SECURITY SUMMIT

Security Summit

Verona 15 ottobre 2025

Clusit 25 2000-2025

ASTREA

Come aumentare la sicurezza e le prestazioni dei tuoi Backup

Simona Riela | Sales & Channel Account Manager Italia, Object First
Filippo Martucci | Sales Engineer Italia, Object First
Mauro Cicognini | Comitato Scientifico, Clusit – Founding Partner, Rexilience

Mauro Cicognini

COMITATO SCIENTIFICO

FOUNDING PARTNER

[Cliente] Ma a chi vuoi che interessino i miei dati!

[Consulente] A te.

OBJECT FIRST

Best Storage for Veeam

Simona Riela
Sales & Channel Account Manager Italia
Tel. +39 3485176097
Email: simona.riela@objectfirst.com

Filippo Martucci
Sales Engineer Italia
Tel. +39 3520291824
Email: filippo.martucci@objectfirst.com

Lo scenario in breve

- **Rapporto Clusit 2025**
- **Veeam Ransomware Trends Report 2025**
- **ESG Research 2025**
- **Object First Research 2025**

Incidenti Cyber periodo 2020–2024

- Estratto dal **Rapporto Clusit 2025**

Nel periodo in esame, tra gennaio 2020 e dicembre 2024, abbiamo censito un totale di 12.732 incidenti, distribuiti come segue.

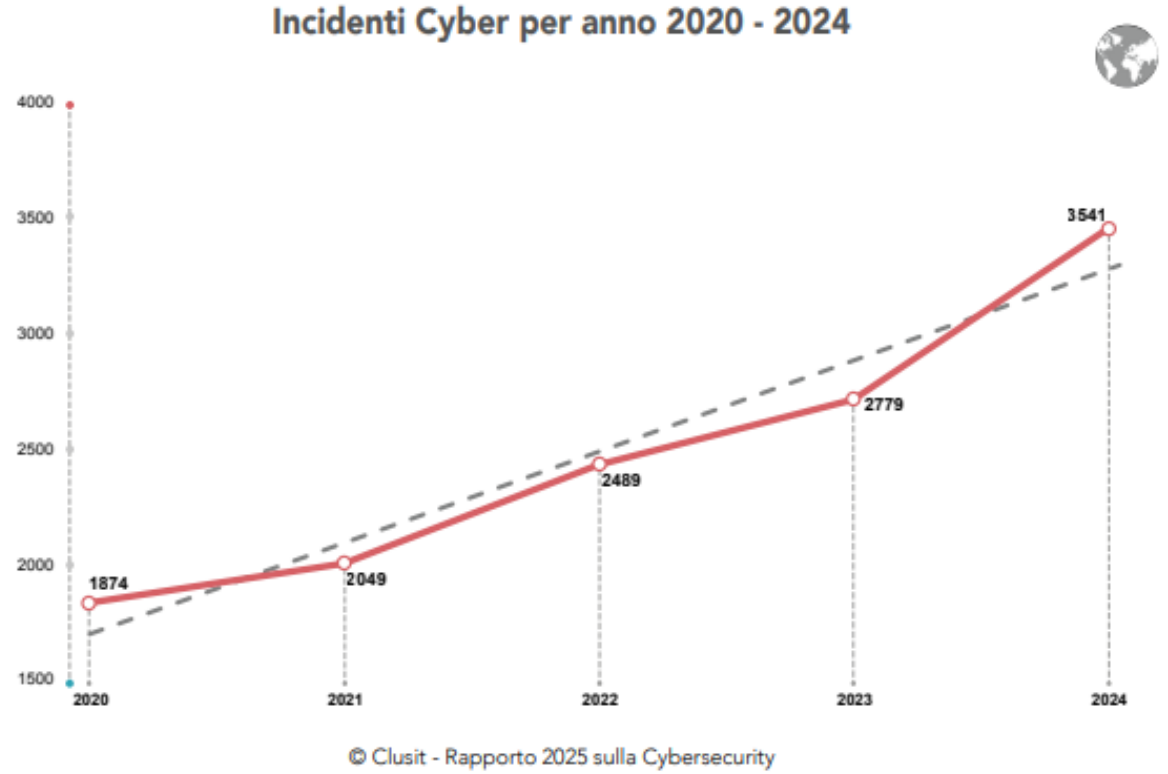


Fig. 1 - Andamento degli incidenti cyber nel periodo 2020-2024

Nell'ultimo anno abbiamo registrato 3.541 incidenti, il numero maggiore di sempre, ed è interessante notare come la realtà stia superando le previsioni indicate in grigio dalla linea di tendenza.

RAPPORTO

Clusit

sulla Cybersecurity
in Italia e nel mondo

2025

1 su 3

incidente è basato su malware

Distribuzione delle tecniche di attacco

Nel 2024, i cybercriminali continuano a puntare su tecniche consolidate e industrializzabili: i Malware sono infatti responsabili di oltre un terzo degli incidenti, mentre lo sfruttamento delle vulnerabilità, sia note che sconosciute (zero-day), incidono per il 15% sul totale (Fig. 9).

I codici malevoli, soprattutto i ransomware, pur registrando un leggero calo percentuale rispetto al 2023 (-4pp), mostrano una crescita dell'11% in termini assoluti (+114 incidenti), confermando la loro affidabilità nelle strategie cybercriminali (Fig. 10).

Estratto da Rapporto Clusit 2025

2025 Ransomware Trends Report di Veeam

69% delle imprese ha subito almeno un attacco ransomware nell'ultimo anno

Impatto economico

- Il **costo medio di un attacco** (tra riscatto, fermo operativo e ripristino) è stimato in **oltre 4,5 milioni di dollari**.
- Solo **il 57% delle imprese** è riuscito a **ripristinare i dati senza pagare** grazie a backup immutabili o air-gapped.

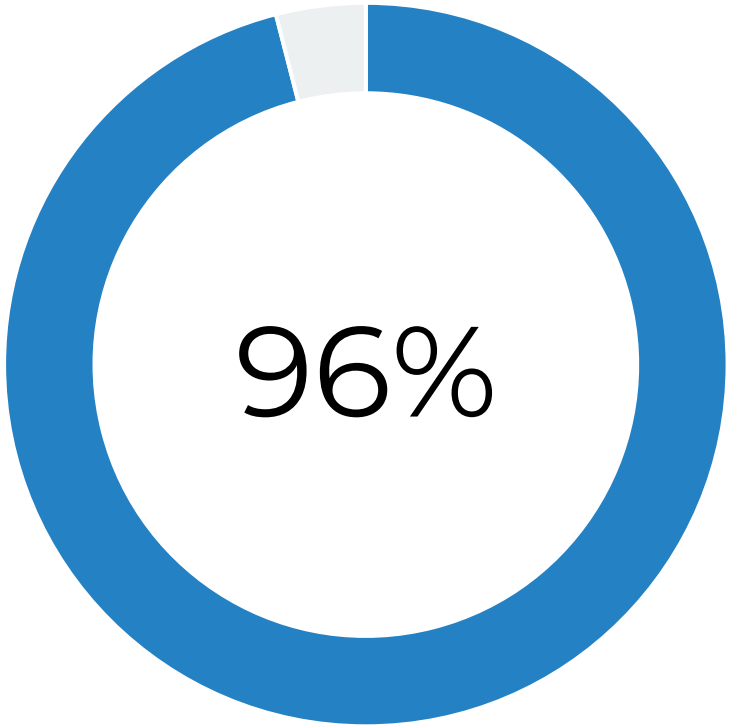
Trend 2025

- Gli attacchi ransomware sono diventati **più mirati e "doppio ricatto"** (esfiltrazione e cifratura dei dati).
- Aumentano i casi in cui i criminali **colpiscono le piattaforme di backup** per impedire il recupero autonomo.

Fonte Agenzia Cybersicurezza Nazionale (ACN)

> Il 2024 ha visto affermarsi **minacce informatiche sempre più sofisticate**, che rendono fondamentale l'adozione di tecnologie avanzate. Tra le principali minacce che stanno ridisegnando il panorama della cybersecurity si distinguono gli **attacchi mirati contro le infrastrutture critiche**, un uso sempre più pervasivo dell'intelligenza artificiale (IA) per eludere i sistemi di difesa e un incremento preoccupante delle campagne ransomware verso i settori manifatturiero, della sanità, dei trasporti e della pubblica amministrazione.

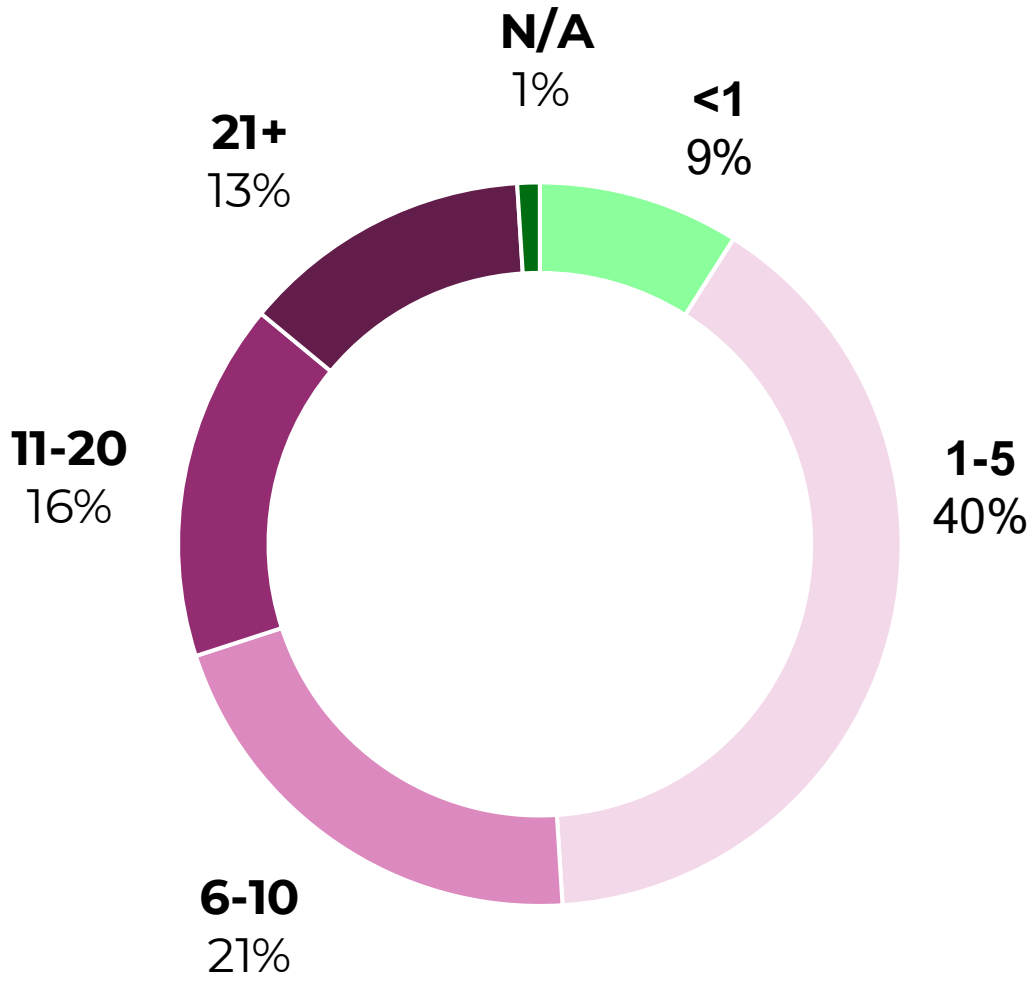
Gli attacchi criminali prendono di mira i backup



Attacchi che hanno preso di mira i backup

Source: ESG Research 2025

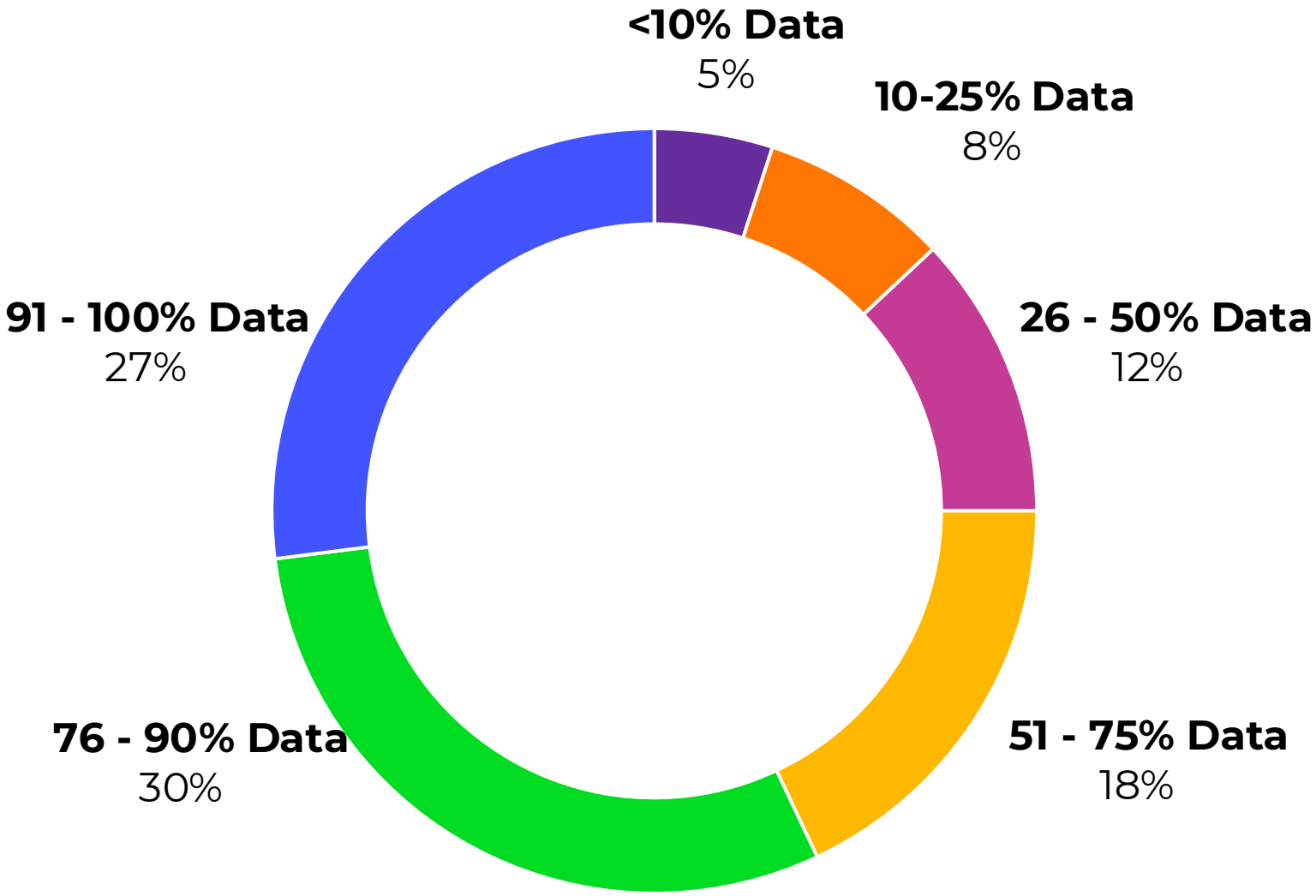
Meno del 50% può ripristinare i propri dati in una settimana lavorativa



Giorni lavorativi necessari per ripristinare la piena operatività

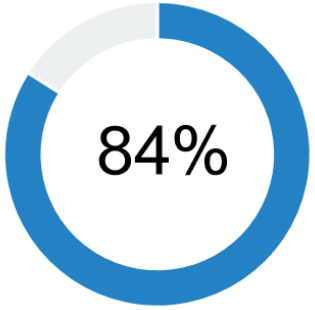
Source: ESG Research 2025

Il 25% delle imprese ha ripristinato meno della metà dei propri dati

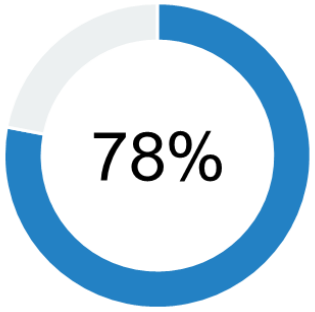


Source: ESG Research 2025

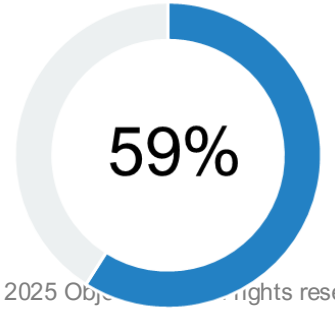
The Human Cost: l'impatto su chi lavora nell'IT



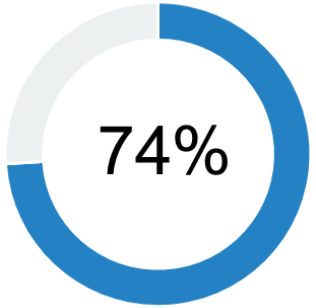
Segnala di sentirsi a disagio e stressato per i rischi derivati dalla sicurezza IT



Temono che gli incidenti di security vengano attribuiti a loro, indipendentemente dalla situazione



Hanno preso in considerazione o hanno iniziato attivamente a cercare un nuovo lavoro a causa della pressioni del loro ruolo in IT

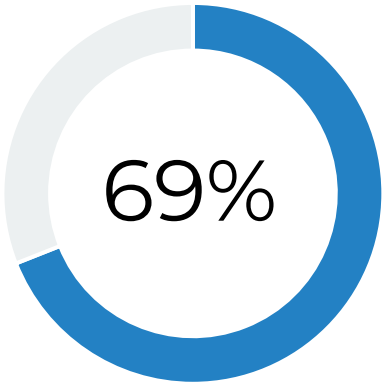


La tecnologia e gli strumenti che utilizzano per il recupero dei dati sono complicati o alquanto complicati da usare e richiedono almeno un certo livello di competenza in materia di sicurezza

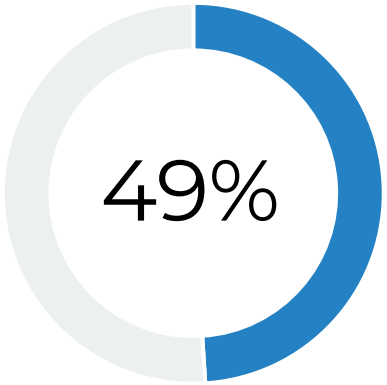
Source: Object First Research 2025

Quando la teoria incontra la realtà...

PRIMA



DOPO



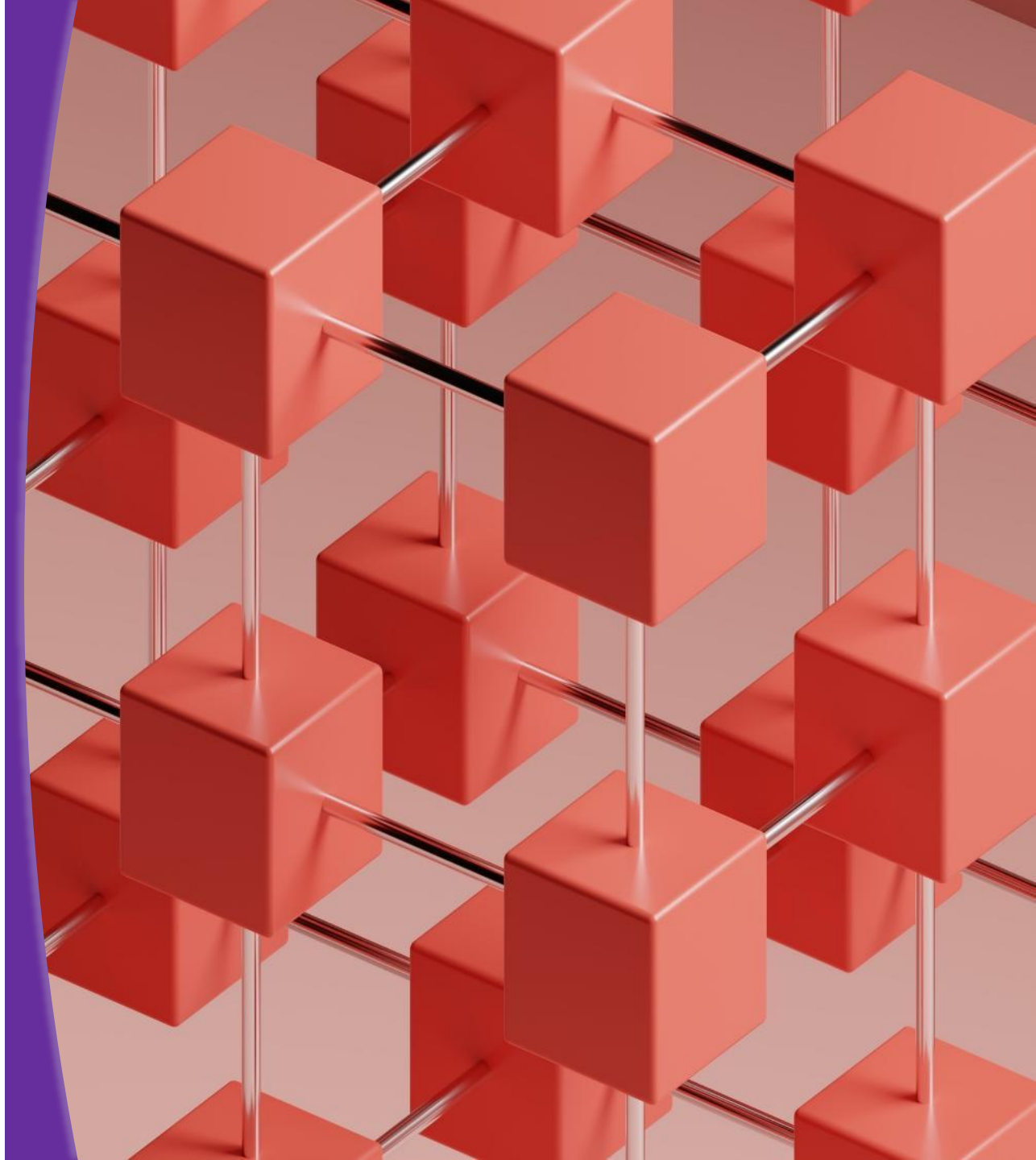
Fiducia delle aziende nei propri preparativi per affrontare un attacco ransomware

Calo del 20% nella fiducia dopo aver subito un attacco ransomware

Source: Veeam Ransomware Survey 2025

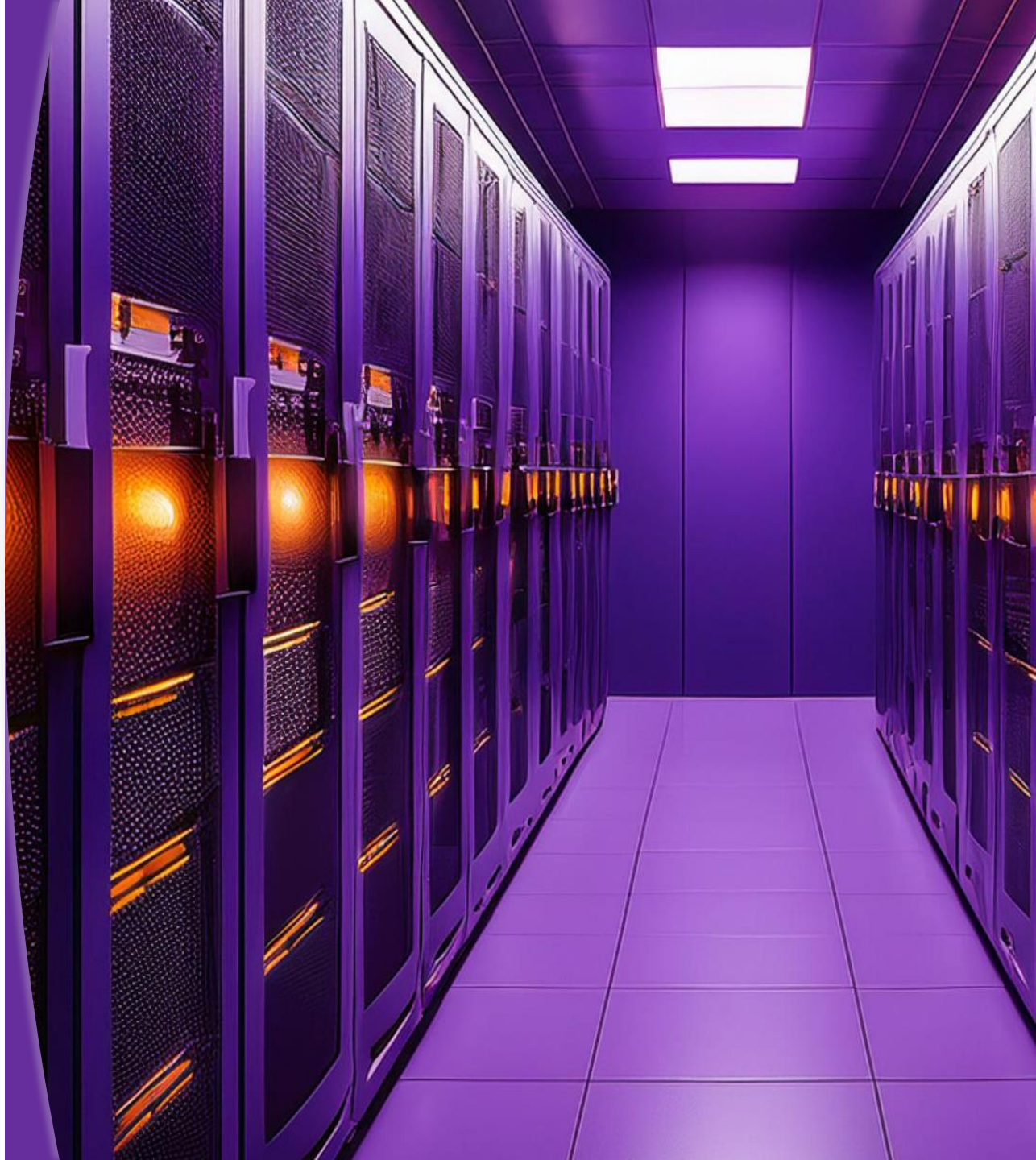
Punti chiave

- Attacchi informatici: "quando" non "se "
- I backup sono ad alto rischio
- Enorme interruzione dell'attività...
- Include lo stress e la fidelizzazione del personale
- Preparato? Potrebbe essere discutibile!
- La tecnologia e gli strumenti potrebbero non essere all'altezza del compito



La resilienza dei dati è necessaria –

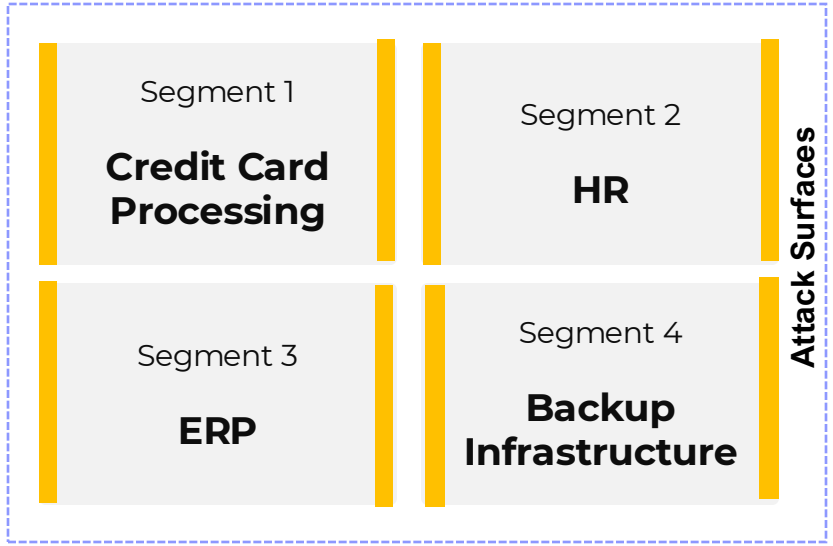
Ma come?



Principi Zero Trust

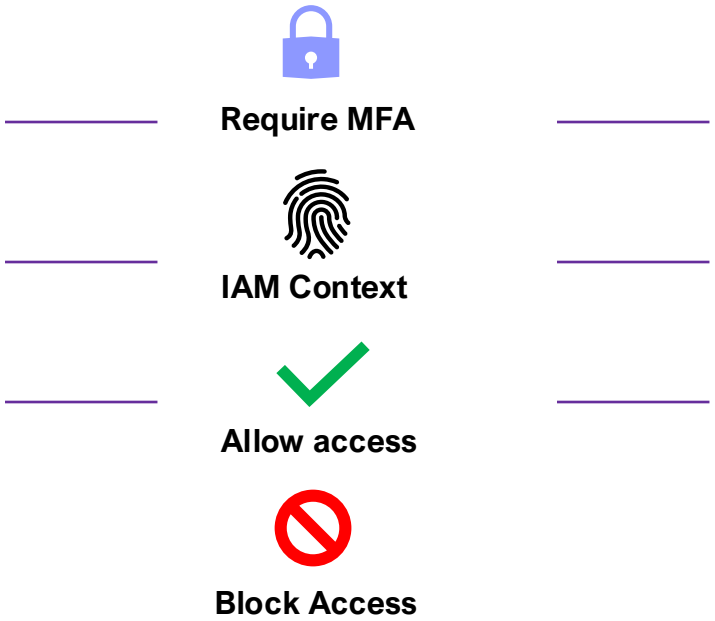
Presumi la violazione
Separa gli accessi

Separa gli accessi e minimizza superficie e raggio d'attacco.



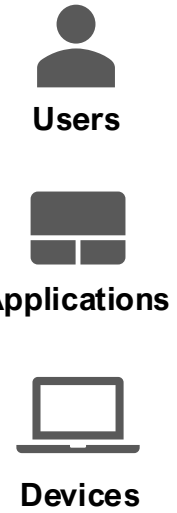
Verifica in modo esplicito

Controlla ogni accesso usando IAM e MFA.



Usa il minimo privilegio

Per ogni utente, dispositivo e applicazione.



Principi Zero Trust

Presumi la violazione
Separa gli accessi

Separa gli accessi e minimizza superficie e raggio d'attacco.

Verifica in modo esplicito

Controlla ogni accesso usando IAM e MFA.

Usa il minimo privilegio

Per ogni utente, dispositivo e applicazione.

Principi Zero Trust Data Resilience (ZTDR)

Estendere i principi Zero Trust al backup e al recovery dei dati aziendali

Segmentazione del software e dello storage di backup

Minimizza superficie e raggio d'attacco.

Più zone di resilienza

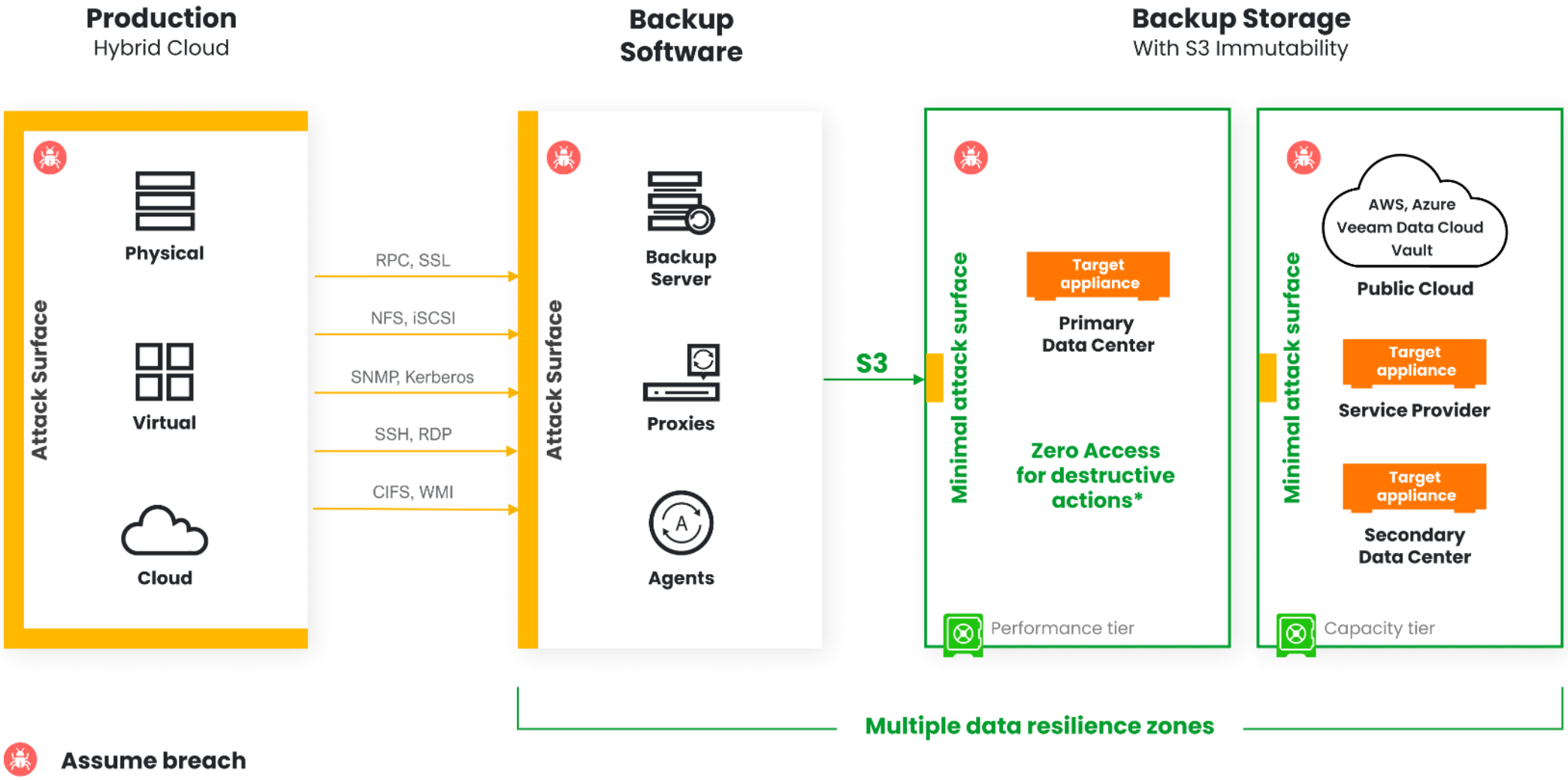
Regola di backup 3-2-1-1-0

Storage di backup immutabile

Proteggi i dati di backup da modifiche o cancellazioni.

Architettura Zero Trust Data Resilience (ZTDR)

Separazione tra software di backup e storage di backup

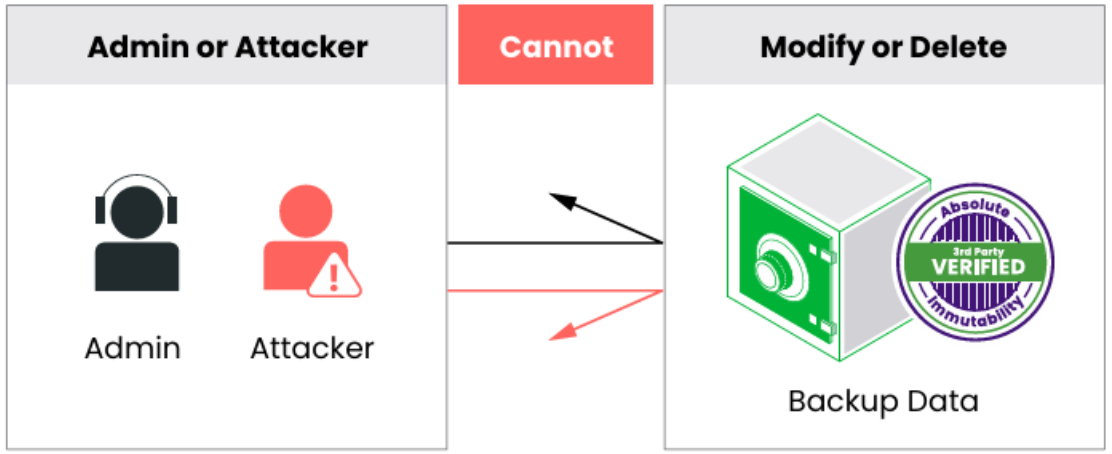


*to the BIOS, OS, the storage application, or data

Immutabilità...
o "Immutabilità assoluta"?

L'immutabilità non significa nulla se può essere compromessa con una violazione.

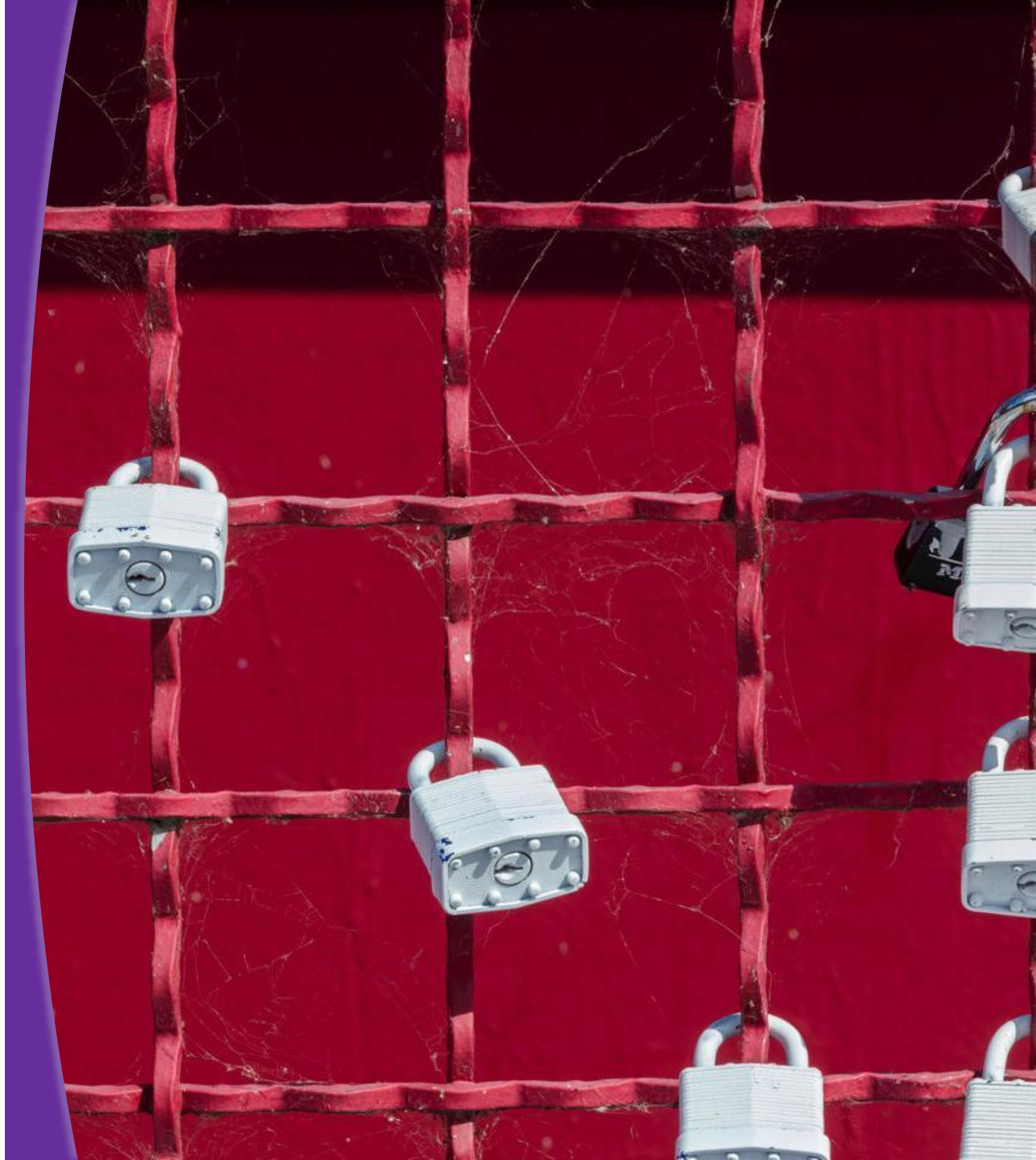
L'immutabilità assoluta significa che anche l'amministratore con i privilegi massimi o un malintenzionato con accesso allo storage di backup non può modificare o eliminare i dati.



Come raggiungere l'Immutabilità Assoluta?

- Object Storage S3
- Appliance di destinazione appositamente progettata
- Zero time per l’Immutabilità

Soddisfacendo questi requisiti, le imprese possono garantire che, qualunque cosa accada, ransomware, minacce interne o violazioni delle credenziali, i dati di backup rimangano protetti e recuperabili.



Chi siamo:
I Fondatori di Object First

Ratmir Timashev
Co-Founder & Board Member

Andrei Baronov
Co-Founder & Board Member

.. fondatori di Veeam

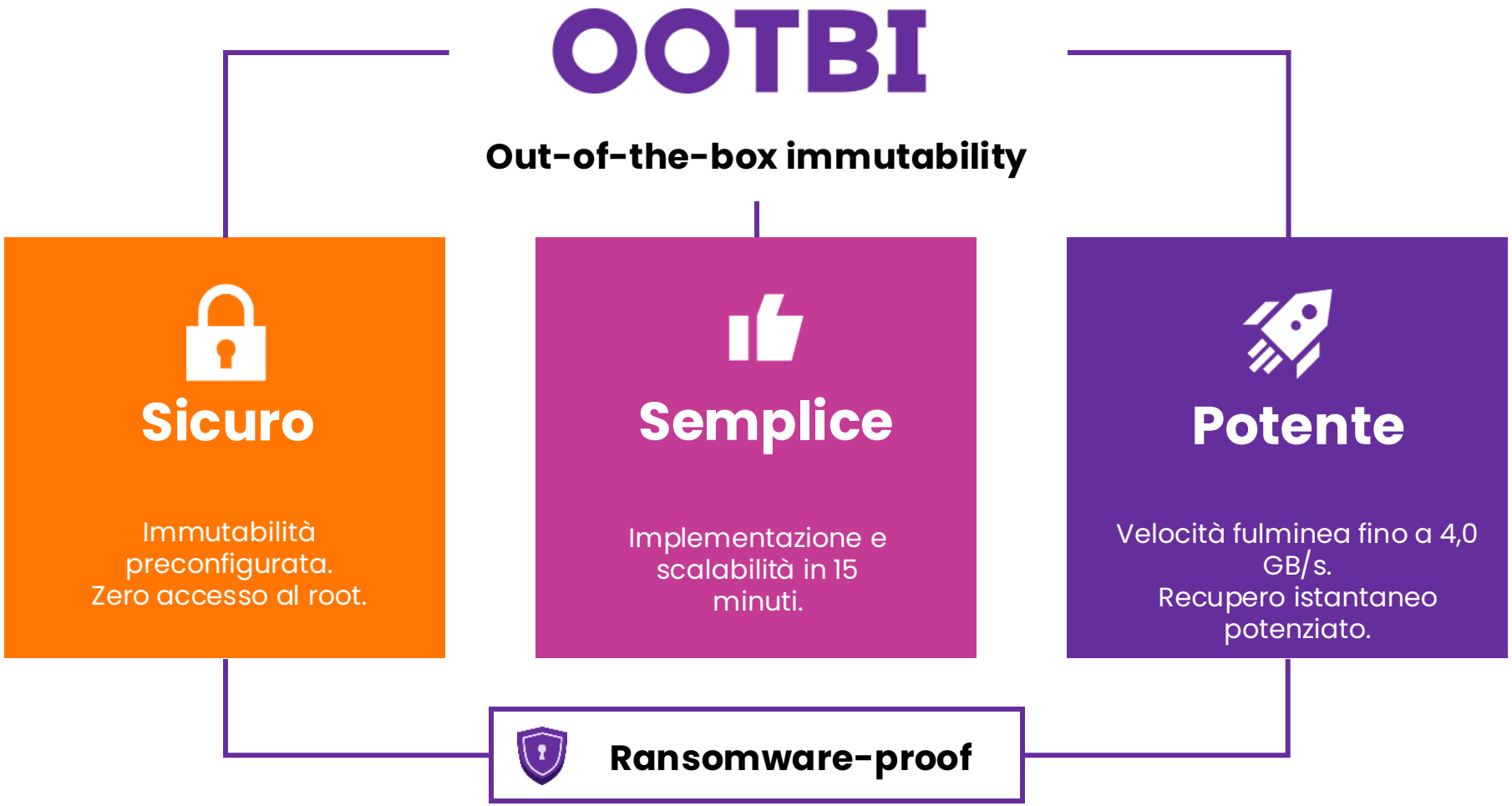
Vision

Fornire il miglior Storage per Veeam

A prova di Ransomware, immutabile, pronto all'uso

Zero Trust Data Resilience

Best Storage for Veeam



Protezione dei dati resiliente con la strategia 3-2-1-1-0

3 Copie dei dati ✓

Proteggi i tuoi dati con tre copie, inclusa la copia di produzione

Best Storage for Veeam

Backup Software

Target Backup Primario

Immutabilità S3

Data center Primario

Immutabilità senza sforzo
+ Recupero istantaneo

Target Secondario

Immutabilità S3

Data center Secondario

Cloud

Conservazione a lungo termine

Direttiva Europea
NIS 2/DORA

Alcuni Punti chiave:

- Rafforzare la sicurezza informatica
- Obbligo di segnalazione degli eventi
- Gestione del rischio, responsabilità e inasprimento sanzioni
- Processi di continuità aziendale, come la gestione dei backup, il disaster recovery, i tempi di ripristino e la gestione della crisi.
- Sicurezza della supply chain
- Soluzioni di autenticazione a più fattori o autenticazione continua laddove appropriato
- Politiche e procedure relative all'utilizzo della crittografia e, laddove appropriato, della cifratura

Direttiva Europea
NIS 2/DORA

Come Object First può essere d'aiuto

- Conformità a Resilienza dei dati Zero Trust
- Archiviazione dati di backup immutabile e certezza di ripristino dei dati
- Raggiungere gli obiettivi dei tempi di ripristino (RPO e RTO)
- Autenticazione multifattore

Focus sulla sicurezza
Test di terze parti

La conclusione di NCC:

L'applicazione Ootbi è progettata per proteggere da qualsiasi violazione di dati o infestazione di malware di un cliente Object First: anche se tutti i segreti del cliente, incluse le credenziali dell'amministratore e le credenziali del bucket, sono note all'utente malintenzionato, quest'ultimo non può comunque modificare i dati archiviati in un dispositivo Ootbi.

NCC Group, Ootbi Product Security Assessment, 31 luglio 2024


OBJECT FIRST

nccgroup

Test Report

Independent Security Test Report

Object First Immutable Backup Storage Appliance

October, 2024

Security Update

Object First is committed to meeting IT security industry standards for its flagship product Ootbi (Out-of-the-box Immutability), which serves as a secure-by-design storage target for Veeam backup data. Security experts continuously improve the hardening of the product, and we regularly engage with independent, third-party testing firms for validation that Ootbi is secure-by-default.

We employed the expertise of the NCC Group, a team of cybersecurity experts, to conduct comprehensive penetration tests on the Ootbi appliance and its software to identify and address undiscovered risks. This paper provides a summary of NCC's findings and important security information about Object First's Ootbi solution.

NCC's Final Takeaway

The Ootbi application is designed to protect against any data breach or malware infestation of an Object First customer: even if all of the customer's secrets, including administrator credentials and bucket credentials, are known to the attacker, the attacker still cannot modify data stored within an Ootbi appliance.

-NCC Group, Ootbi Product Security Assessment, July 31, 2024

nccgroup

1

OBJECT FIRST

Vuoi saperne di più?

Vieni a trovarci al desk Object First

OBJECT FIRST

Grazie!