VARONIS

Combattiamo una battaglia diversa

L'approccio unico di Varonis alla cybersecurity

Introduzione

Man mano che le organizzazioni si incentrano sempre più sui dati, archiviano on-prem e su cloud una quantità sempre maggiore di dati, ai quali i dipendenti possono accedere ovunque tramite telefoni, tablet e laptop. Il perimetro di sicurezza è sempre meno definito e gli endpoint sono intercambiabili: al giorno d'oggi sono pochissimi i dati che "abitano" solo sul telefono o sul computer.

Questa trasformazione digitale ha ribaltato il modello di sicurezza tradizionale focalizzato su perimetro ed endpoint. Invece di adottare un approccio dall'esterno, le organizzazioni hanno iniziato a pensare a una sicurezza dall'interno che metta al primo posto i dati.

La protezione dei dati a livello intuitivo è semplice, ma allo stesso tempo è infinitamente complessa.

Perché la protezione dei dati è semplice a livello intuitivo?

Possiamo dire che se sei in grado di rispondere "sì" a queste tre domande, e di farlo in modo continuativo nel tempo, allora i tuoi dati sono al sicuro:

1. Sai **dove sono archiviati i tuoi dati più importanti?**
2. Hai la certezza **che solo le persone giuste vi abbiano accesso?**
3. Hai la certezza **che queste persone stiano usando i dati in modo corretto?**

Facile, vero?

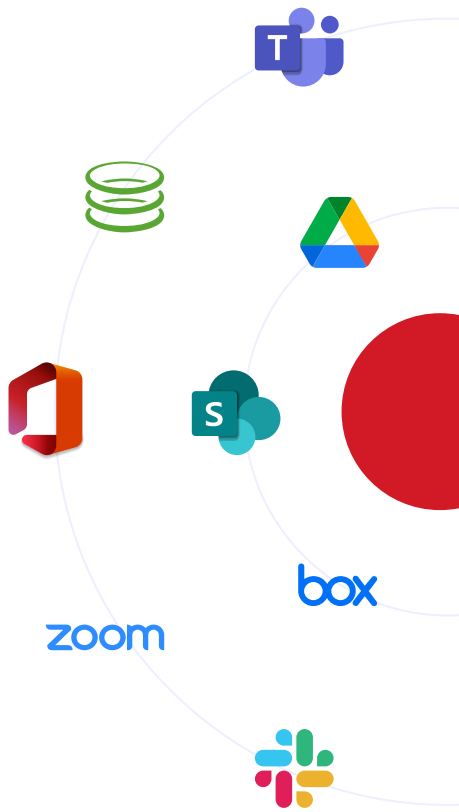
Queste sono le tre dimensioni fondamentali della sicurezza dei dati: importanza, accessibilità e utilizzo. Se lavori nell'IT o nella sicurezza IT, saprai che comprendere veramente queste dimensioni non è affatto semplice.

Forse saprai anche che se non sei in grado di rispondere "sì" a queste domande, o se non hai nessuna risposta, si aprono altre domande che comportano ramificazioni urgenti per i CISO, il personale addetto alla conformità, la dirigenza e gli azionisti:

- Dove si trovano i nostri dati sensibili e regolamentati?
- Dove sono troppo accessibili e più a rischio?
- Qual è la portata dei danni per un account o un dipendente compromesso?
- Come facciamo a sapere se i dati sono stati rubati, crittografati o eliminati?
- Possiamo eliminare il rischio?

Con l'aumento dei dati on-prem e su cloud in applicazioni e data store che adottano i propri modelli di sicurezza individuali, rispondere a queste domande non è certo facile. È già abbastanza difficile riuscire a proteggere i dati in un'unica piattaforma aziendale, figuriamoci quando ce ne sono diverse.

Dove dovrebbero essere i nostri dati?



Il numero di posizioni in cui è possibile archiviare i dati è letteralmente esploso negli ultimi anni, ed è normale che gli utenti vi accedano da diversi dispositivi ed endpoint. Gli endpoint ora servono principalmente da punti di accesso alle posizioni in cui i dati "abitano" veramente, di solito un'applicazione cloud.

La maggior parte delle organizzazioni ora si affida a una combinazione di applicazioni cloud e infrastruttura che si aggiungono a quella locale. Ormai è frequente che venga approvato l'uso dei cloud Microsoft 365, Box, di Google Drive o Slack per le collaborazioni, di GitHub o Jira per il codice sorgente, di AWS, Azure o Google Cloud per l'elaborazione o l'archiviazione, o di una soluzione CRM come Salesforce.com.

E i dati importanti dove si trovano?

Nel vasto panorama di queste applicazioni autorizzate, la superficie è larga e difficile da visualizzare e quantificare in termini di rischio. Alcune organizzazioni scelgono di concentrare i propri sforzi chiedendo ai dipendenti di taggare i file o utilizzando l'automazione per identificare o classificare i dati regolamentati o sensibili, nella speranza di riuscire a dare priorità alle iniziative di protezione dei dati.

Sicuramente è sensato suddividere un problema enorme in tante parti più piccole, ma il problema è diventato talmente vasto che anche i frammenti più piccoli possono causare danni enormi.

La maggior parte delle organizzazioni rimane sorpresa dal numero di file e record sensibili che vengono individuati. Migliaia di file di qua, decine di migliaia di là, e l'elenco cambierà domani, poi il giorno dopo, e via dicendo.

Chi arriva a questo punto senza un piano d'azione chiaro potrebbe non sapere cosa fare. Alcuni adottano un approccio di forza bruta, come spostare tutto quello che trovano in un'altra posizione, ad esempio un archivio locale, eliminando tutto ciò che riescono o crittografando tutto, limitando il materiale trovato ai dipendenti o a un gruppo ristretto che si trova fra le mani un problema vastissimo.

Tuttavia, così facendo non si risolve il problema di base: assicurare che i dati siano accessibili solo alle persone giuste, un principio conosciuto anche come privilegio minimo o, oggi più comune, come Zero Trust.

Per essere sicuri che gli accessi ai dati, sensibili o meno, siano corretti, è prima necessario riuscire a vedere chi vi ha accesso. Questa operazione di solito è molto più difficile di quanto si pensi, specialmente su cloud.

Chi ha accesso ai nostri dati più importanti? Chi *dovrebbe* avere accesso?

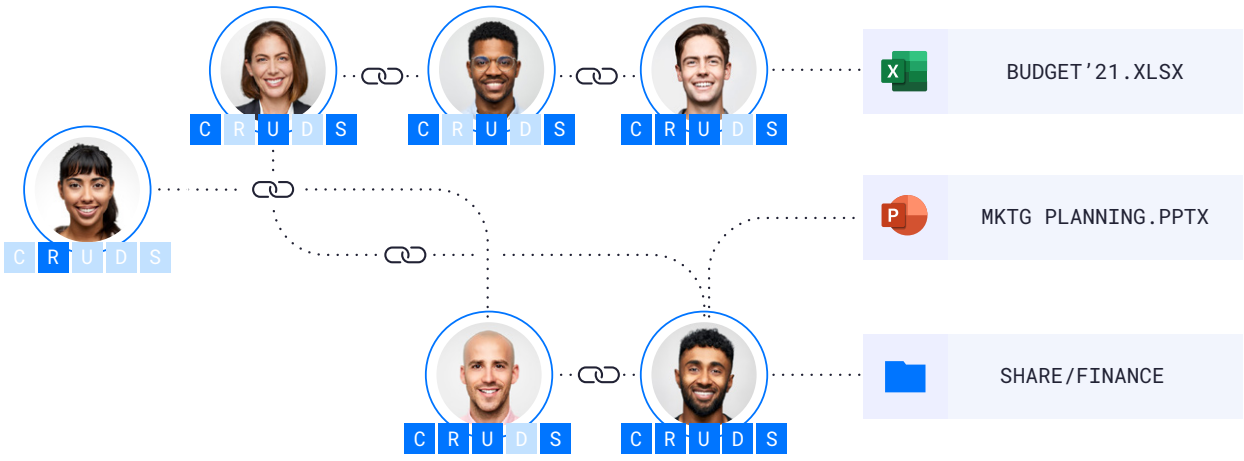
Se non si capisce quali dati sono regolamentati o sensibili, non sorprende che le decisioni su chi debba avere accesso siano state prese senza tenere conto di un contesto molto importante. Ciò che invece spesso sorprende è quanto sia difficile vedere chi vi ha accesso.

L'accesso ai dati viene gestito tramite autorizzazioni, o liste di controllo degli accessi. La logica è piuttosto uniforme nei vari data store e applicazioni:

- C'è un **oggetto,** come un file, una cartella o un record.
- Ci sono le **identità digitali** che corrispondono a utenti, account e gruppi di utenti o account che possono svolgere azioni con questi oggetti.
- C'è una **descrizione delle azioni che possono svolgere,** come creare, condividere, eliminare ecc.

Anche se la logica è grossomodo la stessa, che si tratti di file di sistema Slack, Box, SharePoint Online o locale oppure di UNIX, le implementazioni sono tutte diverse:

- Gli oggetti sono simili, ma esistono tipi di oggetti diversi a seconda dell'applicazione (es. file, siti, record, bucket).
- Gli utenti/account e gruppi sono archiviati in luoghi diversi. Su cloud, ogni data store solitamente dispone del suo database di utenti e gruppi. A volte, questi si connettono ad altri account (come un account Okta), a volte ci sono sia account personali che aziendali da monitorare. Tutte queste applicazioni possono assegnare attributi agli oggetti utente e gruppo, come titolo, ruolo e posizione.



Quello che possono fare è descritto in maniera diversa in ciascuna applicazione, anche se in linea generale si tratta di creare, leggere, aggiornare, eliminare e condividere.

Oltre a queste differenze, calcolare i diritti effettivi per un dato oggetto o utente può essere molto difficile, e cambia notevolmente da un archivio all'altro. Per determinare i diritti su un determinato oggetto, bisogna considerare diversi attributi, fra cui:

- **Autorizzazioni specifiche per oggetto.** Come già detto, ogni oggetto dispone di una lista di controllo degli accessi in cui sono elencati utenti, gruppi o ruoli. La gamma di possibilità è ampia: nelle autorizzazioni base UNIX, ad esempio, esistono 3 tipi diversi di autorizzazione (lettura, scrittura e esecuzione) per 3 tipi di utente/gruppo (root, proprietario, gruppo). Su SharePoint Online, esistono 33 tipi diversi di autorizzazione, raggruppati in 7 livelli predefiniti (ma se ne possono aggiungere altri), e questi livelli di autorizzazione possono essere assegnati a **diversi** utenti e gruppi sugli oggetti.
- **Relazioni tra gruppi.** I gruppi possono contenere utenti o altri gruppi "nidificati". Per determinare le autorizzazioni effettive per un oggetto o utente, è necessario calcolare queste relazioni. In alcuni casi, i gruppi di un servizio di directory possono riferirsi a utenti e gruppi in altri servizi di directory, il che rende questo calcolo ancora più complesso. Ad esempio, SharePoint Online dispone di gruppi locali che possono contenere utenti e gruppi di Azure AD.
- **Ereditarietà gerarchica.** In molti data store, le autorizzazioni vengono trasmesse dall'alto verso il basso seguendo la gerarchia, quindi tutti gli oggetti all'interno di una cartella "erediteranno" le voci di controllo degli accessi dalle cartelle superiori. Alcuni archivi permettono di interrompere l'ereditarietà sugli oggetti secondari, ma non è così per tutti. Box, per esempio, permette solo di aggiungere voci di controllo degli accessi agli oggetti secondari, per cui un oggetto secondario non avrà mai meno autorizzazioni dell'oggetto superiore.
- **Ruoli e gerarchie dei ruoli.** L'accesso può essere garantito agli oggetti in base a un ruolo. I ruoli possono a loro volta contenere altri ruoli e sono assegnati in maniera diversa su applicazioni diverse. Ad esempio, su AWS i ruoli vengono solitamente assunti a seconda delle necessità, mentre su Salesforce la loro assegnazione è più statica.
- **Impostazioni a livello di sistema.** Alcune impostazioni influiscono sull'accesso a tutti gli oggetti. Su Google Drive, ad esempio, le impostazioni del link di condivisione prevalgono su tutte le autorizzazioni e rendono ogni oggetto di nuova creazione accessibile all'intero dominio. Su Salesforce, l'organizzazione "predefinita a livello di organizzazione" (OWD) imposta un accesso di livello base per tutti gli oggetti.

Per visualizzare l'accesso, tutti questi attributi e rapporti funzionali devono essere calcolati in anticipo e normalizzati su tutti i data store e le applicazioni. Senza questa automazione, determinare quali utenti o account dispongono di accesso a un oggetto (la reale portata del danno in caso di attacchi) richiederebbe tempi esagerati, compromettendo così i lavori quotidiani, dalla risposta agli incidenti all'identificazione dei problemi, fino ai report degli audit.

Comprendere l'attività di accesso è più facile che capire le autorizzazioni?

Assolutamente no.

Quando si parla di sicurezza dei dati, esistono diversi tipi di eventi che riguardano direttamente la protezione dei dati.

- **Eventi di accesso ai dati.** Le attività più importanti per la sicurezza coinvolgono l'interazione diretta con i dati, ovvero quando gli utenti creano, leggono, modificano/aggiornano, eliminano o condividono i dati. Purtroppo, ogni applicazione e data store dispone del suo metodo di registrare (o meno) come gli utenti interagiscono direttamente con i dati. Nei registri Salesforce, ad esempio, l'attività di accesso ai dati non illustra a quale oggetto è stato effettuato l'accesso.
- Anche le **modifiche al controllo degli accessi e alla configurazione** che influiscono sull'accessibilità dei dati sono molto importanti. Le modifiche al controllo degli accessi vengono riportate in maniera diversa e, se non si conoscono gli utenti e i gruppi a cui si riferiscono, sono incomplete. Ad esempio, molti sistemi che registrano le autorizzazioni registrano solo che una lista di controllo degli accessi (ALC) è stata modificata, ma non quali voci sono state cambiate. Inoltre, le modifiche agli oggetti riportati nell'ACL potrebbero non essere registrate dal file system o dall'applicazione in quanto potrebbero dover essere registrate nel servizio di directory (come Azure Active Directory). Le modifiche alla configurazione sono altrettanto complesse, anche rispetto all'accessibilità dei dati. Le modifiche GPO nell'Active Directory possono avere effetti su vari tipi di elementi importanti, come le politiche sulle password e le funzionalità degli endpoint. GitHub, ad esempio, registra le modifiche all'accessibilità dei repository di codice, ma non indica quali modifiche sono state apportate.
- Gli **eventi di autenticazione** possono fornire un contesto importante relativo a quali utenti si sono connessi all'applicazione o al data store, da dove e che tipo di autenticazione è stato adottato (ad es. singola o a più fattori). Gli eventi di autenticazione cambiano fra i vari servizi di directory e applicazioni.
- **Eventi sul perimetro.** In un'infrastruttura on-prem, i segnali perimetrali da DNS, gateway VPN e proxy forniscono informazioni approfondite su connessioni insolite all'interno o all'esterno dell'ambiente. Gli eventi dai device perimetrali sono voluminosi e non uniformi. La tentazione potrebbe essere quella di staccare la telemetria da diverse posizioni, ma bisogna stare attenti a non alterare il rapporto fra segnale e rumore. La cosa più comoda è avere una telemetria rilevante dal punto dei vista dei dati, come DNS per intercettare le infiltrazioni e il proxy web per le esfiltrazioni. Per ulteriori dettagli, consulta **5 modi in cui il tuo SIEM ti sta danneggiando**.

Poiché i data store e le applicazioni descrivono questi eventi in maniera così diversa, è molto difficile rispondere alle domande che li riguardano. Capire a quali dati ha avuto accesso un dipendente in un determinato giorno o quali modifiche al controllo degli accessi sono state effettuate da un amministratore diventa un vero e proprio progetto di ricerca invece che una semplice query.

E che dire degli avvisi?

Senza un flusso di eventi uniforme e normalizzato, il sistema di avviso basato su regole diventa impegnativo e gli avvisi basati sul comportamento vengono limitati a una singola applicazione o completamente fatti fuori. Quando si parla di modellare i comportamenti per creare i profili, anche gli eventi devono essere arricchiti perché l'IA disponga di più sfaccettature da valutare. Ad esempio, se si vuole creare un semplice avviso basato su soglie che si attivi quando qualcuno cancella, aggiorna o accede a oltre 1000 file o oggetti in un periodo di 5 minuti senza un flusso di eventi affidabile e uniforme, probabilmente sarà necessario creare un avviso per ogni applicazione. Se si vuole che l'avviso si attivi quando il numero totale degli eventi supera le 1000 operazioni su file in un periodo di 5 minuti su tutti gli store, siamo già a un livello di query piuttosto avanzato.

Se si vuole fare un altro passo in avanti, come ad esempio ricevere un avviso se qualcuno accede a 1000 file sensibili in un arco di tempo di 5 minuti su diversi data store, sarà necessario arricchire gli eventi con informazioni sulla sensibilità dei file prima di elaborare la logica degli avvisi. Forse ora è più chiaro quanto siano importanti eventi puliti e arricchiti per gli avvisi basati su soglie: bene, per gli avvisi basati su IA lo sono ancora di più.

Flussi chiari e arricchiti di eventi sono fondamentali per costruire le basi comportamentali, o profili peace-time, che l'IA può valutare per determinare le deviazioni. Questi profili incentrati sui dati attivano avvisi con rapporto segnale/rumore molto elevato. Ad esempio, quando un dirigente che normalmente accede a decine di file ogni settimana, di cui solo pochi sono importanti, comincia ad accedere a decine di file importanti a cui né lui né i suoi colleghi solitamente accedono, e magari da un dispositivo mai associato al suo utente o da una posizione in cui di solito non si trovano, è necessario prestare subito attenzione.

Le analisi comportamentali richiedono comportamenti rilevanti, arricchiti e affidabili da analizzare. È per questo che le tecnologie di sicurezza che analizzano flussi poco affidabili e rumorosi sono destinate a fallire.

Senza queste tre dimensioni, **si è destinati a fallire**

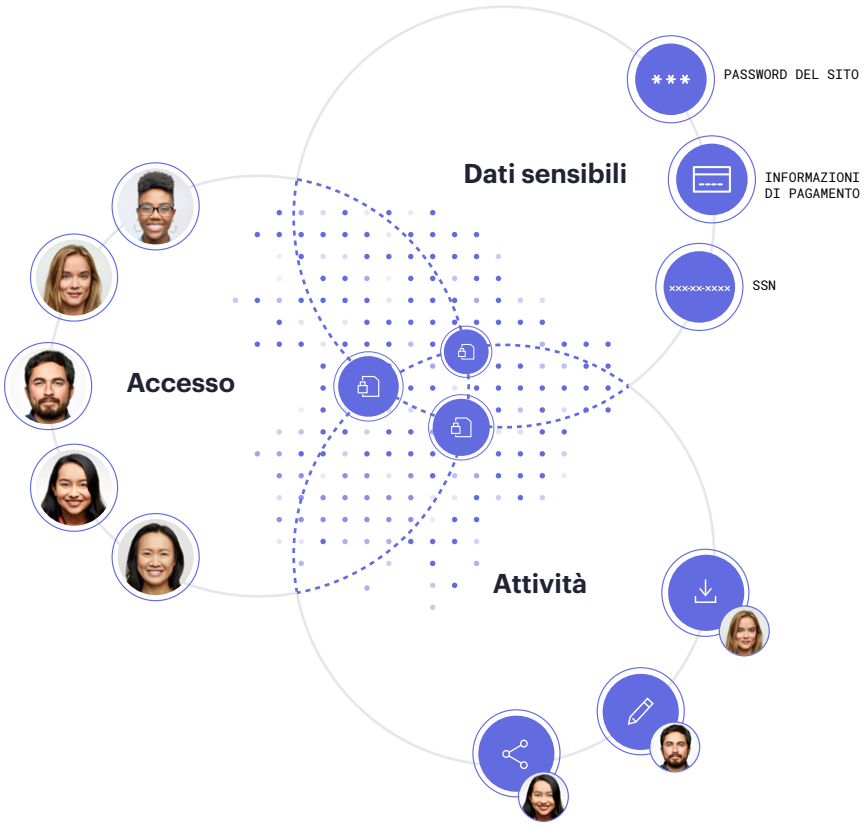
Quando non si riesce a vedere nessuna delle tre dimensioni che abbiamo illustrato finora (sensibilità, autorizzazioni e attività), molti pensano di potersela cavare con una o due. Però, se esploriamo le diverse combinazioni, scopriamo quanto più potenti sono le tre dimensioni insieme.

Come ho già detto in precedenza, sapendo solo quali sono i dati sensibili, quindi senza la dimensione delle autorizzazioni, non è possibile sapere dove si concentrano o dove sono esposti. Senza le attività, non si saprà mai come risolvere in modo sicuro le esposizioni trovate o se i dati sensibili sono stati rubati, né a chi rivolgersi per parlarne. Se si hanno a disposizione solo le attività, si potrà vedere quali dati sono stati sottratti dopo una violazione, o magari si riuscirà a ricevere qualche avviso riguardo alle deviazioni di comportamento, ma non sarà possibile sapere quanto sensibili erano i dati in questione, chi altro poteva avervi accesso o se addirittura erano esposti in modo errato in tutta l'azienda (o su tutto il web).

Quando si tratta di protezione dei dati, è fondamentale avere tutte queste dimensioni per rispondere alle domande fondamentali con cui abbiamo aperto questo articolo:

1. Sai **dove sono archiviati i tuoi dati più importanti?**
2. Hai la certezza **che solo le persone giuste vi abbiano accesso?**
3. Hai la certezza **che queste persone stiano usando i dati in modo corretto?**

Se siamo in grado di rispondere "sì" a tutte queste domande in maniera continuativa nel tempo, allora possiamo rispondere "sì" alla domanda più importante di tutte: **"I nostri dati sono al sicuro?"**



VARONIS

Vuoi sperimentare la differenza di Varonis?

Riduci i rischi senza correrne alcuno. Contatta il nostro team per scoprire che cosa includerà il tuo **data risk assessment** gratuito.

Contattaci

INFORMAZIONI SU VARONIS

Pioniere nell'ambito della sicurezza e dell'analisi dei dati, Varonis combatte una battaglia differente rispetto alle tradizionali aziende di sicurezza informatica. Varonis si concentra sulla protezione dei dati aziendali sia on-prem che nel cloud: file sensibili ed e-mail, dati riservati relativi a clienti, pazienti e dipendenti, dati finanziari, piani strategici e di prodotto e altri tipologie di proprietà intellettuale.

La Data Security Platform Varonis rileva minacce interne e attacchi informatici analizzando i dati, le attività degli account ed il comportamento degli utenti, previene e limita eventi estremamente dannosi bloccando i dati sensibili e dati obsoleti e sostiene efficacemente la sicurezza grazie all'automazione. Con particolare attenzione alla sicurezza dei dati, Varonis offre un'ampia serie di casi d'uso tra cui governance, conformità, classificazione e analisi delle minacce. Varonis ha iniziato la sua attività nel 2005 e vanta migliaia di clienti in tutto il mondo, compresi vari leader di settore in molti campi, tra cui tecnologia, beni di consumo, vendita al dettaglio, servizi finanziari, sanità, produzione, energia, media e istruzione.