Proofpoint Cloud App Security Broker IaaS Protection

Identificazione dei servizi cloud configurati in modo errato e protezione dei dati sensibili negli archivi IaaS

SFIDE

- Errori di configurazione
- Risorse e account IaaS sconosciuti
- Perdita di dati e conformità
- Takeover degli account cloud

PRINCIPALI FUNZIONALITÀ

- Sicurezza multicloud e conformità semplificate grazie a una gestione centralizzata di tutte le risorse IaaS, indipendentemente dal vendor, dall'account a dalla regione
- Identificazione di impostazioni di sicurezza configurate in modo errato che si discostano dagli standard pubblicati
- Monitoraggio e analisi del comportamento degli utenti per rilevare e bloccare le connessioni e le attività amministrative non autorizzate
- Protezione dei dati sensibili negli archivi IaaS
- Individuazione e gestione di account IaaS non approvati
- Distribuzione rapida nel cloud

PRODOTTI

- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint CASB IaaS Protection

L'adozione del cloud sta accelerando. Scegliendo di implementare le applicazioni SaaS per migliorare l'agilità, la flessibilità e la scalabilità, i team aziendali e IT hanno aperto la strada ai team DevOps. Sono sempre più numerosi i team DevOps che stanno sviluppano nuovi servizi e applicazioni su un'infrastruttura cloud.

La tua azienda può avere decine o addirittura centinaia di account IaaS i cui carichi di lavoro sono distribuiti su uno o più servizi cloud. Date le diverse normative sulla privacy, potrebbe essere necessario memorizzare i dati in repository cloud situati in diverse parti del mondo. La mancanza di visibilità sulle vulnerabilità della tua sicurezza cloud può rendere complesso mantenere la sicurezza e la conformità in ambito IaaS. Inoltre, le minacce cloud come la violazione degli account e la carenza di personale qualificato possono aumentare la complessità.

Gli errori di configurazione, di gestione o di altro tipo da parte dei clienti possono portare a violazioni su larga scala. Gli attacchi contro i servizi cloud come Amazon Web Services (AWS), Microsoft Azure o Google Cloud (GCP) possono essere dovuti a questo tipo di errori. I responsabili della sicurezza e del rischio devono identificare e mitigare questi rischi. Inoltre, gli account IaaS, le risorse e i dati sensibili memorizzati nel cloud, come le informazioni sui clienti o le cartelle cliniche dei pazienti, devono essere protetti.

Per proteggere i tuoi ambienti IaaS e garantire la conformità, Proofpoint CASB IaaS Protection (IaaS Protection) offre le seguenti funzionalità:

- Individuazione delle risorse IaaS
- Gestione del livello di sicurezza del cloud
- Sicurezza dei dati
- Protezione contro le minacce
- Controlli adattivi degli accessi

Proofpoint IaaS Protection è un modulo aggiuntivo di Proofpoint CASB.

Identificazione degli errori di configurazione negli ambienti IaaS

IaaS Protection ti aiuta a gestire il livello di sicurezza nel tuo ambiente multicloud. Questa funzionalità di Proofpoint CASB identifica le configurazioni e le impostazioni che si discostano dagli standard pubblicati nei servizi IaaS. Ad esempio, può trattarsi di impostazioni come un account utente "root" che non applica l'autenticazione a più fattori. IaaS Protection valuta le impostazioni relative alle tue macchine virtuali, allo storage, alla rete e al controllo degli accessi in base ai seguenti standard di sicurezza.

- CIS Foundations
- PCI DSS
- ISO 27001
- SOC TSP

Quando identifica delle configurazioni errate che rappresentano un rischio per la sicurezza, raccomanda le best practice per correggerle.

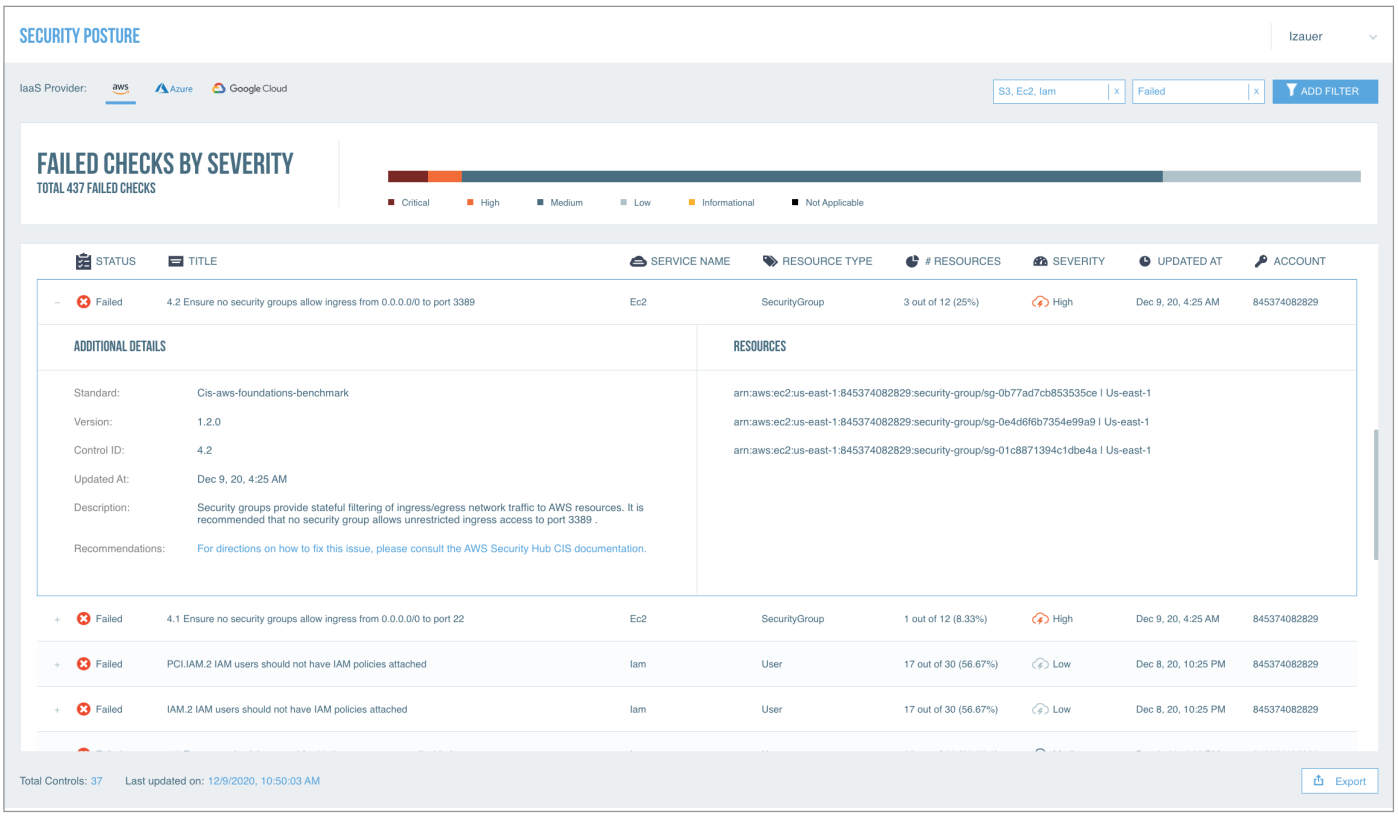

Figura 1: dashboard sul livello di sicurezza che mostra una configurazione errata, le istruzioni su come rispettare gli standard di sicurezza e un elenco di risorse che non soddisfano gli standard.

Monitoraggio e controllo delle attività degli utenti con privilegi

A differenza delle applicazioni SaaS, la maggior parte degli utenti IaaS sono utenti con privilegi, come gli ingegneri DevOps o gli sviluppatori di software. Possono distribuire, rimuovere e configurare risorse IaaS come macchine virtuali e storage cloud. Possono inoltre assegnare privilegi amministrativi. Per questo motivo è essenziale monitorare le attività degli utenti con privilegi.

Proofpoint CASB con IaaS Protection consente di definire policy incentrate sulle persone (Figura 2). Tali policy si basano su un contesto arricchito e ti avvisano in caso di attività non autorizzate da parte di un utente con privilegi. Il contesto fornisce, tra l'altro, informazioni sui rischi associati alle attività dell'utente, alla sua posizione, al dispositivo e alla rete. Fornisce anche informazioni sull'applicazione cloud a cui l'utente sta cercando di accedere. Per esempio, è possibile prevenire attività amministrative come la modifica delle autorizzazioni legate ai bucket da parte di paesi inseriti in una lista di blocco.

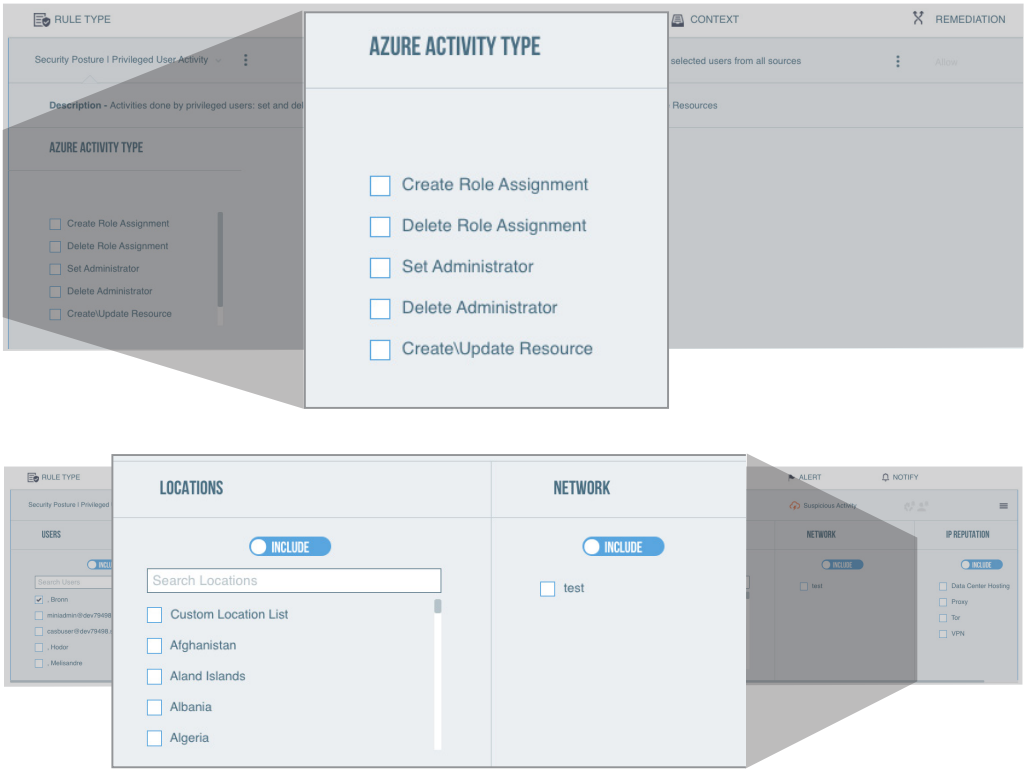

Figura 2: modello di policy per le attività degli utenti con privilegi.

Individuazione delle risorse IaaS

Proofpoint CASB consente di semplificare la sicurezza e la conformità IaaS multicloud e multi-regione grazie alla gestione centralizzata. Inoltre, ottieni visibilità su tutte le applicazioni SaaS e le risorse IaaS, indipendentemente dal fornitore, dall'account o dalla regione (Figura 3).

È possibile visualizzare i trend relativi alla creazione delle risorse e cercare anomalie come la creazione o la cancellazione eccessiva di risorse. Puoi anche esplorare le risorse individuate per tipo e regione e assicurarti che gli account siano distribuiti in conformità con le normative e le best practice. Ad esempio, se la tua è una multinazionale o un'azienda europea, puoi monitorare i bucket distribuiti al di fuori dell'Unione Europea per prevenire le violazioni al GDPR.

Individuazione degli account IaaS non approvati

Proofpoint CASB ti offre visibilità sulle applicazioni non approvate (Shadow IT) in tutta l'azienda. Sono inclusi gli account IaaS che non sono stati approvati o documentati dal team IT (Figura 4). Ti aiutiamo a controllare i registri del traffico di rete. Puoi inoltre individuare quali applicazioni cloud e account IaaS sono stati utilizzati sulla tua rete. Possono essere account IaaS approvati dall'IT, non documentati o anche privati. La console CASB permette di monitorare direttamente lo stato degli account durante la revisione di quelli non approvati. Per esempio, se individui degli account non documentati dopo una fusione, puoi attivarli in base a specifici criteri di sicurezza per garantire la conformità.

Figura 3: dashboard di individuazione delle risorse IaaS che mostra le tendenze, le posizioni e i tipi di risorse.

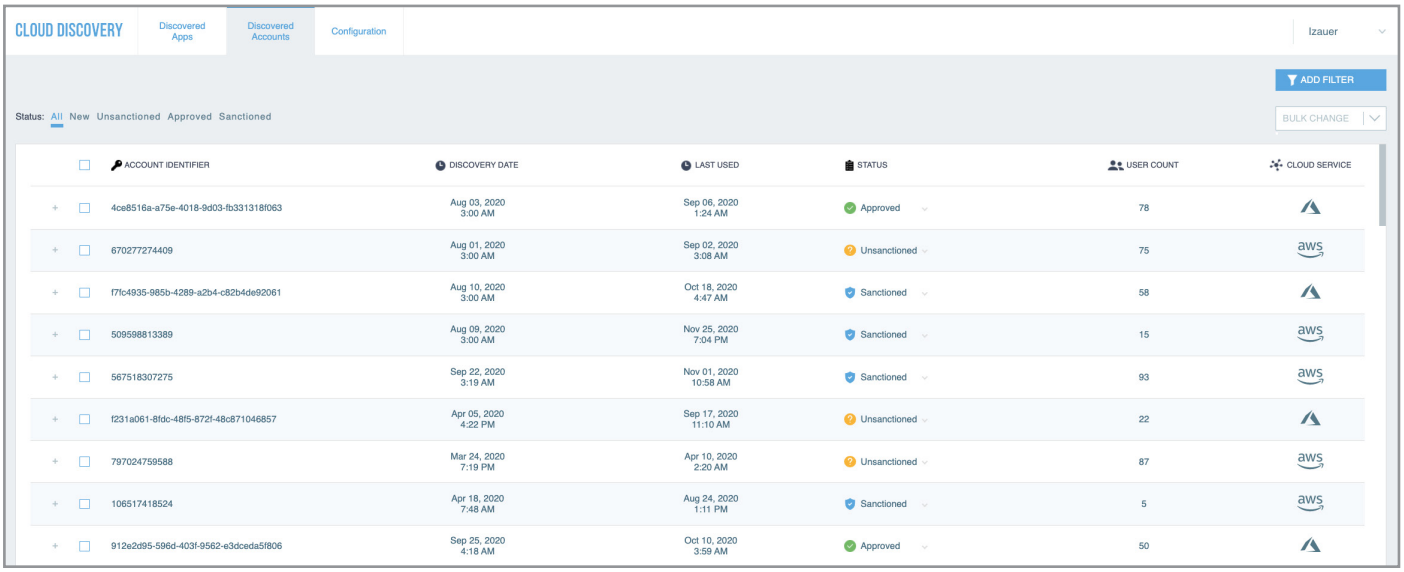

Figura 4: dashboard che mostra lo stato degli account IaaS individuati sulla rete aziendale.

Protezione dei dati sensibili negli archivi cloud

Proofpoint CASB con IaaS Protection consente di identificare e classificare i dati sensibili memorizzati nei tuoi repository di storage cloud, come i bucket AWS S3 e i container Azure Storage Blob. Offre anche le seguenti funzionalità:

- Monitoraggio delle attività dei file per rilevare le violazioni alle policy DLP
- Monitoraggio dei bucket e dei container per rilevare un'eccessiva condivisione
- Creazione di policy di sicurezza dei dati basate su classificatori DLP, inclusi identificatori intelligenti, dizionari, regole e modelli condivisi con altri prodotti DLP Proofpoint

I nostri classificatori predefiniti consentono di ridurre il tempo necessario per individuare e proteggere i dati regolamentati archiviati in cloud e ti aiutano a mantenere la conformità. Come parte della soluzione Proofpoint Enterprise DLP, il nostro modulo CASB ti permette di implementare policy DLP coerenti ad applicazioni SaaS, bucket IaaS, email ed endpoint. Allo stesso modo, ti consente di gestire centralmente gli incidenti DLP per questi canali da un'unica console. Combinando i dati di analisi del contenuto, del comportamento e delle minacce su più canali, puoi stabilire se l'utente che ha attivato l'allarme DLP è stato vittima di una violazione, ha delle intenzioni dolose o è semplicemente negligente.

Funzionalità DLP di Proofpoint CASB:

- 240 classificatori integrati che coprono le normative PCI, sui dati personali e sui dati sanitari e la normativa GDPR
- Dizionari e funzioni di corrispondenza della prossimità per migliorare la prevenzione della perdita di dati
- Corrispondenze esatte dei dati permettono di automatizzare il caricamento di dizionari o identificatori personalizzati al fine di rilevare informazioni specifiche per la tua azienda, come per esempio i numeri di conto e altri dati strutturati provenienti da database
- Analisi dell'impronta digitale dei documenti per rilevare i dati sensibili all'interno di contenuto non strutturato, tra cui formule, codici sorgente, moduli, contratti e altra proprietà intellettuale
- Supporto per 300 tipi di file e strumenti di profilazione dei tipi di file per supportare tipi di file nuovi, personalizzati e proprietari

I modelli di regole flessibili permettono di definire policy relative a contenuto, comportamento dell'utente e tipo di minaccia (Figura 5). In questo modo è possibile controllare come i dati vengono condivisi, caricati e scaricati. Puoi limitare automaticamente i permessi di condivisione per i bucket al fine di garantire la conformità. Per esempio, puoi monitorare la condivisione dei bucket e proibire la condivisione eccessiva degli stessi provenienti da paesi presenti in una lista di blocco.

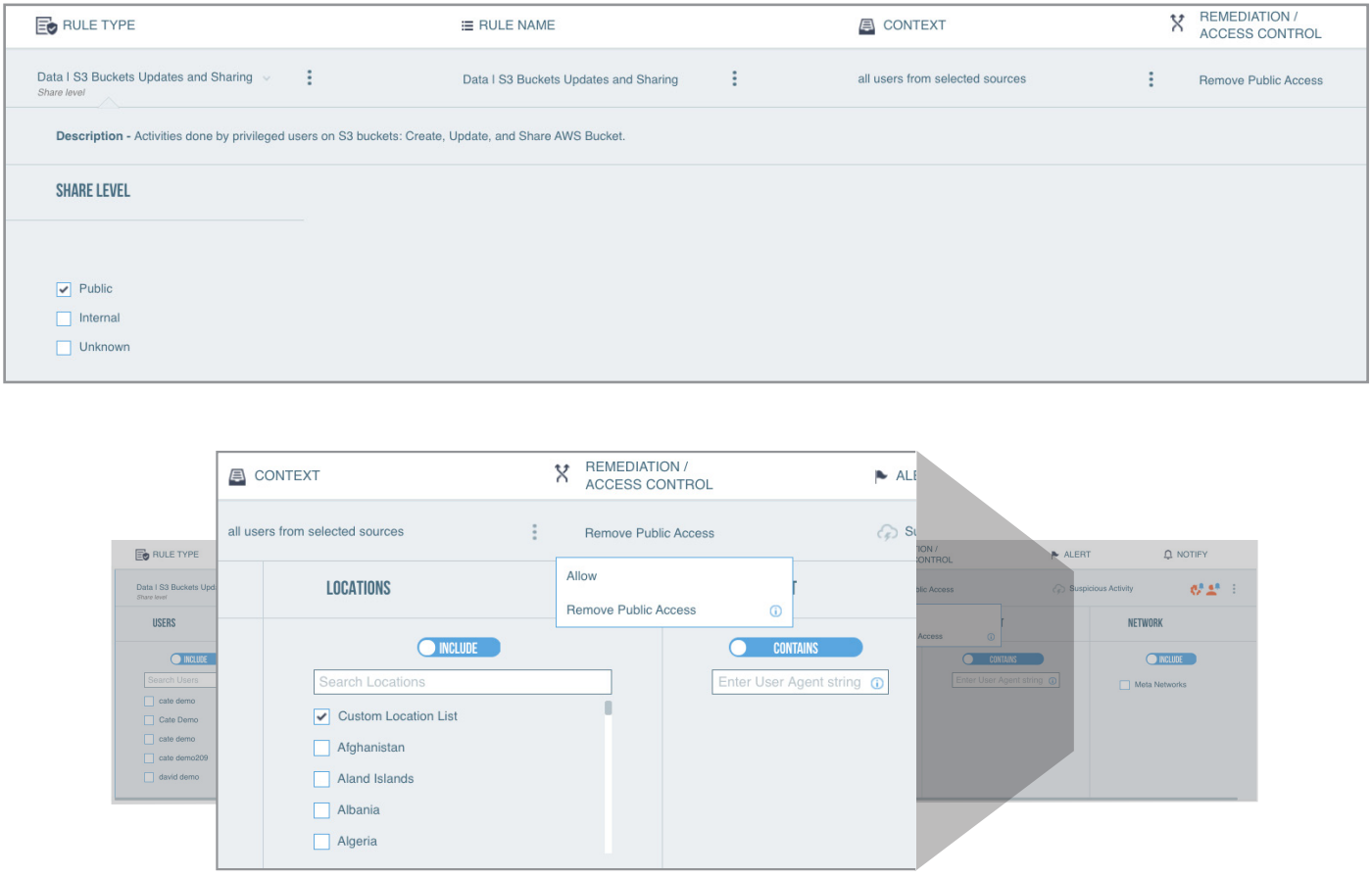

Figura 5: modello di policy per il monitoraggio delle autorizzazioni alla condivisione di bucket/container.

La soluzione facilita anche le indagini sugli incidenti DLP. Puoi correlare accessi sospetti o bucket configurati in modo errato con gli incidenti DLP. Inoltre, puoi filtrare gli eventi e gli avvisi per generare dei report e monitorare attentamente la conformità abbonandoti agli avvisi.

Controlli adattivi degli accessi e protezione contro le minacce

La console di gestione IaaS è un'applicazione web utilizzata per creare e gestire le risorse cloud. Le aziende devono monitorare e controllare l'accesso a questo potente strumento. I controlli adattivi degli accessi di Proofpoint CASB permettono di valutare in tempo reale la sicurezza in base al livello di rischio, al contesto e al ruolo. Questo permette di:

- Proteggere il tuo ambiente IaaS definendo policy per bloccare l'accesso da posizioni e reti a rischio e da parte dei criminali informatici.
- Applicare controlli basati sui rischi a utenti con un elevato livello di rischio e con privilegi elevati, tra cui autenticazione rafforzata, policy per gli endpoint gestiti e l'implementazione di reti private virtuali (VPN).

Proofpoint CASB sfrutta informazioni di threat intelligence complete raccolte da più vettori (cloud, email e altro) e sintetizzate nel grafico delle minacce Proofpoint Nexus, che combina con i dati contestuali specifici degli utenti. Applichiamo a questi dati algoritmi di machine learning per eseguire un'analisi comportamentale e rilevare le anomalie in tutti i servizi e i tenant cloud. Ti aiutiamo a:

- Rilevare le violazioni degli account cloud.
- Analizzare le attività e gli avvisi passati, inclusi gli accessi sospetti ai tuoi servizi IaaS federati.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita **proofpoint.com/it**.