, um den Grad Ihres laufenden Risikos zu ermitteln. Lookout stellt einen dedizierten Cloud Tenant für die Prüfung bereit, der sich über eine API mit einer Ihrer SaaS-Anwendungen verbindet, zum Beispiel Office 365 oder Google Workspace. Die Bereitstellung ist passiv, einfach zu aktivieren und liefert schnell Ergebnisse. Sobald die Verbindung hergestellt ist, scannt die Lookout Security Plattform Ihr verbundenes Cloud-Repository auf Malware, Datenlecks oder Compliance-Verstößen. Nach zwei Wochen wird der Tenant deaktiviert, und es wird eine Zusammenfassung erstellt, in der die entdeckten Risiken hervorgehoben werden. Unsere Erfahrungen zeigen, dass ungewöhnliches Nutzerverhalten und die Gefährdung sensibler Daten in nur 90 Minuten erkannt werden.

Schnelle Ergebnisse mit dem CASB API-Modus



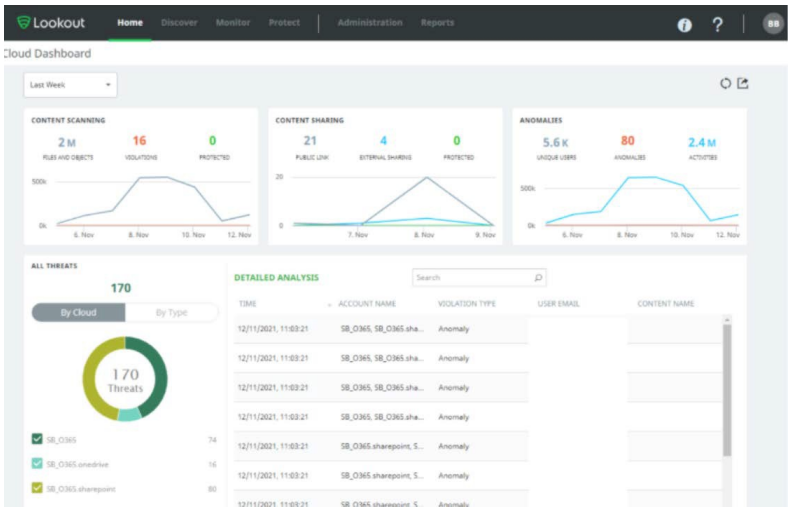
- ✓ **Einfache Konfiguration** – keine Infrastruktur benötigt
- ✓ Vollständiger **Einblick** in **Benutzerinteraktionen, Anomalien, Sharing & Collaboration** und **DLP-Verstöße**
- ✓ **Schnelle Umsetzung**
- ✓ **Erste Ergebnisse innerhalb von 10min**
- ✓ **Vollständige Zusammenfassung** zum Ende des Assessments

Was sind die Voraussetzungen?

Um ein Lookout SaaS Risk Assessment durchzuführen, benötigen Sie die Unternehmensversion einer SaaS-Anwendung, die von Lookout unterstützt wird – Office 365, Google Workspace, Box, Dropbox, Salesforce, etc. Außerdem müssen Sie ein NDA mit Lookout unterzeichnen und einen Service-Account mit Lese-Rechten bereitstellen, um den API-Zugriff auf Ihre SaaS-Anwendung von der Lookout Security Plattform aus zu ermöglichen.

Wie läuft der Prozess ab?

1. Unterzeichnen eines gegenseitigen NDA.
2. Lookout stellt einen dedizierten Tenant auf der Lookout Security Plattform zur Verfügung.
3. Genehmigung von API-Aufrufen von Lookout zu der SaaS-Anwendung.
4. Gemeinsame Konfiguration von bis zu 5 Sicherheitsrichtlinien.
5. Über einen Zeitraum von zwei Wochen scannt Lookout gemäß den vorkonfigurierten Richtlinien nach Verstößen. Während dieser Zeit besteht voller Zugriff auf die Lookout-Konsole, um Aktivitäten und Ereignisse zu überwachen.
6. Nach zwei Wochen wird der Tenant außer Betrieb genommen und eine Zusammenfassung zur Verfügung gestellt.



Datenverarbeitung und Datenschutz

Lookout sammelt und speichert keine Kundendaten. Die Bewertung basiert auf Metadaten, die Benutzer-IDs und Aktivitäten enthalten. Alle Daten befinden sich in einem speziellen Tenant, auf den nur der Kunde und das Lookout-Betriebsteam Zugriff haben. Nach Ablauf der zwei Wochen wird der Tenant außer Betrieb genommen und alle Daten gelöscht.