16 GIUGNO 2025 - ore 14.00

OGR-Tech . Sala Mezzanino . Torino

LAN SERVICE ACADEMY

INTELLIGENZE ARTIFICIALI
SICUREZZE REALI

COLIN CONSULENTE LEGALE INFORMATICO

DATACORE

/LIBRAESVA

REEVO

veeam

LAN SERVICE group

agenda

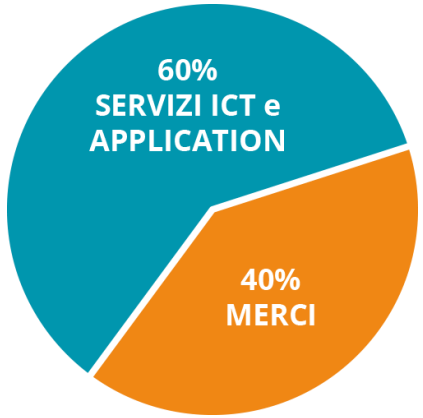
Coffee time e registrazione partecipanti	14.00
Inizio evento – Il Benvenuto di Lan Service group	14.30
Prof. Cataldo Basile, Politecnico di Torino	14.40
Avv. Alessandro Cecchetti, Socio e Manager Colin & Partners	15.00
Prima parte del talk moderato da Marco Lorusso con DataCore, Libraesva, ReeVo, Veeam, Lan Service group. *Relatori: Remi Bargoing, Martino Franzini, Claudio Panerai, Marco Carrara*	15.30
Coffee break	16.10
Seconda parte del talk moderato	16.30
Matteo Ghigo, Consulente Informatico Forense – Di.Fo.B.	17.10
Sezione Q&A e Conclusioni di Lan Service group	17.40
Aperitivo a buffet	18.10
Saluti finali	19.30

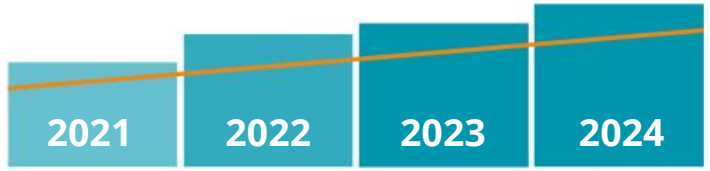
LAN SERVICE group

in numeri

CERTIFICAZIONI

HPE Silver / Aruba Silver
Cisco / Meraki Premier
Microsoft Gold
Citrix
Sentinel One
Wmware Silver
Veeam Gold
Sophos Silver
Fortinet
Dell
Datacore
Kaspersky





Prof. Cataldo Basile, Politecnico di Torino

Intelligenza Artificiale e Cybersecurity

Cataldo Basile

< cataldo.basile @ polito.it >

Politecnico di Torino

Dip. Automatica e Informatica

Machine Learning e Generative AI

- **Machine Learning (ML)**
  - algoritmi e modelli capaci di apprendere dai dati, riconoscere schemi, fare previsioni senza essere esplicitamente programmati per un compito specifico
- **Generative AI (genAI)**
  - produce attivamente nuovi contenuti a partire da dati esistenti
    - testi, immagini, video, musica, codice
  - utilizza modelli addestrati per apprendere le caratteristiche e le strutture dei dati
- **Large Language Model (LLM ~ genAI)**
  - addestrato su enormi quantità di testo per comprendere e generare linguaggio naturale in modo coerente e contestuale
  - ChatGPT, Claude, Gemini, LLaMA, Mistral, ...

AI e Cybersecurity

- **applicazioni dell'AI stanno migliorando la cybersecurity**
  - sistemi di **monitoring**
    - identificazione più precisa delle minacce
    - algoritmi non-supervisionati per identificare minacce ignote
    - migliore correlazione tra eventi di sicurezza
    - generazione di Cyber Threat Intelligence e playbook più precisi grazie agli LLM
  - identificazione di **phishing e spam**
    - pattern linguistici sono più efficienti nell'identificare i contenuti malevoli o sospetti
  - riconoscimento di **malware**
    - più difficile l'evasione, riconoscono polimorfismi, identifiano contenuti a rischio

GenAI e cybersecurity: giusta diffidenza

- **genAI non ancora affidabile**
  - soffre di allucinazioni
  - è troppo accondiscendente
  - risponde anche se non sa una risposta
  - si può convincere a superare limitazioni
- **sconsigliato usarla per ogni tipo di operazione sensibile**
  - OWASP Top Ten: Excessive Agency
    - concedere funzionalità e permessi eccessivi
    - eccessiva autonomia decisionale
- **deve esserci sempre approvazione esplicita dell'utente**
  - amministratori di sicurezza, addetti al SOC
  - supporta ma non può sostituire gli esperti
- **manca tracciabilità e *explainability***

Cybersecurity dell'AI: nuovi rischi

- **l'uso di AI sta aprendo nuovi problemi di cybersecurity**
  - più nascosti e subdoli di quelli tradizionali
- **LLM inseriti in molti contesti**
  - chatbot in sistemi web aziendali
    - addestrati su dati confidenziali
  - catene decisione di sistemi complessi
    - spesso invisibili all'utente finale
    - es. per priorità agli interventi in caso di incidenti
  - supporto alla scrittura di codice o script di gestione
    - insecure code generation / siti web vulnerabili / attacchi a DevOps
  - generazione (e invio) di risposte automatiche alle email

Sicurezza degli LLM

- **LLM devono essere protetti da**
  - accessi non autorizzati
  - abuso di funzionalità da parte di utenti legittimi
- **bisogna garantire che**
  - gli input siano corretti (Prompt Injection)
  - non vengano prodotti in output dati confidenziali
  - i dati di training non alterino le risposte in output (integrità)
  - non vengano richieste operazioni che possano compromettere i sistemi
  - non ci siano violazioni del GDPR
- **sicurezza nello sviluppo di LLM**
  - sviluppo sicuro in tutte le fasi
- **sicurezza dei stistemi che usano gli LLM**

Come mitigare i rischi?

- **l'AI va trattata come un normale utente che genera input**
  - talvolta non è dei più svegli
- **validare tutto con approcci Zero Trust**
  - controllo accessi
  - inclusi i dati per il training
- **applicare il paradigma Security-by-Design**
- ***Human-in-the-Loop***
  - tutte le volte che ci sono decisioni o processi sensibili...
  - l'AI può suggerire ma non dobbiamo lasciarla agire direttamente
- **monitoraggio costante degli strumenti AI**
  - input e output
- **red teaming contro LLM e sistemi che includono LLM**

Avv. Alessandro Cecchetti, Socio e Manager Colin & Partners

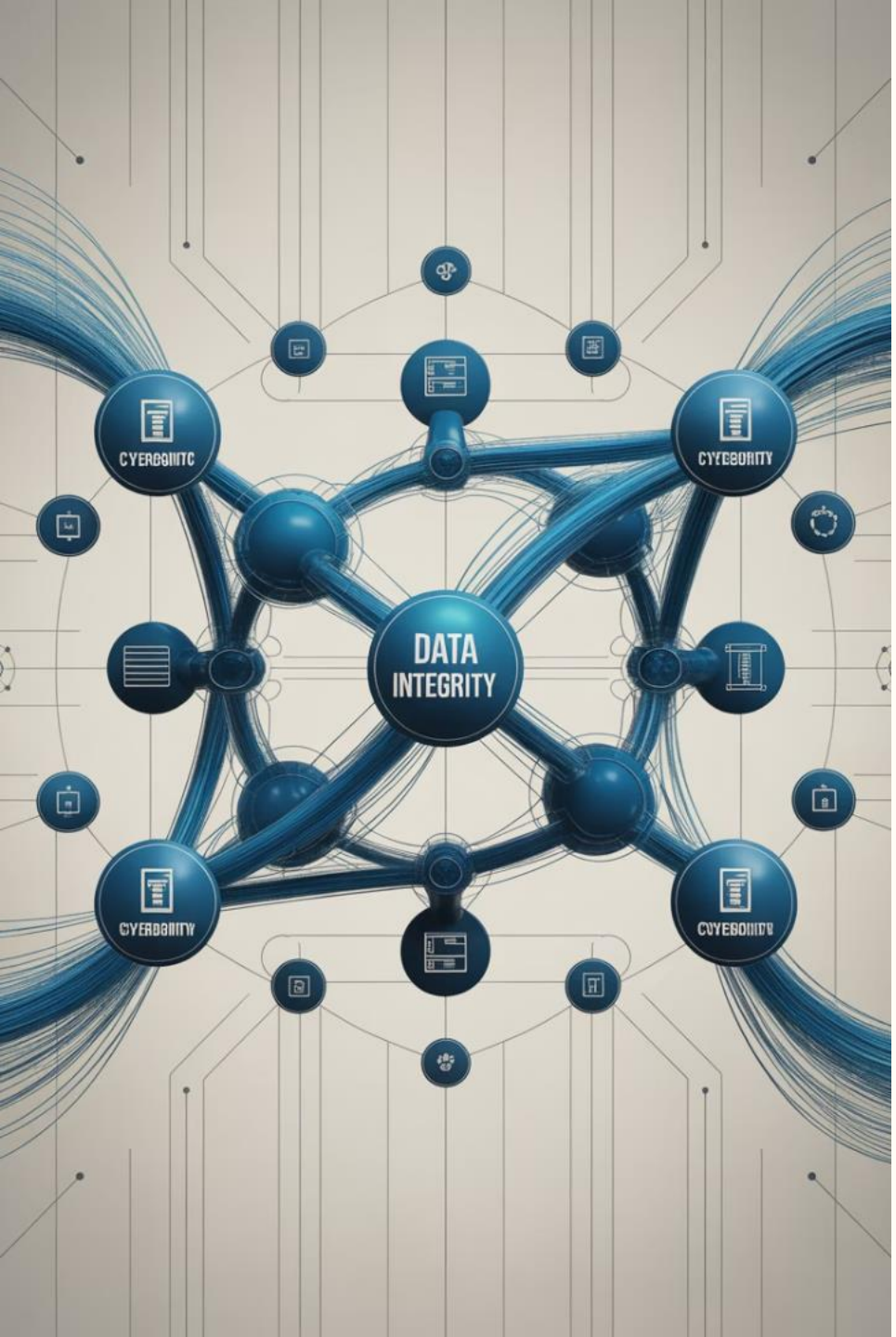
COLIN
CONSULENTE LEGALE INFORMATICO

Decreto NIS-2

L'impatto degli obblighi sulle imprese

Avv. Alessandro Cecchetti

Socio e Manager Colin & Partners



La NIS2 introduce una nuova accountability sulla cybersecurity

Per gestire i rischi di sicurezza dei sistemi informatici e di rete

che utilizzano nella loro attività **o** nella fornitura di servizi

Tenuto conto dei rischi esistenti

Introduzione di misure **tecniche + operative + organizzative**

ADEGUATE E PROPORZIONATE

(in base al grado di esposizione del soggetto, delle dimensioni, della probabilità degli incidenti, della gravità, e del loro impatto sociale ed economico)

Per **prevenire** o **ridurre al minimo** l'impatto degli **incidenti** per i destinatari dei loro servizi.

Art. 7 comma – Identificazione ed elencazione dei soggetti essenziali e importanti

Periodo di notifica

Dal 15 aprile al 31 maggio **di ogni anno**, tramite la piattaforma digitale, i soggetti identificati come importanti o essenziali, **forniscono O aggiornano:**

Informazioni tecniche

lo spazio di indirizzamento **IP pubblico** e i **nomi a dominio** nella disponibilità del soggetto

elenco degli **stati membri** in cui forniscono beni o servizi in perimetro NIS2

Responsabilità personale

Qualsiasi **PERSONA FISICA**:

- **responsabile** che agisca in qualità di suo **rappresentante legale** con l'autorità di **rappresentarlo**
- di **prendere decisioni per suo conto**
- o di **esercitare un controllo** sul soggetto stesso

che assicura il rispetto delle disposizioni NIS2.

Tali persone fisiche possono essere ritenute **responsabili dell'inadempimento** in caso di violazione della normativa da parte del soggetto di cui hanno la rappresentanza

Punto di contatto

Un **sostituto del Punto di Contatto**, indicando i relativi recapiti

Qualsiasi **modifica delle informazioni trasmesse** ai sensi dell'art. 7 devono essere notificate ad ACN tempestivamente, e comunque non oltre 14 giorni dalla data di modifica.

Gli organi amministrativi e direttivi: il ruolo rispetto alla compliance

Approvano le modalità di implementazione delle misure di gestione dei rischi

per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24

Sovrintendono all'implementazione degli obblighi

sanciti dalla normativa

Sono responsabili delle violazioni

di cui al presente decreto

Sono tenuti a seguire una formazione

in materia di sicurezza informatica

Promuovono l'offerta periodica di una formazione ai loro dipendenti

per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti.

Sono informati su base periodica o, se opportuno, tempestivamente, degli incidenti e delle notifiche

Gli organi amministrativi e direttivi: che s'intende?

Definizione secondo ACN - Cfr: FAQ **ACN – AUTORITA' CYBERSICUREZZA NAZIONALE**

Composizione

L'elencazione dei **componenti del Consiglio di amministrazione** dell'organizzazione, o strutture analoghe tenuto conto della natura giuridica e alla struttura organizzativa dell'organizzazione

Esclusioni

Pertanto, ai fini dell'adempimento in parola, **non è attesa l'elencazione** delle persone fisiche che svolgono le funzioni di punto di contatto (e sostituto), di CISO o di responsabile della sicurezza aziendale, né **altre figure apicali sotto ordinate al CDA, salvo che essi siano anche componenti del CDA**

Sanzioni personali

Le sanzioni interdittive personali sui componenti degli Organi Amministrativi e Direttivi

L'applicazione della **sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali** all'interno del medesimo soggetto. Tale sospensione temporanea è applicata finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze **o a conformarsi alle diffide**.

PUNTO DI CONTATTO, il SOSTITUTO DEL PUNTO DI CONTATTO e le MISURE DI BASE

PUNTO DI CONTATTO

Il **PUNTO DI CONTATTO** è una persona fisica designata dal soggetto NIS con il compito di **curare l'attuazione** delle disposizioni del decreto NIS per conto del soggetto stesso

SOSTITUTO DEL PUNTO DI CONTATTO

Il **SOSTITUTO DEL PUNTO DI CONTATTO** è una persona fisica designata con le medesime modalità del punto di contatto, **che lo supporta** nell'esercizio delle proprie funzioni, e può interloquire direttamente con ACN e può effettuare sul Portale NIS

MISURE DI BASE

Le **Determinazioni ACN** sulle **misure di base** e gli **incidenti significativi di base** per i soggetti essenziali ed importanti

Sanzioni previste

10.000.000 €

Soggetti Essenziali

per quelli **essenziali** sono pari a un **massimo di almeno 10 000 000 EUR o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo** per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore

7.000.000 €

Soggetti Importanti

per quelli **importanti** le sanzioni pecuniarie amministrative sono pari a un **massimo di almeno 7 000 000 EUR o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo** per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore

2%

Sanzioni Accessorie

la sospensione temporanea o richiesta a un organismo di certificazione o autorizzazione, oppure a un organo giurisdizionale, secondo il diritto nazionale, di sospendere temporaneamente un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività pertinenti svolti dal soggetto essenziale

La Vigilanza dell'Autorità

Ispezioni in loco

Controlli diretti presso le sedi dei soggetti vigilati

Audit periodici sulla sicurezza

Verifiche programmate dei sistemi di sicurezza

Audit ad hoc

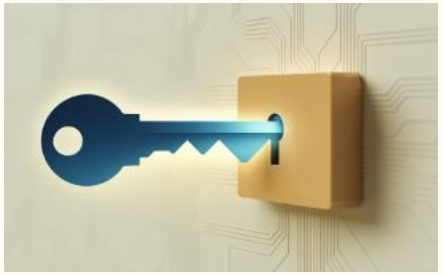
Verifiche non programmate in risposta a specifiche esigenze

Scansioni di sicurezza

Analisi automatizzate per identificare vulnerabilità

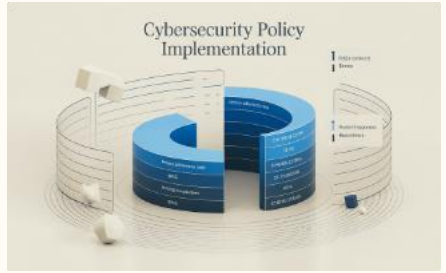
Richieste di informazioni

Sulle misure adottate e relativa documentazione



Richieste di accesso

A dati, documenti ed altre informazioni riservate



Richieste di dati

Che dimostrino l'applicazione di politiche di cybersecurity

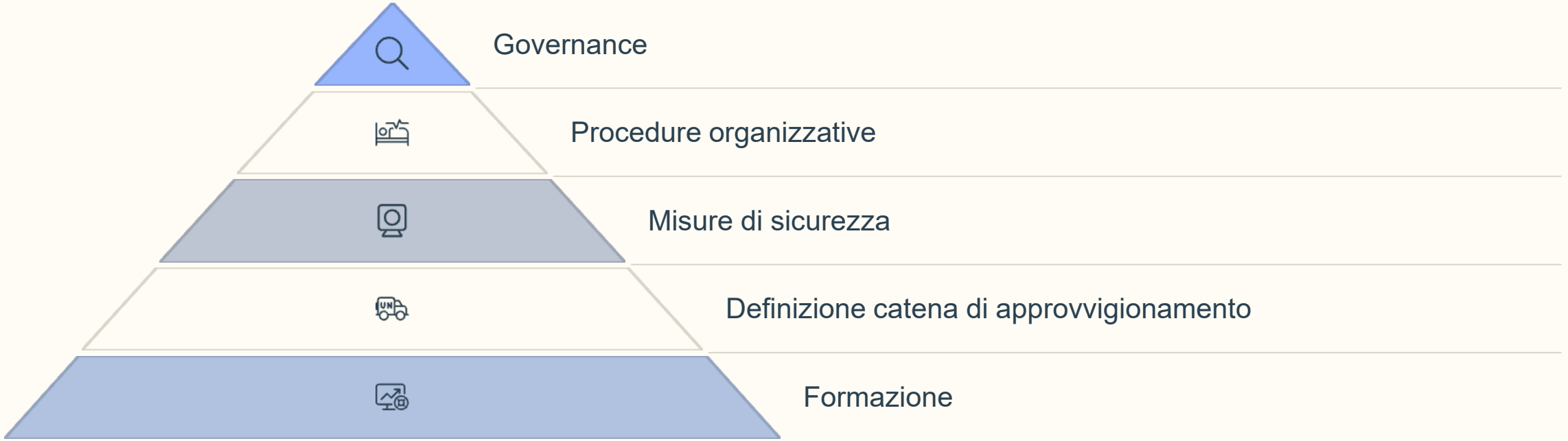
LE MISURE DELL'ART. 24…
e le Determinazioni di ACN

Politiche di analisi dei rischi e di sicurezza dei sistemi informativi	**Gestione degli incidenti**	**Continuità operativa come backup e ripristino in caso di disastro**
Dimostrabilità della sicurezza della catena di approvvigionamento ivi includendo, le valutazioni del Cybersecurity Act se deciso da Commissione ed ENISA	**Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informatici e di rete**	**Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi cyber**
Igiene informatica e formazione in materia cyber	**Politiche di crittografia e cifratura**	**Sicurezza delle risorse umane, strategie di controllo di accesso e gestione degli attivi**

Strong authentication continua, comunicazioni vocali, video e testuali protette, e sistemi di comunicazione di emergenza protetti

Quali temi devono essere analizzati?

È essenziale essere in grado di dimostrare di aver valutato:



NIS COMPLIANCE PROGRAM

Cyber security della supply chain

Fornitori critici: le azioni principali

Flusso rispetto all'ufficio acquisti

Integrazioni contrattuali

Definizione di clausole specifiche per garantire la sicurezza della catena di approvvigionamento

Audit e modalità delle remediations

Procedure di verifica e correzione delle non conformità

La segnalazione

Pre-allarme

entro 24 ore

Relazione finale

entro un mese relazione finale

Notifica iniziale

senza indebito ritardo, e comunque entro 72 ore dalla conoscenza dell'incidente significato con riferimento ad un aggiornamento delle informazioni andando ad indicare una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

Aggiornamenti

su richiesta di un CSIRT o, se opportuno, di un'autorità competente, una **relazione intermedia sui pertinenti aggiornamenti della situazione**;

GRAZIE

Avv. Alessandro Cecchetti

acecchetti@consulentelegaleinformatico.it

Linkedin: https://it.linkedin.com/in/acecchetti

Contatti

Sede legale
Via Privata Maria Teresa, 7 – Milano 20123
Tel. +39 0287198390
Sede operativa e amministrativa:
Via Cividale, 51 – Montecatini Terme (PT) 51016
Tel. +39 0572 78166
Fax +39 0572 294540
Sede operativa
Via Del Lavoro, 57 – Casalecchio di Reno (BO) 40033

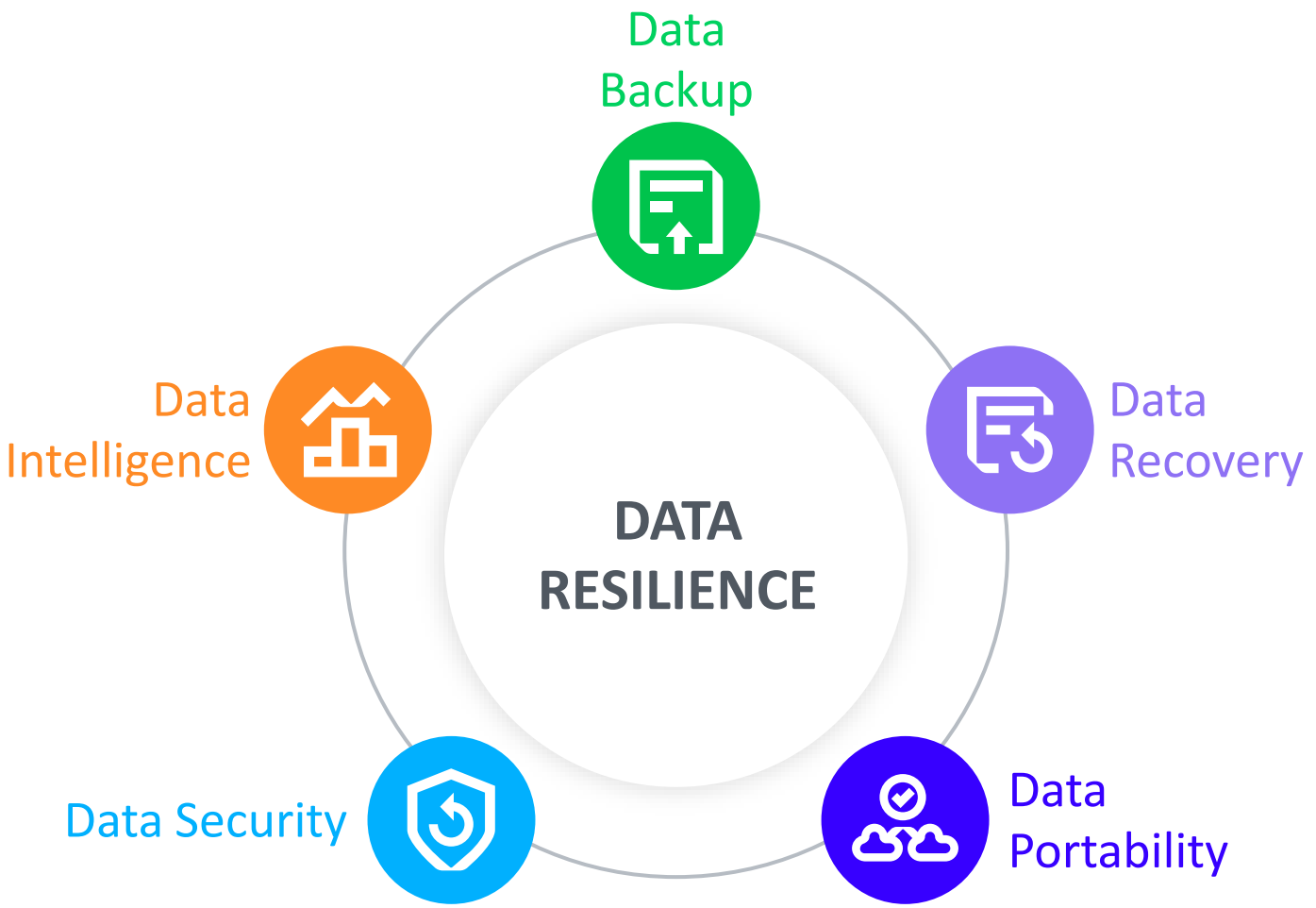
Partita Iva e Codice Fiscale: 01651060475
Le nostre sedi: Montecatini Terme (PT), Milano
www.consulentelegaleinformatico.it

Per richieste progetti e preventivi:
info@consulentelegaleinformatico.it
Per organizzare eventi:
comunicazione@consulentelegaleinformatico.it
Per organizzare corsi di formazione:
thinkfactory@consulentelegaleinformatico.it

agenda

Prima parte del talk moderato da Marco Lorusso con DataCore, Libraesva, ReeVo, Veeam, Lan Service group.
Relatori: Remi Bargoing, Martino Franzini, Claudio Panerai, Marco Carrara

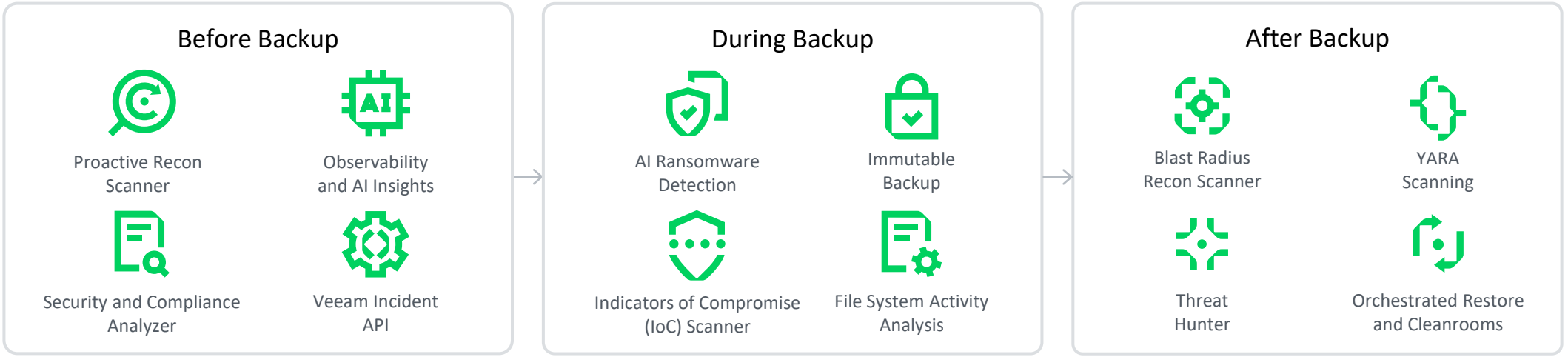
Veeam is purpose-built for powering data resilience



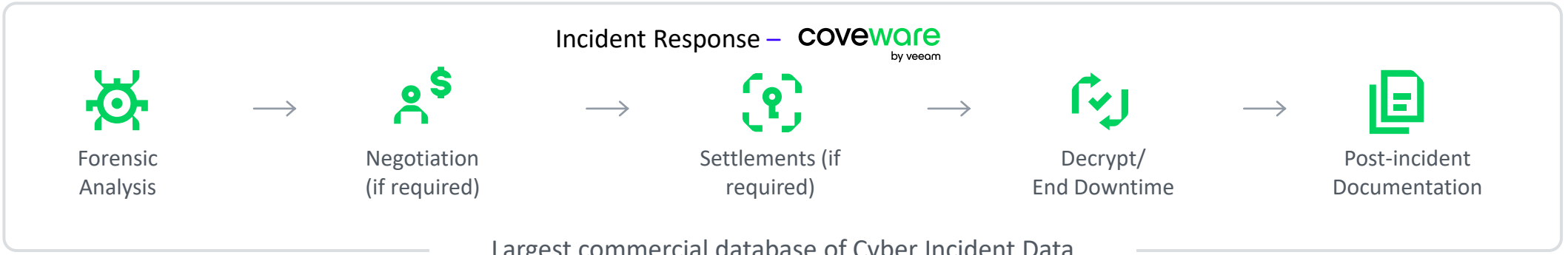
Different Laws, but many Similarities

GDPR	NIS2	DORA
Data Availability *(Art. 32)*	Continuity Requirement *(Annex III)*	Protection & Prevention *(Art. 9)*, Backup Policies *(Art. 12)*
Rapid Access Restoration *(Art. 15-17)*	Service Continuity *(Art. 18)*	Stability Assurance *(Art. 11)*
Portability Rights *(Art. 20)*	System Interoperability *(Recital 19)*	Standardized Exchange *(Art. 12, 25)*
Data Protection *(Art. 32, 33)*	Cybersecurity Risk Management *(Art. 21)*	Detection Capabilities *(Art. 10)*
Transparency & Accountability *(Art. 30, 35)*	Reporting Obligations *(Art. 23)*	Proactive Monitoring (*Art. 19)*

Veeam Cyber Secure – Full Support at Every Step



splunk> SOPHOS CROWDSTRIKE servicenow paloalto NETWORKS



Largest commercial database of Cyber Incident Data

veeam

Veeam Recovery Orchestrator

Dynamic Documentation

Automatically updated reports for checks, tests and executions help correct issues with DR readiness

Zero-Impact Testing

DataLab tests increase confidence, simulating disaster recovery without impacting production systems

Compliance

RTO and RPO reporting help meet compliance standards and SLA targets

1-Click Recovery At Scale

Recover single apps or an entire site with one click, secured by role-based access control

Supported platforms and applications:

Azure, vSphere e Hyper-V

Agents:
Windows & Linux

Apps:
Exchange, SQL, SharePoint

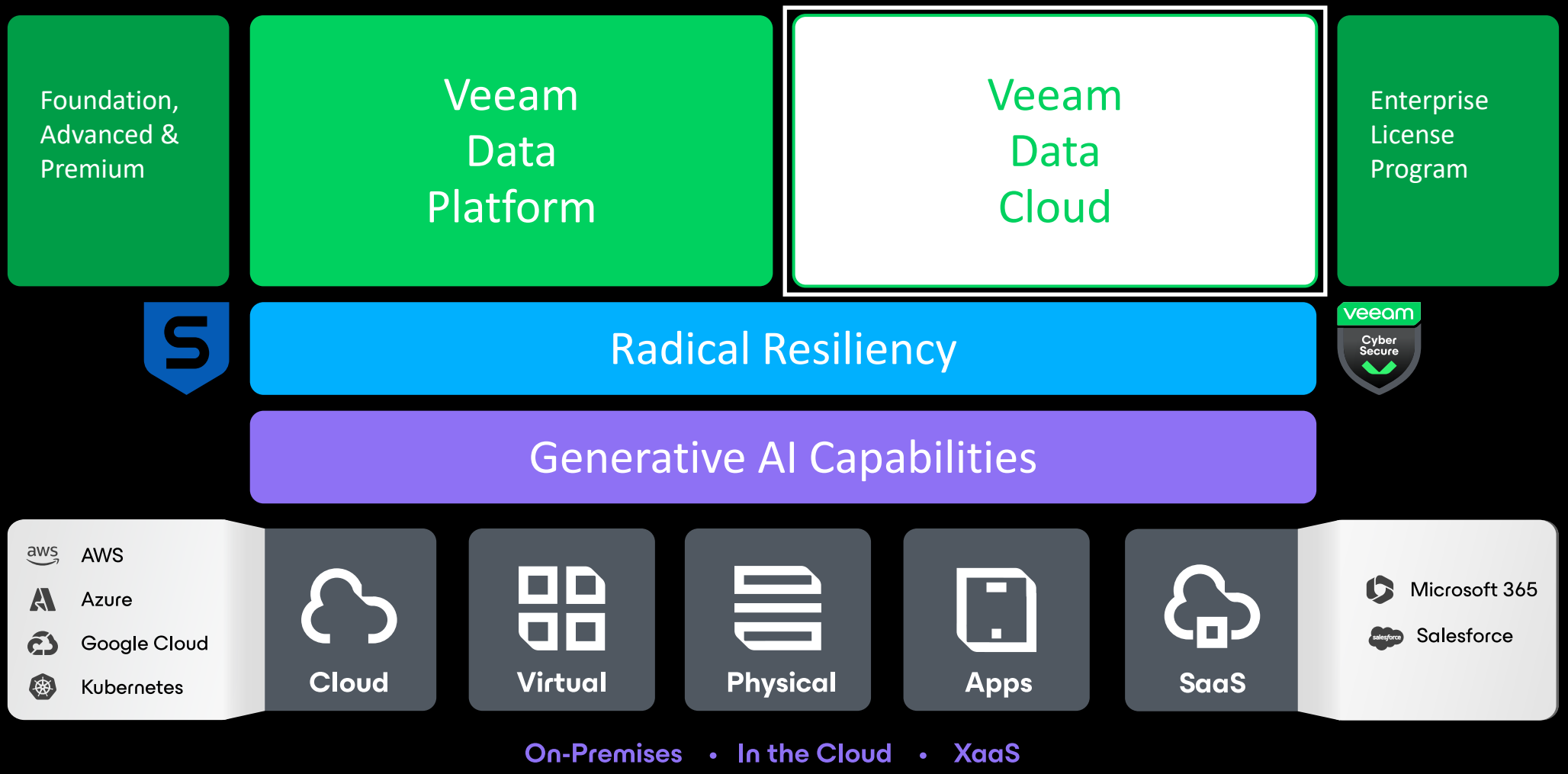
Storage:
NetApp, HPE, Lenovo

Custom scripting

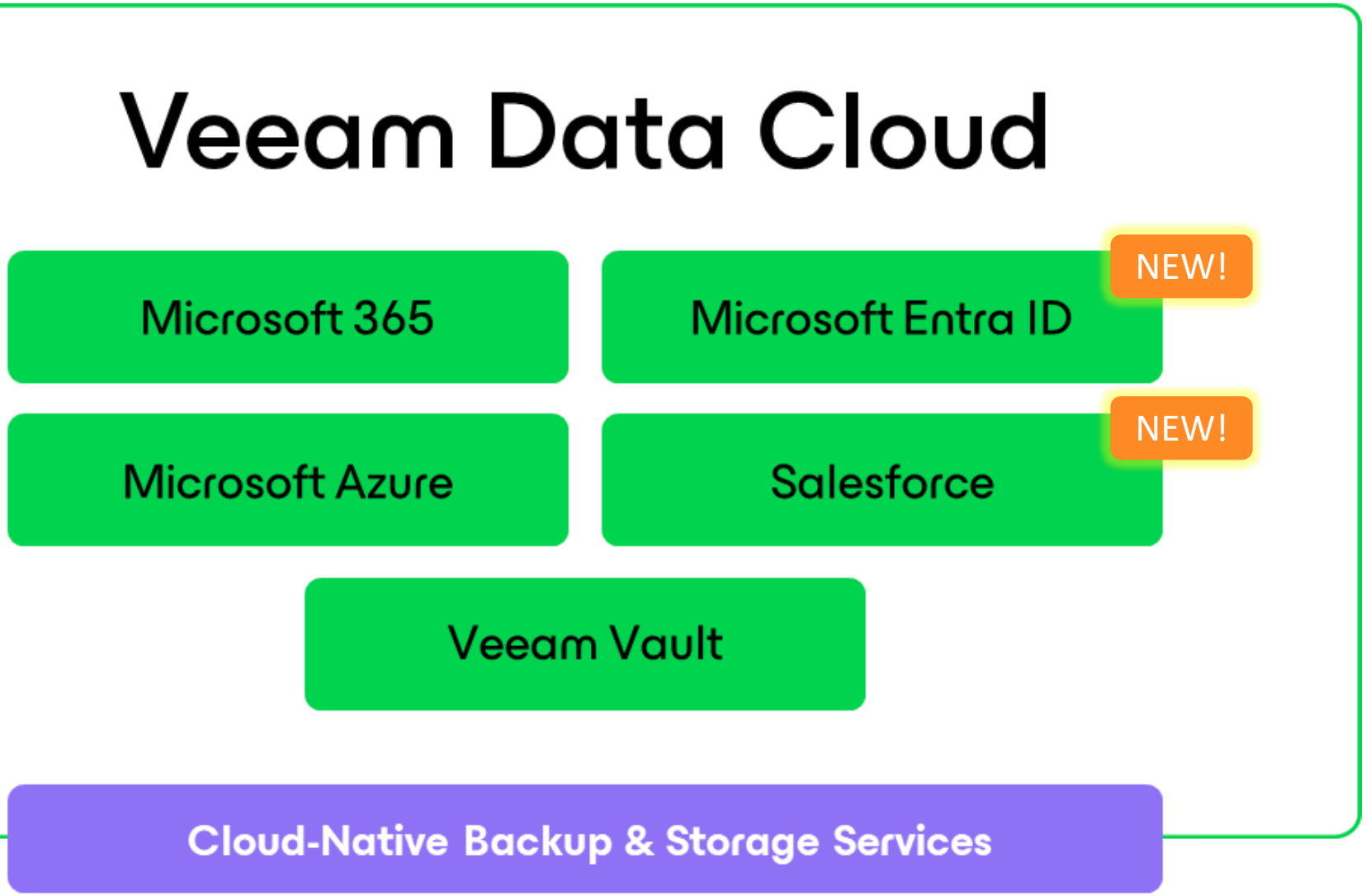
© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Seconda parte del talk moderato

Posizionamento

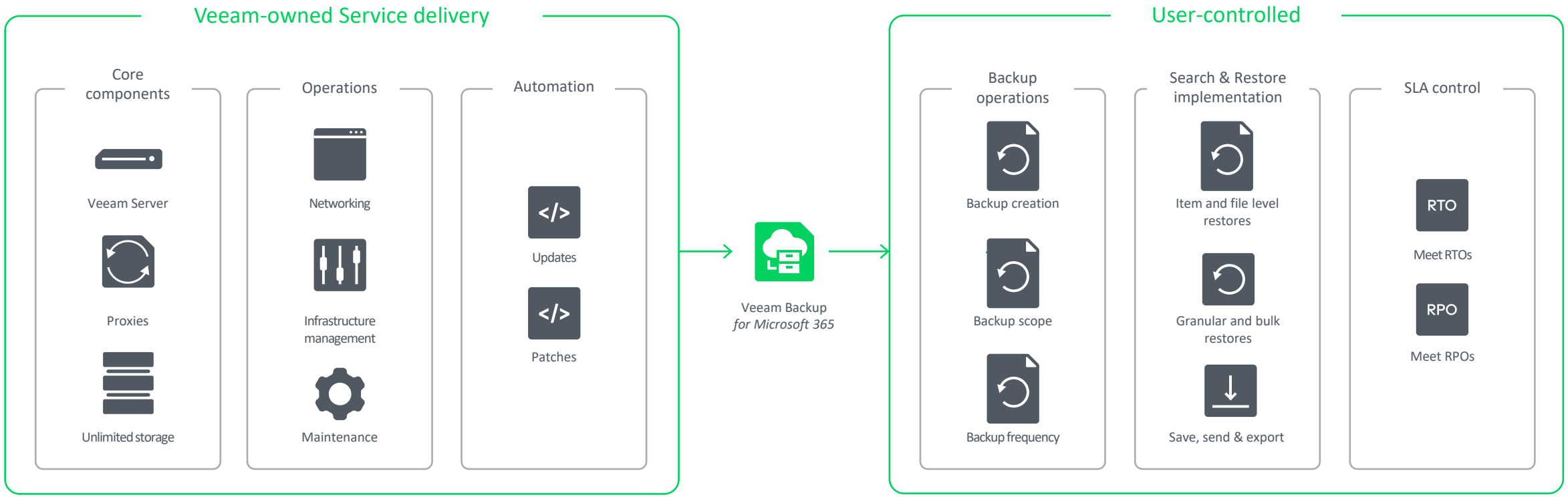


Veeam Data Cloud



VDC for Microsoft 365

Semplifica la strategia di backup di Microsoft 365 fornendo tutto ciò di cui hai bisogno



Veeam Data Cloud Vault

Zero Trust Data Resilience

Separazione del software di backup e dello storage

Segmentation, air-gapping and least privilege access

Zone di resilienza multiple

3 copies of data, 2 different media, 1 offsite

Immutabile e Criptato

Protecting data integrity and confidentiality

LAN SERVICE group

GRAZIE

CASALE MONFERRATO

Via Giacomo Brodolini, 80

Tel. +39 0172 330 500

MILANO

Via Caldera, 21 – Caldera Park

Tel. +39 02 334 310 58

LUGANO

Via S. Balestra. 18

Tel. +41 91 21 04 634

www.lanservicegroup.it – info@lanservicegroup.it

P.Iva e C.F. 01562820066

Iscr. Reg. Imp. AL-01562820066 – Cap. Soc. € 80,645,00