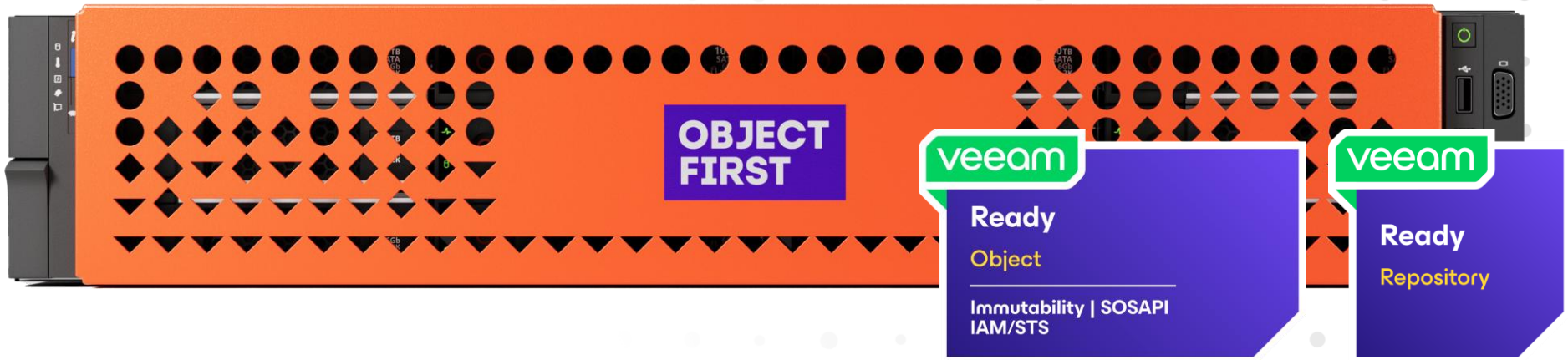
OBJECT FIRST

Simply Resilient



Simona Riela
Channel & Territory Manager

Filippo Martucci
Sales Engineer

OBJECT FIRST

Lo scenario in breve

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

OBJECT FIRST

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.

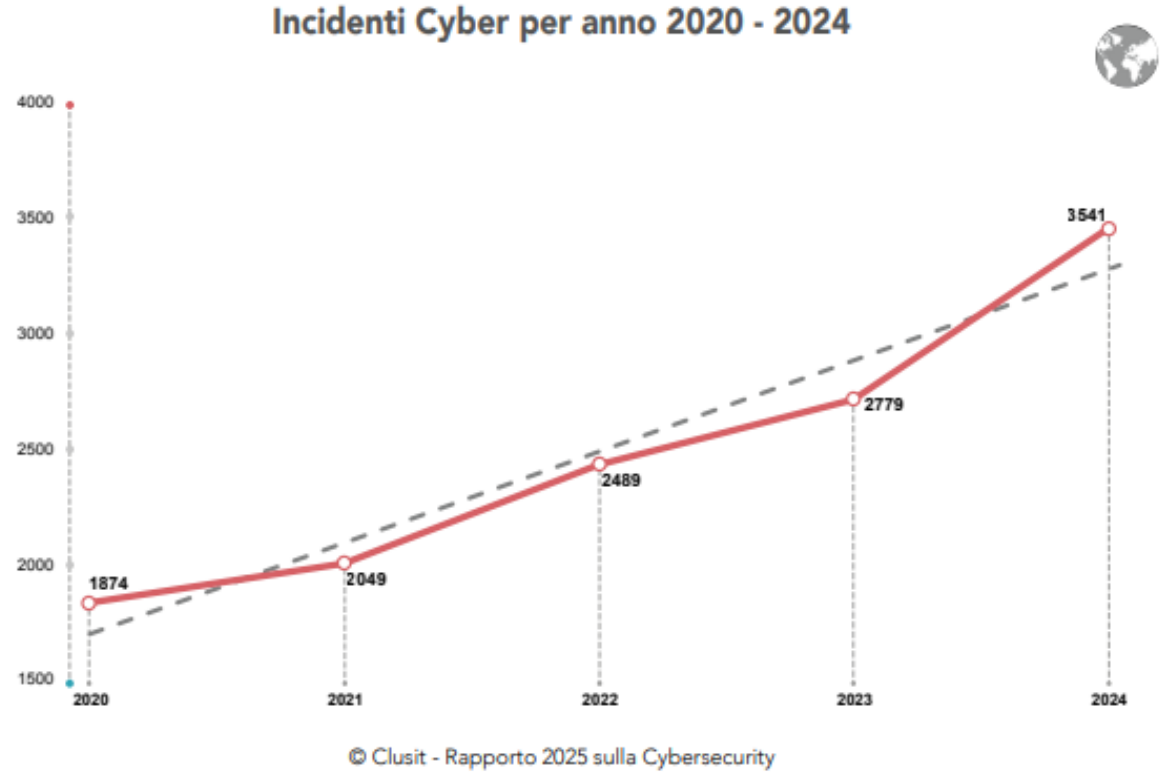


Fig. 1 - Andamento degli incidenti cyber nel periodo 2020-2024

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.

OBJECT FIRST

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).

OBJECT FIRST

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.

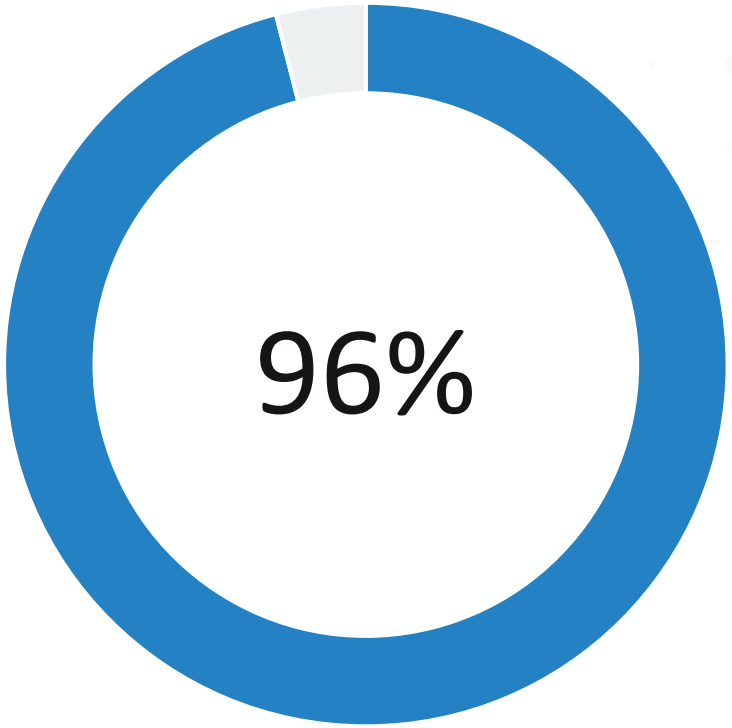
OBJECT FIRST

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.

OBJECT FIRST

Gli attacchi criminali prendono di mira i backup

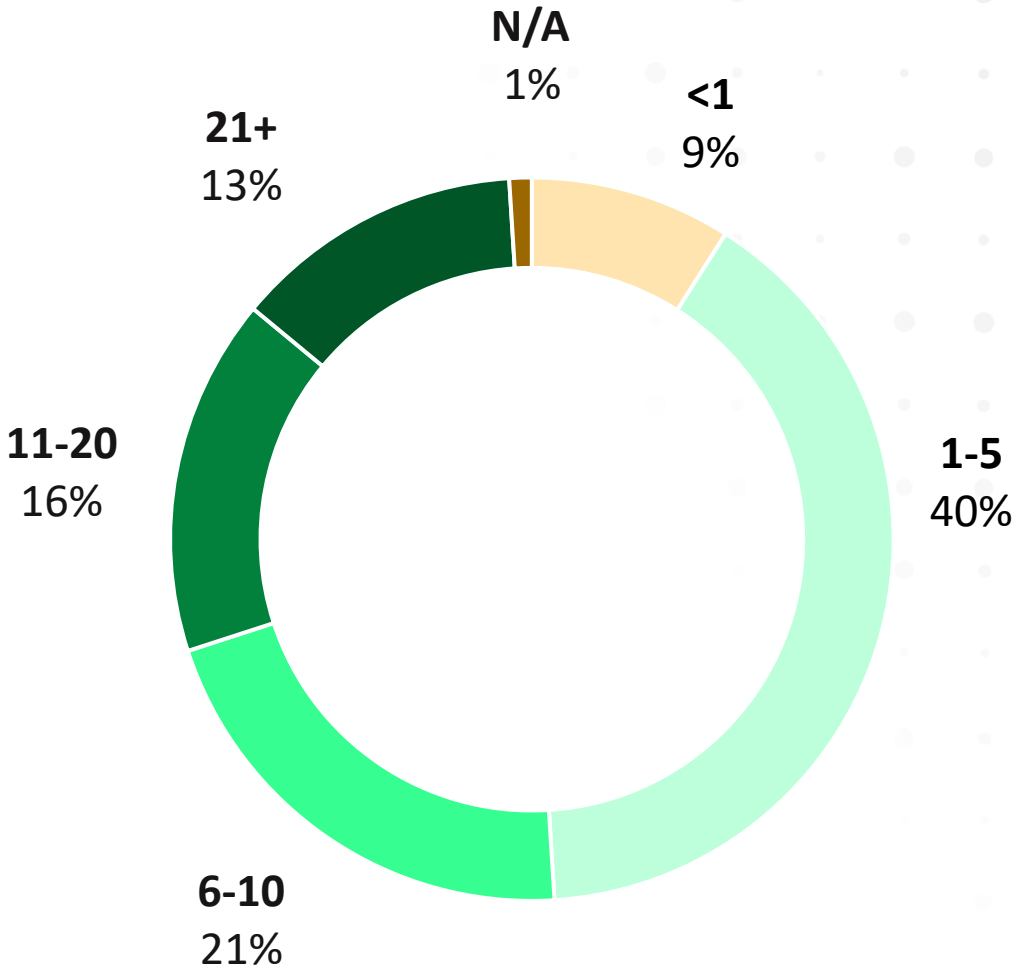


Attacchi che hanno preso di mira i backup

Source: ESG Research 2025

OBJECT FIRST

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

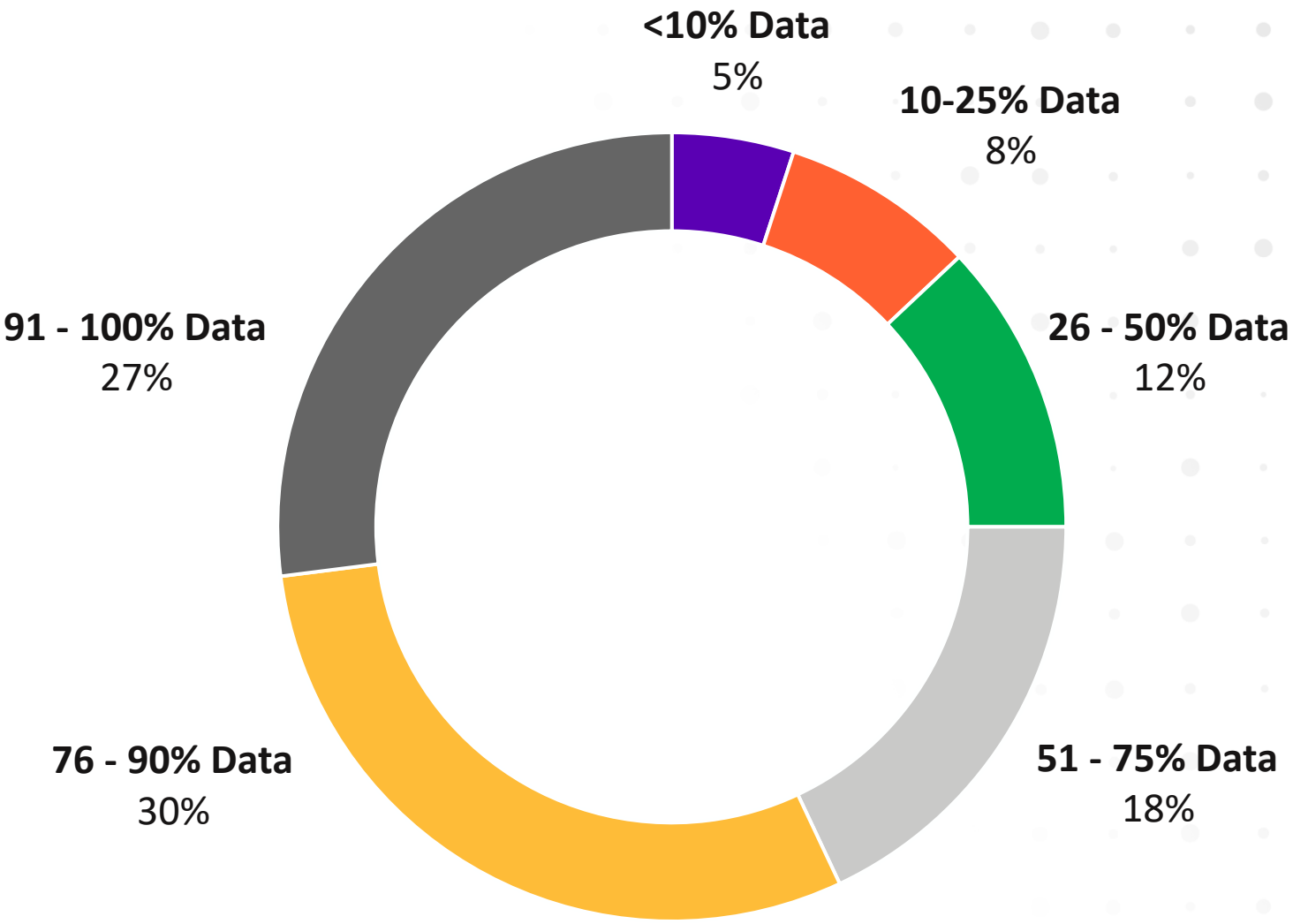


Giorni lavorativi necessari per ripristinare la piena operatività

Source: ESG Research 2025

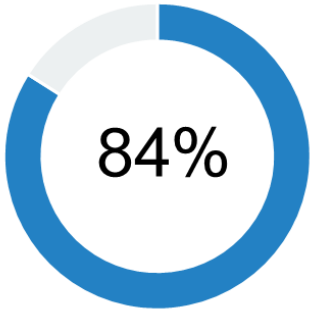
OBJECT FIRST

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

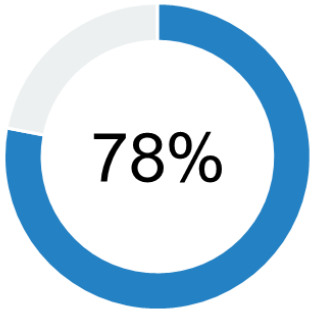


Source: ESG Research 2025

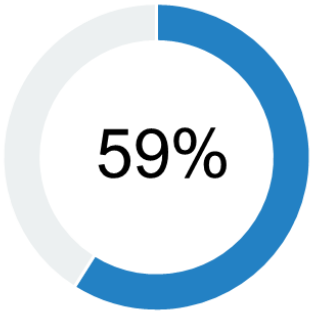
The Human Cost: l'impatto su chi lavora nell'IT



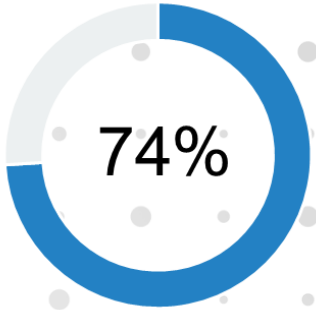
Segnala di sentirsi a disagio e stressato per i rischi derivati dalla sicurezza IT



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

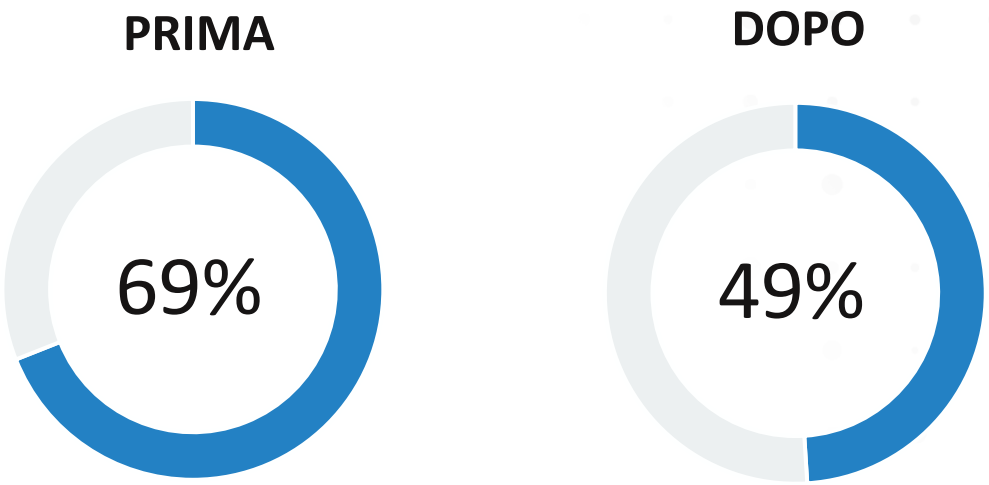


La tecnologia e gli strumenti che utilizzano per il recupero dei dati sono complicati o alquanto complicati da usare e richiedono almeno un certo livello di competenza in materia di sicurezza

Source: Object First Research 2025

OBJECT FIRST

Quando la teoria incontra la realtà...



Fiducia delle aziende nei propri preparativi per affrontare un attacco ransomware

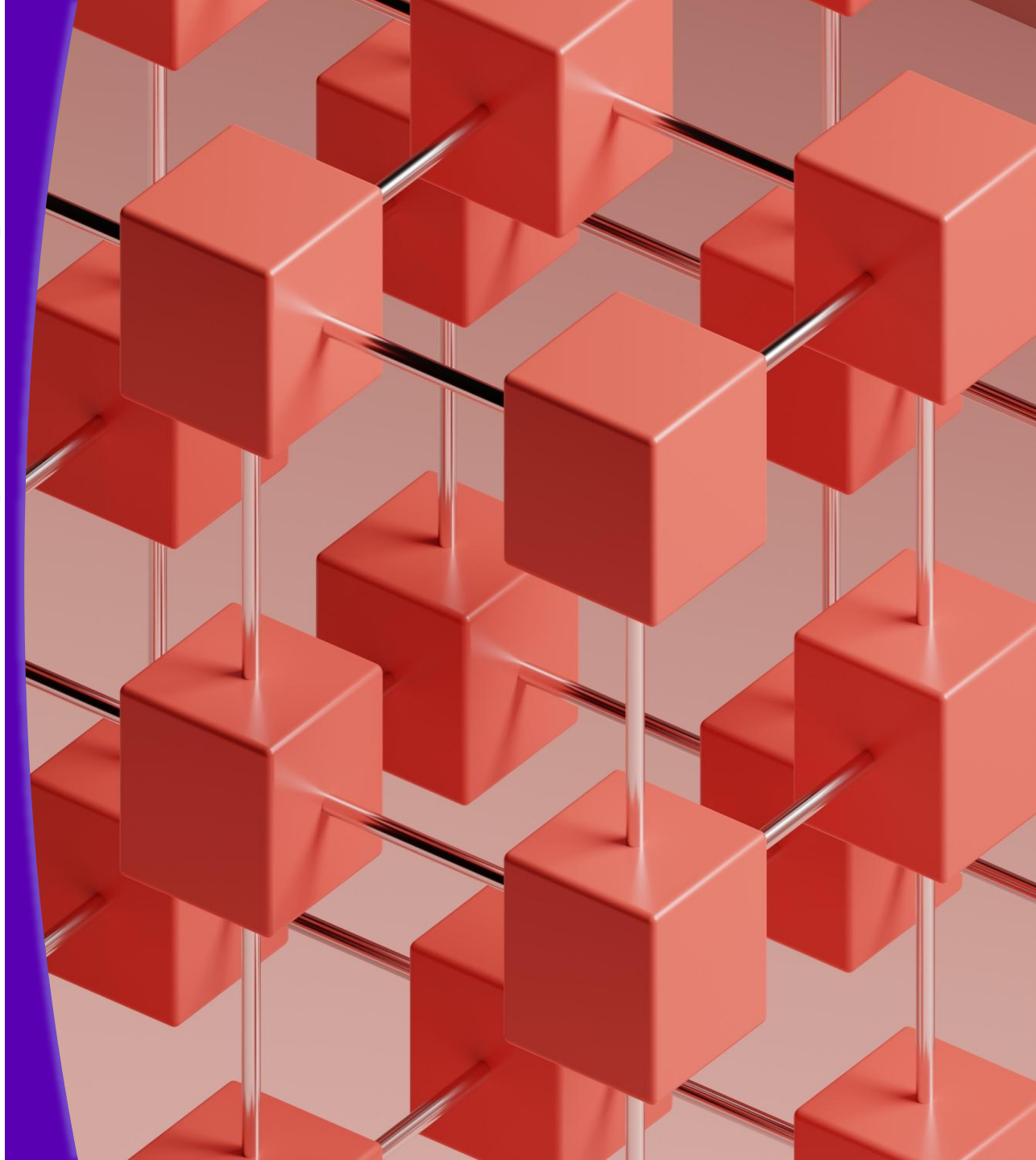
Calo del 20% nella fiducia dopo aver subito un attacco ransomware

Source: Veeam Ransomware Survey 2025

OBJECT FIRST

Punti chiave

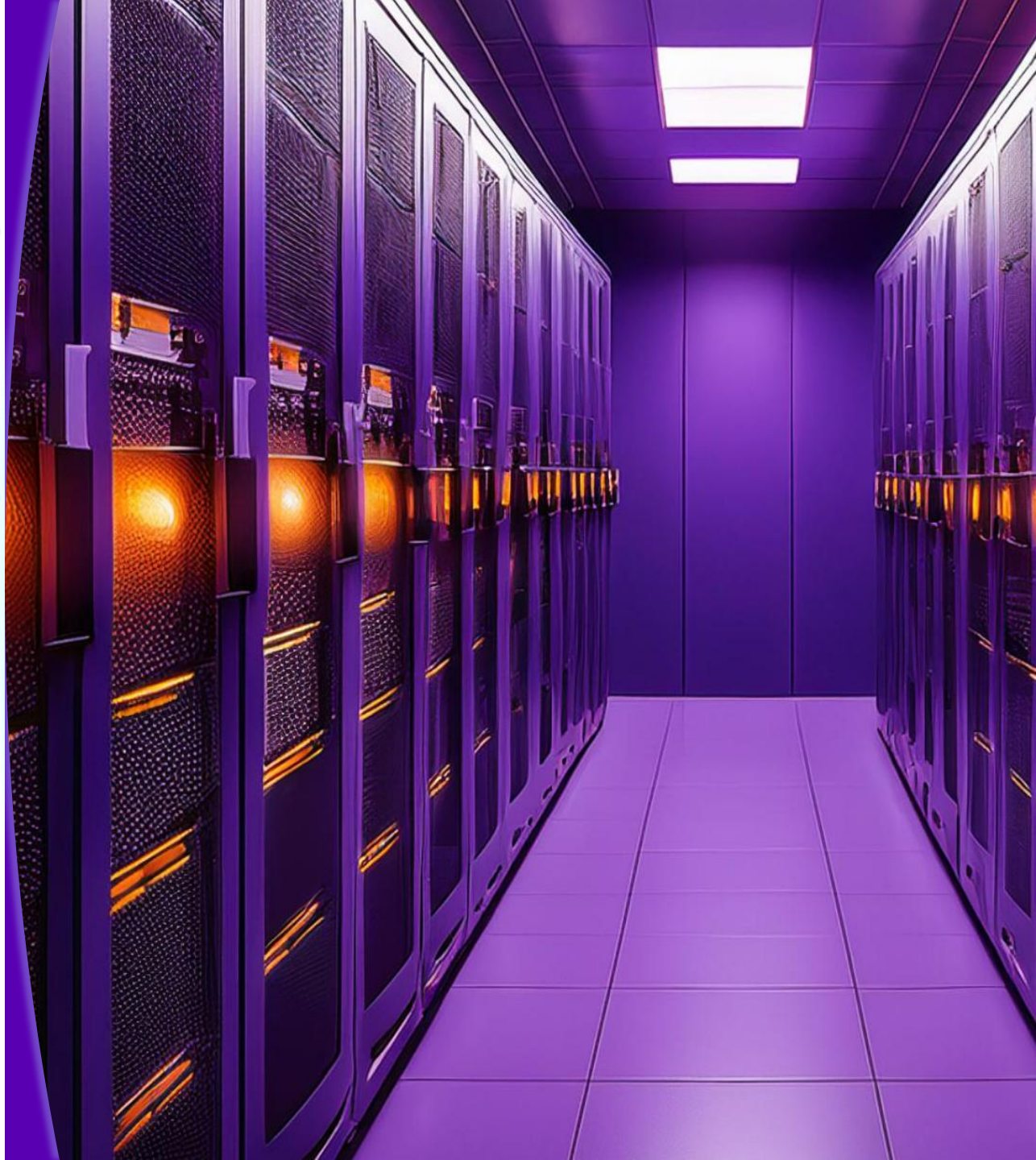
- Attacchi informatici: "quando" non "se "
- I backup sono ad alto rischio
- Enorme interruzione dell'attività...
- Include lo stress e la fidelizzazione del personale
- Preparato? Potrebbe essere discutibile!
- La tecnologia e gli strumenti potrebbero non essere all'altezza del compito



OBJECT FIRST

La resilienza dei dati è necessaria –

Ma come?



OBJECT FIRST

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

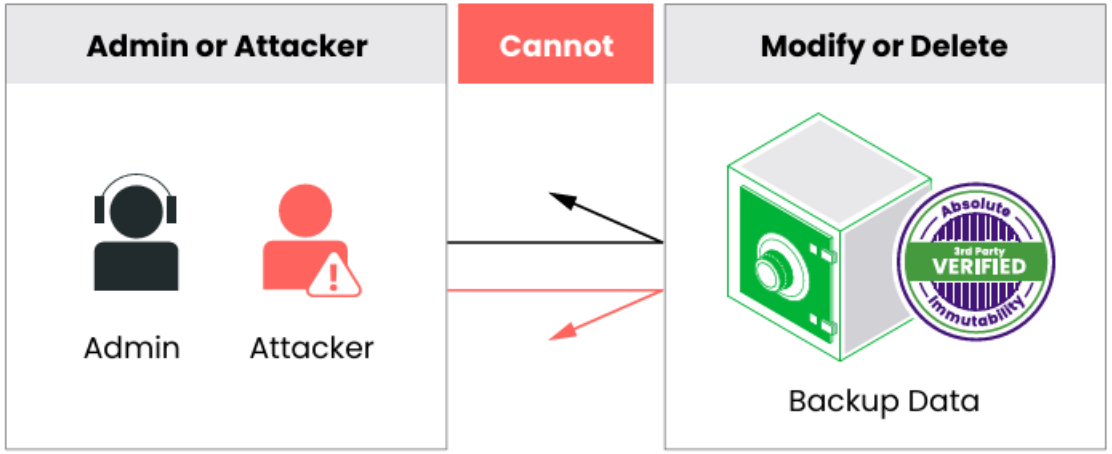
Proteggi i dati di backup da modifiche o cancellazioni.

OBJECT FIRST

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.



OBJECT FIRST

Come raggiungere l'Immutabilità Assoluta?

Absolute Immutability	Unverified Immutability
1. S3 Object Storage	Proprietary Storage
2. Zero Time to Immutability	Time-Delayed Immutability Snapshot-Based Immutability
3. Target Storage Appliance	Integrated Appliance Dedupe Appliance Self-Managed System DIY Storage System

Qualunque cosa accada—ransomware, minacce interne o violazioni delle credenziali—i dati di backup rimangono protetti e recuperabili.

OBJECT FIRST

Fondatori

Ratmir Timashev
Co-Founder & Board Member

Andrei Baronov
Co-Founder & Board Member

Vision

Fornire il miglior storage per Veeam

A prova di Ransomware e con Immutabilità Assoluta

Zero Trust Data Resilience

OBJECT FIRST

Backup Storage con Immutabilità Assoluta

Immutabilità Assoluta

Sicuro

- Architettura Zero Trust con storage ad oggetti nativo S3
- Zero Accesso all'esecuzione di operazioni distruttive
- Testato e verificato da terze parti

Semplice

- Nessuna competenza in tema di sicurezza richiesta
- Implementazione e scalabilità in 15 minuti
- Aggiornato e ottimizzato automaticamente da Object First

Potente

- Backup fulminei, fino a 8 GB/s
- Instant Recovery ultrapotenziato
- Capacità e prestazioni scalano in modo lineare, supportate da bilanciamento automatico del carico

A prova di Ransomware

OBJECT FIRST

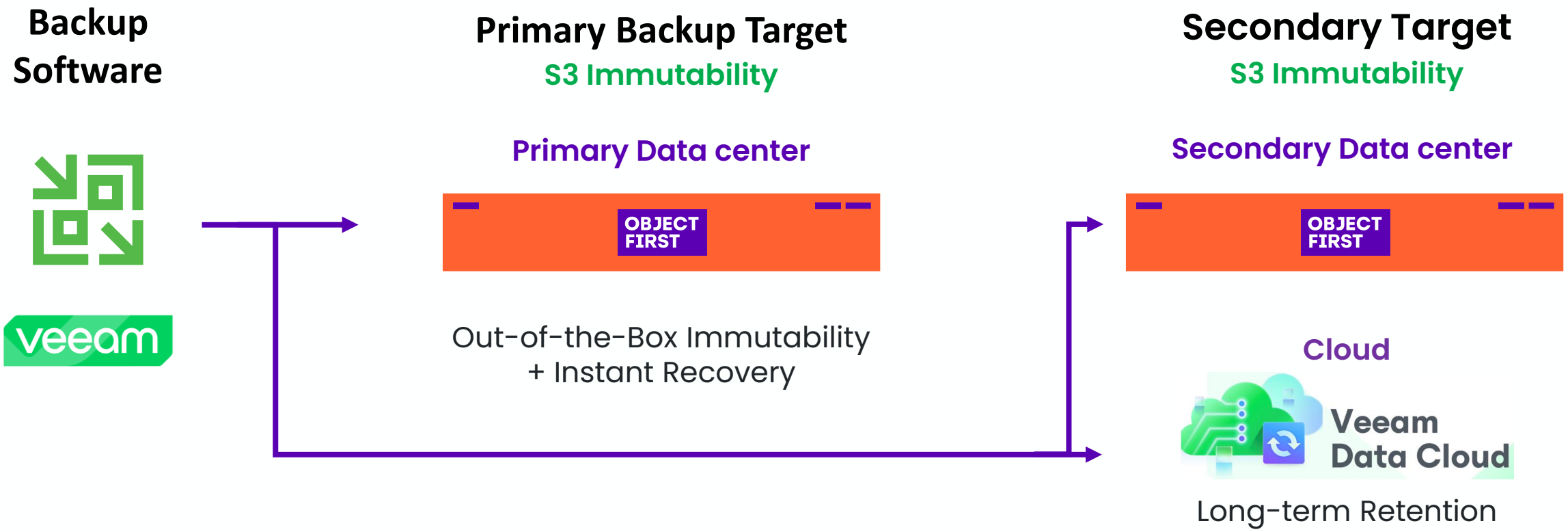
veeam

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

3 Copie dei dati ✓	2 media diversi ✓	1 Copia fuori sede ✓	1 copia air-gapped/immutabile ✓	0 Errori o Malfunzionamenti ✓
Proteggi i tuoi dati con tre copie, inclusa la copia di produzione	Riduci i rischi utilizzando almeno due tipi di supporti di archiviazione distinti, proteggendo dal guasto di ogni singolo dispositivo di archiviazione	Stabilisci una protezione dei dati resiliente dal punto di vista informatico con almeno un backup archiviato in una posizione fisicamente separata, offrendo protezione contro i danni fisici	Mantieni una copia disconnessa dalla rete/Internet o immutabile, fornendo un ulteriore livello di difesa contro le minacce informatiche	Avere i backup non è sufficiente. Testa regolarmente i tuoi backup per assicurarti che possano essere ripristinati correttamente quando necessario.

OBJECT FIRST

Miglior Storage per Veeam



Perchè la copia primaria deve essere immutabile?

Panoramica sull'evoluzione del cyber crime in Italia e nel mondo - Analisi dei principali cyber attacchi noti del 2023 a livello globale

Fig. 28 - Crescita percentuale degli attacchi Italia vs. global - 2019-2023

Fonte Agenzia Cybersicurezza Nazionale

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.

Il cybercrime cresce ai danni delle nostre aziende: il report Clusit 2025

Home > News, Attualità E Analisi Cyber Sicurezza E Privacy

Dalla presentazione del rapporto Clusit 2025 emerge uno scenario preoccupante, con una crescita del cybercrime e un aumento degli attacchi basati su vulnerabilità. Il settore pubblico e le infrastrutture critiche sono sempre più nel mirino, mentre il ransomware continua a dominare la scena. I dati più rilevanti

Cybersecurity 2025: crescita record di attacchi in Italia e nel mondo - Cyber Security 360

OBJECT FIRST

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

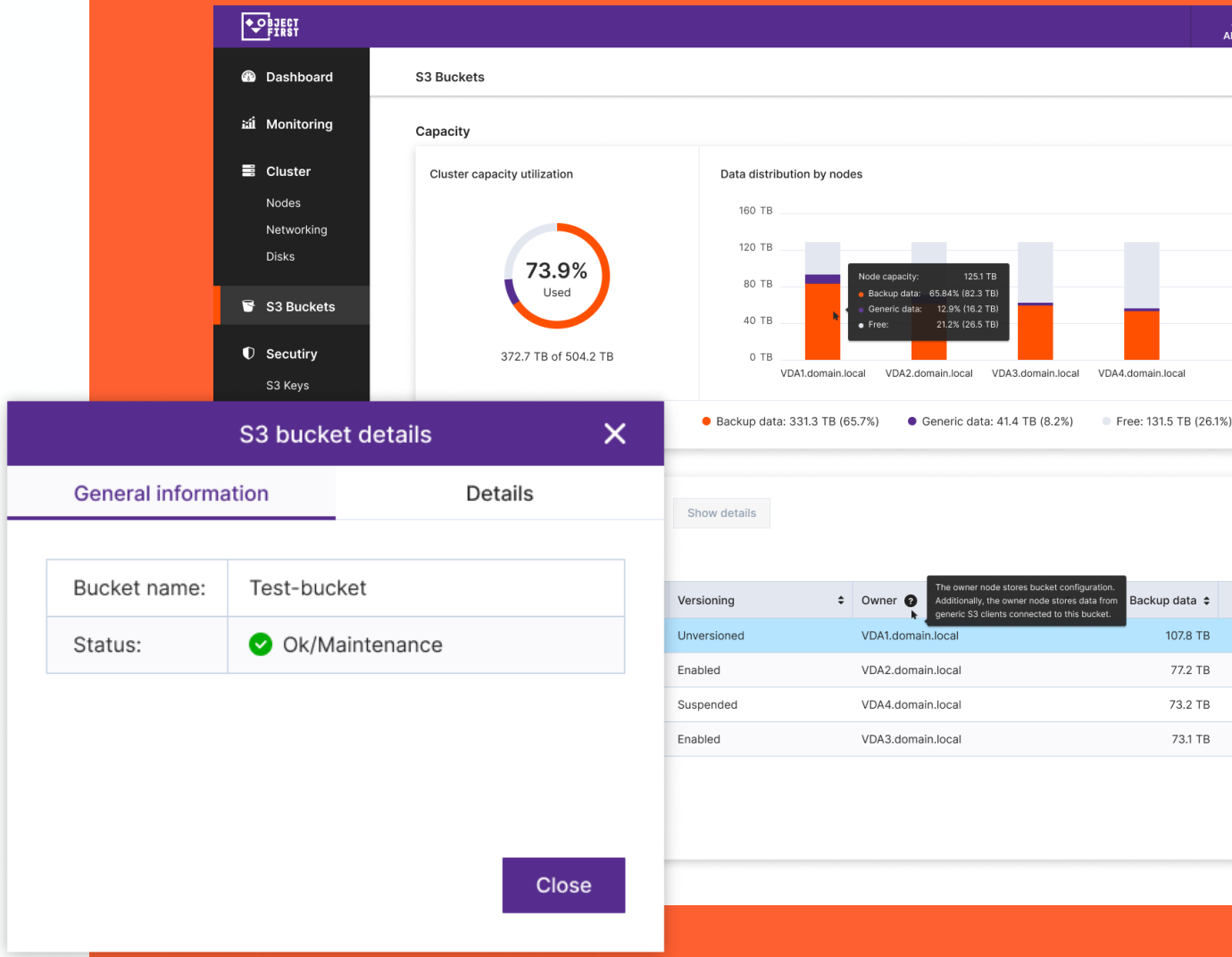
Direttiva Europea
NIS 2/DORA

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)
- Autentificazione multifattore

Sicuro

- Immutabilità Assoluta nativa S3 con comunicazioni sicure
- Storage Hardenizzato con Zero Access per evitare azioni distruttive sui dati di backup
- Separazione fisica dal Veeam Backup Server
- Test e validazione continui di sicurezza da terze parti



Sicurezza Verificata

"L’appliance Ootbi è progettata per proteggere i clienti di Object First da qualsiasi violazione dei dati o attacco malware: anche se l’aggressore dovesse conoscere tutti i segreti del cliente, incluse le credenziali dell’amministratore e quelle del bucket, non sarebbe comunque in grado di modificare i dati archiviati all'interno di un dispositivo Ootbi."
NCC Group
Ootbi Product Security Assessment


OBJECT FIRST

Test Report

Independent Security Test Report

Object First immutable backup storage appliance

October, 2024

nccgroup

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.

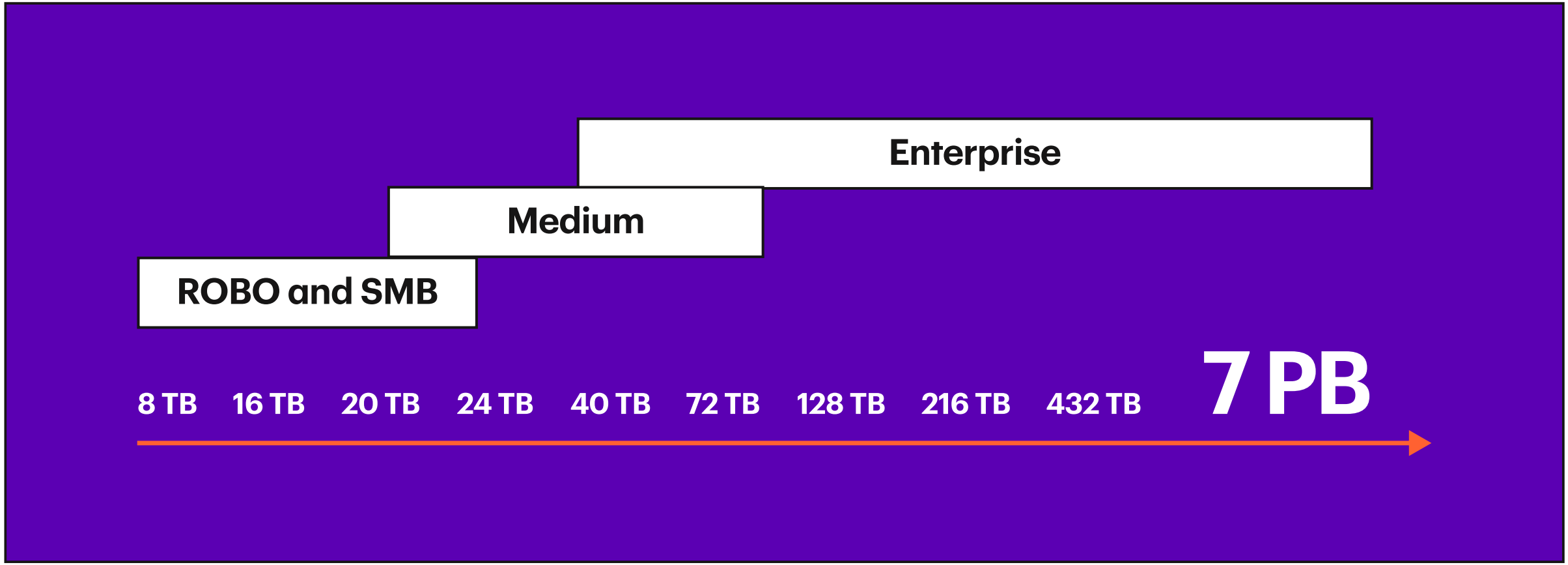
-NCC Group, Ootbi Product Security Assessment, July 31, 2024

1.0_20251118

Page 1

OBJECT FIRST

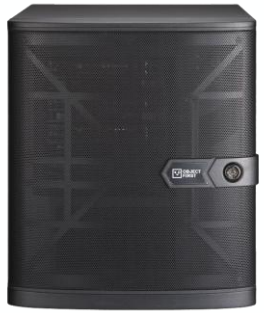
Immutabilità per tutti

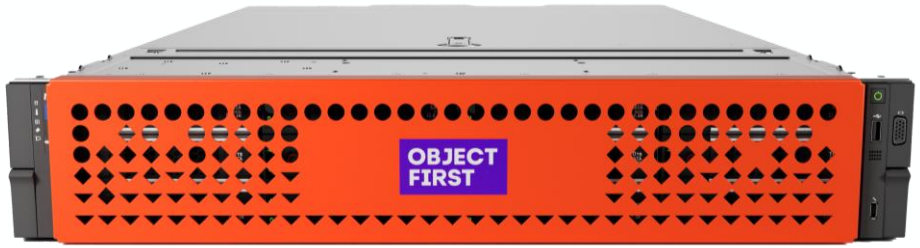


Formato e capacità per soddisfare ogni caso d'uso

Combina, abbina e scala all'interno di ogni formato—fino a 1,7 PB per cluster, 7 PB totali[1]

For ROBO, SMB and Edge	For Data Center	
8 TB	18 TB	144 TB
16 TB	40 TB	216 TB
24 TB	72 TB	432 TB





[1]7 PB capacity in Veeam Scale-Out Backup Repository (SOBR) configuration

OBJECT FIRST

Novità! Scelta dei modelli di acquisto di Ootbi

	CapEx Traditional upfront purchase	Consumption* Pay-per-use subscription
Software, OS, and updates	✓	✓
Technical support	✓	✓
On-site service	✓	✓
Duration	Fixed term (up to 5 years)	As long as your subscription

*Available in USA, European Union, and United Kingdom

OBJECT FIRST

Thank you!