Soluzioni Proofpoint e Amazon Web Services:

Come Proofpoint fornisce ai clienti di AWS sicurezza e conformità incentrate sulle persone

Prodotti

- Controlli adattivi degli accessi
- Proofpoint Cloud App Security Broker
- Gestione del livello di sicurezza del cloud
- Proofpoint Email Fraud Defense
- Proofpoint Emerging Threats Intelligence
- Proofpoint Enterprise Data Loss Prevention
- Proofpoint Insider Threat Management
- Proofpoint Threat Response Auto-Pull
- Proofpoint Zero Trust Network Access

Vantaggi principali

- Semplificazione della sicurezza e della conformità di AWS in più regioni grazie alla gestione centralizzata
- Identificazione e classificazione dei dati sensibili negli archivi cloud
- Blocco degli accessi sospetti per impedire che assumano il controllo degli account delle risorse di AWS
- Visibilità sulle attività degli utenti e degli spostamenti dei dati nelle istanze AWS EC2 e Amazon WorkSpaces
- Accesso remoto sicuro per il tuo team
- Quarantena automatica delle email dannose che aggirano le difese perimetrali

Le piattaforme cloud come Amazon Web Services (AWS) hanno trasformato il modo di lavorare delle imprese. Permettono ai dipendenti di lavorare in remoto nel cloud e alle aziende di ridurre i costi, aumentare l'agilità e accelerare l'innovazione. In risposta, i criminali informatici hanno spostato la loro attenzione dal vecchio perimetro della rete alle persone, ai dati, ai sistemi e alle risorse a cui hanno accesso. In questo panorama mutevole, è necessario proteggere l'accesso alle risorse AWS, prevenire le perdite dei dati e mantenere la conformità. La gamma di prodotti Proofpoint ti aiuta a raggiungere questi obiettivi.

Le nostre soluzioni ti aiutano ad affrontare i seguenti problemi:

- Applicazioni non approvate (Shadow IT)
- Account compromessi
- Violazioni della conformità
- Spoofing delle email
- Accessi non autorizzati
- Perdita ed esfiltrazione dei dati
- Minacce interne
- Attività di rete sospette

Identificazione delle risorse e degli account di AWS

Proofpoint Cloud App Security Broker (CASB) combina controlli incentrati sulle persone con il rilevamento degli account cloud compromessi, la prevenzione delle perdite di dati (DLP) e la gestione di applicazioni cloud e di terze parti. Ti aiuta a proteggere le piattaforme cloud come AWS, mentre la soluzione CASB multimodale supporta i modelli di distribuzione basati su API e proxy.

Proofpoint CASB semplifica la sicurezza e la conformità AWS in più regioni grazie alla gestione centralizzata. Ottieni visibilità su tutte le tue applicazioni SaaS (Software-as-a-Service) e sulle risorse IaaS (Infrastructure-as-a-Service) in AWS.

La nostra soluzione ti permette di:

- Visualizzare le tendenze relative alla creazione delle risorse. Cercare le anomalie, come le attività di creazione o cancellazione eccessive di risorse
- Esplorare le risorse scoperte e assicurarti che gli account siano commissionati in conformità con le normative e le best practice
- Verificare i registri del traffico di rete e identificare le applicazioni cloud e gli account AWS che accedono alla tua rete

Prevenzione delle minacce nel cloud

I controlli degli accessi adattivi di Proofpoint CASB permettono di valutare in tempo reale la sicurezza in base al livello di rischio, al contesto e al ruolo. Bloccano automaticamente l'accesso ai criminali informatici noti o da località e reti pericolose e applicano i controlli basati sul rischio agli utenti che hanno un rischio e privilegi elevati. I controlli basati sul rischio includono un'autenticazione rafforzata, policy per i dispositivi gestiti e implementazione delle reti private virtuali (VPN).

I controlli degli accessi adattivi bloccano le connessioni sospette, impedendo che qualcuno assuma il controllo delle tue risorse AWS.

Questi controlli ti permettono di:

- Bloccare l'accesso agli account degli utenti più attaccati da connessioni sospette
- Creare un elenco di blocco dei paesi in cui la tua azienda non è presente.

Identificazione dei servizi mal configurati

Proofpoint CASB include la gestione del livello di sicurezza cloud, permettendoti di gestire il livello di sicurezza nel tuo ambiente cloud. Puoi così organizzare, configurare e mantenere le tue risorse nel cloud per rispettare meglio gli standard di conformità.

La nostra soluzione ti permette di:

- Identificare le configurazioni e le impostazioni che si discostano dagli standard pubblicati
- Raccomandare le best practice per correggere i problemi di configurazione identificati che rappresentano un rischio per la sicurezza
- Semplificare la sicurezza e la conformità cloud grazie alla gestione centralizzata delle risorse cloud, indipendentemente dall'account e dalla regione.

Protezione dei dati sensibili

Proofpoint Enterprise Data Loss Prevention (DLP) combina le nostre soluzioni DLP per l'email, il cloud e gli endpoint. Combina i dati di analisi dei contenuti, dei comportamenti e delle minacce provenienti da questi canali. Questo ti permette di affrontare tutti gli scenari di perdita di dati incentrati sulle persone.

Proofpoint Enterprise DLP ti aiuta a identificare i dati sensibili e a classificarli nei repository di archivi cloud.

Proofpoint Enterprise DLP ti permette di:

- Monitorare le attività dei file per rilevare le violazioni alle policy DLP
- Monitorare i bucket S3 per prevenire le condivisioni eccessive
- Creare policy di sicurezza per i dati. Questa soluzione integra 240 classificatori DLP, inclusi identificatori intelligenti integrati, dizionari, regole e modelli condivisi con gli altri prodotti DLP Proofpoint.

Protezione degli account AWS

Amazon GuardDuty sfrutta Proofpoint Emerging Threats (ET) Intelligence per proteggere le istanze di AWS.

Proofpoint ET Intelligence è la fonte di informazioni sulle minacce più tempestiva e accurata del settore. Combina un database delle minacce osservate in tutto il mondo, l'analisi del malware, i feed aggiornati sulla reputazione degli IP e dei domini in tempo quasi reale. Questa soluzione fornisce ai tuoi team della sicurezza le informazioni e il contesto necessari per indagare e neutralizzare gli attacchi.

Forniamo prodotti e soluzioni di nuova generazione per sicurezza, conformità, la gestione del rischio digitale e la risposta agli incidenti. Le nostre informazioni sulla reputazione degli indirizzi IP e dei domini si basano su una delle gamme più complete di tecnologie di protezione, che spazia da email, dispositivi mobili, social network, servizi SaaS e ambienti di rete.

Gestione delle minacce interne

Proofpoint ITM fa parte della piattaforma Proofpoint Information and Cloud Security. TI protegge contro perdite di dati, atti dolosi e danni al marchio di origine interna. Proofpoint ITM ti protegge dagli utenti autorizzati che potrebbero essere malintenzionati o negligenti. Inoltre, la soluzione correla le attività degli utenti con gli spostamenti dei dati, per proteggere dalle violazioni dei dati perpetrate da utenti interne.

Proofpoint ITM offre visibilità sulle attività degli utenti e sugli spostamenti dei dati nelle istanze AWS EC2 e Amazon WorkSpaces.

Proofpoint ITM ti permette di:

- Ottenere piena visibilità sulle attività degli endpoint. Ottenere informazioni contestuali complete sugli incidenti imputabili agli utenti
- Visualizzare il contesto delle minacce riguardanti gruppi di utenti specifici per gestire meglio i rischi legati agli utenti

Accesso remoto sicuro alle applicazioni cloud

Proofpoint Zero Trust Network Access (ZTNA) è un'alternativa Zero Trust e incentrata sulle persone. Protegge l'accesso remoto a qualsiasi applicazione aziendale, indipendentemente dalla sua posizione. Proofpoint ZTNA offre agli utenti un accesso sicuro microsegmentato a centinaia di istanze cloud. Puoi automatizzare la connettività da un cloud all'altro e autorizzare il networking di cloud ibrido fra i server on premise e i cloud pubblici.

Proofpoint ZTNA offre a dipendenti, collaboratori, partner e clienti un accesso remoto sicuro alle applicazioni ospitate su AWS.

La nostra soluzione ti permette di:

- Gestire le policy di accesso remoto a tutte le risorse aziendali nel tuo data center o nel cloud da un'unica console
- Beneficiare di un'alternativa Zero Trust che offre un accesso segmentato, verificato e controllato a ogni utente.

Miglior affidabilità dell'email

Proofpoint Email Fraud Defense (EFD) protegge la tua azienda dalla frodi via email. Offre visibilità completa sui domini cugini e sulle email inviate tramite il tuo dominio. Inoltre, mitiga i rischi posti dai fornitori, identificando sia questi ultimi sia i domini cugini registrati da terzi.

Proofpoint EFD protegge le email provenienti da Amazon SES. Ti offre la visibilità, gli strumenti e i servizi necessari per autorizzare le email legittime.

Proofpoint EFD ti permette di:

- Correggere i sistemi di invio delle email che sono stati configurati in modo errato e i problemi di recapito dei messaggi dovuti agli errori di validazione dell'autenticazione dell'email
- Identificare e segnalare lo spoofing delle email
- Esporre i problemi legati alle firme DKIM e ai record SPF riscontrati dai destinatari delle email.

Quarantena automatica delle email dannose

AWS può ospitare l'appliance Proofpoint Threat Response Auto Pull (TRAP), che permette ai team della sicurezza di analizzare le email e rimuovere automaticamente i messaggi pericolosi. Mette in quarantena anche le email indesiderate, dopo il loro recapito nelle caselle email degli utenti.

Proofpoint TRAP semplifica la procedura di risposta agli incidenti legati all'email. Si tratta di una soluzione potente che permette di ridurre il tempo che i team dedicati alla sicurezza dedicano a ripulire l'email dai messaggi dannosi e indesiderati.

Proofpoint TRAP ti permette di:

- Monitorare automaticamente le caselle email
- Ridurre esponenzialmente il tempo che i team di sicurezza e di messaggistica dedicano all'orchestrazione della sicurezza dell'email e alla risposta agli incidenti
- Mettere in quarantena i messaggi inoltrati a singoli o liste di distribuzione

Per saperne di più sulla collaborazione fra Proofpoint e AWS, visita **proofpoint.com/us/partners/aws**.

PER SAPERNE DI PIÙ

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