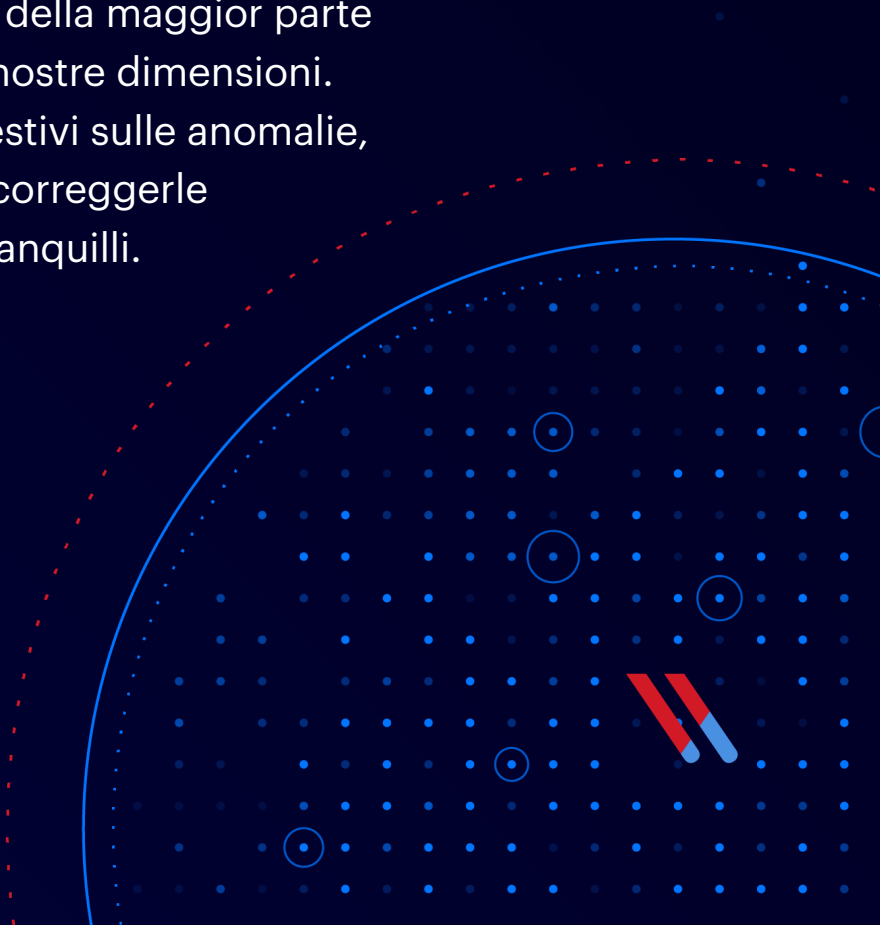
Come Varonis aiuta un'istituzione culturale statunitense a proteggersi dagli attacchi informatici

> Il nostro fattore rischio relativo alle minacce è 25 volte superiore a quello della maggior parte delle altre istituzioni delle nostre dimensioni. Varonis ci invia alert tempestivi sulle anomalie, in modo da consentirci di correggerle immediatamente e stare tranquilli.



Informazioni su questo caso di studio:

Il nostro cliente è un'istituzione culturale statunitense. Abbiamo accolto volentieri la loro richiesta di rendere anonimi tutti i nomi e i luoghi.

Highlight

Sfide

- Protezione dalle costanti minacce informatiche
- Miglioramento di un processo di audit dispendioso in termini di tempo
- Individuazione di una piattaforma di sicurezza per proteggere i dati nel cloud

La soluzione

La **Varonis Data Security Platform:**

- Offre visibilità e controllo completi sui dati critici in Google Drive, Zoom e Box
- Individua e classifica automaticamente i dati sensibili
- Ripara e mantiene le autorizzazioni del file system
- Monitora e rileva comportamenti anomali nei sistemi critici

Risultati

- 72% di riduzione di interruzione delle autorizzazioni
- Maggiore protezione dagli attacchi informatici
- Più visibilità sull'ecosistema SaaS

Sfide

Elevato livello di minacce da parte di attori esterni

Un'istituzione culturale statunitense vive sotto la costante minaccia di attacchi esterni. Con questo rischio in testa alle preoccupazioni, proteggere la privacy dei donatori è il compito più importante del team di sicurezza.

Il team di sicurezza ha sviluppato un processo di audit che contribuisce a individuare e difendere i dati sensibili. Ma rimaneva un problema: il processo era rigoroso e inefficiente. Un audit completo avrebbe richiesto settimane, tempo che il team di sicurezza non poteva permettersi di dedicare.

Abbiamo parlato con Michael Trofi, di Trofi Security, che da oltre 30 anni opera nel settore della sicurezza fornendo servizi di vCISO, SOC, audit e valutazione.

> **Non avevamo mai tempo sufficiente per eseguire correttamente l'audit, quindi abbiamo sempre temuto che qualcosa ci sfuggisse.**

Un data breach si è rivelato lo scenario peggiore. Se le informazioni personali dei donatori fossero esposte, potrebbero essere prese di mira dagli aggressori.

> **La cosa peggiore che potrebbe accadere è che trapeli un foglio di calcolo con le informazioni sui donatori.**

L'istituzione doveva sapere: qual era l'entità del rischio? Per rispondere a questa domanda e ottenere un rapporto reale sulla vulnerabilità dei dati, l'istituzione ha incaricato Varonis di effettuare un Data Risk Assessment gratuito.

VARONIS

I risultati sono stati sconfortanti: il cliente aveva un'enorme quantità di dati obsoleti nel cloud e on-prem e un numero allarmante di accessi aperti. I problemi erano più di quelli che lo snello team di sicurezza era in grado di gestire autonomamente.

> **Le scansioni di rilevamento durante un audit hanno mostrato che avevamo molte informazioni condivise. Sapevo che c'era un problema, ma era molto peggiore di quanto pensassi.**

Fortunatamente, Varonis porta la sicurezza automatizzata dei dati nei repository cloud, nelle app SaaS e nei data store on-prem, alleggerendo il peso delle attività del team di sicurezza in modo che possano stare al passo con dati e condivisioni in continua crescita.

> **Ho una cartella di alert Varonis in Outlook e la esamino ogni giorno per capire cosa sta accadendo nel mio ambiente.**

“Siamo sempre sotto minaccia. Riceviamo minacce pari a quelle delle principali agenzie governative”.

La soluzione

Protezione delle informazioni dei donatori

La **Varonis Data Security Platform** costituisce la base della Varonis Data Security Platform. Con questi prodotti, il team di sicurezza dell'istituto può osservare la reale portata dell'esposizione dei dati e ottenere un maggiore controllo sui dati critici nel cloud e on-prem.

Cosa dice il CISO:

> **Tendiamo ad affidarci sempre alle stesse procedure. Ma questo ci ha spinto a dar vita a nuove politiche sull'archiviazione dei dati per ridurre il rischio di perdita dei dati e ridurre al minimo l'impronta delle minacce.**

L'istituzione culturale ha anche implementato la classificazione dei dati per Windows e SharePoint per individuare e classificare i dati sensibili che potrebbero mettere a rischio i donatori.

Con Varonis, la remediation dei rischi è più rapida ed efficiente. Varonis ha permesso all'istituto di accelerare l'impegno di riduzione del rischio analizzando chi effettivamente necessita di accedere ai dati e rimuovendo l'accesso a tutti gli altri. Questo aiuta a controllare l'accesso ai dati sensibili e riduce drasticamente il danno potenziale che un attore malintenzionato potrebbe arrecare.

Estensione della protezione al cloud

Successivamente, il team di sicurezza ha lanciato **Varonis per Google Drive**. In soli 15 minuti, il team ha potuto vedere quali informazioni sensibili erano state salvate in Google Drive e come venivano condivise.

Ciò ha consentito al team di sicurezza una visibilità molto superiore alla precedente. E la visibilità ha portato con sé nuove sorprese, secondo il CISO:

> **Abbiamo scoperto che una buona percentuale del personale condivideva cartelle personali con le proprie e-mail personali. Quando un dipendente se ne va, disattiviamo i suoi account, ma il dipendente continuava comunque ad avere accesso ai propri dati. È stato illuminante.**

Era un problema enorme, di cui il team IT non era a conoscenza. Il team è entrato in azione, creando nuovi criteri di conservazione dei dati e configurando unità condivise con una sicurezza più rigorosa. Hanno anche istruito nuovamente tutto il personale IT illustrando le migliori pratiche da adottare.

Oltre a **Varonis per Google Drive**, l'istituzione culturale ha anche adottato **Varonis per Box** e **Zoom**. Queste aggiunte contribuiranno a proteggere la riservatezza dei dati, eliminare l'esposizione e accelerare le indagini su più cloud.

Alert in tempo reale su tutti i dati, sempre

Dopo il blocco dell'accesso ai dati, restava un problema da affrontare: rilevare le minacce esterne.

L'istituzione culturale doveva sapere quando il comportamento degli utenti metteva a rischio i dati. E doveva avere la capacità di bloccare gli attacchi dannosi in tempo reale. È qui che entra in gioco Varonis.

> **La perdita di dati mi teneva sveglio la notte. Gli utenti tendono a fare clic su molte e-mail e messaggi dannosi. Ma Varonis rileva le firme ransomware e le chiude automaticamente.**

“Non avevamo idea di chi stesse condividendo e cosa stesse condividendo su Google. Varonis ha classificato i nostri dati, consentendoci una visibilità che prima non avevamo”.

Risultati

Un'istituzione culturale è libera di continuare il suo importante lavoro

Oggi, le condivisioni di file dell'istituzione culturale sono più sicure e richiedono molta meno manutenzione manuale. Gli audit, che prima richiedevano settimane, vengono ora completati con un clic e le autorizzazioni per la pulizia sono altrettanto semplici.

Varonis ha aiutato il CISO e il suo team di sicurezza a individuare in modo proattivo i rischi e successivamente a implementare misure per formare altro personale a prestare maggiore attenzione alla sicurezza nelle comunicazioni online e nella condivisione di file. L'impegno è stato premiato con un notevole calo degli alert, secondo il parere del CISO:

> **Ora individuiamo i dati nel cloud e on-prem per capire dove avviene la trasmissione dei dati PII o dove vengono archiviati, in modo da poter seguire le migliori pratiche relative alla privacy dei dati.**

Quando il CISO ha eseguito un test di penetrazione, il Blue Team (che simulava un team di sicurezza difensivo) ha utilizzato Varonis per rilevare e interrompere tutte le possibili minacce del Red Team (che simulava hacker malintenzionati).

> **Abbiamo condotto un test di penetrazione e rilevato tutto ciò che abbiamo testato. Questo ha confermato che le nostre difese informatiche funzionano.**

Anche nel peggiore dei casi, un'igiene dei dati dell'istituzione culturale efficace ha ridotto al minimo il blast radius di qualsiasi attacco. È stato ridotto il numero di cartelle con dati obsoleti del 54% e il numero di utenti obsoleti del 44% in soli sette mesi.

Nello stesso lasso di tempo, è stato anche ridotto del 72% il numero di cartelle con autorizzazioni interrotte.

Oggi il CISO è soddisfatto del lavoro svolto per proteggere questa importante istituzione culturale.

> **La maggior parte dei responsabili della sicurezza ritiene che se l'azienda non ha subito violazioni o perso dati sia tutto a posto. Ma in realtà non è così.**

“Varonis rivela i punti deboli nella sicurezza che prima non pensavi di avere. E non puoi risolvere i problemi se non li si conosci.”

VARONIS

Individua e correggi i punti deboli della sicurezza dei dati.

Richiedi una demo