Sfruttate la potenza delle soluzioni CASB

I 5 principali vantaggi di Lookout Secure Cloud Access

Indice

Presentazione di Lookout Secure Cloud Access

Nell'attuale panorama digitale basato sul cloud, i dati sono più preziosi che mai. E la superficie di attacco in continua espansione rende il rilevamento, la classificazione e la protezione dei dati una sfida continua.

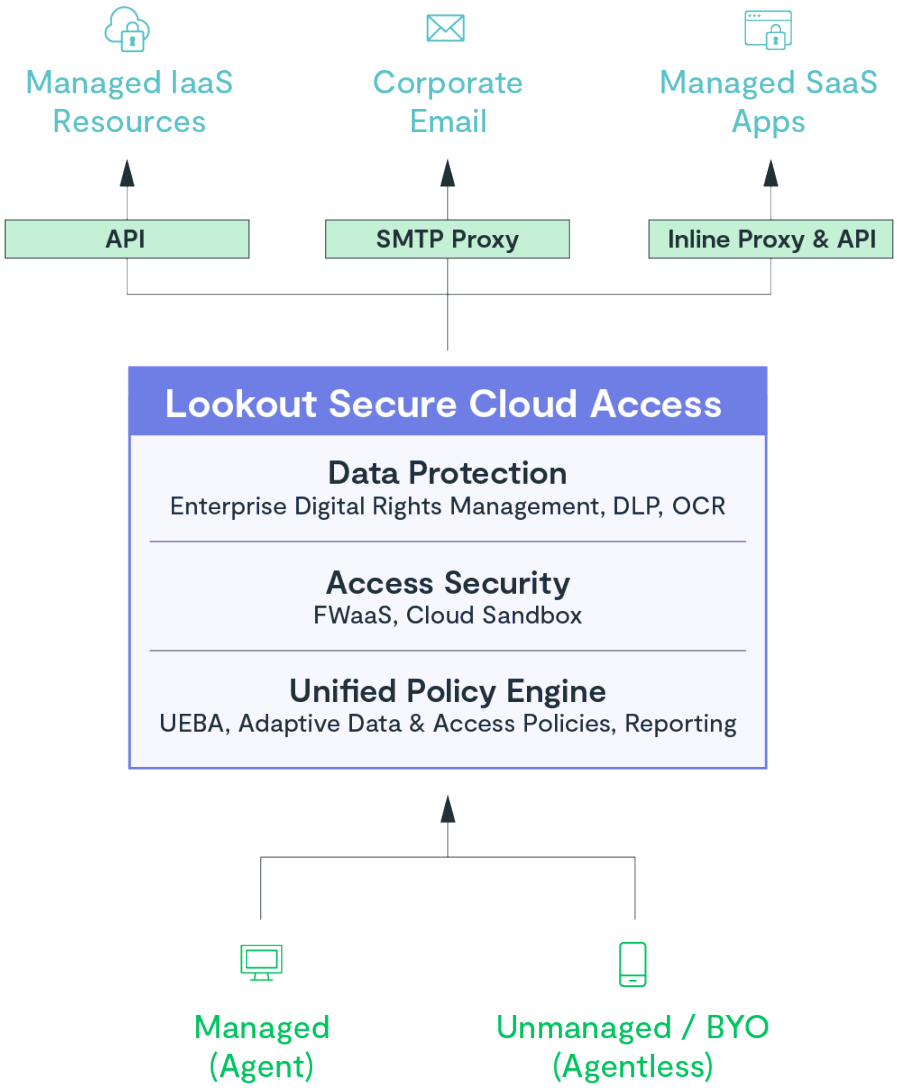
I numeri illustrano il rischio. Solo il 54% delle aziende sa dove sono archiviati i propri dati sensibili.[1] Un incredibile 65% raccoglie così tanti dati da non essere in grado di classificarli o analizzarli.[2] Con i dipendenti e i collaboratori esterni che accedono ai dati da una varietà di luoghi e dispositivi, questa mancanza di visibilità rappresenta un grave rischio per la sicurezza, in particolare quando gli utenti adottano comportamenti ad alto rischio.

Per proteggere efficacemente i dati, le organizzazioni devono poter vedere dove questi risiedono, come vengono condivisi e chi vi ha accesso.

Lookout Secure Cloud Access è una soluzione Cloud Access Security Broker (CASB) costruita sul principio Zero Trust ("a fiducia zero"). Un numero crescente di organizzazioni si affida a questo strumento per rilevare, valutare e proteggere i dati in tutte le applicazioni cloud e SaaS.

A differenza delle policy di sicurezza dei dati statiche offerte dalle soluzioni tradizionali, le policy adattive di Lookout Secure Cloud Access forniscono il contesto di ogni richiesta di accesso ai dati o alle applicazioni. In questo modo si riducono i falsi positivi per la condivisione dei dati e i ticket di assistenza per l'IT, migliorando la produttività del personale.

Lookout Secure Cloud Access permette di controllare i dati mentre si muovono, ovunque si muovano. Il suo motore centralizzato per le policy fornisce funzionalità di prevenzione della perdita di dati (DLP, Data Loss Prevention) granulari e adattive, semplificando la definizione e l'applicazione delle policy di sicurezza in tutte le applicazioni cloud e Saas.



Questo white paper offre una panoramica dell'approccio innovativo di Lookout alla fornitura di funzionalità CASB sulla propria piattaforma di sicurezza unificata. Si concentra sui principi fondamentali del nostro modello, che forniscono un valore strategico essenziale alle organizzazioni desiderose di proteggere la loro risorsa più importante: i dati.

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

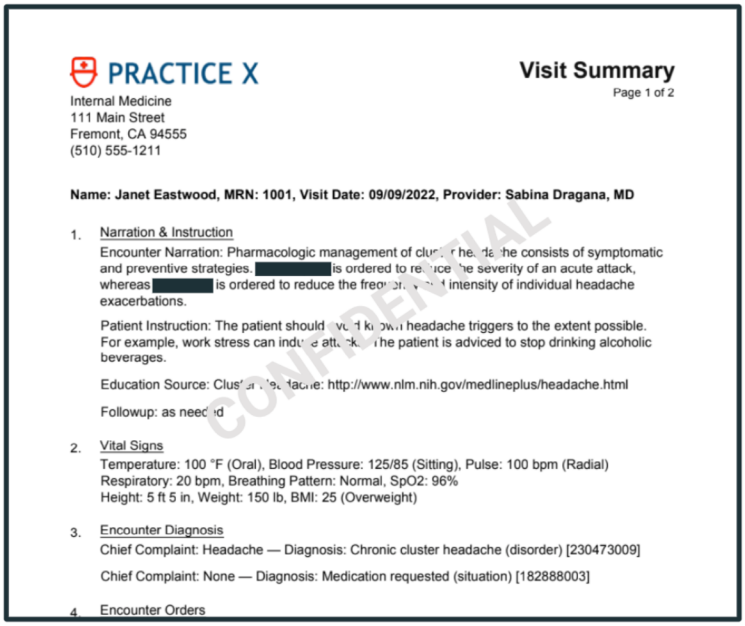
Controllo granulare sui dati

La vostra organizzazione poggia su molteplici stakeholder che utilizzano vari strumenti di collaborazione. Non tutti risiedono all'interno dell'organizzazione stessa, il che rappresenta una sfida non da poco. Occorre mantenere i dati al sicuro mentre vengono condivisi tra collaboratori esterni e partner. Poi, una volta completati i progetti, è necessario proteggere i dati condivisi.

Le funzionalità di gestione dei diritti digitali (DRM, Digital Rights Management) integrate in Lookout Secure Cloud Access offrono un controllo completo sui dati sensibili, indipendentemente da chi li condivide e da come lo fa. I dati sono al sicuro, sia che i dipendenti, i collaboratori esterni e i partner cooperino tramite e-mail sia che utilizzino strumenti come Slack, Microsoft Teams, Box, Dropbox, Google Drive e Microsoft OneDrive.

A differenza di altre soluzioni per la protezione dei dati che si limitano ad applicare policy per consentire o negare l'accesso ai dati, Lookout consente di adottare policy flessibili che mettono dei paletti di sicurezza intorno a tale accesso.

Le tecnologie EDM (Exact Data Matching) e OCR (Optical Character Recognition) di Lookout identificano e proteggono i dati sensibili in una varietà di formati, tra cui testo, immagini e altri documenti scansionati. Lookout analizza i file e le cartelle quando vengono condivisi e identifica e protegge le informazioni riservate in base a policy predefinite con diverse opzioni di applicazione.



PRACTICE X

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

Visit Summary
Page 1 of 2

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] headache triggers to the extent possible. For example, work stress can indu[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

Le policy DRM di Lookout rielaborano tutte le informazioni riservate riconducibili alle normative sulla privacy sanitaria e incorporano una filigrana per impedire la condivisione di dati sensibili con utenti non autorizzati e mantenere la compliance.

Lookout offre potenti funzionalità DRM native che consentono alle organizzazioni di controllare l'accesso a dati e contenuti, anche dopo che sono stati condivisi con altri. Le organizzazioni mantengono il controllo sui propri dati anche quando sono archiviati su dispositivi non gestiti.

- **Mascherare o rielaborare:** Lookout identifica i dati sensibili come i numeri di previdenza sociale e di carta di credito, nonché i dati specifici di regioni e settori. Ciò consente agli amministratori di applicare policy che permettono la condivisione dei dati, mascherando o rielaborando le informazioni sensibili. Gli strumenti privi di funzionalità DRM possono identificare i documenti sensibili, ma non possono mascherare né rielaborare le informazioni, per cui il reparto IT è costretto a bloccare la condivisione dei dati, ostacolando così il lavoro.
- **Filigrana:** per mantenere la sicurezza dei dati, Lookout può applicare automaticamente delle filigrane (in inglese "watermark") per avvisare gli utenti dei contenuti riservati nei file sensibili. Le filigrane scoraggiano i dipendenti dal fare screenshot o condividere i documenti.
- **Crittografia:** Lookout può crittografare i file per garantire l'accesso solo agli utenti autorizzati. Tale accesso può scadere dopo un determinato periodo di tempo. La crittografia può inoltre essere combinata con altre regole DLP. Ad esempio, le informazioni riservate possono rimanere mascherate all'interno di un file decrittato. In questo modo si impedisce a un dipendente o a un collaboratore esterno di accedere a documenti sensibili una volta lasciata l'organizzazione.

È possibile fare un ulteriore passo avanti nella protezione dei dati definendo policy dinamiche di gestione dei diritti digitali per limitare chi può decrittare i contenuti. Ciò può comportare una combinazione di opzioni configurabili come le credenziali utente, i livelli di rischio dell'utente e la geo-localizzazione.

I vantaggi delle funzionalità DRM native sono evidenti: facilitano la collaborazione sicura e aumentano la produttività, fornendo al contempo una solida protezione dei dati sensibili.

Identificazione delle anomalie e blocco tempestivo delle minacce

Lookout Secure Cloud Access applica l'analisi del comportamento di utenti ed entità (UEBA, User and Entity Behavior Analytics) per monitorare e valutare costantemente utenti, dispositivi e attività. Ciò consente al vostro team di identificare le deviazioni dal comportamento normale in modo da poter porre rimedio rapidamente a un'ampia gamma di potenziali minacce, tra cui: insider malintenzionati, account compromessi e minacce persistenti avanzate (APT, Advanced Persistent Threat).

60%

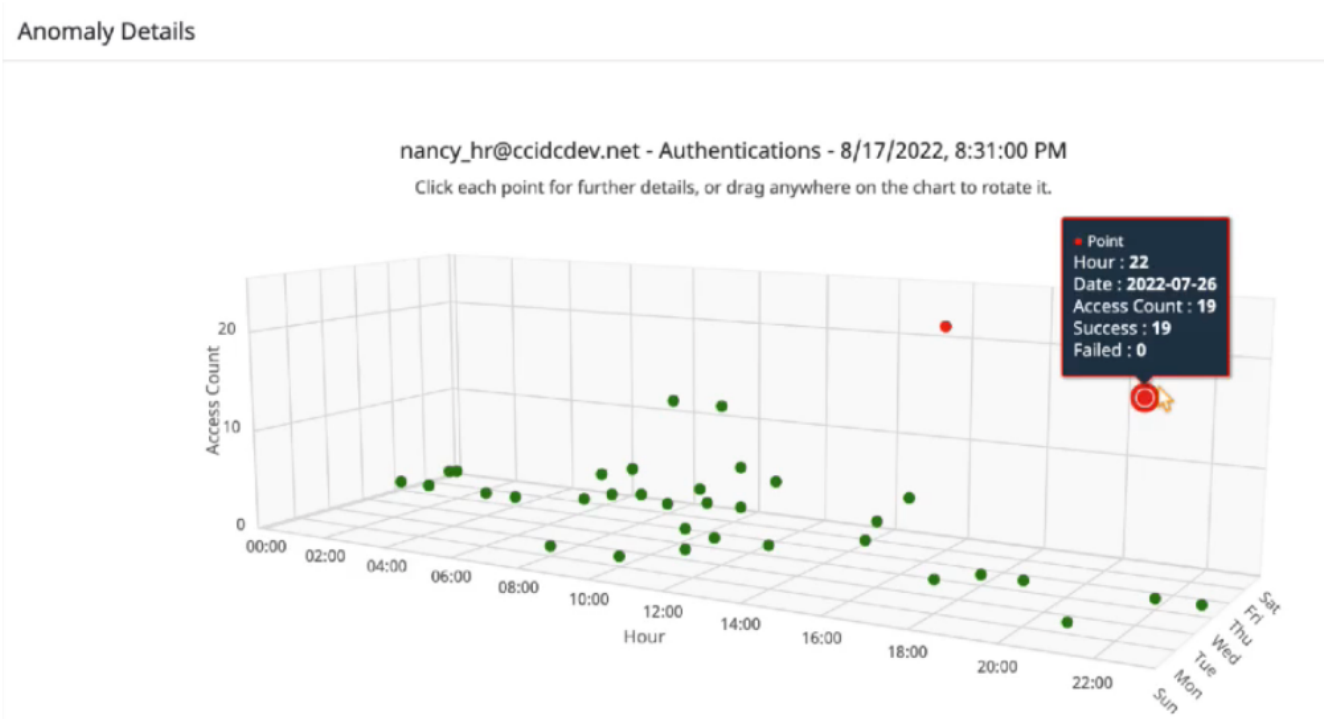
Il 60% delle violazioni dei dati è causato da utenti autenticati. Monitorando il comportamento degli utenti e identificando download di dati di grandi dimensioni e anomalie simili, la tecnologia UEBA è in grado di rilevare attività dannose come l'esfiltrazione dei dati o le frodi.

La tecnologia UEBA non solo monitora le anomalie a livello di geo-localizzazione, ma identifica anche attività rischiose come download di massa da parte di singoli utenti, l'uso di dispositivi non gestiti che potrebbero essere infettati da malware, i tentativi di accesso persistenti, le modifiche ai dati o gli utenti che accedono a molti file a cui non hanno mai avuto accesso prima.

Monitoraggio del rischio con accesso adattivo

Grazie all'analisi in tempo reale dei modelli di utente, dispositivo e posizione, Lookout genera punteggi di rischio precisi per gli utenti, che possono essere personalizzati in base alle policy aziendali. La nostra funzione di accesso adattivo utilizza l'apprendimento automatico per analizzare il comportamento dell'utente, l'integrità del dispositivo e la posizione. Lookout assegna a ciascun utente un punteggio di rischio che può aumentare in base all'attività dell'utente, dell'IP, dell'app e alla postura del dispositivo, quindi determina se concedere o negare l'accesso a dati specifici in base a tale punteggio.

Un punteggio di rischio elevato può attivare avvisi per il follow-up dell'amministratore o imporre automaticamente azioni aggiuntive basate su policy di sicurezza preimpostate, come la richiesta di ri-autenticazione dell'utente, il mascheramento o la rielaborazione dei dati oppure il blocco totale dell'accesso dell'utente.



Le discrepanze nelle attività di accesso attivano gli avvisi di anomalia.
Questo grafico mostra diversi accessi al di fuori delle date e degli orari normali per un utente.

Secure Cloud Access si basa sui principi Zero Trust. Convalida il contesto dell'utente prima di concedere l'accesso alle app e ai dati e verifica continuamente i diritti di accesso. Che gli utenti cerchino di accedere alle app per cloud e SaaS da dispositivi gestiti o non gestiti, essi vengono autenticati e autorizzati in base alla postura di sicurezza dei loro dispositivi e ai loro profili di rischio. Il livello di accesso di ciascun utente può cambiare dinamicamente in base agli indicatori di rischio.

Riduzione della complessità e dei costi con una piattaforma di sicurezza unificata

Parallelamente all'evoluzione e alla crescente complessità delle reti e delle minacce informatiche, gli sviluppatori hanno creato nuovi prodotti e soluzioni per affrontare le sfide che esse comportano. Ciò ha portato a una proliferazione di prodotti mirati, ciascuno progettato per affrontare una specifica minaccia alla sicurezza.

Di conseguenza, alcune organizzazioni si trovano a dover gestire fino a 76 strumenti di sicurezza. I team sono sovraccarichi. E il costo di operare con così tanti fornitori è diventato insostenibile.

Tali condizioni hanno iniziato a favorire un certo consolidamento all'interno del mercato della sicurezza. Ma quello di cui i professionisti della sicurezza hanno più bisogno sono la visibilità e la capacità di gestire tutto da un'unica postazione: una piattaforma di sicurezza che integri una serie di tecnologie di sicurezza in un'unica architettura unificata.

Gli stack di sicurezza tradizionali possono essere complessi da gestire e costosi da acquistare e mantenere. A peggiorare le cose, ogni prodotto mirato ha una console e un'interfaccia di amministrazione diverse. I pacchetti devono passare attraverso più appliance prima di raggiungere la loro destinazione, con conseguenti problemi di latenza e prestazioni. Inoltre, l'accesso basato su VPN è lento e macchinoso. Il tutto si traduce in una esperienza negativa per l'utente.

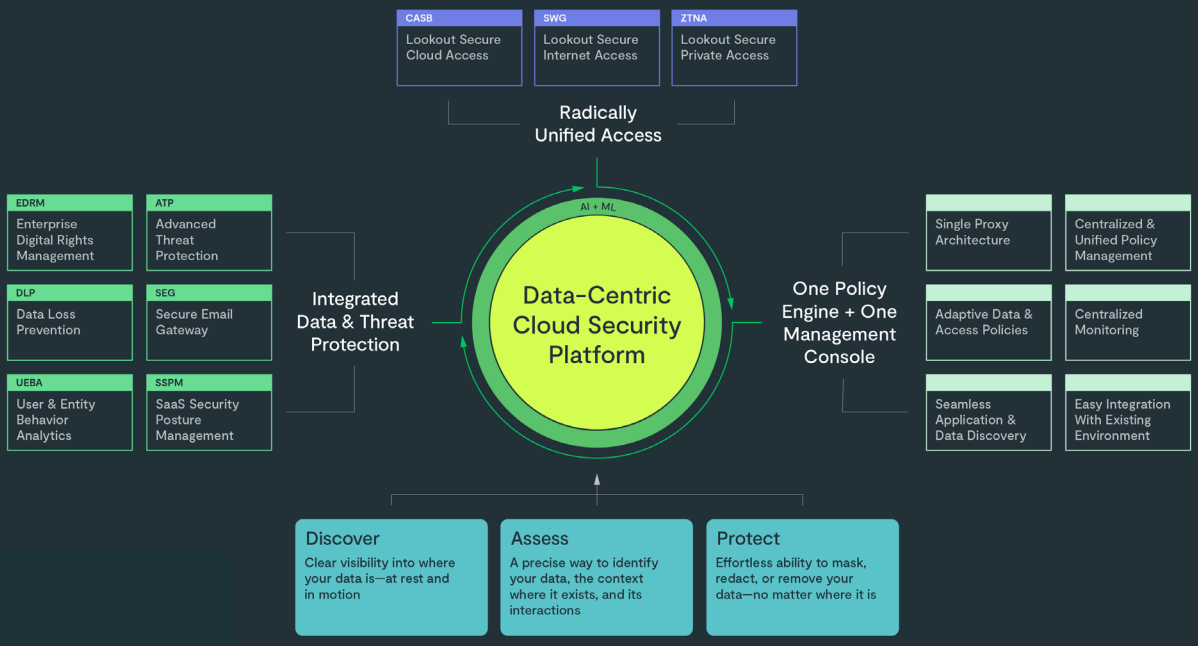
L'architettura unificata della piattaforma di sicurezza di Lookout riduce sia i costi che la complessità della gestione della sicurezza. Grazie a una sola console e a una sola interfaccia di amministrazione, si riducono i tempi necessari per la gestione delle policy e delle configurazioni tra gli strumenti, l'integrazione di nuovi servizi e l'interazione con più fornitori. I variegati prodotti mirati, invece, non sempre si integrano bene, o addirittura non si integrano affatto. Spesso richiedono ai team IT di passare da una piattaforma all'altra, da una schermata di amministrazione all'altra e da uno strumento all'altro.

Lookout Secure Cloud Access offre prezzi in bundle e costi complessivi inferiori per la configurazione, l'amministrazione e la manutenzione di una piattaforma unificata e ciò può portare anche a una riduzione dei costi di licenza.

Uno dei principali vantaggi di una piattaforma di sicurezza unificata è l'applicazione centralizzata delle policy di amministrazione, che consente di imporre policy di sicurezza coerenti, comprese quelle per DLP e governance dei dati, a tutti gli utenti, i dispositivi e le sedi. In questo modo si eliminano gli errori di allineamento e di configurazione delle policy.

Oltre a consentire un approccio unificato e coerente alla sicurezza del cloud e a fornire una protezione e una governance estese in ambienti multi-cloud e multi-data center, l'applicazione centralizzata delle policy di Lookout offre anche una serie di vantaggi aggiuntivi:

- **Miglioramento della latenza e delle prestazioni.** I prodotti per la sicurezza del cloud di Lookout utilizzano un'architettura a singolo proxy che riduce il numero di servizi attraverso cui il traffico deve passare per l'ispezione e l'applicazione delle policy.
- **UEBA in tempo reale e analisi forense avanzata.** Grazie a un modello di dati centrale unificato, la tecnologia UEBA opera in tempo reale per rilevare e rispondere alle minacce. Questo migliora la sicurezza e riduce il tempo necessario per indagare e risolvere gli incidenti.
- **Tracciamento coerente delle minacce.** L'architettura unificata della piattaforma di sicurezza di Lookout offre ai team addetti alla sicurezza una chiara comprensione delle minacce che incombono sull'organizzazione, su tutte le app e su tutti i dati, in modo da poterle mitigare rapidamente.



Risposta alle moderne esigenze di sicurezza con un proxy intelligente per le applicazioni

I proxy fungono da intermediari tra gli utenti e le applicazioni e forniscono un prezioso livello di sicurezza. Tuttavia, non tutti i proxy sono costruiti allo stesso modo. I proxy tradizionali, in particolare, si limitano a identificare le destinazioni come buone o cattive, senza fornire un contesto aggiuntivo.

Il proxy di Lookout invece fornisce un contesto. Ad esempio, identifica le differenze delle policy di sicurezza tra l'uso personale e quello aziendale di applicazioni come Google Workspace e Microsoft 365 e quindi adatta l'accesso in base a tali policy.

Applicando il proprio proxy intelligente, costruito ad hoc su una piattaforma unificata, Lookout consente un approccio coerente e completo alla protezione di tutto il traffico Internet, delle applicazioni SaaS e delle applicazioni aziendali private. L'architettura a proxy unico semplifica la gestione e l'implementazione degli strumenti di sicurezza, garantendo un'applicazione coerente delle policy.

Il proxy intelligente di Lookout combina funzionalità di sicurezza avanzate, applicazione unificata delle policy e visibilità completa per offrire una solida protezione del traffico Internet e dei dati.

Grazie a funzionalità quali il coaching degli utenti, la collaborazione sicura e il blocco della condivisione pubblica di dati sensibili, il proxy intelligente per le applicazioni di Lookout raggiunge il perfetto equilibrio tra produttività e sicurezza.

Utilizzo del cloud pubblico per un'architettura altamente scalabile

Troppi fornitori di soluzioni SSE (Security Service Edge) sono vincolati da architetture cloud proprietarie per la distribuzione dei punti di presenza (POP).

L'AWS Global Accelerator di Lookout comprende una rete globale di 109 punti di presenza in 92 città di 50 paesi. Questo offre un enorme vantaggio strategico, permettendo alla vostra azienda di crescere più velocemente della concorrenza. Quando sorgerà il bisogno di disporre di una nuova sede POP, Lookout sarà in grado di implementarla in pochi giorni, rispetto ai mesi normalmente richiesti da altri fornitori.

Lookout consente ai clienti di scalare ovunque su richiesta con AWS, offrendo i vantaggi dei microservizi cloud-first, una migliore velocità degli strumenti e delle funzionalità e un migliore time-to-market.

Sfruttate il cloud pubblico per ottenere velocità, scalabilità e costi altamente competitivi. **Il 76% di Internet è raggiungibile da un'architettura cloud. Il 50% del primo milione di siti è nel cloud e il 42% dei primi 100.000 siti è su Amazon.** Al contrario, l'architettura cloud privata non ha la velocità e l'agilità necessarie per stare al passo con l'esigenza di scalare il business in modo rapido e affidabile.

Lookout Secure Cloud Access protegge i dati nel cloud

Ogni giorno i dipendenti caricano, scaricano e condividono i dati aziendali dalle applicazioni SaaS approvate.
Se da un lato ciò è ottimo per la produttività, dall'altro aumenta il rischio di perdite di dati, di condivisioni non autorizzate, di violazioni delle normative o di incursioni di malware.

Lookout Secure Cloud Access protegge i dati nel cloud e offre un controllo sull'uso delle applicazioni cloud gestite e non gestite. I vantaggi includono:

- accelerazione della velocità e della scala di distribuzione;
- capacità di identificare e bloccare le minacce in tempi più brevi;
- riduzione dei costi.

Fate il passo successivo. Richiedete subito una valutazione del rischio SaaS.

Abbiamo descritto come Lookout Secure Cloud Access può aiutare a proteggere i dati, a rispettare le normative e a ottenere un ritorno sugli investimenti. Scoprite ora come stanno andando gli attuali sforzi della vostra azienda sul fronte della sicurezza dei dati. Registratevi alla nostra valutazione gratuita del rischio SaaS. Con essa, potrete:

- individuare i punti ciechi e le aree che vi espongono al rischio;
- ottenere visibilità su utenti, dispositivi e dati associati alle applicazioni SaaS;
- ricevere spunti pratici su come Lookout può aiutarvi.

A proposito di Lookout

Lookout, Inc. è un'azienda di cyber security nell'ambito endpoint to cloud, specializzata nella protezione di dati aziendali e personali che convergono. Proteggiamo le informazioni nei dispositivi, nelle app, nelle reti e in cloud, attraverso una piattaforma di sicurezza unificata e cloud-native, attraverso un modello fluido e flessibile, come richiesto dalle esigenze di un mercato sempre più dipendente dal digitale. Forniamo maggiore controllo sui dati di organizzazioni ed individui, consentendo loro di beneficiarne e prosperare in tranquillità. Lookout fornisce aziende di ogni dimensione in tutti i segmenti di mercato, inclusa la pubblica amministrazione e protegge i dati di milioni di consumatori, consentendo loro di lavorare e connettersi in modo flessibile e sicuro. Per approfondimenti sulla Lookout Cloud Security Platform, visitate il sitowww.lookout.com e seguite Lookout sul nostroblog, su LinkedIn e su X (precedentemente Twitter).

Per maggiori informazioni visitate **lookout.com**

È possibile richiedere una demo su **lookout.com/request-a-demo**