Unlock the Power of CASB

5 entscheidende Vorteile von Lookout Secure Cloud Access

Inhalt

Wir stellen vor: Lookout Secure Cloud Access

Der zunehmende Einsatz von Clouds macht die Sicherheit von Unternehmensdaten wichtiger, den je. Zudem wird das Erkennen, Klassifizieren und Schützen von Daten durch die immer größer werdende Angriffsfläche zu einer ständigen Herausforderung.

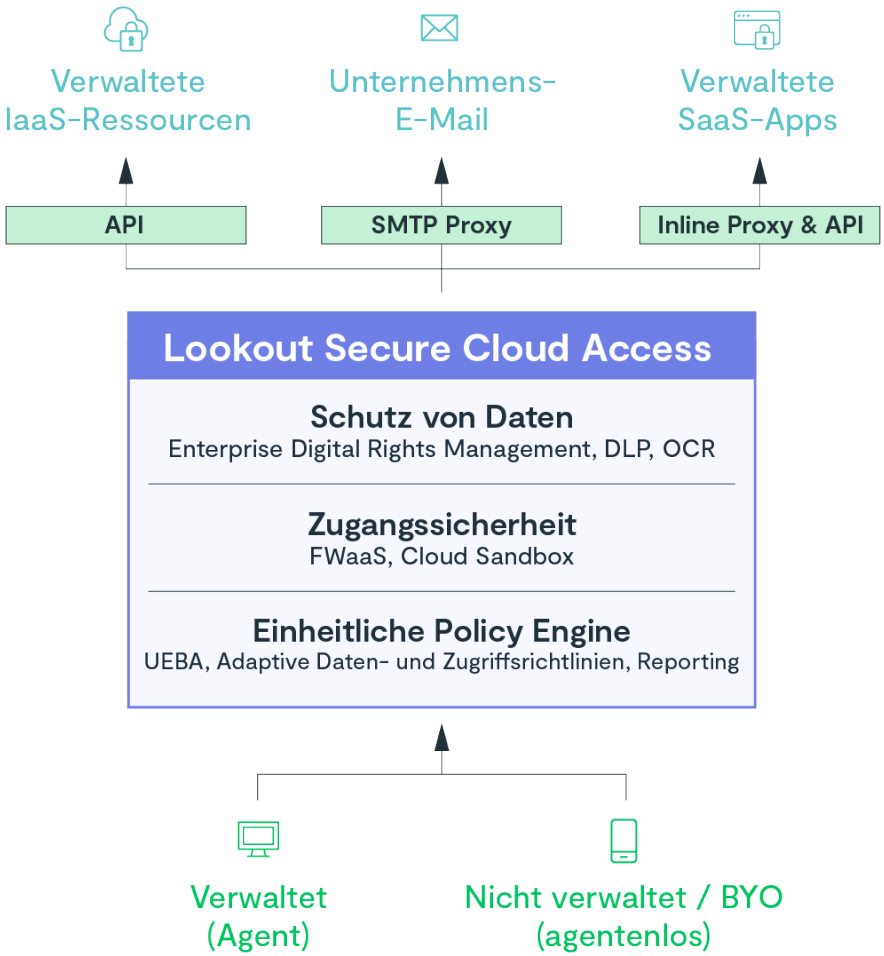
Zahlreiche Statistiken veranschaulichen das Risiko. Nur 54 % der Unternehmen wissen, wo ihre sensiblen Daten gespeichert sind[1]. Ganze 65 % erfassen so viele Daten, dass sie nicht in der Lage sind, diese zu kategorisieren oder zu analysieren[2]. Da Mitarbeiter und Auftragnehmer von einer Vielzahl von Standorten und Geräten aus auf Daten zugreifen, stellt dieser Mangel an Transparenz ein großes Sicherheitsrisiko dar, vor allem, wenn Benutzer riskante Verhaltensweisen aufweisen.

Um Daten wirksam zu schützen, müssen Unternehmen wissen, wo sich Daten befinden, wie sie weitergegeben werden und wer Zugriff darauf hat.

Lookout Secure Cloud Access ist ein Cloud Access Security Broker (CASB), der auf Zero Trust basiert. Immer mehr Unternehmen vertrauen auf diesen Ansatz, um Daten in Cloud- und Saas-Apps zu erkennen, zu bewerten und zu schützen.

Im Gegensatz zu den statischen Datensicherheitsrichtlinien traditioneller Anbieterlösungen geben Ihnen die adaptiven Richtlinien von Lookout Secure Cloud Access den Kontext jeder Anfrage zum Zugriff auf Daten oder eine App. Dadurch werden Falschmeldungen bei der Datenfreigabe und Support-Tickets für die IT-Abteilung reduziert und die Produktivität der Mitarbeiter verbessert.

Lookout Secure Cloud Access ermöglicht die Kontrolle über Daten, egal wie und wo sie verarbeitet werden. Die zentralisierte Policy Engine bietet granulare und adaptive DLP-Funktionen und vereinfacht die Definition und Durchsetzung von Sicherheitsrichtlinien für alle Cloud- und Saas-Apps.



Dieses Whitepaper gibt einen Überblick über Lookouts innovativen Ansatz zur Bereitstellung von CASB-Funktionen auf unserer integrierten Sicherheitsplattform. Es konzentriert sich auf unser zentrales Designprinzip, das Unternehmen, die ihre Daten schützen wollen, einen entscheidenden strategischen Mehrwert bietet.

1. https://www.spirion.com/data-classification/
2. https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/businesses-collect-more-data-than-they-can-handle-reveals-gemalto

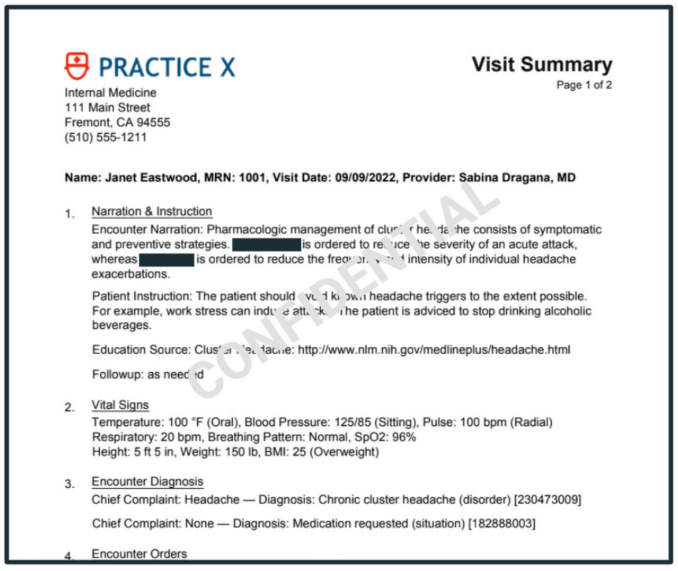
Genaue Kontrolle über Daten

Ihr Unternehmen ist auf eine Vielzahl von Beteiligten angewiesen, die verschiedene Tools für die Zusammenarbeit verwenden. Nicht alle von ihnen befinden sich innerhalb des Unternehmens, was eine große Herausforderung darstellt. Beim Austausch von Daten zwischen externen Auftragnehmern und Partnern müssen Sie für deren Sicherheit sorgen - Dies gilt auch für den Schutzt der Daten nach ablauf eines Projektes.

Die nativen DRM-Funktionen (Digital Rights Management) von Lookout Secure Cloud Access bieten vollständige Kontrolle über sensible Daten, unabhängig davon, wer sie weitergibt und wie sie weitergegeben werden. Daten sind somit sicher, egal ob Mitarbeiter, Auftragnehmer und Partner per E-Mail oder über Tools wie Slack, Microsoft Teams, Box, Dropbox, Google Drive und Microsoft OneDrive zusammenarbeiten.

Im Gegensatz zu anderen Datenschutzlösungen, die lediglich Richtlinien für die Erlaubnis oder Verweigerung des Zugriffs auf Daten durchsetzen, ermöglicht Lookout flexible Richtlinien, die diesen Zugriff mit Sicherheitsmaßnahmen einschränken.

Lookouts Technologien für EDM (Exact Data Matching) und OCR (Optical Character Recognition) identifizieren und schützen vertrauliche Daten in einer Vielzahl von Formaten, darunter Text, Bilder und andere gescannte Dokumente. Lookout scannt Dateien und Ordner, sobald sie freigegeben werden, und identifiziert und schützt vertrauliche Informationen auf der Grundlage vordefinierter Richtlinien mit verschiedenen Durchsetzungsoptionen.



PRACTICE X

Visit Summary

Page 1 of 2

Internal Medicine
111 Main Street
Fremont, CA 94555
(510) 555-1211

Name: Janet Eastwood, MRN: 1001, Visit Date: 09/09/2022, Provider: Sabina Dragana, MD

1. Narration & Instruction

   Encounter Narration: Pharmacologic management of clu[redacted]he consists of symptomatic and preventive strategies. [redacted] is ordered to re[redacted]e severity of an acute attack, whereas [redacted] is ordered to reduce the freq[redacted] intensity of individual headache exacerbations.

   Patient Instruction: The patient should [redacted] known headache triggers to the extent possible. For example, work stress can ind[redacted] att[redacted] The patient is adviced to stop drinking alcoholic beverages.

   Education Source: Clus[redacted]e: http://www.nlm.nih.gov/medlineplus/headache.html

   Followup: as need[redacted]

2. Vital Signs

   Temperature: 100 °F (Oral), Blood Pressure: 125/85 (Sitting), Pulse: 100 bpm (Radial)
   Respiratory: 20 bpm, Breathing Pattern: Normal, SpO2: 96%
   Height: 5 ft 5 in, Weight: 150 lb, BMI: 25 (Overweight)

3. Encounter Diagnosis

   Chief Complaint: Headache — Diagnosis: Chronic cluster headache (disorder) [230473009]

   Chief Complaint: None — Diagnosis: Medication requested (situation) [182888003]

4. Encounter Orders

CONFIDENTIAL

Lookout DRM-Richtlinien redigieren vertrauliche Informationen im Zusammenhang mit den Datenschutzbestimmungen im Gesundheitswesen und enthalten ein Wasserzeichen, um die Weitergabe sensibler Daten an unbefugte Benutzer zu verhindern und die Einhaltung gesetzlicher Anforderungen zu gewährleisten.

Lookout bietet eine leistungsstarke native DRM-Funktionalität, die es Unternehmen ermöglicht, den Zugriff auf Daten und Inhalte zu kontrollieren, auch nachdem diese mit anderen geteilt wurden. Unternehmen behalten so die Kontrolle über Daten, auch wenn diese auf nicht verwalteten Geräten gespeichert sind.

- **Maskieren oder redigieren:** Lookout identifiziert sensible Daten wie Sozialversicherungsnummern und Kreditkartennummern, aber auch Daten, die für bestimmte Regionen und Branchen spezifisch sind. So können Administratoren Richtlinien anwenden, die die gemeinsame Nutzung von Daten ermöglichen und gleichzeitig sensible Informationen maskieren oder unkenntlich machen. Tools ohne DRM-Funktionalität können zwar sensible Dokumente identifizieren, aber keine Informationen maskieren oder unkenntlich machen, so dass die IT-Abteilung gezwungen ist, die gemeinsame Nutzung von Daten zu blockieren, wodurch die Arbeit der Mitarbeiter erschwert wird.
- **Wasserzeichen:** Um die Sicherheit der Daten zu gewährleisten, kann Lookout automatisch Wasserzeichen anbringen, um Benutzer auf vertrauliche Inhalte in sensiblen Dateien hinzuweisen. Wasserzeichen halten die Mitarbeiter davon ab, Screenshots zu machen oder die Dokumente weiterzugeben.
- **Verschlüsseln:** Lookout kann Dateien verschlüsseln, um sicherzustellen, dass nur autorisierte Benutzer Zugriff haben. Dieser Zugriff kann nach einer bestimmten Zeitspanne ablaufen. Die Verschlüsselung kann auch mit anderen DLP-Regeln kombiniert werden. So können zum Beispiel vertrauliche Informationen in einer entschlüsselten Datei verborgen bleiben. Dadurch wird verhindert, dass ein Mitarbeiter oder ein Auftragnehmer auf sensible Dokumente zugreift, sobald er das Unternehmen verlässt.

Sie können beim Schutz von Daten noch einen Schritt weiter gehen, indem Sie dynamische Richtlinien zur Verwaltung digitaler Rechte definieren, um einzuschränken, wer Inhalte entschlüsseln darf. Dies kann eine Kombination aus konfigurierbaren Optionen wie Benutzeranmeldeinformationen, Risikostufen und geografische Lage beinhalten.

Die Vorteile der nativen DRM-Funktionen sind eindeutig: Sie erleichtern die sichere Zusammenarbeit und steigern die Produktivität, während gleichzeitig ein robuster Schutz für sensible Daten geboten wird.

Auffälligkeiten erkennen und Bedrohungen früher stoppen

Lookout Secure Cloud Access wendet User and Entity Behaviour Analytics (UEBA) an, um Benutzer, Geräte und Aktivitäten kontinuierlich zu überwachen und zu bewerten. Auf diese Weise kann Ihr Team Abweichungen vom normalen Verhalten erkennen, sodass Sie eine Vielzahl potenzieller Bedrohungen schnell beseitigen können, darunter: böswillige Insider, kompromittierte Konten und APTs (Advanced Persistent Threats).

60%

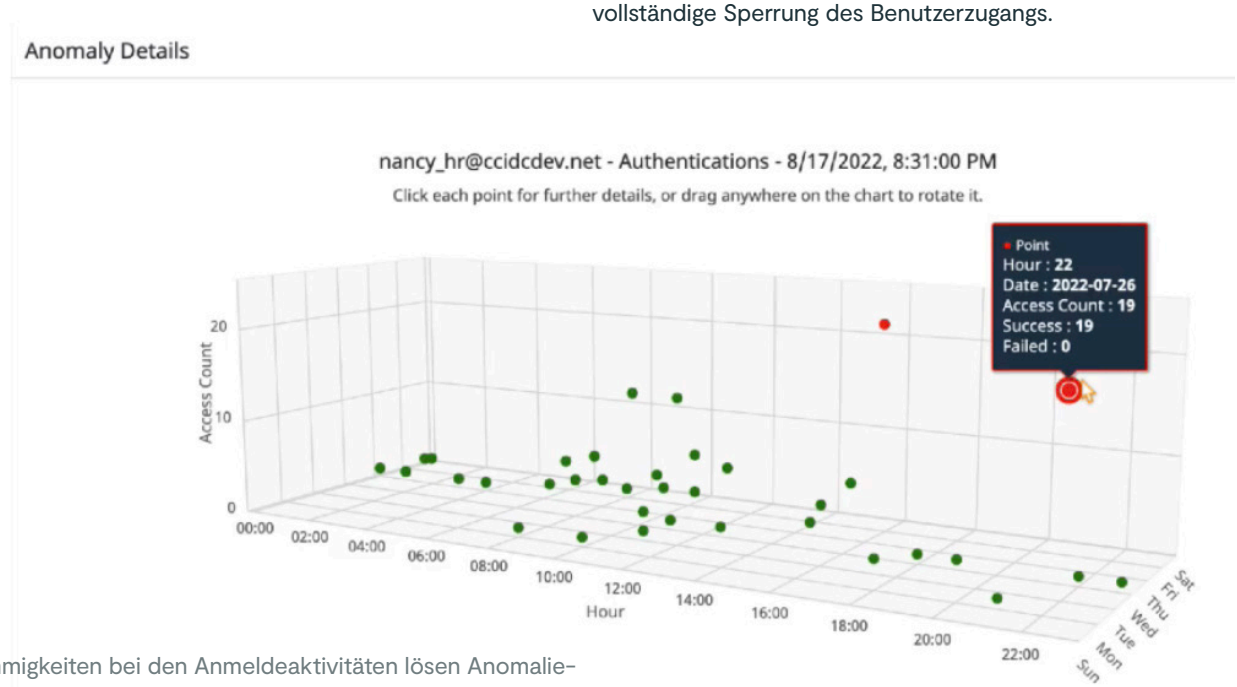
60 % der Datenschutzverletzungen werden von authentifizierten Benutzern verursacht. Durch die Überwachung des Nutzerverhaltens und die Erkennung großer Datendownloads und ähnlicher Anomalien kann die UEBA-Technologie böswillige Aktivitäten wie Datenexfiltration oder Betrug erkennen.

UEBA überwacht nicht nur Anomalien in Bezug auf den geografischen Standort, sondern identifiziert auch riskante Aktivitäten wie Massendownloads von einzelnen Nutzern, die Verwendung von nicht verwalteten Geräten, die mit Malware infiziert sein könnten, anhaltende Anmeldeversuche, Datenänderungen oder den Zugriff auf viele Dateien, auf die der Nutzer zuvor nicht zugegriffen hat.

Risikoüberwachung mit adaptivem Zugang

Durch die Echtzeitanalyse von Benutzer-, Geräte- und Standortmustern generiert Lookout präzise Risikobewertungen für Benutzer, die an Ihre Richtlinien angepasst werden können. Unsere adaptive Zugriffsfunktion nutzt maschinelles Lernen, um Benutzerverhalten, Gerätezustand und Standort zu analysieren. Lookout weist jedem Benutzer einen Risikowert zu, der sich je nach Benutzer, IP, App-Aktivität und Gerätestatus erhöhen kann, und entscheidet dann, ob der Zugriff auf bestimmte Daten auf der Grundlage dieses Wertes gewährt oder verweigert wird.

Ein erhöhter Risikowert kann Warnmeldungen zur Nachverfolgung durch den Administrator auslösen oder automatisch zusätzliche Maßnahmen auf der Grundlage voreingestellter Sicherheitsrichtlinien vorsehen, wie z. B. die Anforderung einer erneuten Benutzerauthentifizierung, das Maskieren oder Redigieren von Daten oder die vollständige Sperrung des Benutzerzugangs.



Unstimmigkeiten bei den Anmeldeaktivitäten lösen Anomalie-Warnungen aus. Diese Grafik zeigt mehrere Anmeldungen außerhalb der normalen Daten und Zeiten für einen Benutzer.

Secure Cloud Access basiert auf dem Prinzip von Zero Trust. Es validiert den Kontext eines Benutzers, bevor der Zugriff auf Anwendungen und Daten gewährt wird, und überprüft dann kontinuierlich die Zugriffsrechte. Unabhängig davon, ob Benutzer versuchen, von verwalteten oder nicht verwalteten Geräten auf Cloud- und SaaS-Apps zuzugreifen, werden sie auf Basis der Sicherheitslage ihrer Geräte sowie ihrer Risikoprofile authentifiziert und autorisiert. Die Zugriffsberechtigung jedes Benutzers kann sich dynamisch auf der Grundlage der Risikoindikatoren ändern.

Komplexität und Kosten mit einer einheitlichen Sicherheitsplattform reduzieren

Da sich Netzwerke und Cyber-Bedrohungen weiterentwickelt haben und immer komplexer geworden sind, haben Anbieter neue Produkte und Lösungen entwickelt, um die damit verbundenen Herausforderungen zu bewältigen. Dies hat zu einer Vielzahl von Einzelprodukten geführt, die jeweils auf eine bestimmte Sicherheitsbedrohung ausgerichtet sind.

Dadurch müssen mittlerweile jedoch viele Unternehmen bis zu 76 Sicherheitstools verwalten. Teams sind damit zunehmend überfordert und die Kosten für die Zusammenarbeit mit so vielen Anbietern sind nicht mehr tragbar.

Diese Bedingungen haben zu einer Konsolidierung auf dem Sicherheitsmarkt geführt. Was Sicherheitsexperten jedoch brauchen, ist Transparenz und Verwaltung von einem zentralen Ort aus - eine Sicherheitsplattform, die eine Vielzahl von Sicherheitstechnologien in eine einzige, einheitliche Architektur integriert.

Veraltete Sicherheits-Stacks können komplex in der Verwaltung und teuer in der Anschaffung und Wartung sein. Erschwerend kommt hinzu, dass jedes einzelne Produkt über eine eigene Konsole und Verwaltungsoberfläche verfügt. Datenpakete durchlaufen diverse Systeme, bevor sie ihr Ziel erreichen, was zu Latenz- und Leistungsproblemen führt. Zudem ist der VPN-basierte Zugriff langsam und umständlich. All dies führt zu einer schlechten Benutzererfahrung.

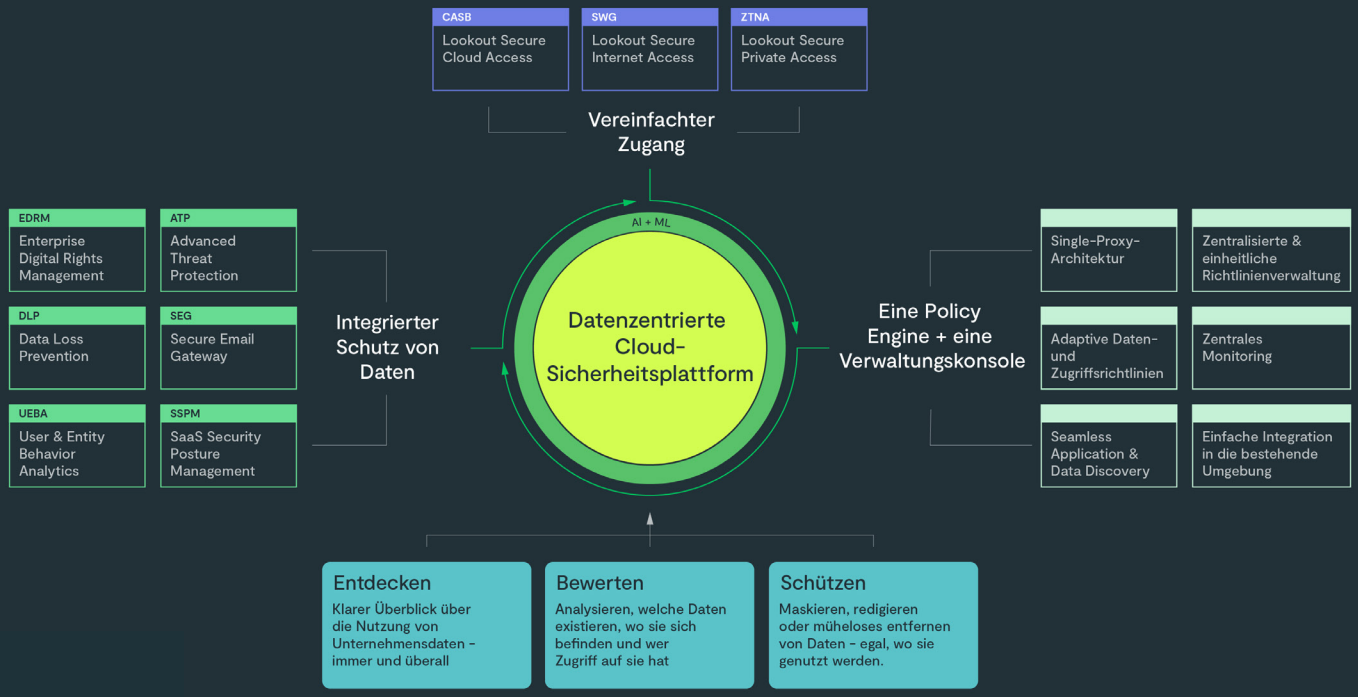
Die integrierte Sicherheitsplattform von Lookout reduziert sowohl Kosten als auch Komplexität der Sicherheitsverwaltung. Durch die einheitliche Konsole und Verwaltungsoberfläche entfällt der Aufwand für die Verwaltung von Richtlinien und Konfigurationen für verschiedene Tools, die Integration neuer Dienste und die Zusammenarbeit mit mehreren Anbietern. Im Vergleich dazu lassen sich unterschiedliche Einzelprodukte nicht immer gut oder überhaupt nicht integrieren. Oft müssen IT-Teams zwischen verschiedenen Plattformen, Verwaltungsbildschirmen und Tools wechseln.

Lookout Secure Cloud Access bietet gebündelte Preise und niedrigere Gesamtkosten für die Konfiguration, Verwaltung und Wartung einer zentralen Plattform, was auch die Lizenzkosten senken kann.

Einer der Hauptvorteile einer integrierten Sicherheitsplattform ist die zentralisierte Durchsetzung von Verwaltungsrichtlinien, so dass Sie konsistente Sicherheitsrichtlinien, einschließlich der Richtlinien für Data Loss Prevention (DLP) und Data Governance, für alle Benutzer, Geräte und Standorte anwenden können. Dadurch werden Fehlanpassungen der Richtlinien und Fehlkonfigurationen vermieden.

Die zentralisierte Richtliniendurchsetzung von Lookout ermöglicht einen einheitlichen und konsistenten Cloud-Sicherheitsansatz und bietet umfassenden Schutz und Governance innerhalb von Multi-Cloud- und Multi-Rechenzentrumsumgebungen sowie eine Reihe von zusätzlichen Vorteilen:

- **Verbesserte Latenz.** Die Cloud-Sicherheitsprodukte von Lookout nutzen eine Single-Proxy-Architektur, wodurch die Anzahl der Dienste, die der Datenverkehr zur Überprüfung und Durchsetzung von Richtlinien durchlaufen muss, reduziert wird.
- **Echtzeit UEBA und tiefergehende Untersuchung.** Auf der Grundlage eines einheitlichen Kerndatenmodells arbeitet UEBA in Echtzeit, um Bedrohungen zu erkennen und darauf zu reagieren. Dies verbessert die Sicherheit und verkürzt die Zeit, die für die Untersuchung und Behebung von Vorfällen benötigt wird.
- **Konsistente Überwachung von Bedrohungen.** Die zentrale Sicherheitsplattform von Lookout verschafft Ihrem Sicherheitsteam einen klaren Überblick über die Bedrohungen, denen das Unternehmen ausgesetzt ist, und zwar über alle Apps und Daten hinweg, so dass Sie diese schnell entschärfen können.



Moderne Sicherheitsanforderungen mit einem innovativen Anwendungsproxy erfüllen

Proxys fungieren als Vermittler zwischen Benutzern und Apps und bieten eine zusätzliche Sicherheitsebene. Allerdings sind nicht alle Proxys gleich aufgebaut, und herkömmliche Proxys neigen dazu, Zielsysteme nur als gut oder schlecht zu identifizieren, ohne zusätzlichen Kontext zu liefern.

Der Proxy von Lookout bietet Kontext. Er erkennt zum Beispiel die Unterschiede in den Sicherheitsrichtlinien zwischen der privaten und der geschäftlichen Nutzung von Apps wie Google Workspace und Microsoft 365 und passt dann den Zugriff auf Basis dieser Richtlinien an.

Da Lookout seinen speziell entwickelten Proxy über eine zentrale Plattform einsetzt, ermöglicht er einen konsistenten, ganzheitlichen Ansatz zur Sicherung des Internetverkehrs, von SaaS-Apps und privaten Unternehmensanwendungen. Die zentrale Proxy-Architektur vereinfacht die Verwaltung und Bereitstellung von Sicherheitstools und gewährleistet eine einheitliche Durchsetzung von Richtlinien.

Durch Funktionen wie Benutzer-Coaching, sichere Zusammenarbeit und Verweigerung der öffentlichen Freigabe sensibler Daten schafft der Lookout Proxy die perfekte Balance zwischen Produktivität und Sicherheit.

Der Lookout Proxy kombiniert fortschrittliche Sicherheitsfunktionen, eine einheitliche Richtliniendurchsetzung und umfassende Transparenz, um einen zuverlässigen Schutz für den Internetverkehr und Daten zu gewährleisten.

Einsatz der öffentlichen Cloud für eine hoch skalierbare Architektur

Zu viele Anbieter von SSE sind durch veraltete Cloud-Architekturen für die Bereitstellung von POPs (Points of Presence) belastet.

Der AWS Global Accelerator von Lookout umfasst ein globales Netzwerk von 109 Points of Presence in 92 Städten in 50 Ländern. Dies bietet einen enormen strategischen Vorteil. So können Sie schneller wachsen als Ihre Wettbewerber. Wenn Sie einen neuen POP-Standort benötigen, kann Lookout diesen in nur wenigen Tagen einrichten, während andere Anbieter in der Regel Monate benötigen.

Lookout ermöglicht es Kunden, mit AWS überall nach Bedarf zu skalieren. So profitieren Sie von den Vorteilen der Cloud-first-Microservices, einer besseren Tooling- und Funktionsgeschwindigkeit und einer schnelleren Markteinführung.

Nutzen Sie die öffentliche Cloud für Geschwindigkeit, Skalierbarkeit und äußerst wettbewerbsfähige Kosten. **76 % des Internets kann über eine Cloud-Architektur erreicht werden. 50 % der Top-1-Million-Websites befinden sich in der Cloud, und 42 % der Top-100.000-Websites sind auf Amazon.** Im Gegensatz dazu verfügt die private Cloud-Architektur nicht über die Geschwindigkeit und Flexibilität, um mit der Notwendigkeit einer schnellen und zuverlässigen Skalierung Ihres Unternehmens Schritt zu halten.

Lookout Secure Cloud Access schützt Daten in der Cloud

Jeden Tag bearbeiten Mitarbeiter Unternehmensdaten aus SaaS-Apps und geben diese weiter. Zwar fördert das die Produktivität, aber es erhöht auch das Risiko von Datenlecks, unbefugter Freigabe, Verstößen gegen gesetzliche Vorschriften oder Malware.

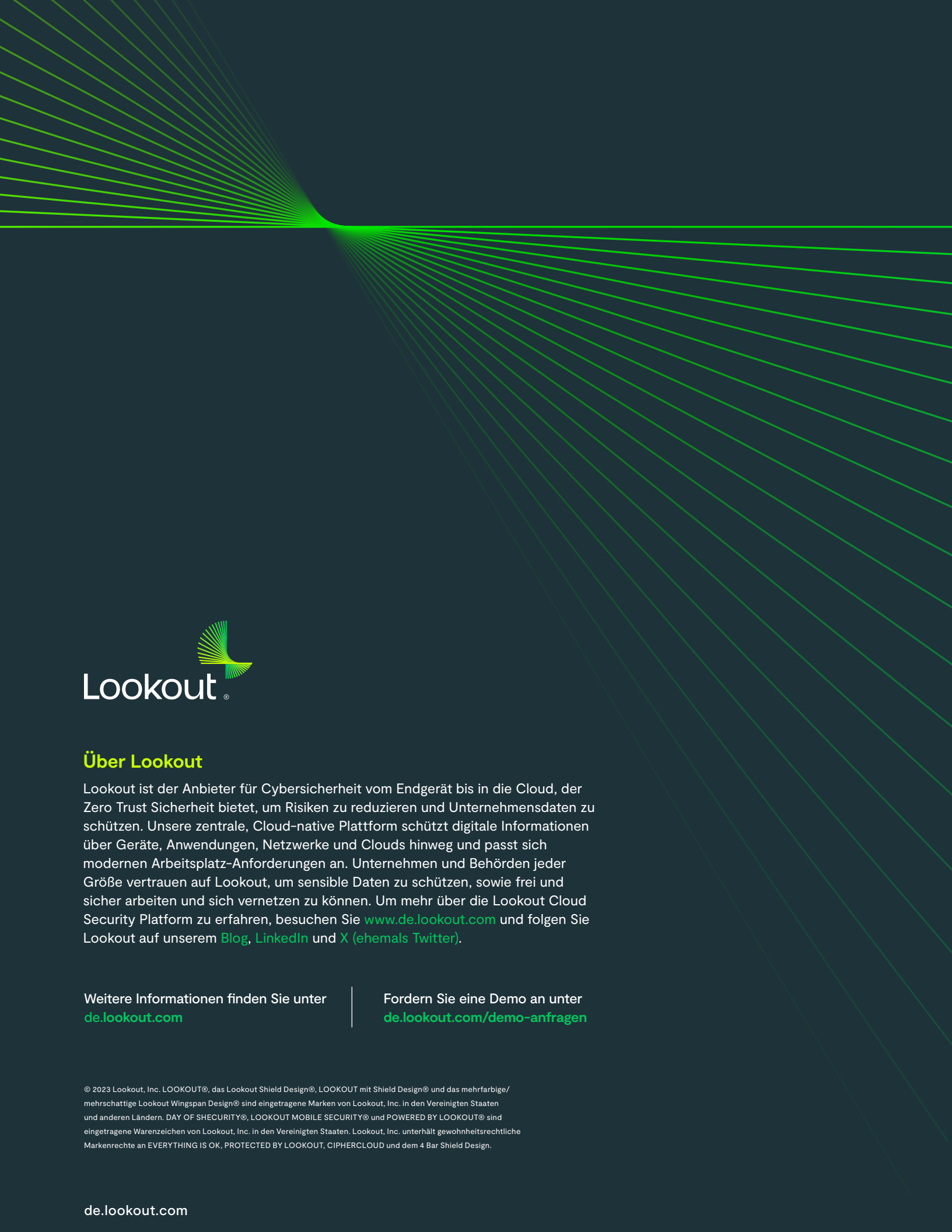
Lookout Secure Cloud Access schützt Unternehmensdaten in der Cloud und gibt Ihnen die Kontrolle über die Nutzung von verwalteten und nicht verwalteten Cloud-Apps. Die Vorteile umfassen:

- Schnellere und effizientere Einführung;
- Bedrohungen können früher erkannt und gestoppt werden, und;
- Niedrigere Kosten.

Machen Sie den nächsten Schritt. Fordern Sie jetzt ein SaaS Risk Assessment an.

Wir haben geschildert, wie Lookout Secure Cloud Access Ihnen dabei helfen kann, Daten zu schützen, gesetzliche Vorschriften einzuhalten und die Rentabilität Ihrer Investitionen zu erhöhen. Erfahren Sie jetzt mehr darüber, wie es um Ihre aktuelle Sicherheit steht. Fordern Sie unser kostenloses SaaS Risk Assessment an. Die Bewertung hilft Ihnen dabei:

- Schwachstellen und Bereiche aufzuzeigen, die Sie einem Risiko aussetzen;
- Einblick in Benutzer, Geräte und Daten zu erlangen, die mit Ihren SaaS-Apps verbunden sind, und;
- Umsetzbare Erkenntnisse darüber zu erhalten, wie Lookout helfen kann.



Über Lookout

Lookout ist der Anbieter für Cybersicherheit vom Endgerät bis in die Cloud, der Zero Trust Sicherheit bietet, um Risiken zu reduzieren und Unternehmensdaten zu schützen. Unsere zentrale, Cloud-native Plattform schützt digitale Informationen über Geräte, Anwendungen, Netzwerke und Clouds hinweg und passt sich modernen Arbeitsplatz-Anforderungen an. Unternehmen und Behörden jeder Größe vertrauen auf Lookout, um sensible Daten zu schützen, sowie frei und sicher arbeiten und sich vernetzen zu können. Um mehr über die Lookout Cloud Security Platform zu erfahren, besuchen Sie www.de.lookout.com und folgen Sie Lookout auf unserem Blog, LinkedIn und X (ehemals Twitter).

Weitere Informationen finden Sie unter
de.lookout.com

Fordern Sie eine Demo an unter
de.lookout.com/demo-anfragen