Rubrik Zero Labs

LA SICUREZZA DEI DATI OGGI:

UNA CRISI DIFFUSA

RIEPILOGO ESECUTIVO:

USCIRE DA UNA CRISI SILENZIOSA

Il passaggio da un'infrastruttura IT esclusivamente on-premise a un ambiente ibrido che combina on-premise e cloud è uno degli eventi più significativi nella storia dell'IT aziendale.

HA AUMENTATO LA SCALABILITÀ, LA FLESSIBILITÀ E LE OPPORTUNITÀ DI INNOVAZIONE.

Spesso si è dimostrato un passaggio essenziale per i flussi di lavoro aziendali e la collaborazione tra aziende.

Ecco perché il

90%

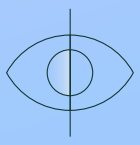
dei leader IT dichiara di gestire ambienti ibridi distribuiti.

Ma come mostrano i dati della telemetria Rubrik e la ricerca condotta da Wakefield Research, questi ambienti hanno anche introdotto rischi senza precedenti:

I leader IT segnalano difficoltà nel proteggere i dati a livello di sistema, lamentano una scarsa visibilità e l'assenza di un controllo centralizzato.

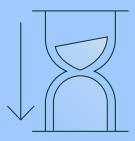
Il 90% degli intervistati dichiara di aver subito un attacco. Quasi un quinto segnala attacchi con una frequenza media di uno ogni due settimane. E questi sono solo gli attacchi dichiarati.

I criminali informatici lo sanno e sfruttano sistematicamente le vulnerabilità degli ambienti cloud ibridi.



Le tecniche di attacco stanno cambiando: si passa da malware a strategie di ingegneria sociale e attacchi basati sull'identità. Gli attacchi che sfruttano l'identità potrebbero essere ormai quasi l'80% del totale.

Gli attacchi avvengono attraverso almeno 10 vettori diversi, molti di più rispetto al passato.



Il motivo? Funzionano. Gli attacchi andati a segno sono in aumento, e il tempo che intercorre tra la violazione iniziale e il pieno controllo dei dati sensibili si sta riducendo rapidamente.

Di conseguenza:

86%

DELLE AZIENDE INTERVISTATE HA DICHIARATO DI AVER PAGATO UN RISCATTO A SEGUITO DI UNA RICHIESTA DI ESTORSIONE.

Quasi tre quarti affermano che gli aggressori sono stati in grado di violare e danneggiare i loro dati.

QUESTI PERICOLI SI STANNO TRASFORMANDO IN UNA CRISI REALE E NESSUNO NE PARLA

probabilmente perché pochi hanno un piano davvero efficace. Molte aziende migrano lentamente verso il cloud sperando che siano i provider a risolvere il problema, oppure ignorano la questione, considerandola un costo inevitabile del business.

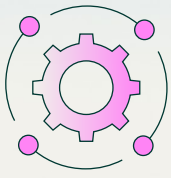
Ma non deve per forza andare così.

LE AZIENDE DEVONO

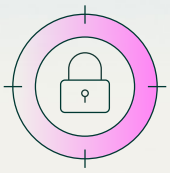
GIOCARE D'ANTICIPO CONTRO GLI HACKER

RAGIONANDO COME LORO

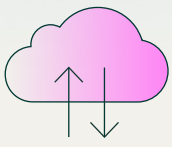
Gli hacker puntano a individuare e controllare i dati più preziosi con l'obiettivo di bloccare le operazioni. Se possono farlo loro, possono farlo anche le aziende.



Come prima cosa bisogna riprendere il controllo della situazione con una maggiore consapevolezza del sistema, quindi definire un piano di protezione, difesa e ripristino dando priorità ai dati sensibili e alla continuità operativa.



I dati sensibili vanno localizzati e classificati in categorie come informazioni personali, dati finanziari e proprietà tecniche. In questo modo si possono identificare in anticipo gli obiettivi degli hacker, dimostrando controllo e conoscenza del cloud.



Un processo continuo di backup e ripristino dovrebbe essere parte integrante della strategia di sicurezza, tanto nel cloud quanto on-premise.

DATI E METODOLOGIA

L'obiettivo di Rubrik Zero Labs è fornire informazioni pratiche e imparziali per aiutare le organizzazioni a ridurre i rischi legati alla sicurezza dei dati. Per raggiungere questo scopo, abbiamo incluso informazioni provenienti da tre fonti principali.

01

TELEMETRIA RUBRIK

Abbiamo utilizzato la telemetria di Rubrik per ottenere informazioni sull'ambiente dati tipico delle aziende e sui rischi associati

02

RICERCA WAKEFIELD

I punti di vista di oltre 1600 leader del settore IT e della sicurezza tramite la ricerca Wakefield

03

ORGANIZZAZIONI CHE HANNO CONTRIBUITO

Ricerche di autorevoli organizzazioni e società di cybersecurity

TELEMETRIA DI RUBRIK

Abbiamo utilizzato la telemetria di Rubrik per ottenere informazioni sull'ambiente dati tipico delle aziende e sui rischi associati

Si basa su due fonti:

DATI DI BACKUP

sono i dati cloud, SaaS e on-premise di cui abbiamo eseguito il backup dagli ambienti dei clienti.

DATI DI PRODUZIONE

sono i dati cloud, SaaS e di produzione che Rubrik monitora di continuo, in modo che le organizzazioni possano prendere decisioni su come gestire i rischi nei loro ambienti.

NUMERO DI FILE CLOUD PROTETTI:

I dati si riferiscono al periodo compreso tra: 1 gennaio 2024 e 31 dicembre 2024

5,8 MILIARDI

file totali negli ambienti cloud e SaaS in produzione

OLTRE 175 MILIONI

file sensibili classificati in tutti gli ambienti cloud e SaaS gestiti

---

WAKEFIELD RESEARCH

OLTRE 1.600

Leader IT e della sicurezza

10

Paesi

OLTRE 50%

CIO o CISO

50%

CIO o CISO

1.625

decisori di aziende con almeno 500 dipendenti in 10 Paesi (Australia, Francia, Germania, India, Italia, Giappone, Paesi Bassi, Singapore, Regno Unito e Stati Uniti); in tre regioni (Americhe, APAC ed EMEA)

50%

Direttori o VP

ORGANIZZAZIONI CHE HANNO CONTRIBUITO

Per offrire una visione più completa e imparziale, Rubrik ha inoltre integrato informazioni strategiche provenienti da organizzazioni diverse, ognuna con un suo specifico punto di vista.

ABBIAMO UTILIZZATO:

CROWDSTRIKE

Le analisi basate su cloud e identità di CrowdStrike, relative a intrusioni e tempi di escalation.

Microsoft

I dati di Microsoft sulle analisi basate sull'identità e sulla frequenza degli attacchi.

Allied Market Research®

Le informazioni di Allied Market Research sull'adozione del cloud.

LA PROLIFERAZIONE DEI DATI

NELL'ERA DEL CLOUD

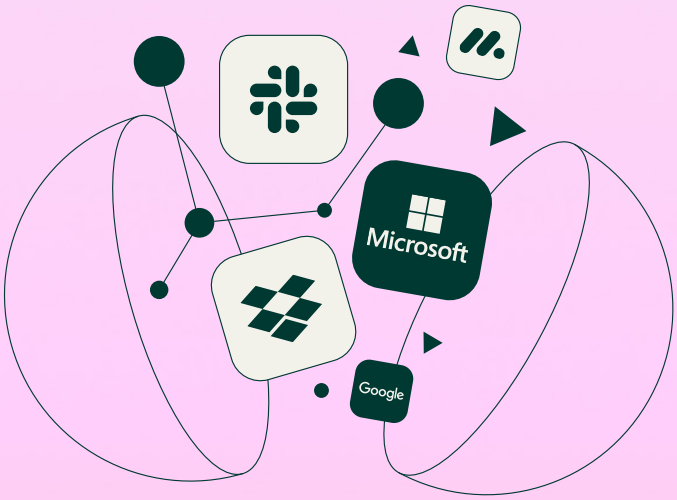
Individuare e proteggere i dati rappresenta una sfida
da quando il primo computer è stato collegato alla rete.

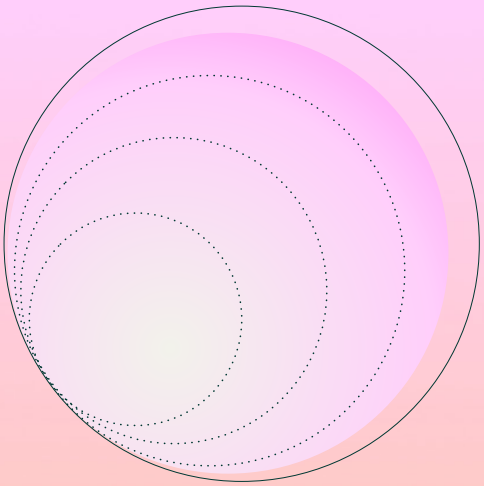
In passato, i dati risiedevano nei data center aziendali o sui computer delle persone, prima fissi sulle scrivanie e poi anche su laptop, tutti collegati a un'unica rete. Oggi, i dati sono sparsi su molteplici dispositivi che attraversano numerose reti per raggiungere i "gioielli di famiglia", ora distribuiti tra ambienti on-premise e cloud.

A UN CERTO PUNTO, LA SCALA E LA COMPLESSITÀ DI QUESTO SCENARIO HANNO PORTATO I PROFESSIONISTI IT IN UN TERRITORIO COMPLETAMENTE NUOVO.

Negli ultimi vent'anni, il business ha spinto le aziende verso i benefici offerti dal cloud e dai servizi SaaS.
E con buone ragioni!

IL CLOUD HA SEMPLIFICATO MOLTI ASPETTI DELLA NOSTRA VITA.





89%

delle organizzazioni continua ad aumentare l'adozione di servizi cloud e SaaS e le strategie ibride e multi-cloud sono ormai la norma, con l'89% delle organizzazioni che utilizza più piattaforme cloud, Secondo Allied Market Research.*

LA NOSTRA INDAGINE FORNISCE INOLTRE I SEGUENTI RISULTATI:

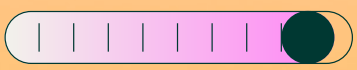
89%

dei leader IT e della sicurezza ha dichiarato di gestire ambienti cloud ibridi.
(Wakefield)

50%

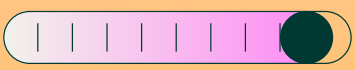
di tutti i leader IT e della sicurezza ha dichiarato di gestire prevalentemente workload basati su cloud e SaaS, rispetto a quelli on-premise.
(Wakefield)

92%



dei leader IT e della sicurezza ha affermato di utilizzare da 2 a 5 piattaforme cloud e SaaS per l'archiviazione dei dati, le applicazioni e i servizi.
(Wakefield)

66%

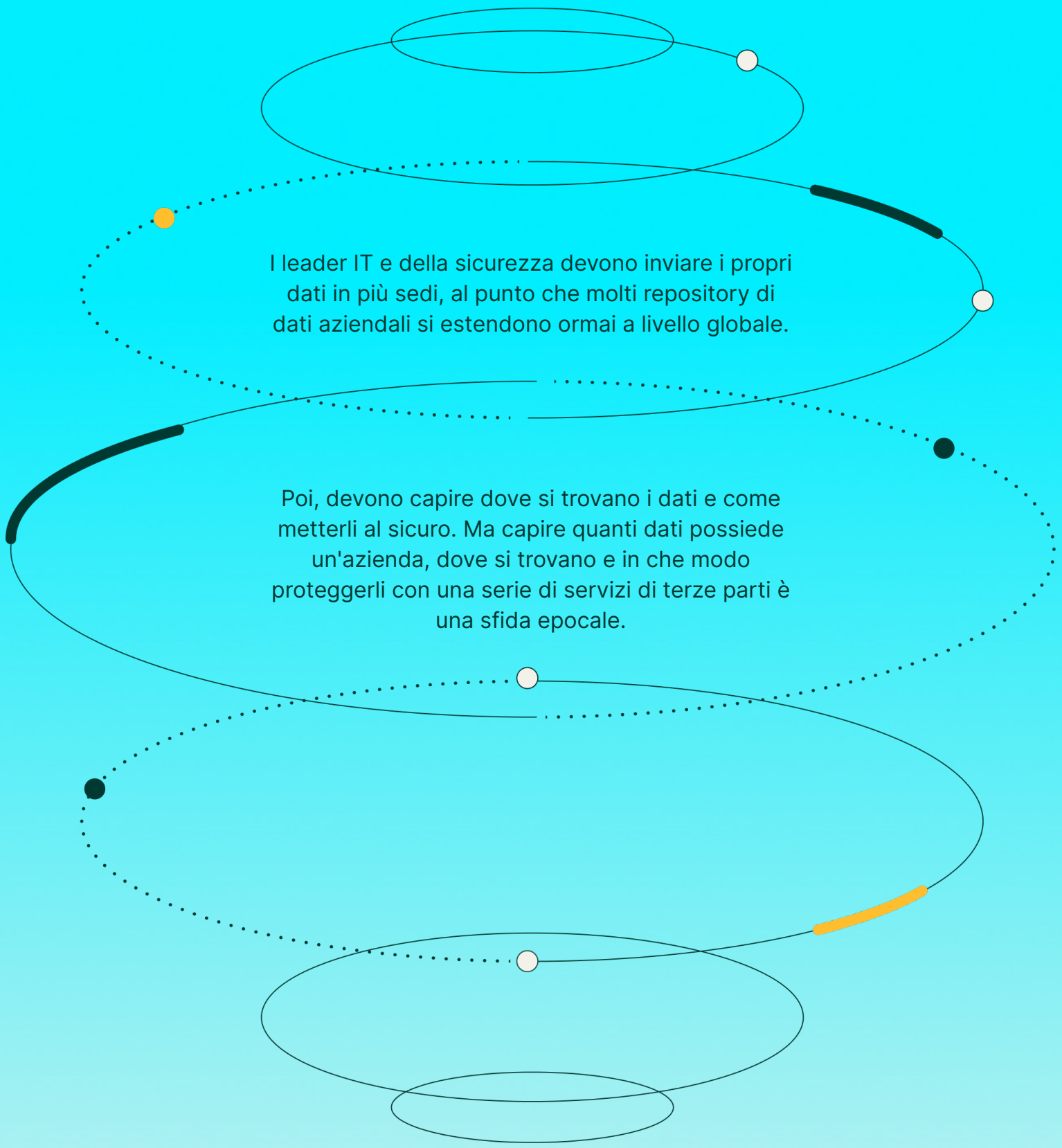


dei leader IT e della sicurezza intervistati ha dichiarato di voler aumentare l'utilizzo di servizi cloud e SaaS nel prossimo anno, mentre il 31% prevede di mantenere invariato il mix tra ambienti cloud ibridi e on-premise.
(Wakefield)

*https://www.alliedmarketresearch.com/cloud-native-applications-market-A210373

COMPLESSITÀ DEI DATI NELL'ERA DEL CLOUD

Per le aziende, ogni nuovo caso d'uso legato al cloud o ai servizi SaaS comporta una piccola perdita di controllo sui propri dati.

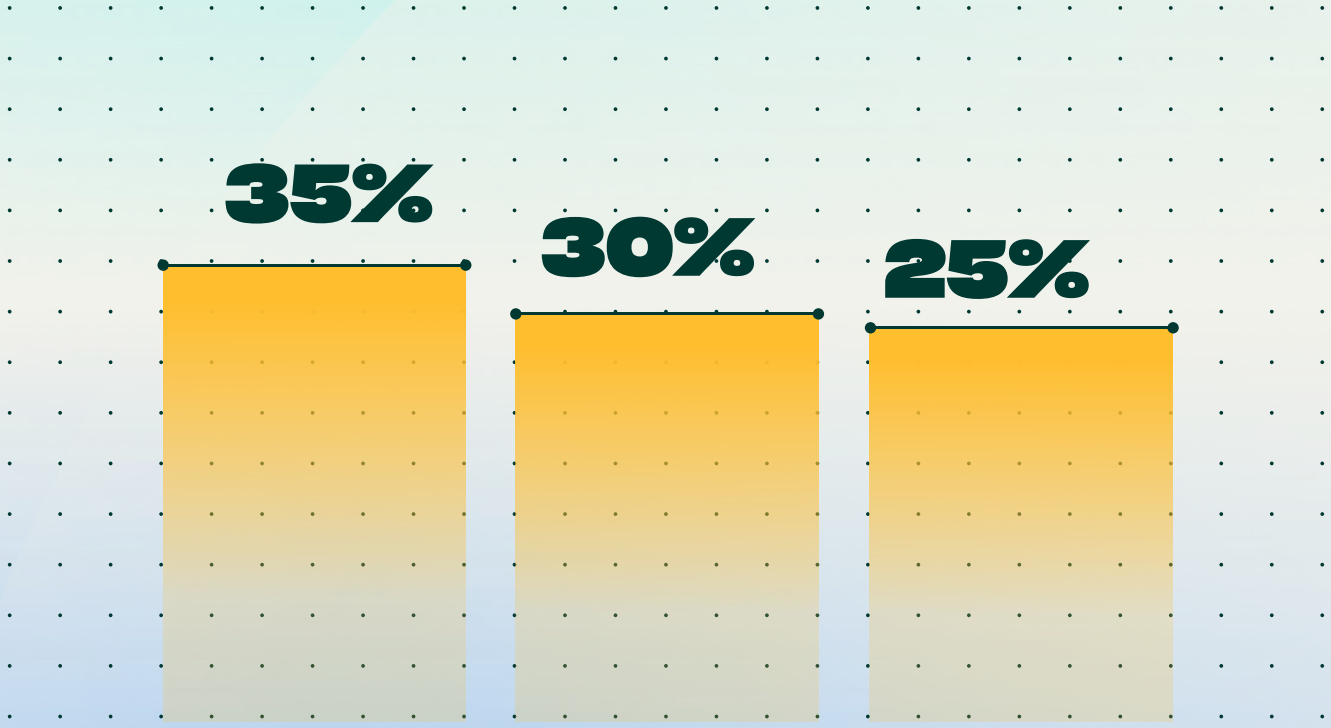


I leader IT e della sicurezza devono inviare i propri dati in più sedi, al punto che molti repository di dati aziendali si estendono ormai a livello globale.

Poi, devono capire dove si trovano i dati e come metterli al sicuro. Ma capire quanti dati possiede un'azienda, dove si trovano e in che modo proteggerli con una serie di servizi di terze parti è una sfida epocale.

SECONDO I LEADER IT LA SFIDA RIGUARDA PRINCIPALMENTE TRE FRONTI:

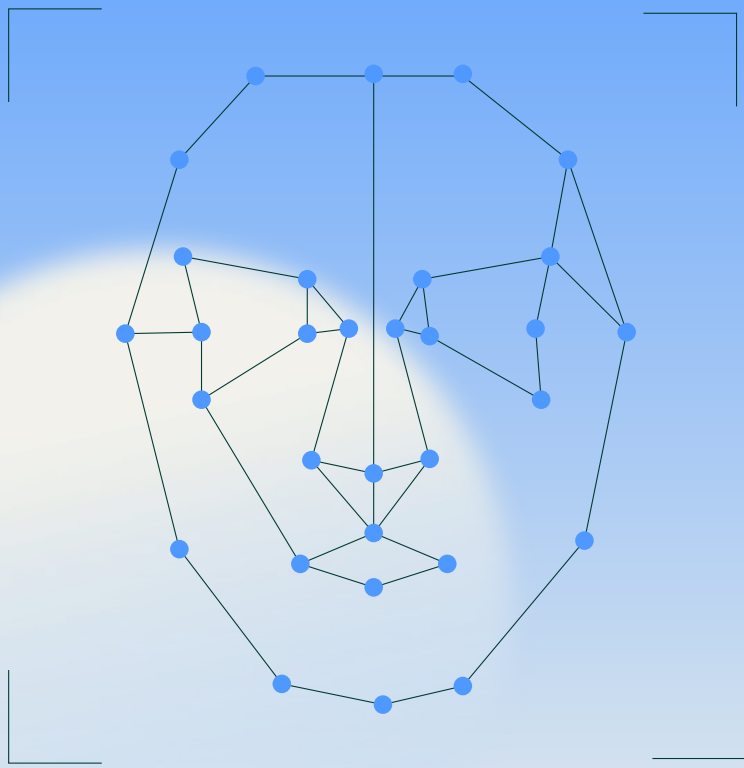
(Wakefield)

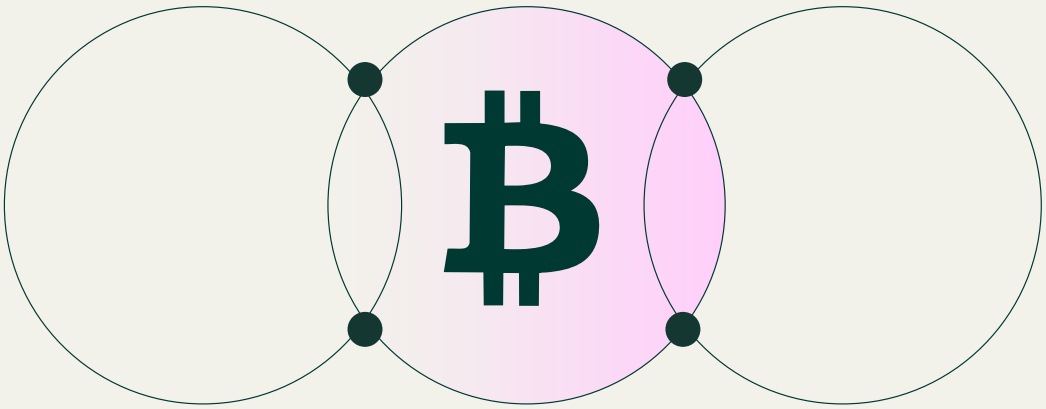


1. Protezione dei dati sensibili in più ambienti
2. Mancanza di una gestione centralizzata
3. Mancanza di visibilità e controllo sui dati basati sul cloud

GLI HACKER SONO CAMBIATI NEL TEMPO

Gli hacker oggi agiscono con metodo, disciplina e con una precisione quasi aziendale, adattando costantemente le proprie tecniche per attaccare le infrastrutture IT moderne.





L'uso sempre più diffuso delle aziende di infrastrutture cloud, accessi basati sull'identità e modelli di lavoro distribuito ha indotto i criminali informatici a utilizzare nuove modalità operative, sempre più scalabili ed efficaci.

Con l'evoluzione delle minacce, gli aggressori si affidano sempre meno al malware e sempre più a tecniche come l'abuso di credenziali valide, gli attacchi manuali e l'ingegneria sociale. Le loro strategie riflettono un vero e proprio approccio imprenditoriale, incentrato su innovazione, efficienza operativa e competenze tecniche.

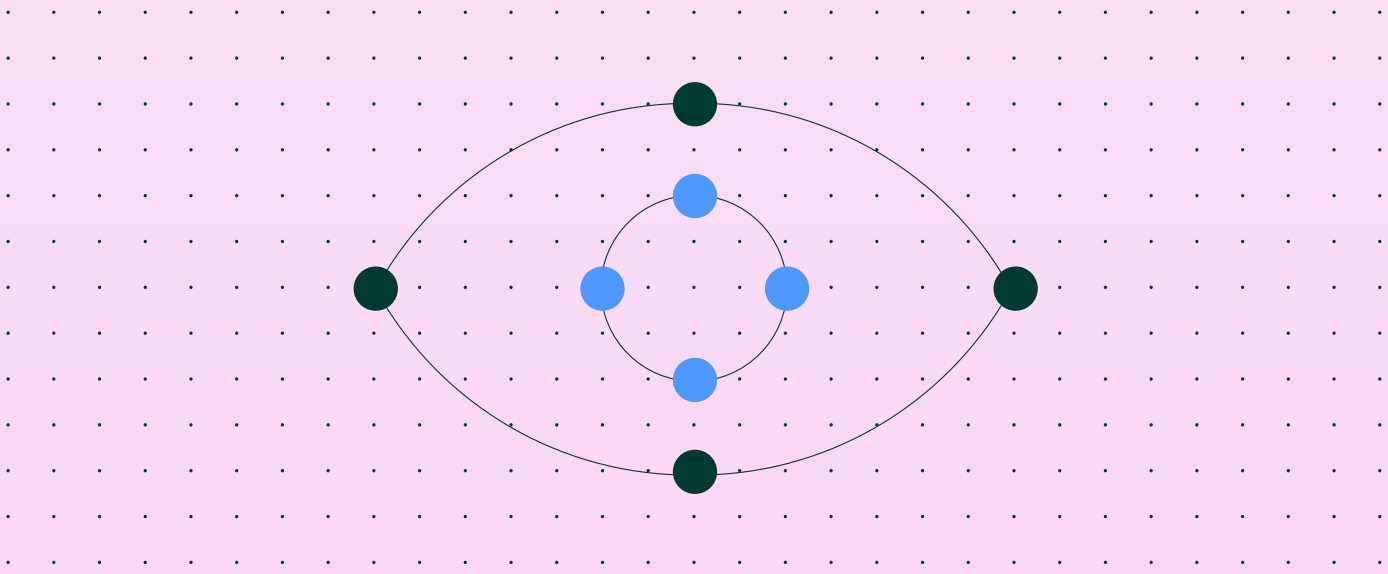
Secondo il CrowdStrike 2025 Global Threat Report: "Nel 2024,

LE INTRUSIONI CLOUD NON ATTRIBUITE SONO AUMENTATE DEL 26%

rispetto al 2023, segno che un numero crescente di attori malevoli punta a compromettere i servizi cloud. CrowdStrike ha osservato un maggior numero di intrusioni in cui gli aggressori hanno ottenuto accesso iniziale tramite account validi, si sono mossi lateralmente sfruttando strumenti di gestione dell'ambiente cloud e hanno abusato delle CLI fornite dai provider".[1]
(CrowdStrike)

"Nel 2024 sono esplose le attività di vendita illegale di accessi degli "access broker", con un + 50% rispetto al 2023. Nel frattempo, l'abuso di account validi è stato responsabile del 35% degli incidenti legati al cloud, a conferma del crescente focus degli hacker sull'identità come vettore di compromissione per gli ambienti aziendali".[1]
(CrowdStrike)

Nel Microsoft Digital Defense Report, Microsoft ha riportato un numero impressionante di attacchi basati sull'identità, affermando che ne blocca oltre 600 milioni ogni giorno.[2]
(Microsoft)



"Nel 2024, le attività senza malware hanno rappresentato il 79% delle rilevazioni, rispetto al 40% nel 2019".[1]
(CrowdStrike)

È stato inoltre osservato un calo drastico del breakout time, ossia il tempo impiegato dagli hacker per passare dall'area inizialmente compromessa ad altri sistemi.

"Nel 2024, il tempo medio per le intrusioni eCrime interattive è sceso a 48 minuti, contro i 62 minuti del 2023.

Il breakout più rapido mai registrato in secondi di tempo è di appena

00:51

Questo significa che i difensori hanno meno di un minuto per rilevare e reagire prima che l'aggressore prenda il controllo del sistema".[1]

(CrowdStrike)

Queste statistiche sono allarmanti per qualsiasi organizzazione che conservi i dati in ambienti cloud o SaaS.

I DATI DI TUTTI NOI SONO UN POTENZIALE TARGET.

E con l'aumento degli attacchi basati sull'identità, gli aggressori accedono normalmente, non in modo illegale, un'attività molto più difficile da rilevare e fermare in tutti gli ambienti. Questo sistema di accesso iniziale rende anche molto più facile muoversi rapidamente tra i sistemi IT.

ECCO COSA DICONO I LEADER IT E DELLA SICUREZZA CHE OPERANO IN PRIMA LINEA RIGUARDO A QUESTA SITUAZIONE:

90%

dei leader IT e della sicurezza ha dichiarato che la sua organizzazione ha subito un attacco informatico lo scorso anno.

(Wakefield)

18%

di questi leader ha dichiarato di aver subito un attacco informatico più di 25 volte nell'ultimo anno. È una media di almeno un attacco ogni due settimane.

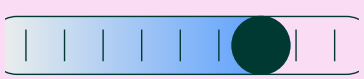
(Wakefield)

86%

dei leader IT e della sicurezza che hanno subito un attacco ransomware nel 2024, ha dichiarato di aver pagato un riscatto per recuperare i propri dati o fermare l'attacco. Si tratta di un calo del 7% rispetto all'anno precedente.

(Wakefield)

74%



dei leader IT e della sicurezza che ha subito un attacco ransomware, ha dichiarato che gli attori della minaccia sono stati in grado di danneggiare almeno in parte le opzioni di backup e ripristino.

(Wakefield)

35%

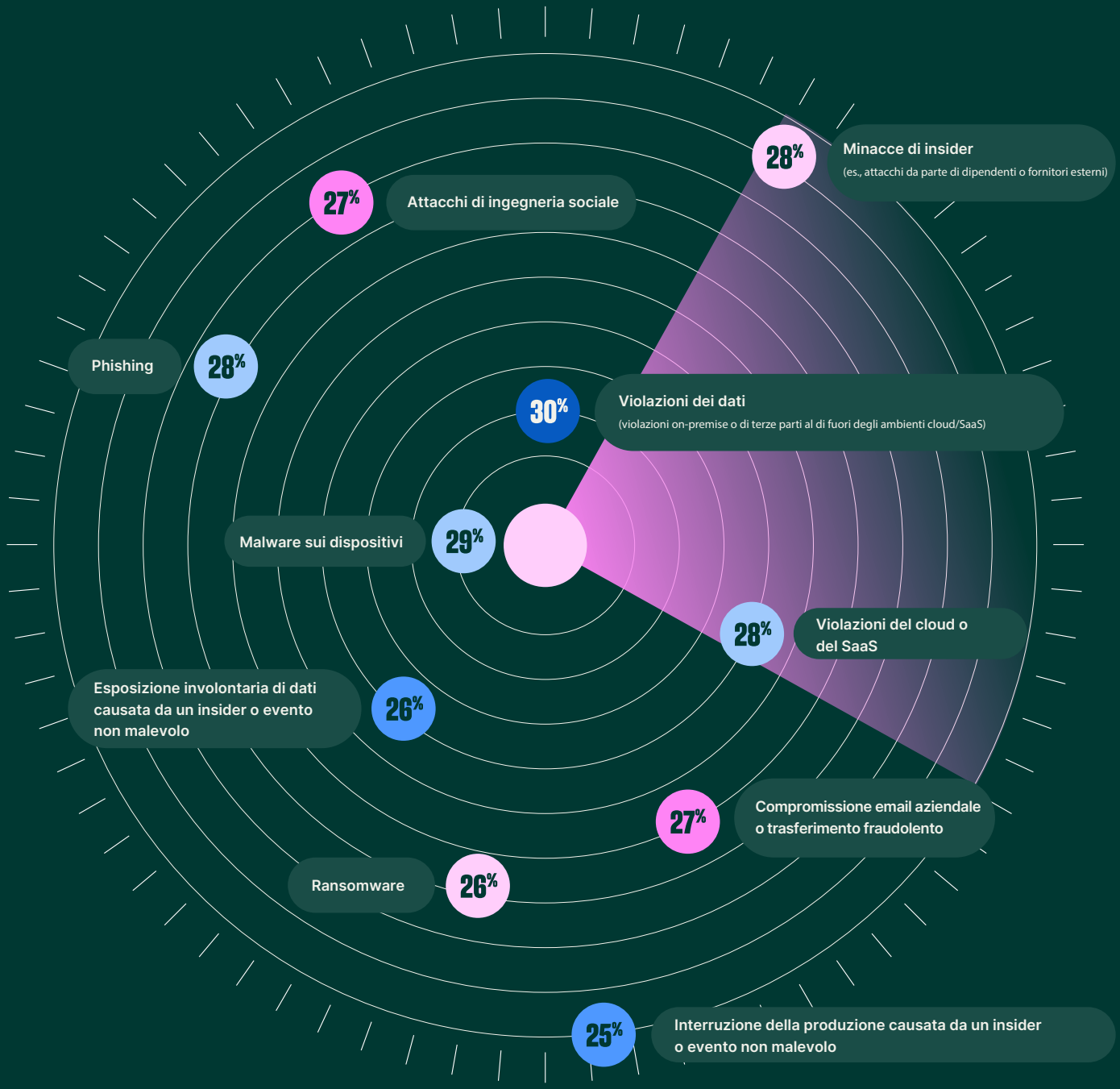
ha affermato che gli attori della minaccia sono riusciti a danneggiare le opzioni di backup e ripristino.

(Wakefield)

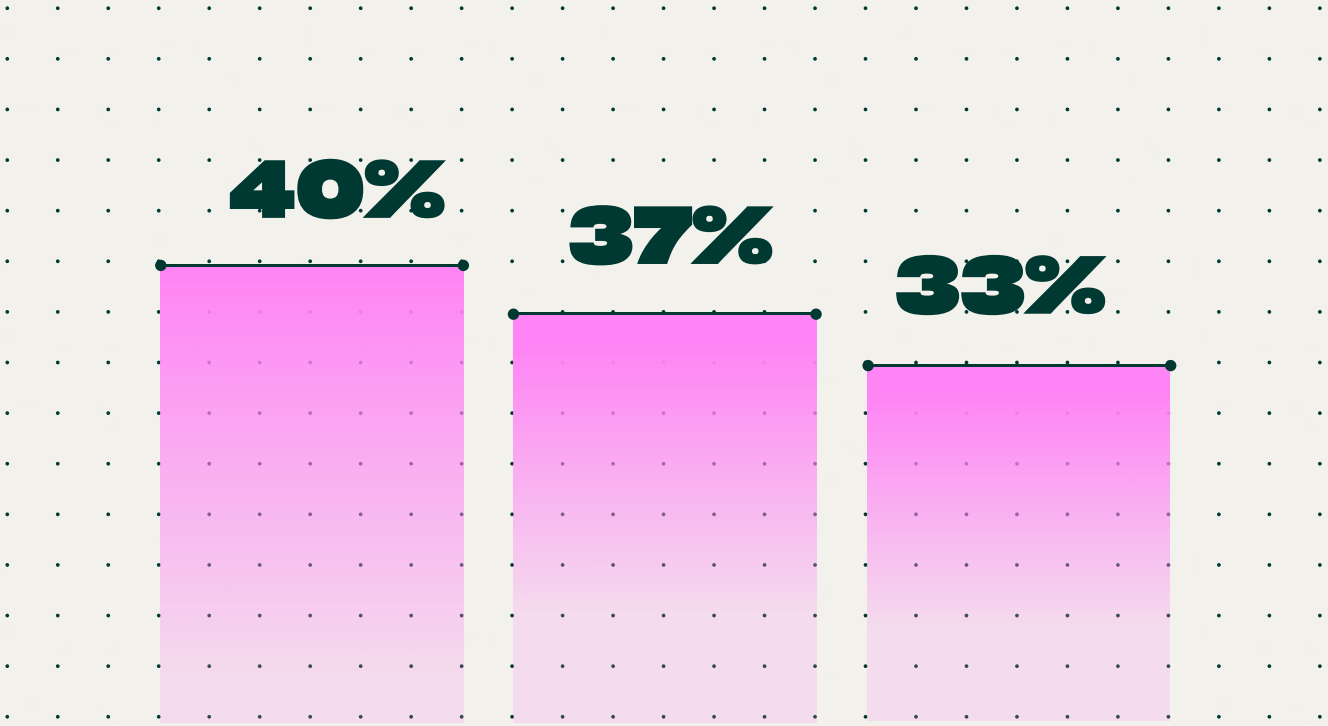
I leader IT e della sicurezza affermano che gli attacchi oggi

ARRIVANO DA OGNI DIREZIONE.

(Wakefield)



ECCO COSA DICONO I LEADER IT E DELLA SICUREZZA CHE OPERANO IN PRIMA LINEA RIGUARDO A QUESTA SITUAZIONE:



1. Aumento delle misure di sicurezza e dei costi
2. Danni alla reputazione aziendale e perdita di fiducia dei clienti
3. Leadership costretta a cambiare

In sintesi, le conseguenze spaziano da un incremento dei costi di sicurezza a perdite di dati non recuperabili.

[1] CrowdStrike - 2025 Global Threat Report

[2] Microsoft - Microsoft Digital Defense Report

PASSARE DAL CAOS ALLA FIDUCIA:

UN PIANO D'AZIONE

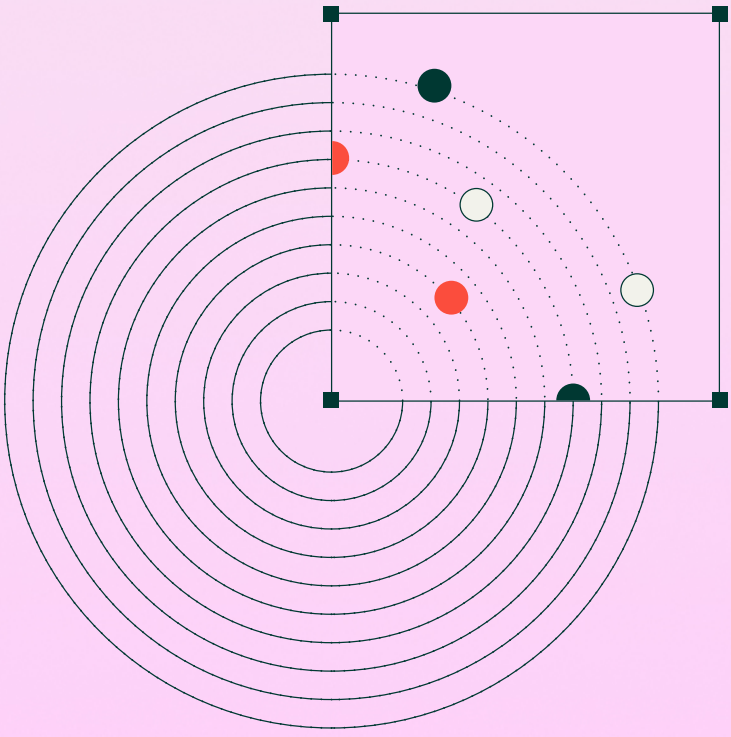
Di fronte a queste nuove complessità e alle minacce che ne derivano, come possono i leader IT e della sicurezza avere fiducia nelle loro soluzioni di sicurezza dei dati?

E in che modo i leader IT e della sicurezza possono trasmettere fiducia ai dirigenti e ai membri del consiglio, assicurando che quando (non "se") succederà qualcosa, le misure adottate dall'azienda saranno sufficienti?

Molte aziende nutrono ancora falsi miti sulla sicurezza intrinseca del cloud, ritenendo che siano i provider cloud a doversi occupare completamente della protezione dei dati. Questo tipo di fiducia può generare un falso senso di sicurezza, lasciando le organizzazioni esposte a rischi come violazioni o perdite di dati, soprattutto in caso di eventi gravi o catastrofici.

Anche se l'adozione del cloud è diventata un must delle pratiche aziendali moderne, alcune organizzazioni sono ancora restie a integrare pienamente questo cambiamento. Ostacoli comuni sono la difficoltà nel comprendere le dipendenze tra applicazioni, il confronto dei costi tra ambienti on-premise e cloud e la valutazione della fattibilità tecnica.

UN MODELLO DI SICUREZZA ZERO TRUST



In contrasto, alcune organizzazioni stanno adottando il modello di sicurezza Zero Trust, secondo il quale nessun utente o dispositivo può essere considerato affidabile a priori, ovunque si trovi.

Benché sia utile per rafforzare la postura di sicurezza, questo approccio è molto impegnativo e richiede una pianificazione rigorosa, con la valutazione di ogni dispositivo, applicazione e utente all'interno dell'organizzazione. La natura rigorosa del modello Zero Trust richiede un profondo cambiamento culturale e operativo, che può comportare un aumento dei costi, una maggiore complessità e un impatto negativo sui workflow. Ciò rende difficile l'implementazione del modello senza rallentare la velocità del business e porta le aziende a scegliere tra sicurezza e agilità operativa.

Ma c'è un'alternativa. La gestione dei dati ibridi e distribuiti a livello globale inizia dalla consapevolezza: sapere dove si trovano i dati. I dati sensibili devono essere individuati e classificati, in modo che le aziende possano identificare e proteggere i target più esposti sin dalle prime fasi.

Ad esempio, grazie alla telemetria Rubrik sui dati di produzione, possiamo dire che i dati strutturati sensibili dei nostri clienti si trovano di norma nei seguenti ambienti

[Telemetria Rubrik - Dati di produzione]

DYNAMODB
35,51%

Amazon DynamoDB **(archivio di documenti con valore chiave)**
- Profili degli utenti dei social media
- Dati o telemetria dei sensori IoT/dispositivi
- Cataloghi di prodotti (e-commerce)

SERVIZIO DI DATABASE RELAZIONALE
6,81%

Amazon RDS **(Servizio di database relazionale)**
- Database dei dipendenti HR
- Gestione degli ordini (e-commerce)
- Cartelle cliniche dei pazienti

SNOWFLAKE
19,09%

Snowflake è un data warehouse su cloud
- Dati dei clienti (retail/e-commerce)
- Transazioni finanziarie (banche)
- Transazioni di vendita
- Aggregati analitici (ricavi totali, valore del ciclo di vita del cliente)
- Registri di sicurezza (integrazione SIEM)

MACCHINE VIRTUALI
4,53%

Macchine Virtuali **(EC2, AzureVM)**
- Hosting di database
- Hosting di applicazioni
- Carichi di lavoro legacy
- Dati di configurazione
- Dati di log utilizzati per l'analisi

E che le più grandi cache di dati sensibili non strutturati si trovino in questi ambienti:

(Telemetria Rubrik - Dati di produzione)

56,67%

dei file di OneDrive sono file sensibili

25,56%

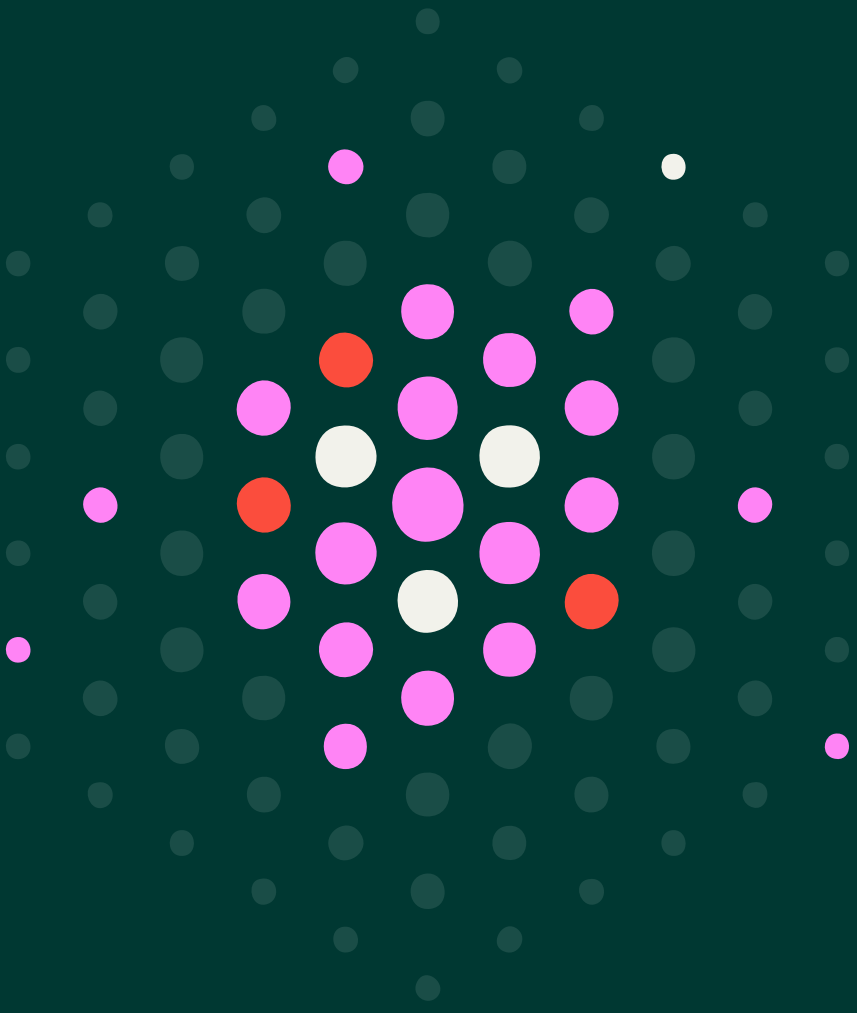
dei file SharePoint sono file sensibili

14,27%

dei file S3 sono file sensibili

PROTEGGERE I TUOI DATI SENSIBILI

Come leader IT e della sicurezza, anche con questa enorme quantità di dati, puoi iniziare a prendere decisioni. In definitiva, tutti i dati sono importanti, ma quelli davvero essenziali sono i dati sensibili.



Sapere quanti ne hai e dove risiedono è il primo passo per metterli al sicuro.

Da qui puoi iniziare a valutare quanto sono sensibili i tuoi dati cloud e SaaS. Ecco alcuni esempi per iniziare.

Cloud | Ambiente SaaS | Cloud e SaaS combinati

NEL CLOUD:

36,29%

di tutti i file sensibili (inclusi file strutturati e non strutturati) è classificato ad ALTA sensibilità

14,66%

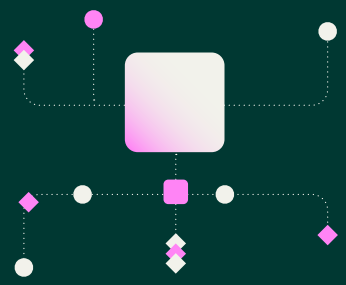
di tutti i dati non strutturati è classificato ad ALTA sensibilità

45,49%

di tutti i file sensibili (inclusi file strutturati e non strutturati) è classificato a MEDIA sensibilità

Cloud | Ambiente SaaS | Cloud e SaaS combinati

IN AMBIENTI SAAS:



5,78%

di tutti i file sensibili (inclusi file strutturati e non strutturati) è classificato ad ALTA sensibilità

79,23%

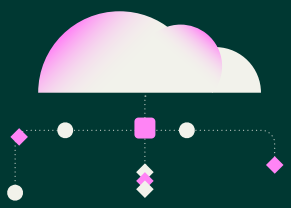
di tutti i dati non strutturati è classificato ad ALTA sensibilità

0,85%

di tutti i file sensibili (inclusi file strutturati e non strutturati) è classificato a MEDIA sensibilità

Cloud | Ambiente SaaS | Cloud e SaaS combinati

CON SAAS E CLOUD COMBINATI:



42,07%

di tutti i file sensibili (inclusi file strutturati e non strutturati) è classificato ad ALTA sensibilità

93,89%

di tutti i dati non strutturati è classificato ad ALTA sensibilità

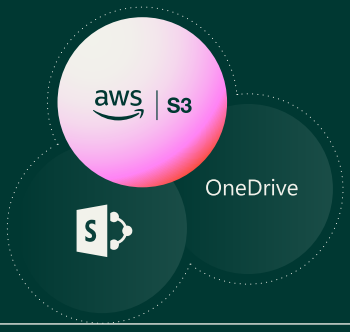
46,34%

di tutti i file sensibili (inclusi file strutturati e non strutturati) è classificato a MEDIA sensibilità

E puoi iniziare a individuare dove si trovano i dati altamente sensibili.

Cloud S3 | SaaS OneDrive | SaaS SharePoint

CLOUD S3:



34,70%

di tutti i file sensibili si trova in S3 ed è classificato ad **ALTA** sensibilità

41,68%

di tutti i file sensibili si trova in S3 ed è classificato a **MEDIA** sensibilità

13,58%

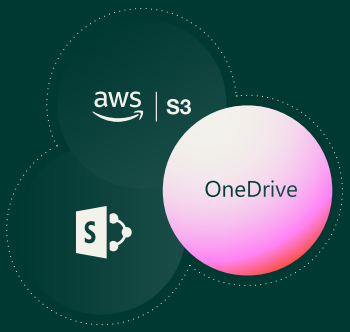
di tutti i file sensibili è di tipo non strutturato ed è classificato ad **ALTA** sensibilità

0,51%

di tutti i file sensibili è di tipo non strutturato ed è classificato a **MEDIA** sensibilità

Cloud S3 | SaaS OneDrive | SaaS SharePoint

SAAS ONEDRIVE:



3,89%

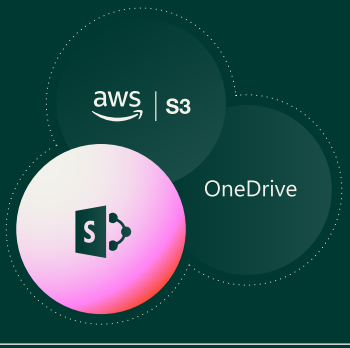
di tutti i file sensibili si trova su ONEDRIVE ed è classificato ad **ALTA** sensibilità

54,41%

di tutti i file sensibili è di tipo non strutturato ed è classificato ad **ALTA** sensibilità

Cloud S3 | SaaS OneDrive | SaaS SharePoint

SAAS SHAREPOINT:



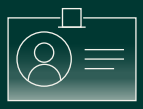
1,81%

di tutti i file sensibili si trova su SHAREPOINT ed è classificato ad **ALTA** sensibilità

24,04%

di tutti i file sensibili è di tipo non strutturato ed è classificato ad **ALTA** sensibilità

A questo punto, puoi iniziare a tracciare un quadro più chiaro di quali dati sensibili includere.



PERSONALI

PII (informazioni personali identificabili), tra cui: numeri di previdenza sociale, date di nascita, indirizzi, numeri di telefono, ecc.

64,51%

di tutti i dati sensibili è di tipo PII

93,84%

di tutti i dati sensibili non strutturati è di tipo PII

DIGITALE

Chiavi API, nomi utente, numeri di conto, indirizzi IP, ID di dispositivi mobili, ecc.

26,96%

di tutti i dati sensibili è di tipo DIGITALE

1,89%

di tutti i dati sensibili non strutturati è di tipo DIGITALE

AZIENDALI

Proprietà intellettuale, tra cui: progetti di prodotti, codice sorgente, informazioni di R&D, piani strategici, logistica della supply chain, dati di inventario, ecc.

24,25%

di tutti i dati sensibili è di tipo AZIENDALE

3,79%

di tutti i dati sensibili non strutturati è di tipo AZIENDALE

FINANZIARI

Dati PCI (dati del settore delle carte di pagamento), tra cui: registrazioni di transazioni, informazioni bancarie, informazioni su carte di credito/debito, documenti fiscali, rapporti di audit interno, ecc.

13,97%

di tutti i dati sensibili è di tipo FINANZIARIO

7,82%

di tutti i dati sensibili non strutturati è di tipo FINANZIARIO

Questo esercizio rappresenta il primo passo per recuperare consapevolezza e controllo sui propri dati. È anche un ottimo modo per guadagnare il sostegno del top management per la tua strategia di sicurezza.

Il messaggio, a livello strategico, cambia da:

"ABBIAMO DATI SENSIBILI SPARSI IN DIVERSI PUNTI NON TRACCIATI E CON LIVELLI DI SICUREZZA VARIABILI", A "ECCO UN ELENCO DI COME VENGONO UTILIZZATI I NOSTRI DATI SENSIBILI E COME LI STIAMO PROTEGGENDO".

DEFINIRE POLICY CHIARE E COMPLETE

Dopo aver acquisito più consapevolezza sul tipo di dati e su dove si trovano nell'ambiente ibrido, è fondamentale definire policy di protezione chiare e complete. Purtroppo, oggi molte aziende adottano un approccio disorganico e frammentato.

Confrontando i dati che monitoriamo negli ambienti di produzione con quelli effettivamente sottoposti a backup, abbiamo notato un divario enorme tra la protezione riservata ai dati on-premise e quella dedicata ai dati in ambienti cloud o SaaS.

La gestione del backup è uno degli aspetti più evidenti di questa disparità. I dati on-premise vengono regolarmente sottoposti a backup, con policy di conservazione rigorose, copie air-gapped e piani di disaster recovery affinati nel tempo.

I dati cloud e SaaS, invece, vengono spesso salvati in modo occasionale e, in alcuni casi, non vengono proprio salvati. Le conseguenze di un attacco ransomware mirato al cloud possono quindi essere disastrose.

Queste osservazioni ci portano a credere che molte aziende facciano affidamento esclusivo sugli strumenti di backup nativi offerti dai provider cloud. Purtroppo, gli strumenti di backup nativi sono spesso limitati, poco frequenti o strettamente legati all'infrastruttura del provider, e quindi potrebbero non essere in linea con le esigenze reali di recovery dell'azienda. Anche ipotizzando performance eccellenti da parte di ogni provider cloud o SaaS, rinunciare alla consapevolezza e al controllo sui propri backup rappresenta un errore strategico.

Nessun approccio sensato alla gestione del rischio si basa sull'assunto che "tutto funzioni perfettamente". La verità è che i dati critici archiviati in applicazioni cloud e piattaforme SaaS sono più esposti a cancellazioni accidentali, attacchi ransomware e configurazioni errate rispetto ai dati gestiti on-premise.

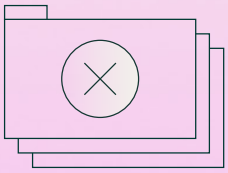
Controllare la capacità di backup, dentro e fuori dal perimetro aziendale, è parte integrante della strategia di sicurezza informatica.

Questo non è un problema esclusivamente tecnico. È un punto cieco strategico.

LA DOMANDA CHE I LEADER DELLA SICUREZZA DOVREBBERO PORSI:

La nostra strategia di backup cloud e SaaS è matura e solida quanto quella di backup on-premise?

ABBIAMO UN ESEMPIO REALE CHE CI AIUTA A RIFLETTERE: L'INCIDENTE DEL DATABASE GITLAB DEL 31 GENNAIO 2017.



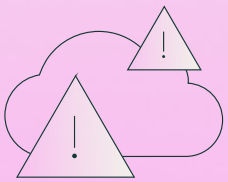
1.

Un ingegnere ha cancellato accidentalmente il database di produzione, causando la perdita di sei ore di dati critici, tra cui segnalazioni, richieste di merge e commenti.

3.

Questo incidente ha evidenziato i rischi legati alla convinzione che gli ambienti cloud-native siano intrinsecamente protetti a livello di backup. Il post-mortem pubblicato da GitLab ha rivelato che la loro strategia di backup non era all'altezza delle pratiche consolidate in ambienti on-premise.[1]

[1] https://about.gitlab.com/blog/gitlab-dot-com-database-incident/



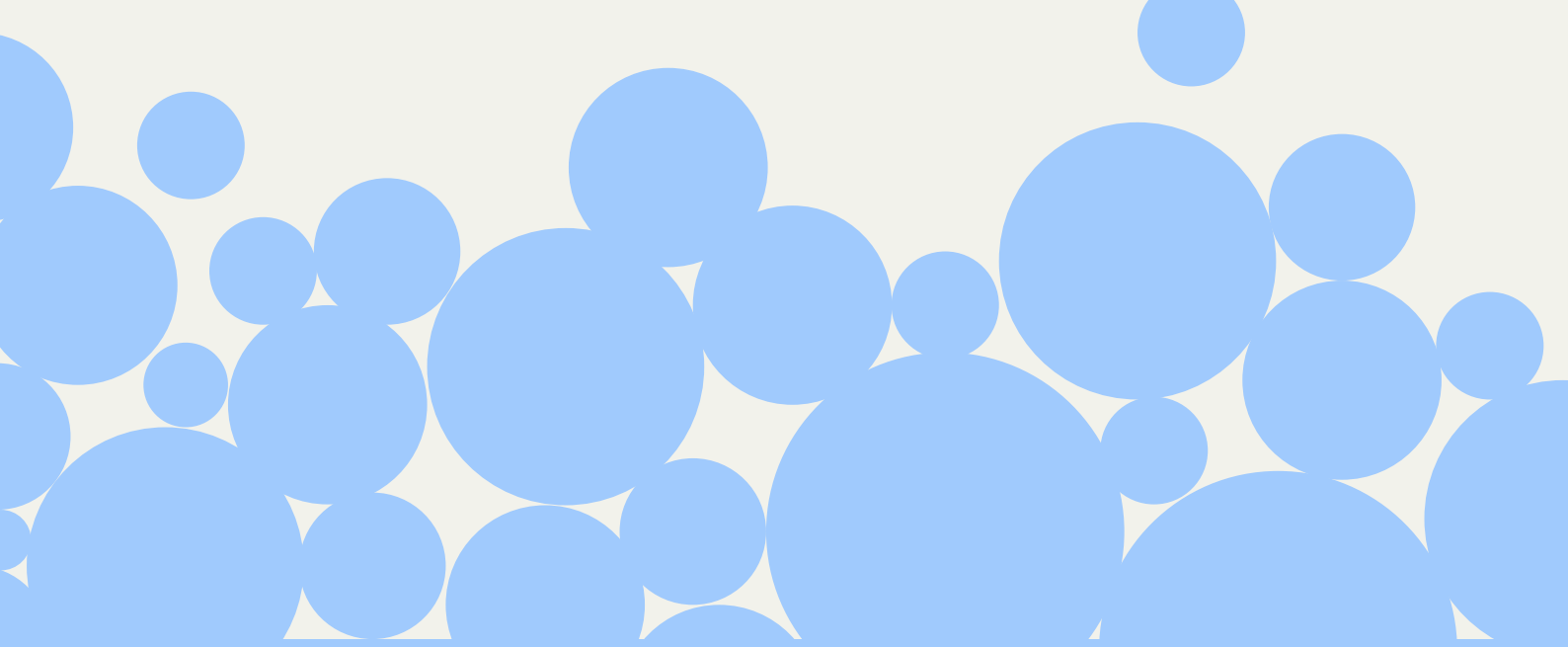
2.

Il processo di ripristino è fallito a causa di molteplici errori di backup: i backup primari erano corrotti, le snapshot LVM obsolete e la replica non era affidabile.

Affrontare il problema richiede un'azione concreta: adottare un approccio unificato alla protezione dei dati, che estenda le policy di backup e recovery oltre il perimetro on-premise, fino al mondo cloud-native.

RACCOMANDAZIONI

Ecco come i leader IT e della sicurezza possono aumentare le loro competenze e fiducia nella loro capacità di proteggere i dati in ambienti cloud, SaaS e on-premise.



N. 1

Innanzitutto, devi sapere dove si trovano i tuoi dati, soprattutto quelli sensibili, sia in transito che a riposo.

La definizione delle priorità è importante, soprattutto perché le risorse sono limitate per tutti. Non ha senso proteggere una cartella di vecchi video marketing di cinque anni fa con la stessa intensità riservata alla proprietà intellettuale più preziosa dell'organizzazione.

Questo compito potrebbe rivelarsi più complesso di quanto sembri. Come tutti i dati, anche quelli sensibili possono cambiare natura nel tempo. Un'idea che nasce come riflessione estemporanea di un dipendente può diventare, in poche settimane, un elemento chiave della strategia aziendale. Nonostante questo, devi sapere dove si trovano tutti i dati e proteggerli in base al loro valore.

N. 2

Imposta policy, processi e procedure in base alla consapevolezza e alla priorità dei dati.

POLICY

Definisci policy appropriate. Ad esempio, regola le condizioni in cui determinati file sensibili possono essere scaricati.

Potresti stabilire, ad esempio, che non è possibile modificare il codice sorgente aziendale da una rete Wi-Fi pubblica a meno che non si utilizzi una VPN. Può sembrare banale, ma molte organizzazioni dimenticano di applicare sistematicamente queste misure di buon senso.

PROCESSI E PROCEDURE

Stabilisci modalità concrete per applicare le policy. Per esempio, se agli utenti non è consentito scaricare determinati file in certe condizioni:

- Come pensi di far rispettare questa policy?
- Come farai a sapere quando è stata violata?
- Quali azioni verranno intraprese in caso di violazione?
- Chi ha la responsabilità di verificare che tutto questo avvenga?

Le aziende devono rispondere chiaramente a tutte queste domande per garantire la sicurezza dei dati e rassicurare il Consiglio di Amministrazione e il top management sul fatto che la locazione dei dati sensibili è nota e che questi sono protetti e gestiti con un piano preciso.

N. 3

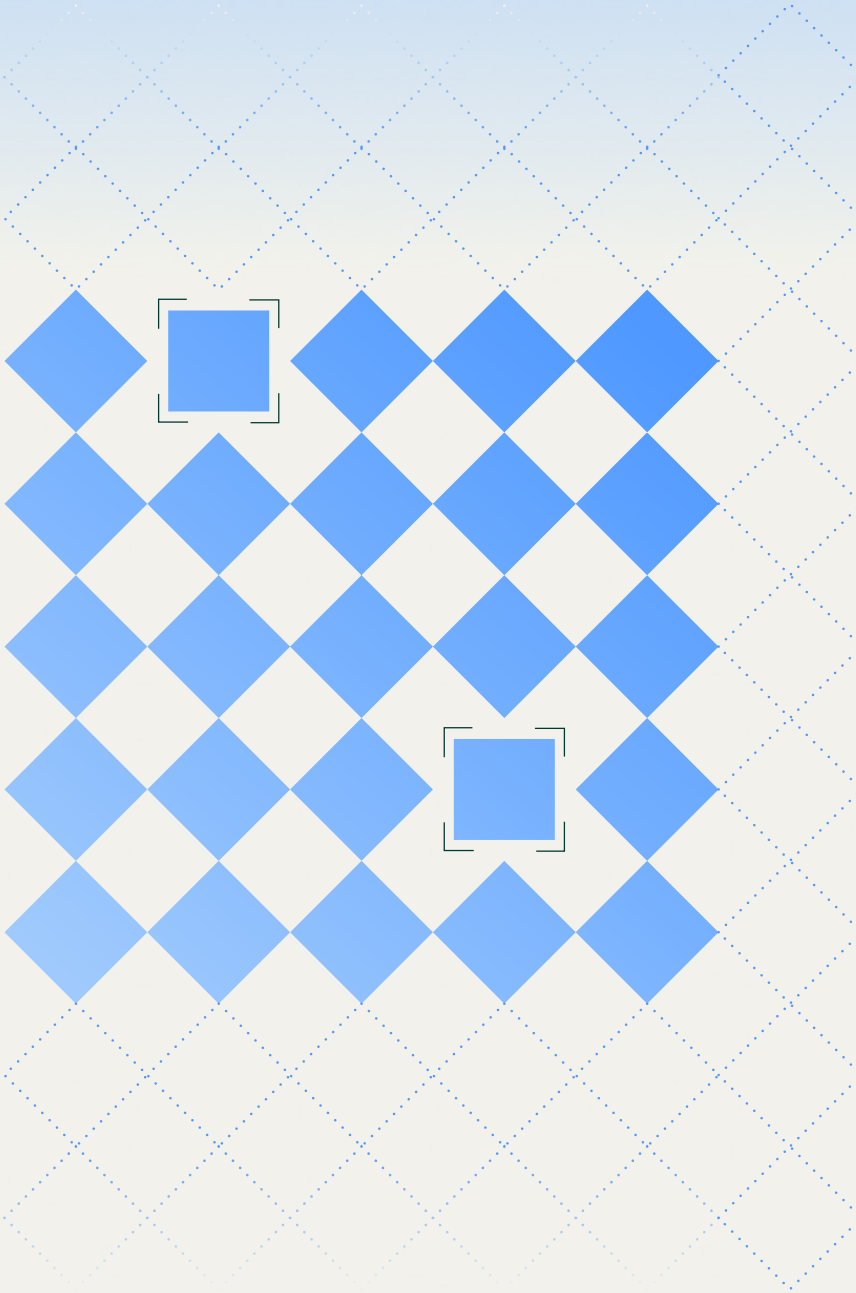
Utilizza l'automazione per aiutare i tuoi team IT e di sicurezza a operare in condizioni migliori.

Nessuno oggi può aspettarsi che i team IT e sicurezza riescano a tenere sotto controllo tutto ciò che accade con la quantità di dati generati da un'organizzazione, senza un supporto adeguato. Anche con strumenti di monitoraggio e aggregazione, la quantità di avvisi che si riversa su team spesso sotto organico è tale da mettere in crisi anche i professionisti più esperti.

L'automazione è l'unico modo efficace per garantire il rispetto delle policy e l'effettiva applicazione di processi e procedure.

Per esempio, in caso di incidenti di sicurezza, è fondamentale eseguire un'analisi delle cause. Senza automazione, gli analisti devono setacciare manualmente enormi volumi di dati, con un considerevole dispendio di tempo ed energia. E come sappiamo, le attività ripetitive aumentano le probabilità di errore umano. Un esempio frequente è un analista del SOC che contrassegna per errore un allarme reale come falso positivo, lasciando potenzialmente una minaccia non gestita.

Automatizzando le attività ripetitive e operative, le aziende riducono gli errori e liberano risorse qualificate che potranno dedicarsi a compiti di sicurezza più strategici e ad alto valore aggiunto.



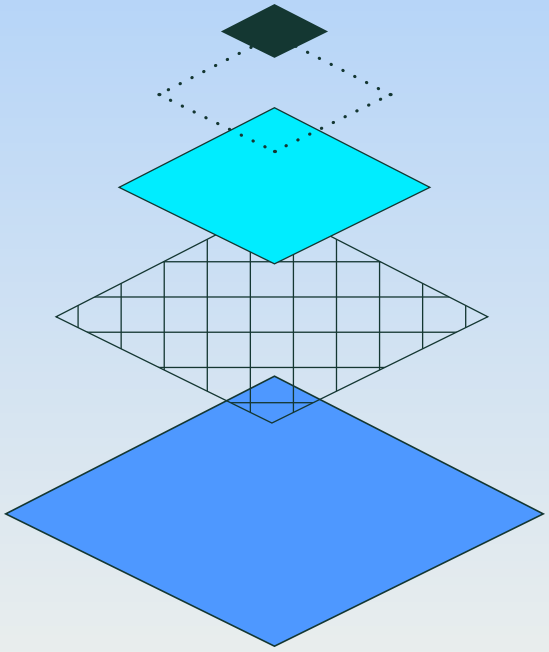
BACKUP E RECOVERY DEI DATI

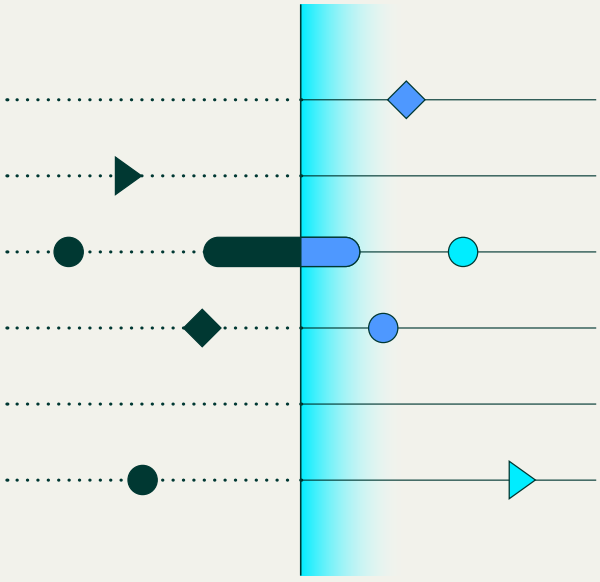
SENZA AUTOMAZIONE:

I team IT gestiscono manualmente i backup e devono monitorare i calendari, validare l'integrità dei dati e coordinare le attività di ripristino in caso di incidente. Questo approccio non solo richiede molto tempo, ma è anche soggetto a errori, come backup mancanti o recovery falliti, e questo rende l'organizzazione vulnerabile nei momenti critici.

CON L'AUTOMAZIONE:

Le soluzioni di backup e recovery automatizzate assicurano un backup dei dati costante e sicuro senza necessità di interventi manuali. In caso di attacco ransomware o guasto di sistema, queste soluzioni garantiscono backup immutabili e sempre disponibili, consentono il ripristino immediato dei dati, riducendo fortemente i downtime e la perdita di dati. Automatizzando questi processi, i team IT possono focalizzarsi su misure di sicurezza proattive anziché dover gestire flussi di recovery complessi, assicurando la continuità operativa e una difesa più solida contro le minacce informatiche.





RILEVAMENTO DELLE MIINACCE E TRIAGE DEGLI AVVISI

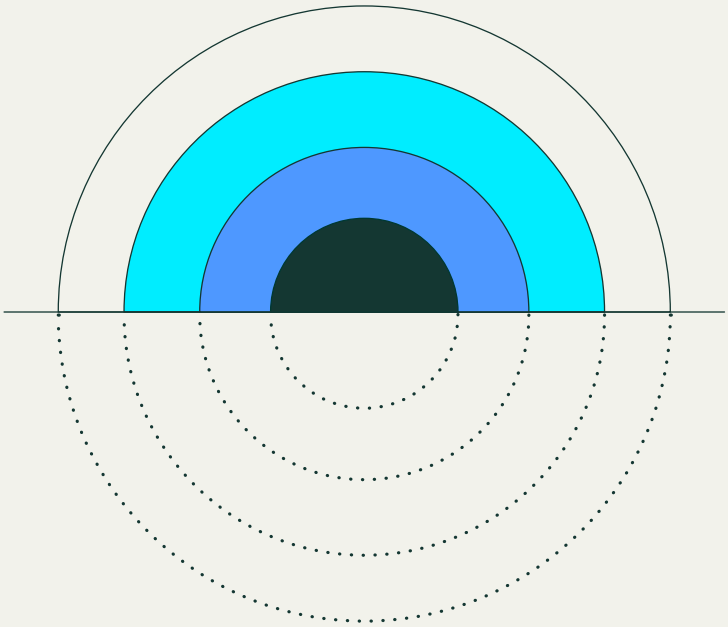
SENZA AUTOMAZIONE:

Gli analisti della sicurezza devono esaminare manualmente migliaia di alert, un processo troppo faticoso e che rischia di non far rilevare potenziali minacce.

CON L'AUTOMAZIONE:

Gli strumenti automatizzati di rilevamento e risposta alle minacce possono categorizzare, dare priorità e anche correggere le cause di specifici alert, consentendo agli analisti di occuparsi di minacce nuove o avanzate.

RISPOSTA AGLI INCIDENTI E ANALISI DELLE CAUSE

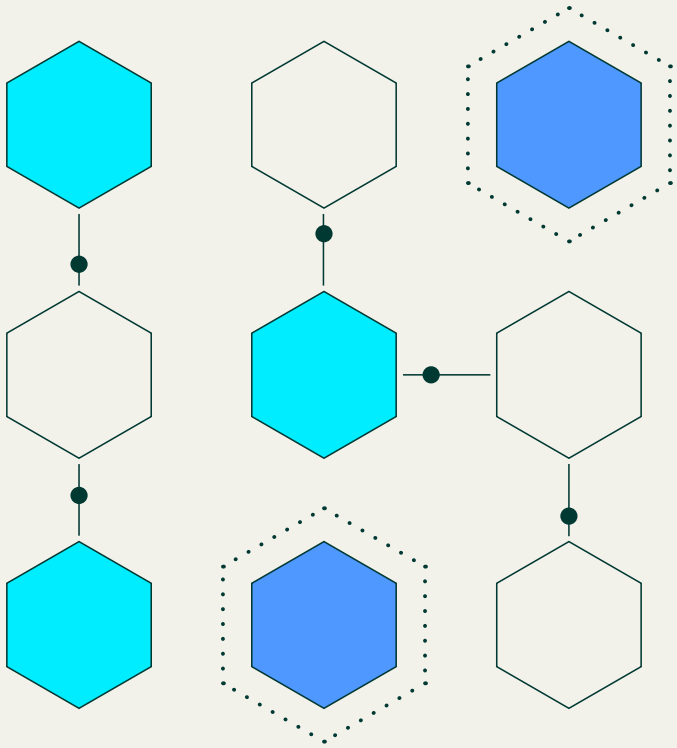


SENZA AUTOMAZIONE:

I team di sicurezza devono correlare manualmente log di varie fonti (firewall, SIEM, sistemi di protezione degli endpoint) per stabilire la causa principale di un incidente.

CON L'AUTOMAZIONE:

Le piattaforme SOAR (Security Orchestration, Automation, and Response) raccolgono e analizzano automaticamente i dati di log, riducendo significativamente i tempi di indagine.



GESTIONE DELLE VULNERABILITÀ E PATCHING

SENZA AUTOMAZIONE:

I team IT monitorano manualmente le vulnerabilità, valutano i rischi e implementano le patch: un processo lungo e soggetto a errori.

CON L'AUTOMAZIONE:

Le soluzioni automatizzate di scansione delle vulnerabilità e gestione delle patch identificano e risolvono proattivamente i rischi.

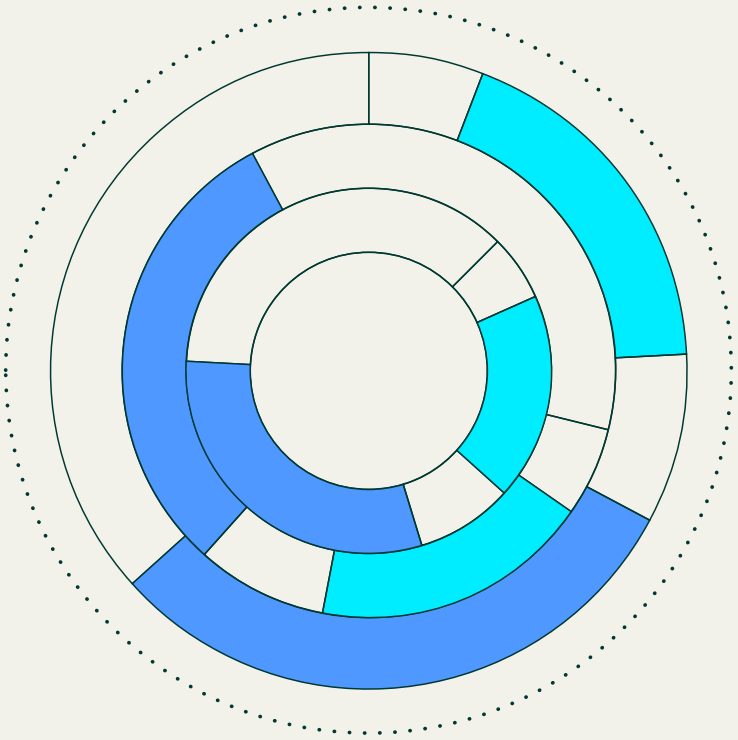
CONTROLLO DEGLI ACCESSI E GESTIONE DELLE IDENTITÀ

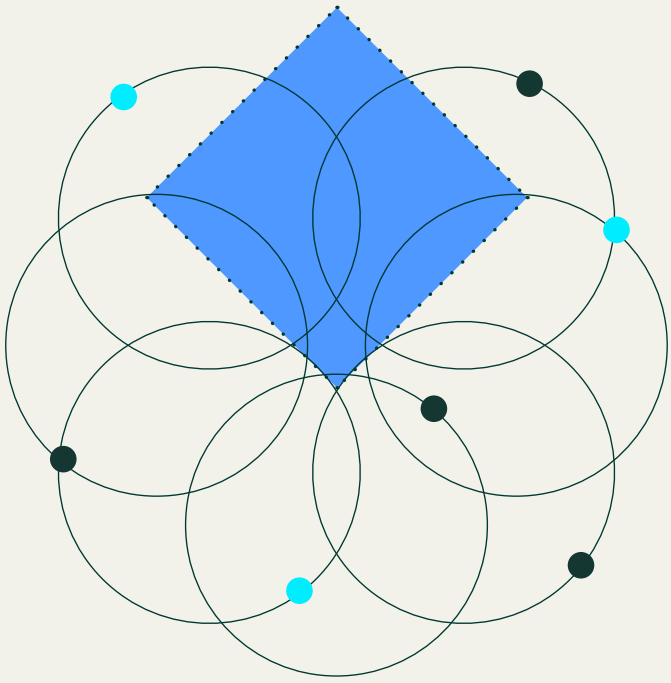
SENZA AUTOMAZIONE:

Gli amministratori IT assegnano e revocano manualmente l'accesso degli utenti, aumentando il rischio di persistenza degli account privilegiati.

CON L'AUTOMAZIONE:

Le soluzioni IAM di gestione delle identità e degli accessi modificano dinamicamente le autorizzazioni in base ai cambiamenti di ruolo, riducendo i rischi di minacce interne.





RILEVAMENTO DELLE ANOMALIE COMPORTAMENTALI

SENZA AUTOMAZIONE:

I team di sicurezza si basano su regole statiche per segnalare le attività sospette, il che può portare a un eccesso di falsi positivi.

CON L'AUTOMAZIONE:

Gli strumenti di sicurezza basati su AI apprendono costantemente dai comportamenti degli utenti e si adattano per rilevare nuovi modelli di attacco.

CONCLUSIONE

Il passaggio verso ambienti ibridi multi-cloud rappresenta una delle trasformazioni più significative nella storia dell'IT aziendale.

È diventato un elemento essenziale per i flussi di lavoro e la collaborazione tra organizzazioni. Tuttavia, come dimostrato da questa analisi, i suoi vantaggi comportano anche un prezzo elevato in termini di pericoli per la sicurezza. Gli ambienti ibridi introducono rischi senza precedenti: i leader IT segnalano difficoltà nel garantire la sicurezza dei dati a livello di sistema, mancanza di visibilità e l'impossibilità di stabilire un controllo centralizzato. Gli aggressori stanno sfruttando queste vulnerabilità senza sosta, adottando tecniche sempre più evolute come gli attacchi basati sull'identità, che rappresentano oggi la maggior parte dei casi.

I RISULTATI SONO ALLARMANTI

~90%

delle organizzazioni intervistate ha subito attacchi, molte delle quali in modo ripetuto

86%

delle aziende che hanno subito richieste di estorsione ha dichiarato di aver pagato il riscatto

3/4

confermano che gli aggressori sono stati in grado di violare e danneggiare i loro dati

RICONOSCIMENTI

Rubrik desidera estendere il proprio ringraziamento a tutte le organizzazioni esterne che hanno contribuito a questo studio mettendo a disposizione le proprie conoscenze e dati.

Come per ogni iniziativa di Rubrik Zero Labs, serve un reale lavoro di squadra per portare a termine un progetto di questa portata. Wakefield Research ha fornito dati esterni per garantire l'obiettività della ricerca. ShapedBy ha saputo trasformare questi dati in contenuti di chiara comprensione. Grazie a tutte le persone in Rubrik hanno contribuito con competenze, contesto e indicazioni durante la realizzazione del report. Desideriamo ringraziare in particolare: Amanda O'Callaghan, Linda Nguyen, Lynda Hall, Ben Long, Peter Chang, Ajay Kumar Gaddam, Dan Eldad, Gunakar Goswami, Prasath Mani, Ethan Hagan, Kevin Nguyen, Caleb Tolin, Sindhu Nagendra, Trinetra Reddy, Heather Webb, Meghan Fintland, Görkem Otman, e Fareed Fityan.