October 2024

Ransomware Resilience:
No More User Blame

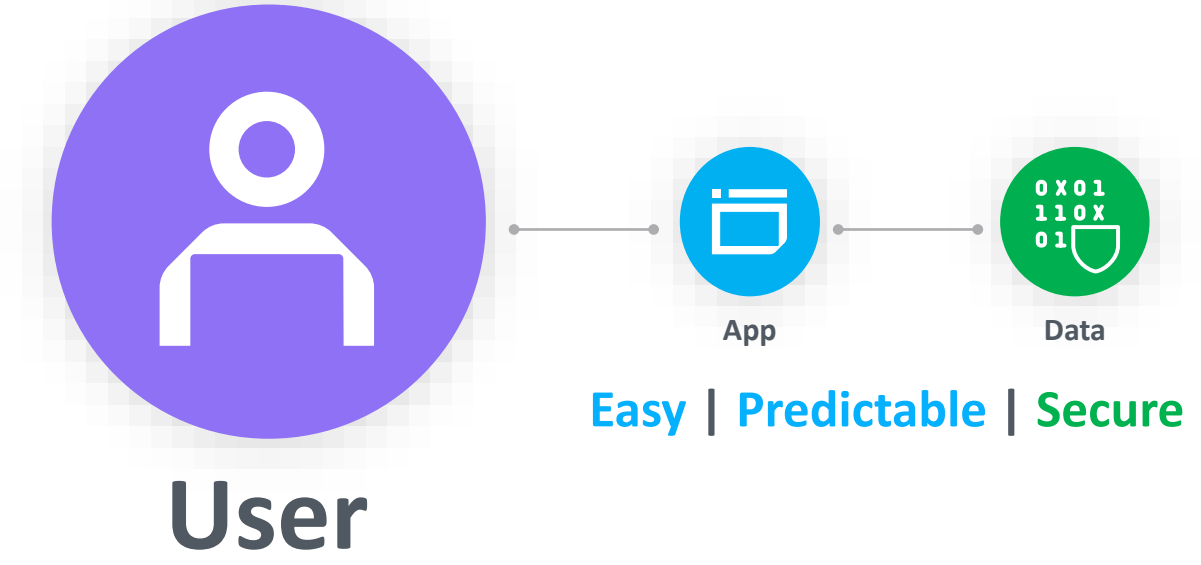
Edwin Weijdema
Field Chief Technology Officer EMEA
@Viperian | community.veeam.com

What does the User expect?

when working with Tech

Always
Available
Anywhere

It Just Works!



But . . .

Disruptions Happen

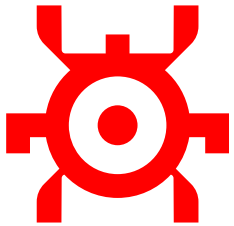
Top 5 - Disruptions

All causes 2023
Most impactful 2023
Most impactful 2022
Most impactful 2021

4th year

cyber-attack was **most common** & **most impactful** cause of outages

Over the past two years, what were the most common causes of the outages that your organization experienced? Which was the most impactful in 2021, 2022, and 2023?



18%
16%
15%

Cyber Security Event

40%

9%
10%
8%

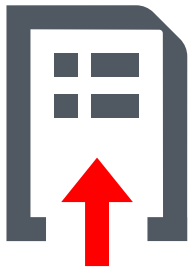
Outages of public cloud resources

31%

10%
10%
10%

Application software Outage

34%



10%
8%
8%

Storage hardware Outage

35%

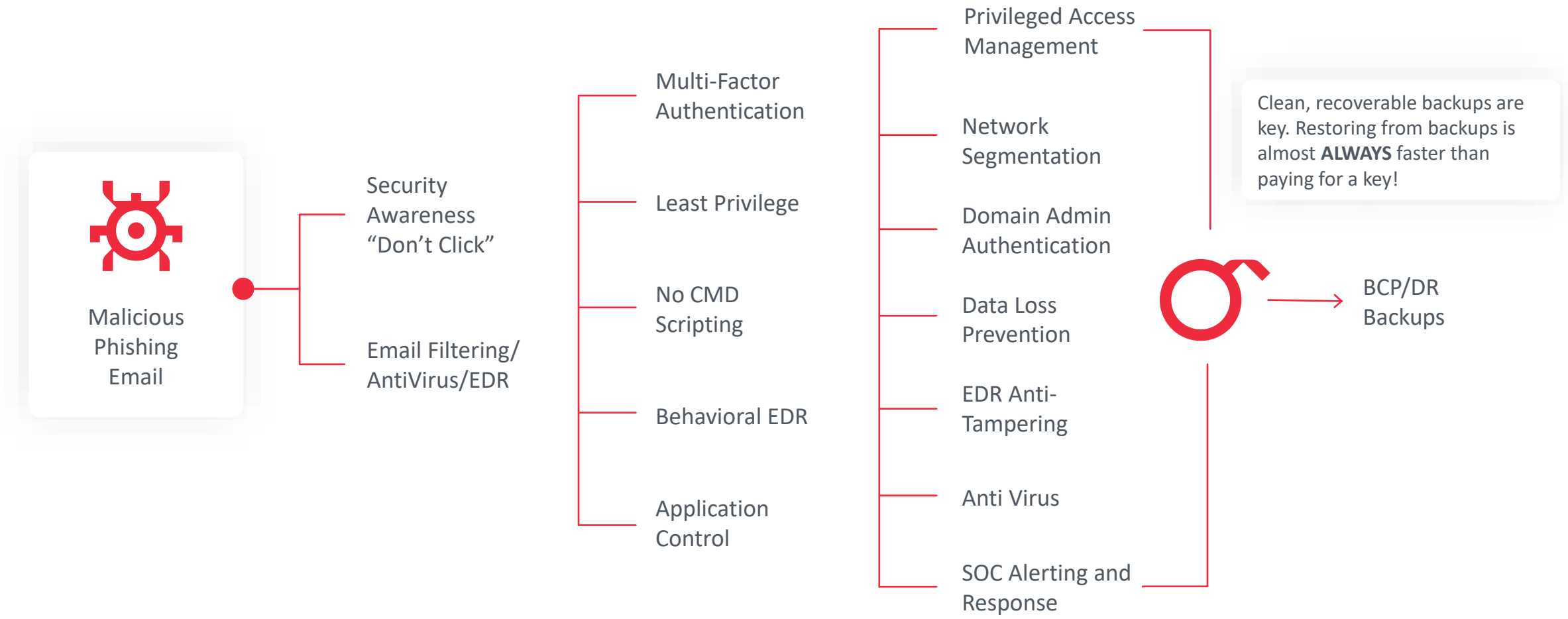
10%
12%
14%

Infrastructure/networking Outage

37%

Source: **Data Protection Trends Report 2024**
https://vee.am/DPR24

Compounding Failures in the Cyber “Kill Chain”



Lets . . .

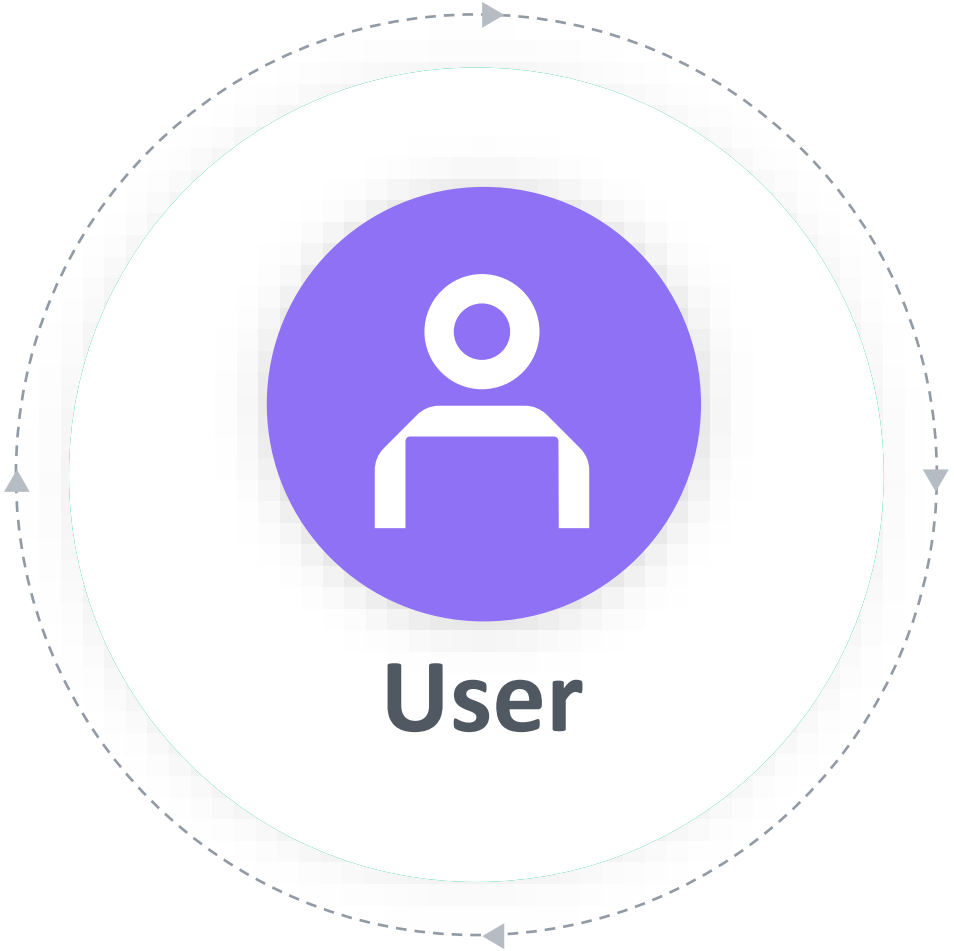
Empower the User

Cyber Safe Zone

creating a culture of openness and safety

Report Suspicious Activity without Fear

"If you experience something, say something"



Healthy Data

Give the user Peace of Mind that their data is safe, and service can be restored fast and easy!

Fast Reliable Recovery

The perfect storm of complexity and threats:

Data Explosion

150+ ZB

created in 2024
doubling every year…

Infrastructure Complexity

92%

Enterprises have a multi-cloud strategy

Vendor Lock-In

Every 3 Years

IT Hardware Refresh

Surge in Ransomware Complexity

1 in 4

27% of organizations paid the ransom and never got their data back

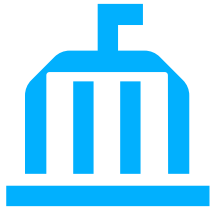
Complexity

Threats

veeam

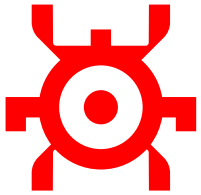
The Problem:
Data Infrastructure

- Cyberattacks are common
- Attempts to access infrastructure are frequent, including backups
- Large number of tactics, techniques, and procedures (TTPs) utilized by threat actors
- Indicators of compromise are hard to identify
- Unpredictable dwell time (between compromise and attack)



75%

of organizations suffered at least one ransomware attack



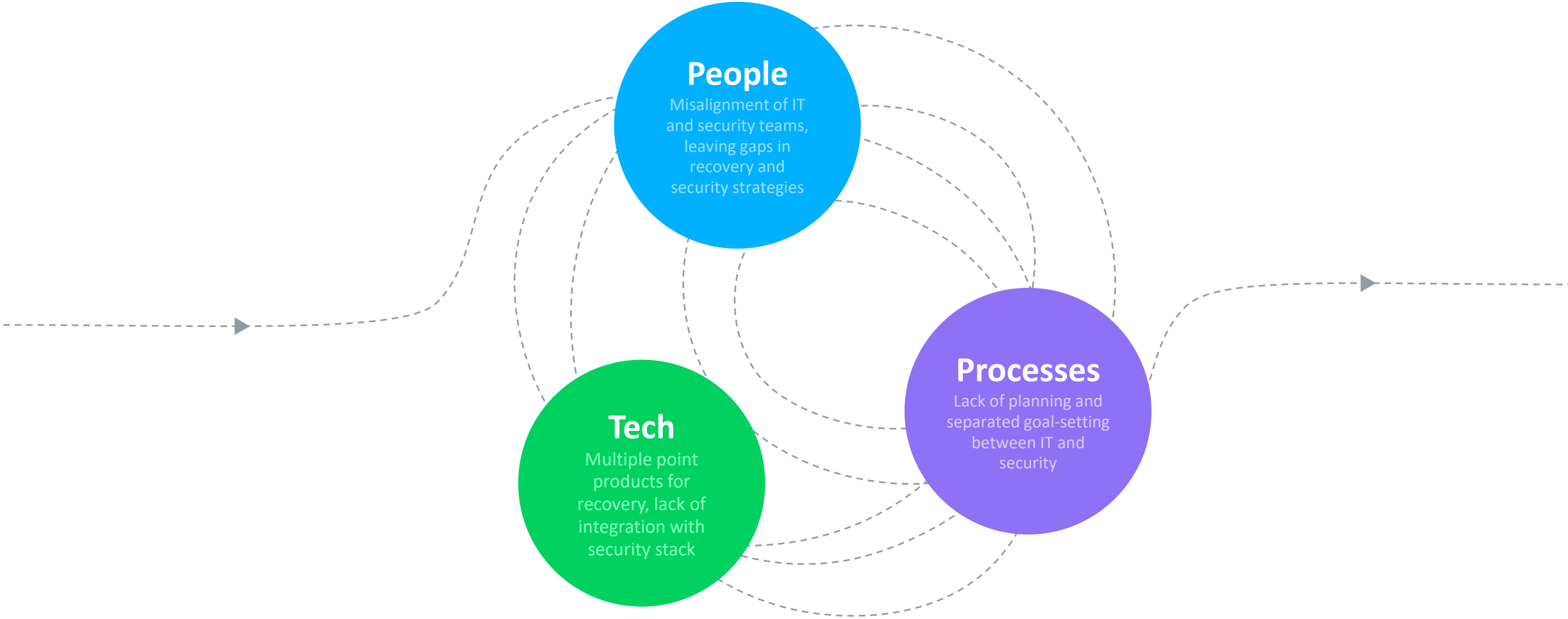
96%

of cyber attacks target backups

68%

of financial impact attributed to costs other than the ransom payment

Technology alone won't solve for true **resiliency**



We power
data resilience,
to keep every
business running.

New approaches to recovery are needed for true **data resilience**

aligned security and IT teams

rapid and clean data recovery at scale

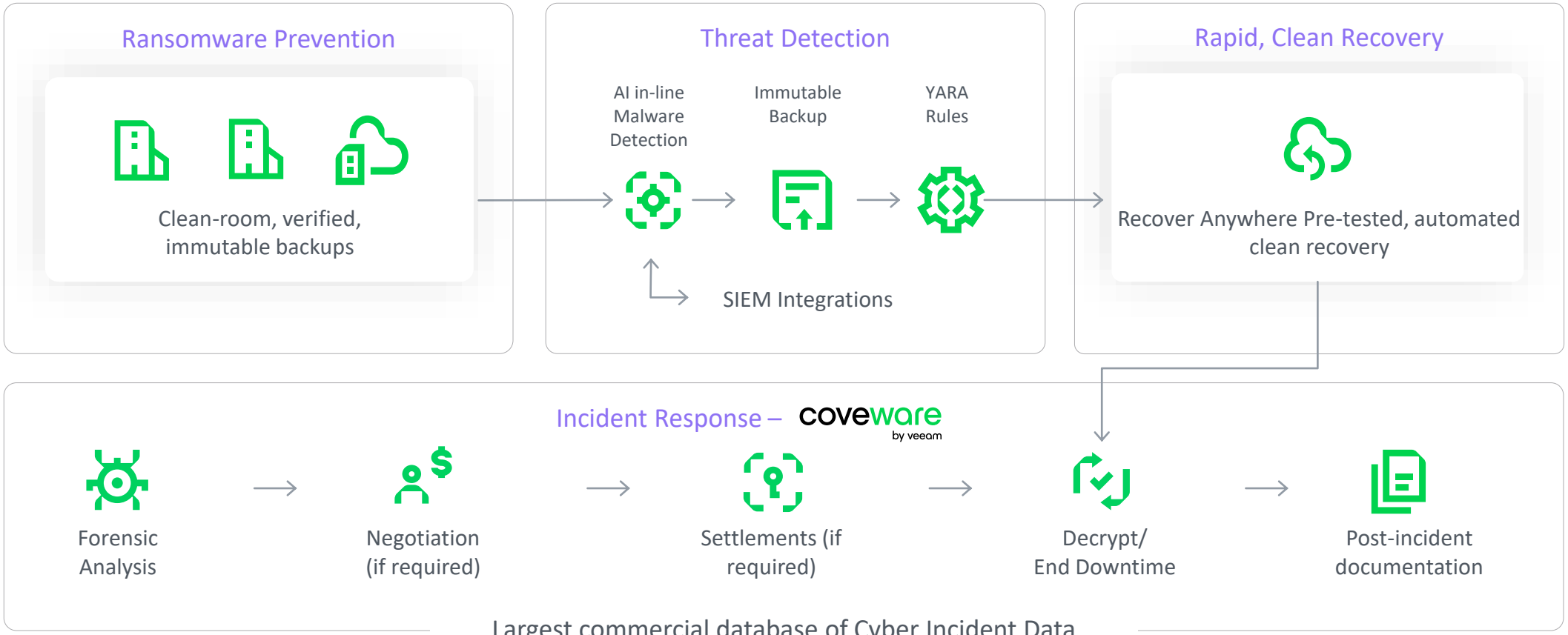
stay resilient and keep the business up and running

ransomware prevention and threat detection efforts

Veeam provides the most complete end-to-end ransomware protection and recovery

Veeam Cyber Secure Program

24/7/365 SWAT Team | Health Checks | Ransomware Warranty | Incident Response Retainer



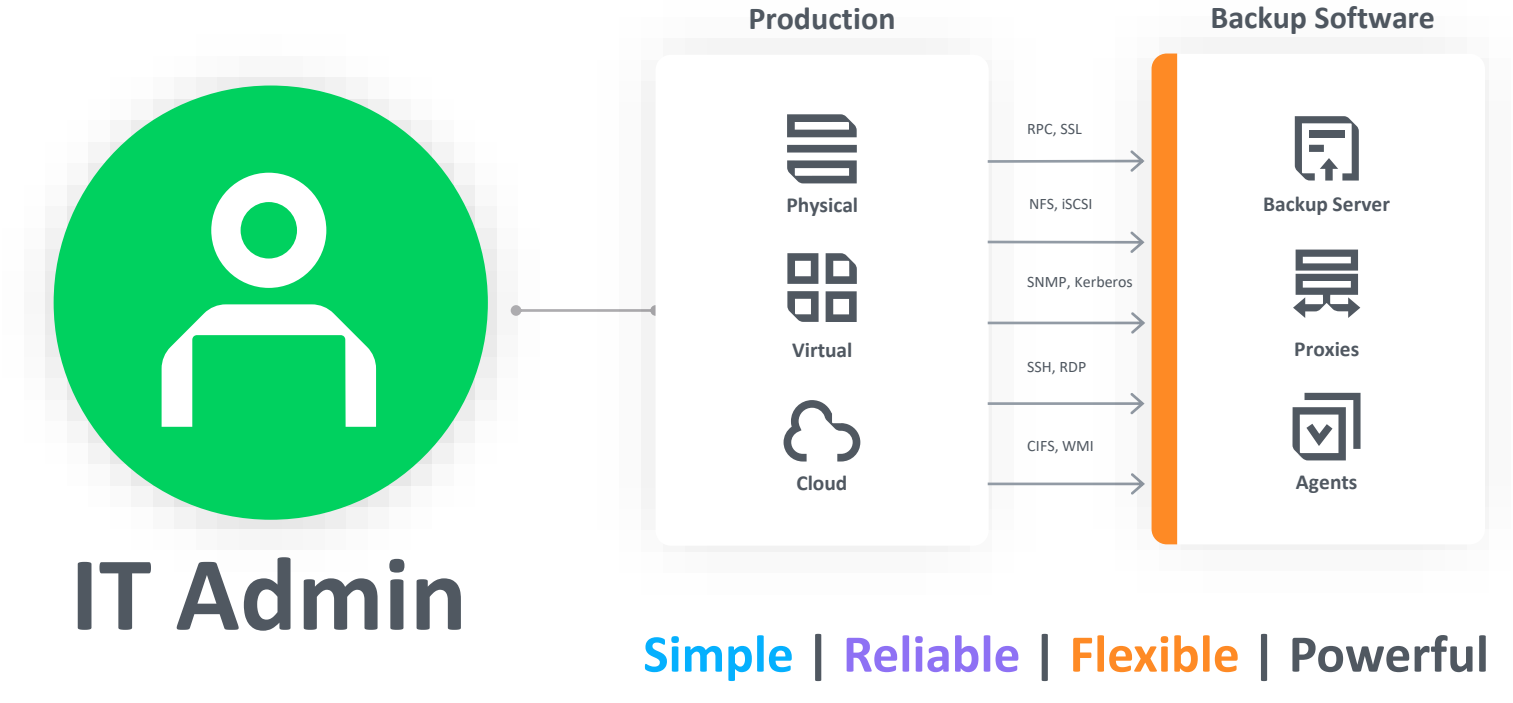
What does the IT Admin expect?

when working with Tech

Always Available Anywhere

It Just Works!

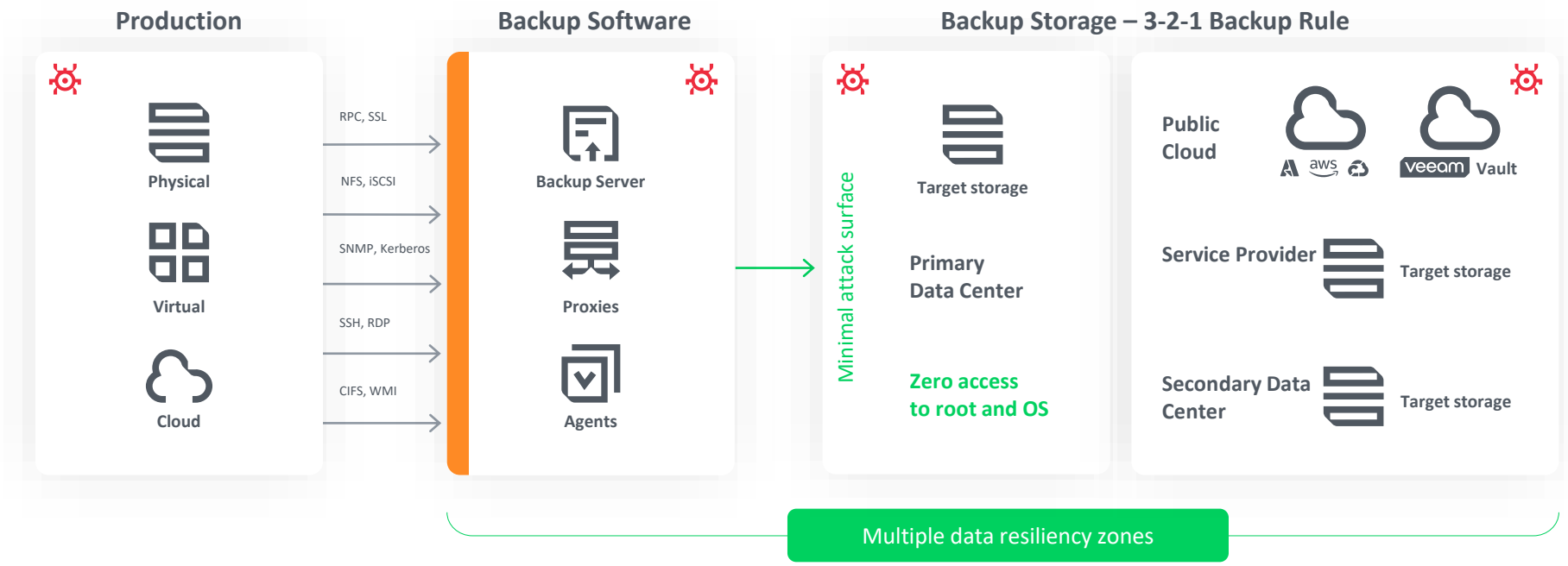
VEEAM
IT JUST WORKS!™



Simple | Reliable | Flexible | Powerful

Hardware-agnostic security with Zero Trust Data Resilience

Secure by design with Zero Trust Architecture

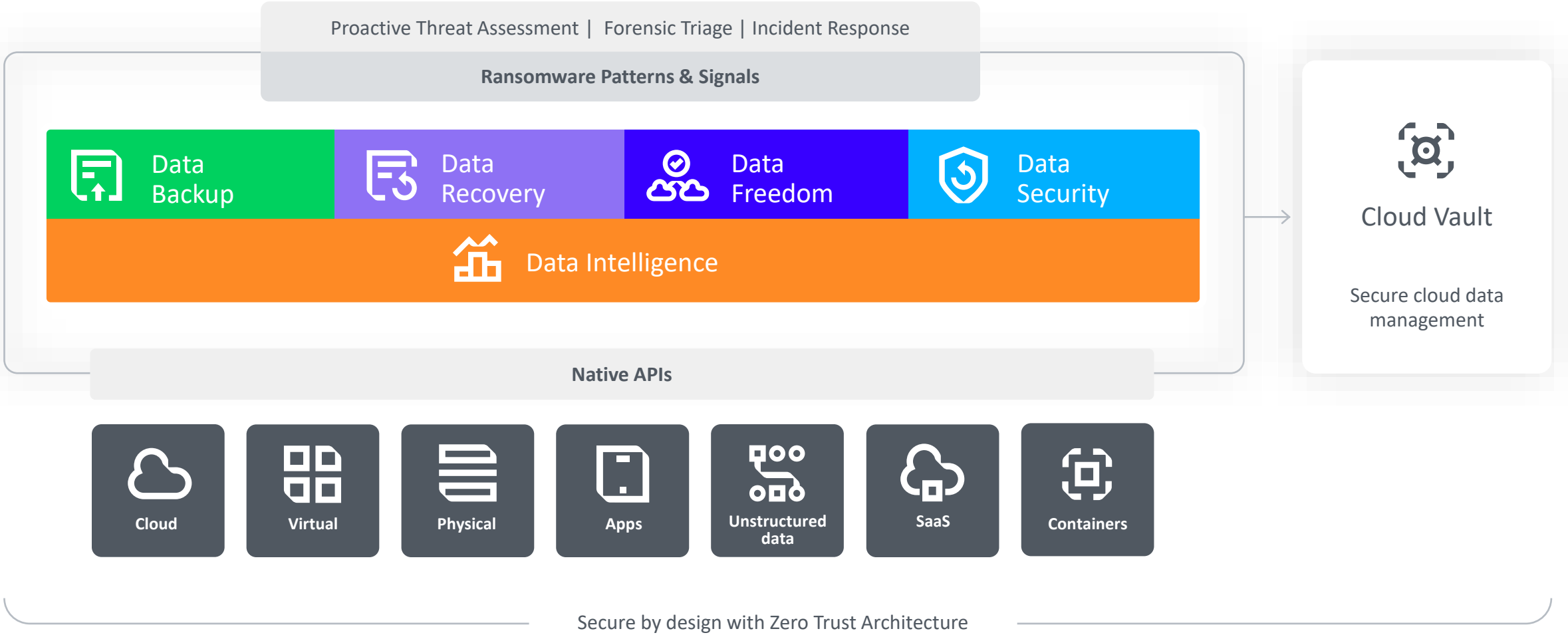


Segmentation of software & storage

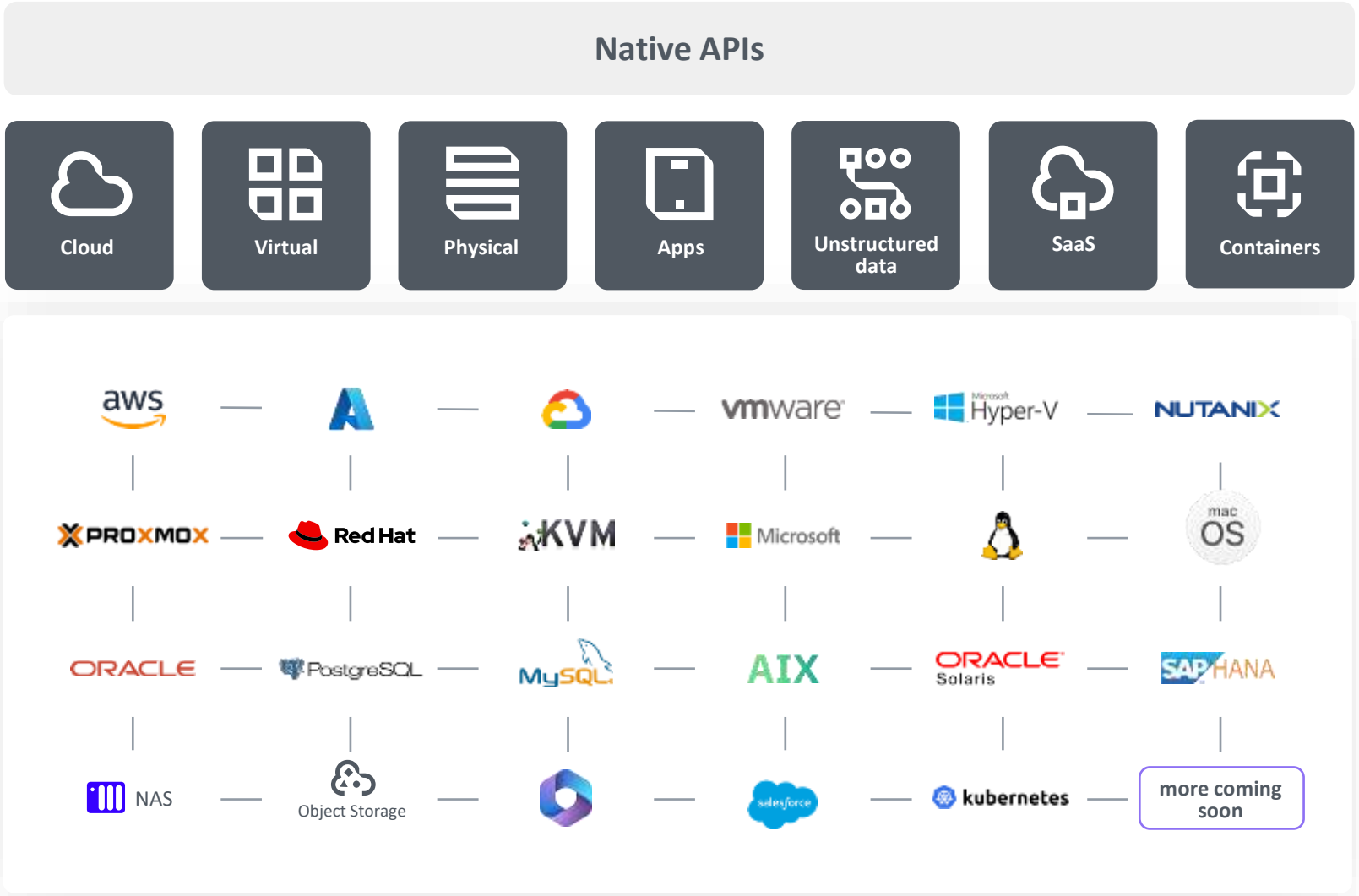
Multiple **data resilience zones**

Immutable backup storage

Products that bring data resilience to life



Extensive workload coverage unmatched in the industry



New for 2024

Cloud

- Amazon FSx
- AmazonRedShift
- Azure Cosmos DB

Virtual/Database

- Proxmox VE
- MongoDB

Coming soon in 2024

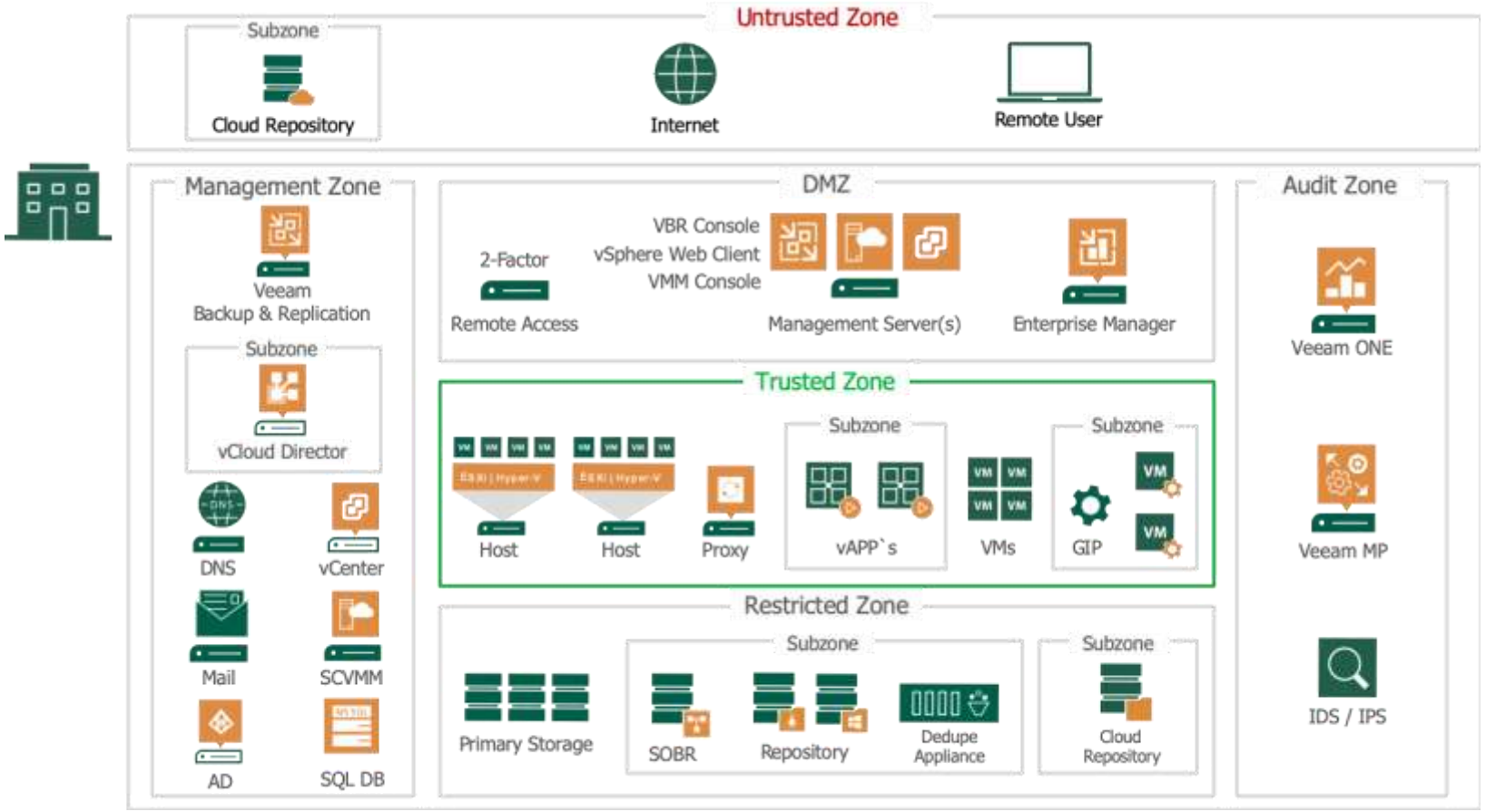
Cloud

- Microsoft Entra ID
- Azure Data Lake Storage Gen2

Follow BP

- 3-2-1-1-0 Rule
- Segmentation
- Segregation of Duties
- Security Domains
- Firewalls
- Encryption
- Secure Access
- Patching & Updates
- Principle of Least Privilege
- See All, Know All
- Resilient by Design
- Zero Trust Data Resilience

Building a Cyber Safe Zone



Ready to trade concern for confidence?
Get data resilient with veeam

Visit us at:
Hall 9 – Booth Number 9-322

Edwin Weijdema
Field Chief Technology Officer EMEA
edwin.weijdema@veeam.com

https://www.veeam.com/contact-sales.html