Lookout®

EBOOK

Sicurezza dei dati dall'endpoint al cloud per la collaborazione remota

Punti chiave

- Proteggere utenti, dispositivi mobili, app, connessioni e dati utilizzati per le piattaforme di collaborazione e messaggistica.
- Collaborare e comunicare in sicurezza con dispositivi gestiti e non gestiti, su qualunque rete e da qualunque località.
- Prevenire le perdite di dati e rilevare precocemente malware ed exploit.
- Identificare i comportamenti pericolosi di utenti, dispositivi mobili e app.
- Impedire la condivisione di cartelle cliniche, numeri di previdenza sociale, dati di carte di credito e altre informazioni di identificazione personale (Personally Identifiable Information, PII).
- Rispettare le norme in materia di protezione dei dati, come il GDPR, l'HIPAA e il CCPA.

Introduzione

Il ricorso epocale allo smart working ha portato le imprese a spostare sul cloud le app di collaborazione e messaggistica per facilitare i contatti da remoto tra i dipendenti e l'azienda. Slack, Microsoft Teams e altri strumenti favoriscono la comunicazione e lo scambio di informazioni in tempo reale, consentendo ai dipendenti di essere produttivi e sempre aggiornati.

Considerato che si scambia di tutto ovunque, quali misure adotta la tua impresa per protegge i dati, le applicazioni e la privacy aziendali su questo tipo di piattaforme?

Il Cloud Access Security Broker (CASB) offerto da Lookout® protegge Slack, Teams e le altre piattaforme di comunicazione aziendale fornendo controlli granulari delle condivisioni di file e analisi stateful di dati e app.

Grazie alla visibilità approfondita sui contenuti, alla classificazione dei dati e ai controlli basati sul contesto, gli utenti possono collaborare in sicurezza anche utilizzando dispositivi non gestiti dall'azienda.

Dagli endpoint al cloud, Lookout CASB protegge i dati, identifica le minacce informatiche e applica le norme di conformità per tutelare le informazioni aziendali riservate ovunque. Lookout CASB offre protezione e controllo completi, rendendo più sicura la distribuzione delle app nel cloud aziendale.

Il design agentless di Lookout CASB garantisce un deployment rapido e agevole senza i costi e il carico amministrativo legati all'installazione e alla gestione manuale degli agenti su ogni dispositivo mobile.

Visibilità approfondita su utenti e applicazioni SaaS

Report "The State of Cloud Monitoring" di Keysight

Lookout CASB offre una visibilità approfondita sulla sicurezza delle app di collaborazione e messaggistica nel cloud, consentendoti di capire meglio in che modo i dati vengono condivisi dagli utenti di Slack e Teams. In questo modo è possibile evitare la divulgazione e l'esposizione accidentali di dati sensibili e riservati.

- Un unico ambiente permette di visualizzare e monitorare il sistema e l'attività utente a livello di e-mail, collaborazione, messaggistica e infrastruttura.
- Il rilevamento dello shadow IT calcola automaticamente il punteggio di rischio del cloud in base ai risultati di analisi di oltre 20.000 app cloud e 60 attributi.
- L'app intelligence avanzata protegge tutte le attività, non sono gli upload e i download dei dati. Il CASB rileva e distingue le istanze delle app per gestire in tempo reale la collaborazione dall'esterno ed evitare la condivisione aperta di cartelle e file protetti.
- Gli insight consentono di restringere l'analisi di incidenti ed entità con la creazione di query relative a scenari ben precisi. Le analisi delle entità possono riguardare utenti, dispositivi, posizioni geografiche e app.
- In oltre 30 pagine, il report illustra a CIO/CISO come si articola il profilo di sicurezza del cloud aziendale a fini di audit e analisi del rischio.

"Secondo l'87% dei professionisti del cloud, la mancanza di visibilità sul cloud tiene le organizzazioni all'oscuro delle minacce alla loro sicurezza."

- Report "The State of Cloud Monitoring" di Keysight

Accesso protetto per i dispositivi mobili non gestiti

Lookout CASB identifica e protegge le app SaaS dall'accesso non autorizzato agli account con controlli di sicurezza cloud Zero Trust, offrendoti una sicurezza completa di utenti e dati con qualsiasi dispositivo mobile, app, utente e posizione.

- Classifica gli endpoint mobili come gestiti o non gestiti tramite certificati digitali per la durata della connessione alle app cloud.
- Si integra con Okta e altre soluzioni identity-as-a-service (IDaaS) per verificare l'integrità degli utenti e controllare gli accessi con l'autenticazione Single Sign-on (SSO) e multifattore (MFA).
- Valuta continuamente i rischi degli utenti verificati con il controllo adattivo degli accessi (AAC, Adaptive Access Control). Questa funzione blocca l'accesso agli utenti autorizzati in base alla piattaforma, all'ora e ad altre informazioni contestuali che indicano la possibilità di furto, compromissione delle credenziali di autenticazione o attacco informatico. Ad esempio, se qualcuno tenta di eseguire l'accesso da Shanghai con le credenziali di un utente che si era disconnesso un'ora prima da Detroit, la funzione AAC rileva immediatamente questa attività e la blocca.
- Le policy controllano l'accesso alle risorse cloud a seconda che si tratti di dispositivo gestito o non gestito. Ad esempio, i dispositivi non gestiti possono solo eseguire l'accesso via browser alle app SaaS, mentre l'accesso tramite applicazioni thick client è negato. Analogamente, le policy di controllo degli accessi possono impedire la sincronizzazione dei dati sui dispositivi non gestiti.

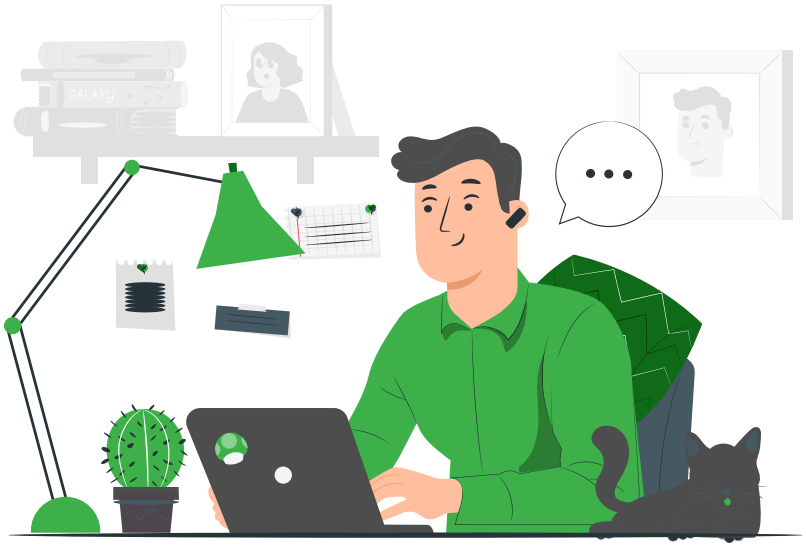
"La metà delle organizzazioni ci mette circa 120 giorni, ovvero quattro mesi, per rilevare una violazione delle credenziali, e solo dopo la segnalazione da parte di terzi."

- Dark Reading, 2021

Protezione e privacy dei dati all'avanguardia

Principali problemi di sicurezza cloud

- Sicurezza della rete (58%)
- Mancanza di esperienza con il cloud (47%)
- Trasferimento dei carichi di lavoro sul cloud (44%)
- Personale insufficiente per gestire gli ambienti cloud (32%)



Cloud Security Alliance, "State of Cloud Security Concerns, Challenges, and Incidents", marzo 2021

Vale la pena notare che il 79% degli intervistati ha fatto presente problemi legati al personale, sottolineando come le organizzazioni hanno difficoltà a gestire i deployment cloud e il personale che lavora in gran parte da remoto.

Lookout CASB fornisce policy DLP, crittografia end-to-end e gestione completa delle chiavi di crittografia all'avanguardia per limitare l'accesso ai contenuti sensibili nel cloud e prevenire le perdite di dati, il furto di proprietà intellettuale e la mancata conformità a leggi e regolamenti.

La piattaforma di sicurezza scalabile e a gestione centralizzata fornita da Lookout semplifica i processi di inserimento di nuovi cloud e i flussi di lavoro per la creazione di policy di protezione dei dati.

- L'analisi avanzata dei contenuti unita alle policy DLP protegge le informazioni di identificazione personale, di pagamento e sanitarie, insieme ad altri contenuti sensibili tramite classificazione, crittografia, mascheramento, aggiunta di filigrane, messa in quarantena ed eliminazione dei dati. CASB comprende modelli DLP integrati per l'analisi di patenti, numeri di passaporto, indirizzi IP e MAC, e-mail, codici EIN e numeri di telaio.
- La crittografia Zero Trust protegge i dati ovunque siano: a riposo, in transito, a livello di app cloud (API, middleware, memoria) e in uso. La conformità allo standard FIPS 140-2 soddisfa i requisiti regolamentari e garantisce i più alti livelli di protezione dalle minacce informatiche, compresi gli attacchi alle API che prendono di mira i dati crittografati. Le chiavi di crittografia dei dati sono sempre protette e non vengono mai condivise con i fornitori cloud.
- Il riconoscimento ottico dei caratteri (OCR) consente al CASB di rilevare le informazioni sensibili nei file immagine caricati nel cloud. La protezione OCR viene applicata anche ai file PDF e Microsoft Word.

Proteggere i dati scaricati sui dispositivi di proprietà personale

La gestione dei diritti informatici (Information Rights Management, IRM) in Lookout CASB applica controlli di protezione dei dati, crittografia e gestione centralizzata dei dati sensibili, anche quando vengono condivisi all'esterno. In base ai livelli di riservatezza, l'IRM racchiude automaticamente i dati in buste crittografate, garantendo la massima protezione dei dati stessi e delle persone.

- L'IRM nativa protegge l'accesso ai dati offline, impedendo il download dalle app cloud sui dispositivi degli utenti. Solo gli utenti autorizzati con un'app mobile IRM e chiavi valide possono decrittografare e visualizzare i contenuti sensibili nei file scaricati.
- Per evitare l'uso improprio dei dati scaricati, è possibile ritirare l'accesso anche se sono stati scaricati e copiati su un altro dispositivo. Lookout CASB si integra con Microsoft e altri pacchetti IRM di terze parti.
- Il controllo remoto dei dati con l'integrazione del proxy ActiveSync consente di bloccare i dispositivi connessi o cancellare da remoto i contenuti di Teams da un dispositivo mobile personale a seconda del livello di sicurezza.
- È possibile limitare la condivisione di file e cartelle con gruppi e dispositivi personali esterni su Slack, Teams e altre app di collaborazione e messaggistica.

"I dispositivi mobili personali sono molto più soggetti ad attacchi di phishing rispetto a quelli aziendali. Secondo i nostri dati, il tasso di esposizione agli attacchi di phishing dei dispositivi personali nel primo trimestre 2021 è stato del 19,4%, contro il 13,5% dei dispositivi aziendali."

- Lookout Threat Report, 2021

Prevenzione delle minacce zero-day negli ambienti SaaS

In collaborazione con FireEye, Lookout offre la prima protezione in tempo reale da minacce zero-day dai dispositivi mobili agli ambienti SaaS. Questa consente di aggregare e correlare le minacce dagli endpoint al cloud per fermare l'ondata in ingresso di minacce alla sicurezza informatica che prendono di mira il personale in smart working.

- La protezione antivirus e antimalware (AV/AM) contro ransomware e altre minacce tiene al sicuro i dati nei servizi di condivisione file e gestione dei contenuti cloud. La protezione dei link URL e l'integrazione della sandbox on-premise permettono di rilevare e correggere minacce zero-day difficili da scovare. In questo modo l'AV/AM rileva e isola i documenti cloud infetti prima che il malware si diffonda.
- L'analisi dei comportamenti di utenti ed entità (UEBA) utilizza tecniche avanzate di machine learning per monitorare l'attività utente, inclusi orari, tentativi di download dei file in blocco e altri comportamenti anomali. L'UEBA segnala o blocca in tempo reale l'attività insolita in base alle differenze dai comportamenti usuali, ad esempio impedendo il download di moli di documenti insolitamente grandi a orari inconsueti.
- La gestione del livello di sicurezza cloud (Cloud Security Posture Management, CSPM) valuta automaticamente il livello di sicurezza SaaS e IaaS della suite di Microsoft Office 365, Microsoft Azure, Amazon Web Services e Google Cloud Platform. La gestione centralizzata della sicurezza di tutti i servizi e le infrastrutture cloud riduce enormemente la complessità operativa.

"Per le organizzazioni con più di 1 miliardo di dollari di fatturato, il costo medio del ripristino in seguito a un attacco informatico si aggira sui 4,6 milioni di dollari."

- TechBeacon

Governance e conformità centralizzate

Lookout CASB rende le app di collaborazione e messaggistica come Slack e Teams conformi a un'ampia gamma di norme sulla privacy dei dati in vigore o in via di formazione, come gli standard Payment Card Industry (PCI), Personally Identifiable Information (PII), l'Health Insurance Portability and Accountability Act (HIPAA), il Regolamento generale sulla protezione dei dati (GDPR), il California Consumer Privacy Act (CCPA), per citarne alcuni.

- Il rilevamento dei dati cloud (CDD) analizza i dati storici, individua e classifica i contenuti sensibili e definisce le policy di protezione per rispettare le norme in materia di residenza dei dati. Lookout CASB include modelli DLP predefiniti per garantire la conformità alle norme GDPR, HIPAA, CCPA, GLBA e altre.
- Ogni Paese ha le proprie regole di conformità in materia di privacy, tutela, sovranità e residenza dei dati. Lookout permette alle multinazionali di gestire un'unica distribuzione protetta e integrata per le app cloud più importanti con controlli e gestione delle chiavi configurabili per soddisfare tutta una serie di requisiti normativi diversi.
- Lookout CASB aumenta la protezione delle informazioni personali nei vari Paesi e aree geografiche in conformità alle norme sulla residenza dei dati dei Paesi di hosting. In questo modo le aziende di tutto il mondo possono utilizzare le app senza preoccuparsi di aggiungere controlli di sicurezza per la protezione dei dati.

"Entro il 2023, le informazioni personali del 65% della popolazione mondiale saranno oggetto di norme per la tutela della privacy, a partire dal 10% attuale."

- Gartner

Lookout®

Informazioni su Lookout

Lookout è una società che fornisce soluzioni di sicurezza integrata da endpoint a cloud. La nostra mission è quella di proteggere e potenziare il futuro digitale in un mondo sempre più attento alla privacy, nel quale la mobilità e il cloud sono essenziali per il lavoro e lo svago. Garantiamo a consumatori e dipendenti protezione dei dati e connessioni sicure nel rispetto della privacy e della fiducia riposta. Lookout è utilizzato da milioni di consumatori, dalle più grandi aziende ed enti governativi e da partner come AT&T, Verizon, Vodafone, Microsoft, Google e Apple. Con sede a San Francisco, Lookout ha uffici ad Amsterdam, Boston, Londra, Sydney, Tokyo, Toronto e Washington D.C. Per ulteriori informazioni, visita il sito web **www.lookout.com** e segui Lookout sul **blog**, su **LinkedIn** e su **Twitter.**

Per ulteriori informazioni, visita il sito

lookout.com

Per saperne di più su Lookout CASB, visita il sito

lookout.com/products/cloud-access-security-broker