

Notfall Cyberangriff: Reicht eine Bedrohungsabwehr aus oder braucht es eine Strategie zur Cyber-Resilienz?

Atos Cyber Recovery
mit Veeam Data Platform

12.10.2023

Dr. Christian Hillebrand – Atos

Marc Heuser - Veeam

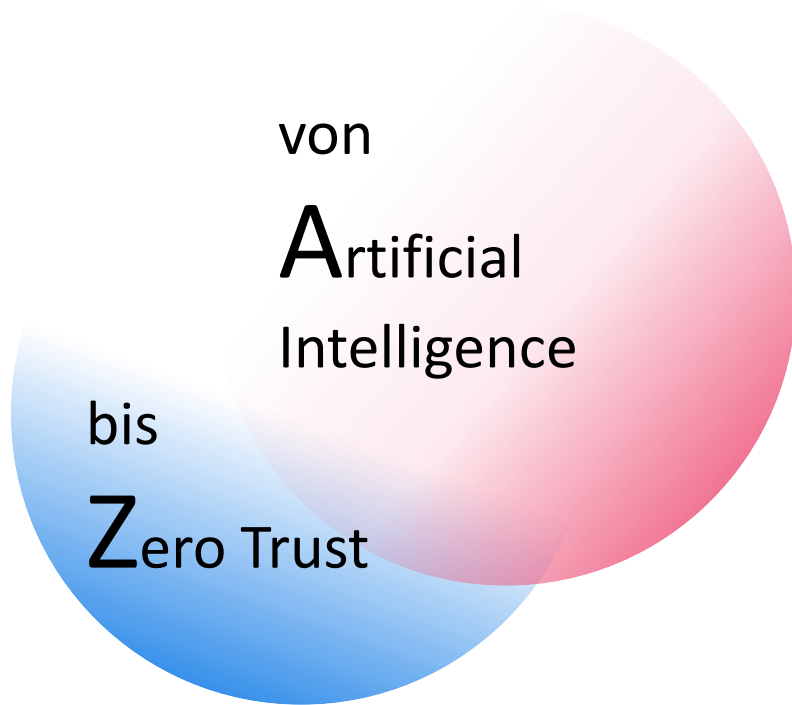


Atos

Atos – IT Service aus Deutschland

Lokale Nähe mit Globalem Backbone

#MittelstandmitAtos



Weltweit 62.500 Beschäftigte in über 70 Ländern.

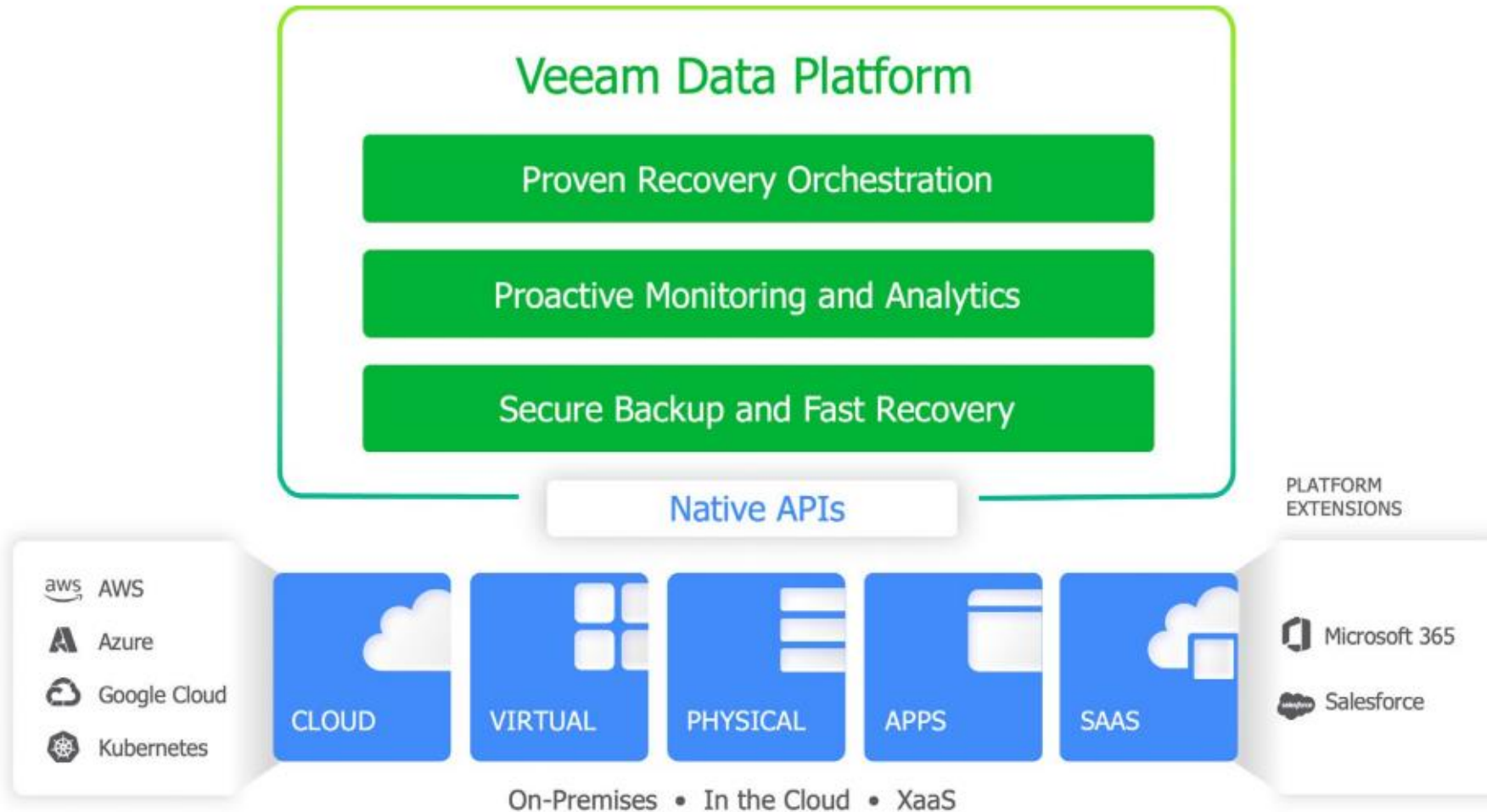
Das datentechnisch größte Atos Datacenter, welches auch die weltweit eingesetzten Hybriden Cloud Lösungen beinhaltet, **steht in Fürth/Feucht** und bedient eine Vielzahl unserer 1.200 Kunden weltweit.

Moderne End 2 End Lösungen in den Bereichen Infrastruktur, Cloud, Security, SAP, Enduser Experience.

Gartner **Global Leader:** Atos ist Marktführer bei Data Center- und Infrastructure-Services (2022)

Gartner **Global Leader:** Atos ist Marktführer bei Outsourced Digital Workplace Services (2022)

Veeam Data Platform



Veeam Data Platform Packages

Platform Editions	Backup and Recovery	Monitoring and Analytics	Recovery Orchestration	Ransomware Warranty (add-on)
Premium	✓	✓	✓	✓
Advanced	✓	✓		
Foundation	✓			
Essentials	✓	✓		
Supporting product components	Veeam Backup & Replication	Veeam ONE	Veeam Recovery Orchestrator	

Also Available:

- Veeam Backup & Replication Community Edition

Aktuelle Lage

Cybercrime



Bundeskriminalamt

Lagebericht Cybercrime (12.7.2023):

- 136.865 Fälle von Cybercrime in 2022
- nur “Spitze des Eisbergs” (90% Dunkelziffer)
- Ransomware “existenzbedrohend”

bitkom

Wirtschaftsschutz (1.9.2023): “Organisierte Kriminalität greift verstärkt die deutsche Wirtschaft an”

- Schaden 203 Milliarden € in 2022 (Wert von 2019 verdoppelt)
- 9 von 10 Unternehmen werden Opfer
- Zunahme organisierter Kriminalität

Cybercrime

Aktuelle Vorfälle

24. August 2023 (konbriefing.de)

Angriff
[Sta
fahre

2. Oktober 2023 (konbriefing.com)

Cyberangriff auf kommunales

29. August 2023 (shz.de)

Internet-Hackerangriff auf Konradion

konbriefing.de)

im Landkreis
re installiert

28. September

Sicherheit
Betreiber
in D



Die Frage ist nicht ob,
sondern wann

ment.com)

legen
m

me-ze

8. September

Ransom
Reche
Gesundheits

6. Oktober 2023 (faz.net)

Hackerangriff auf Uniklinikum in
Frankfurt. [...] es werde Wochen
dauern, bis die Systeme [...]
wiederhergestellt sind

28. September 2023 (e

Cyberangriff auf
Stadtverwaltung in

Sind Sie darauf
vorbereitet ?

Cybercrime

Schadenspotential



400%

Zunahme Ransomware Attacken während Corona



nur 62%

der verschlüsselten Daten konnten nach Lösegeldzahlung im Durchschnitt wiederhergestellt werden



34%

der Attacken kommen von innerhalb der Firmen



21

Tage durchschnittliche Downtime (RTO)



180 Tage

Im Mittel zwischen Infektion und Aktivierung Ransomware

Häufigkeit von Ransomware-Vorfällen

Von wie vielen Ransomware-Angriffen war Ihre Organisation in den letzten 12 Monaten betroffen? (n = 1.932)

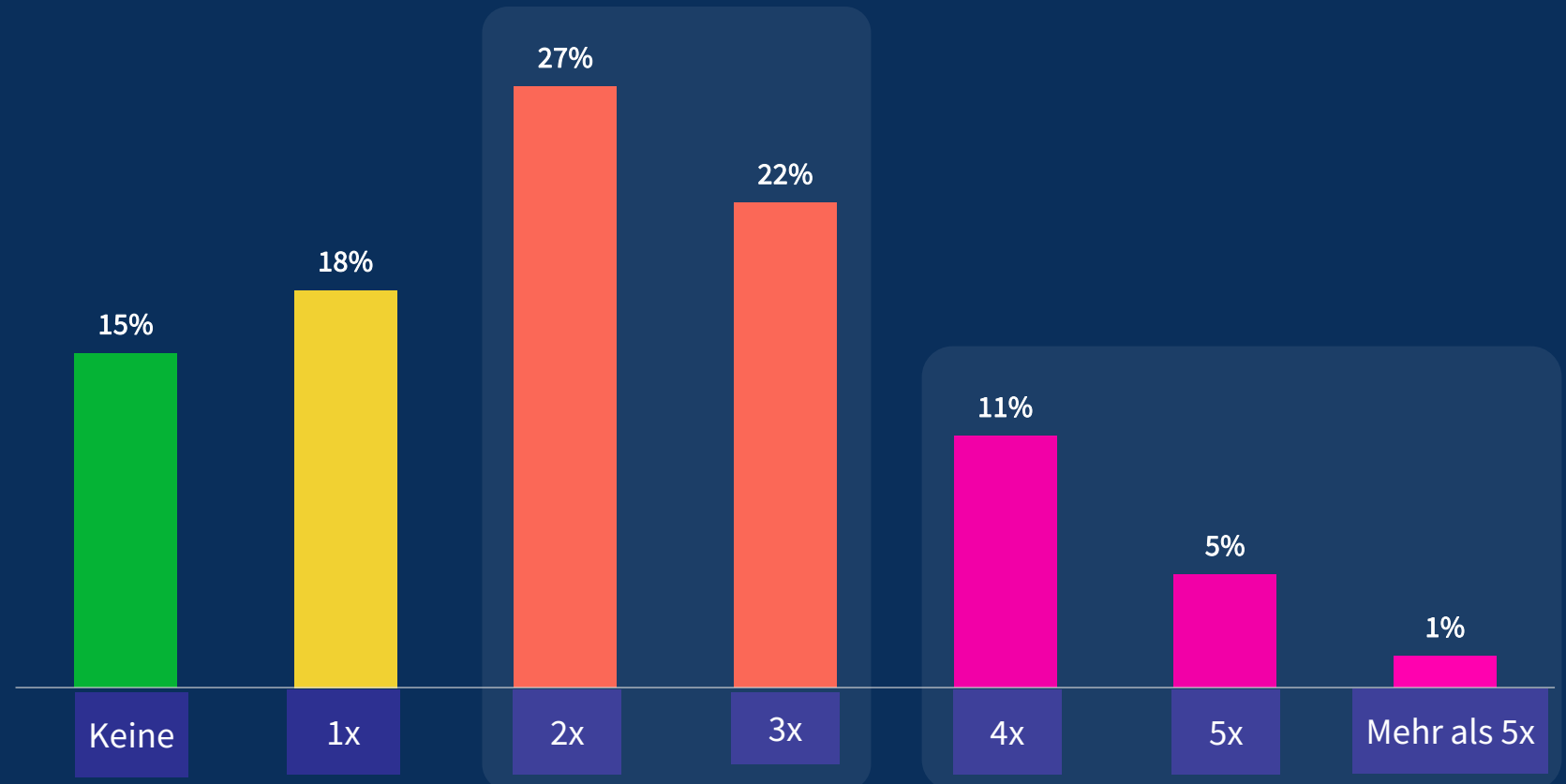
85%

der Organisationen waren mindestens einmal von Ransomware betroffen.

Die Anzahl derer, die von vier oder mehr Angriffen betroffen waren (17%), war größer als derer, die von überhaupt nicht attackiert wurden (15%).

49%

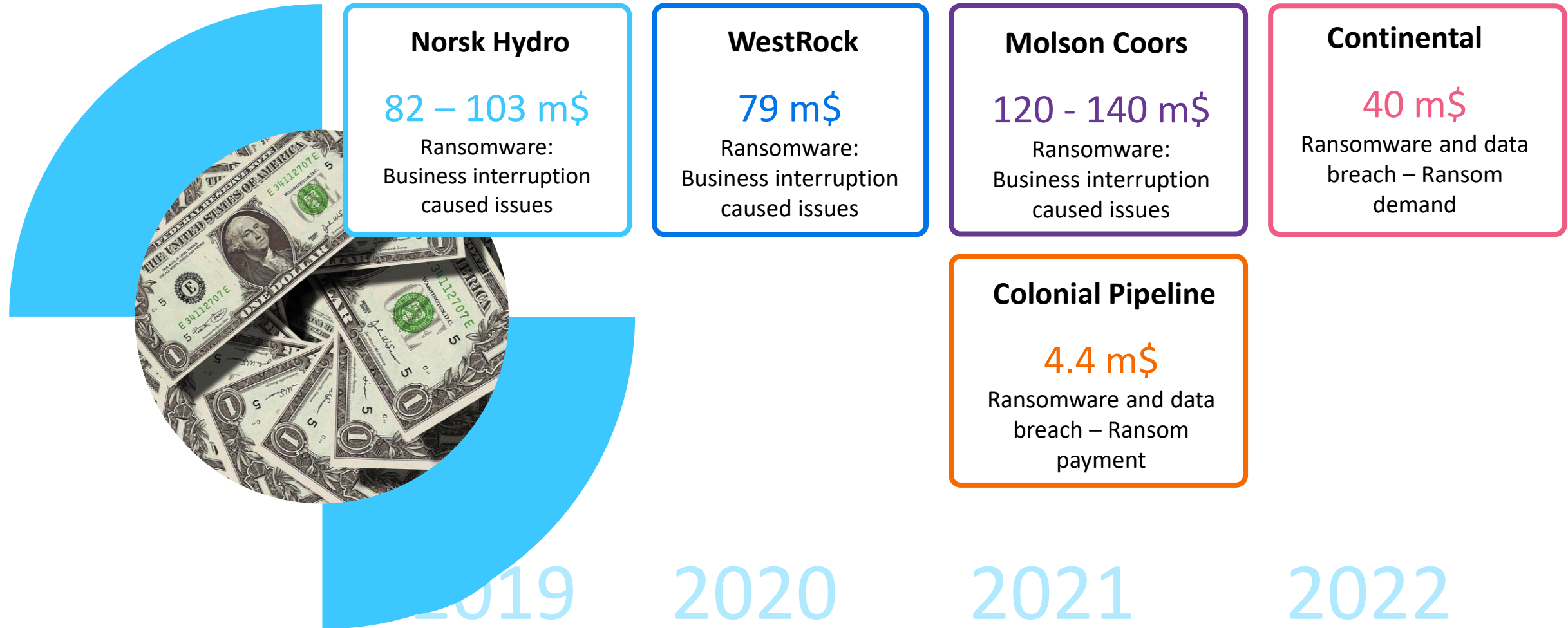
der Organisationen waren von zwei oder drei Angriffen betroffen.



Quelle: Data Protection Trends Report 2023
<https://vee.am/DPR23>

Schaden “Big Tickets”

International mit Schadenshöhe



Gesetzliche Verordnungen

und mögliche Strafzahlungen



2018

General Data Protection Regulation (GDPR) / Allgemeine Datenschutzgrundverordnung (DSGVO)

- Vorbereitung auf Datenverlust
- Meldepflicht bei Verlust von Personenbezogenen Daten

Strafen:

(Stufe 1) 10 m€ / 2% Jahresumsatz
(Stufe 2) 20 m€ / 4% Jahresumsatz

17.10.
2024

Network and Information Security Richtlinie (NIS2)

- mehr Branchen
- kleine Unternehmen (ab 50 Mitarbeiter / 10 m€)

Strafen:

(Essential) 10 m€ / 2% Jahresumsatz
(Important) 7 m€ / 1,4% Jahresumsatz

Anfang
2024

Cyber Resillience Act – (CRA)

Produkte mit digitalen Elementen und Daten-verbindungen in 3 Stufen.

Strafen *):

bis 15 m€ / 2.5% Jahresumsatz

NIST- konformes

Cybersicherheits-
Framework



veeam



Identifikation

Tracking und Auditing
von Änderungen

Intelligente
Diagnosefunktionen



Schutz

DataLabs – Patch-
Management-Forensik

Kontinuierliche
Datensicherung (CDP)

Veeam Disaster Recovery
Orchestrator

Sichere Wiederherstellung
(Secure Restore)

Mehrstufige
Wiederherstellung
(Staged Restore)



Erkennung

Veeam® DataLabs™

API für die
Datenintegration



Reaktion

Unveränderlicher

Speicher

Unveränderlicher Cloud-
Speicher

Verschlüsselung
und Schutz

Snapshot-
Orchestrierung

Moderne
Datensicherung



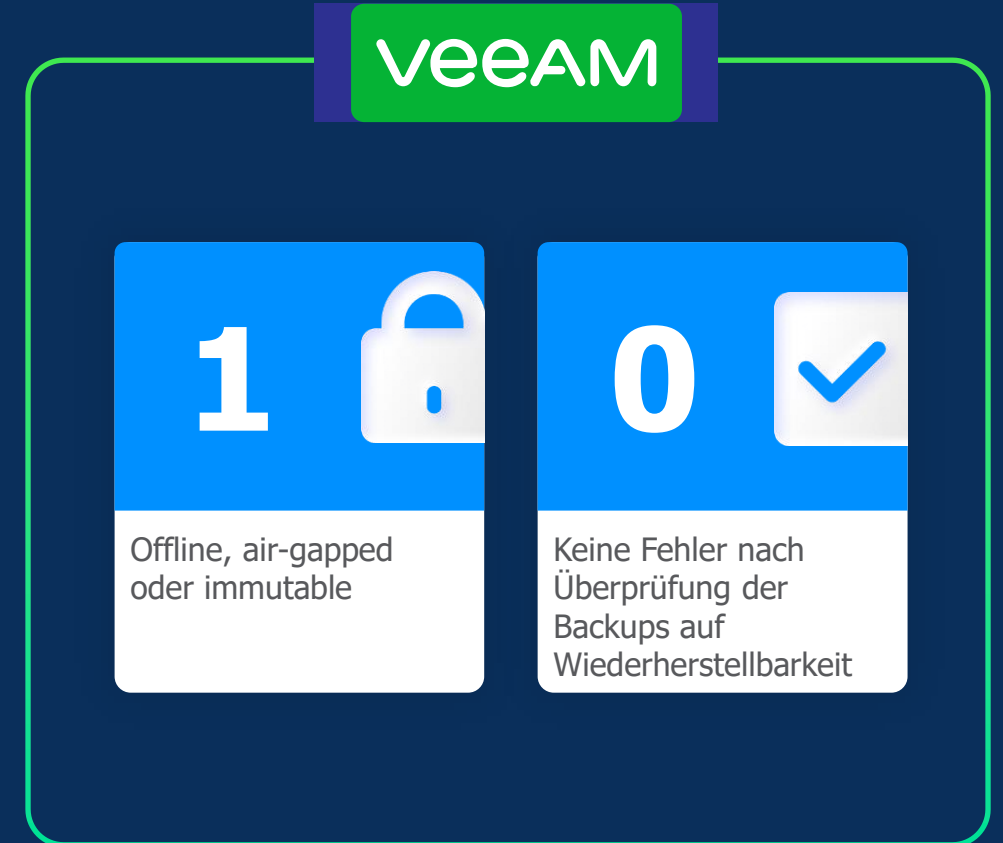
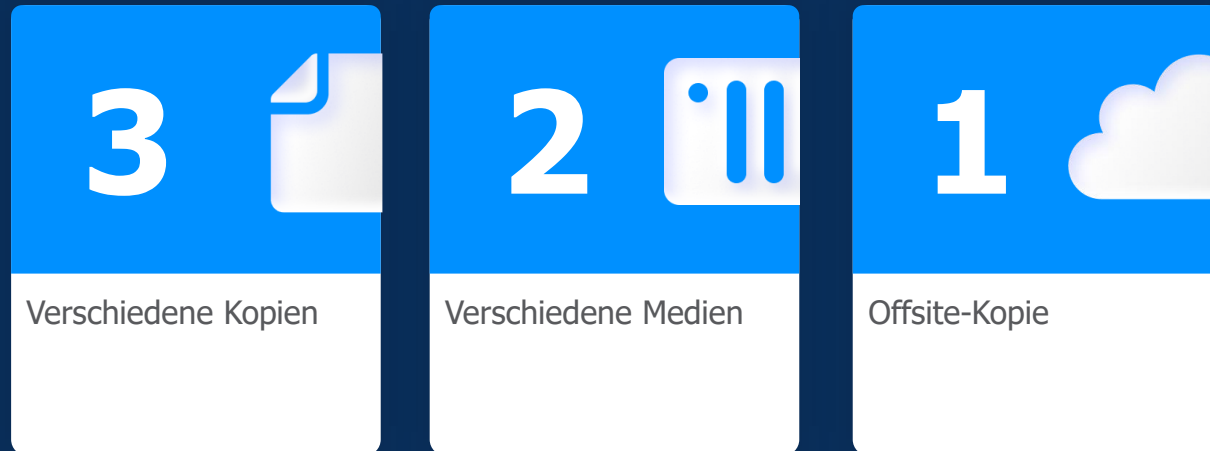
Wieder- herstellung

Sofortige

Wiederherstellungen



Vorbereitet sein: die Datenschutz-Postleitzahl



Atos Cyber Recovery

Umsetzung & Business Value



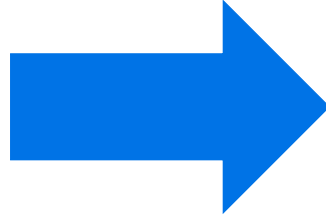
Daten
örtlich getrennt in
Recovery Vault



Locked
Daten können nicht
verändert werden



Analyse
der Daten (z.B.
Ransomware)



Schnell
wieder produktiv
mit geringer
Ausfallzeit (1 Tag)




Sicher
im Sinne der
Geschäftsführerhaftung




Vorbereitet
auf einen Angriff
und seine Folgen



Effizient
durch geringe
Wiederherstellungs-
kosten der Daten



Unabhängig
durch erfolgreiches
Daten-Recovery ohne
Lösegeldzahlungen



Konform
100 % Data
Compliance

Sie
sind

Cyberresilienzbereiche



Immutable

Verschlüsselt

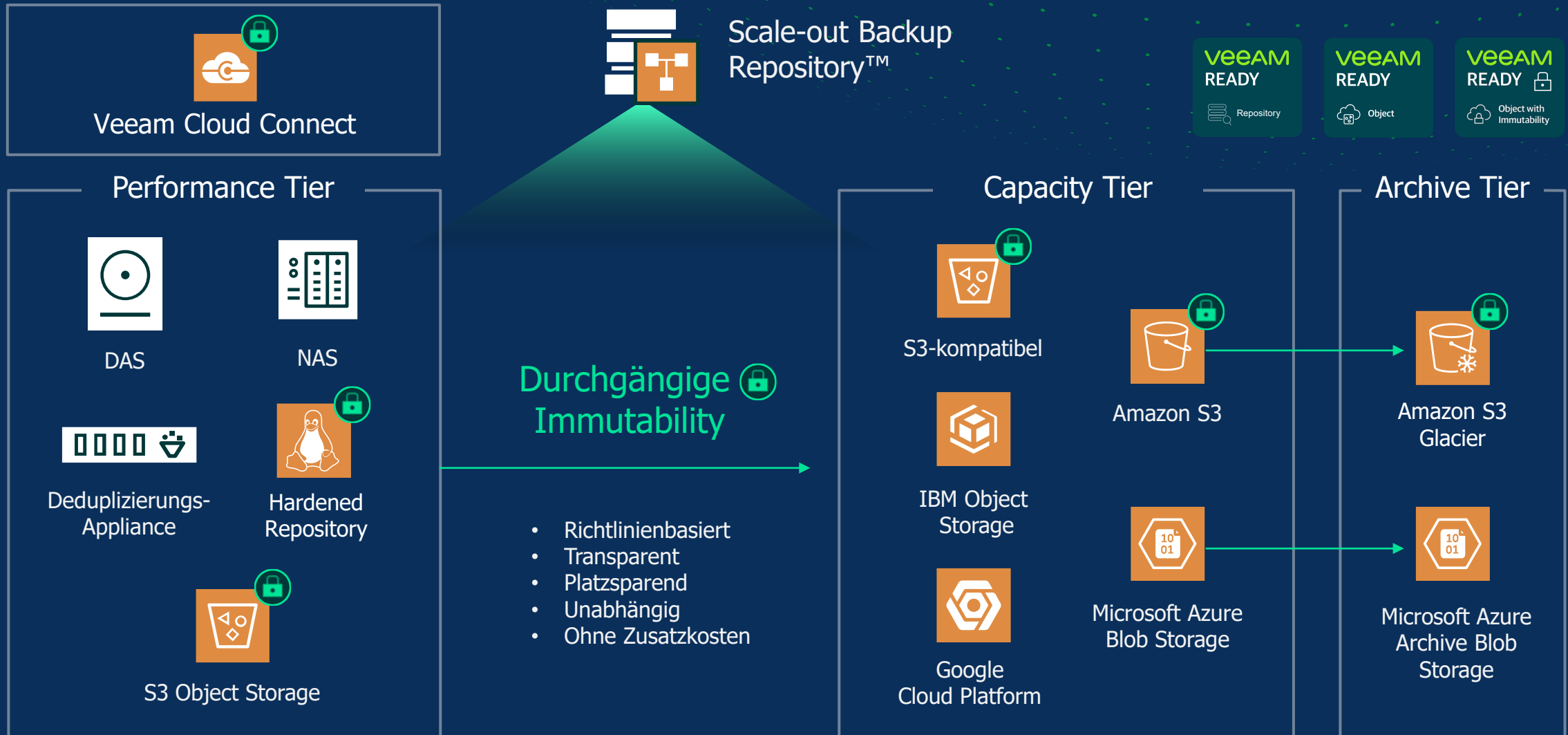
3-2-1-1-0

Sicherer Zugang

- Verhinderung von unberechtigt Zugriff
- Aktivieren Sie MFA
- Aktivieren Sie die automatische Abmeldung bei Inaktivität
- Verwenden Sie rollenbasierte Zugriffskontrollen (RBAC)
- Protokollierung und Meldung jedes Zugriffs



Durchgängige Immutability



Backup-Ziele

Performance
Backup/Wiederherstellung

Skalierbarkeit

Preis/Leistung



DAS (lokale Festplatten)

+++

++

+++



SAN (Block-Storage)

+++

++(+)

+



File (SMB, NFS)

++

++(+)

++



Deduplizierungseinheit

+

++

+(+)



Veeam Cloud Connect Backups
mit Insider-Schutz

++

++

++



Object Storage mit Object Lock

++(+)

+++

++(+)



Hardened Linux Repository

+++

++

+++



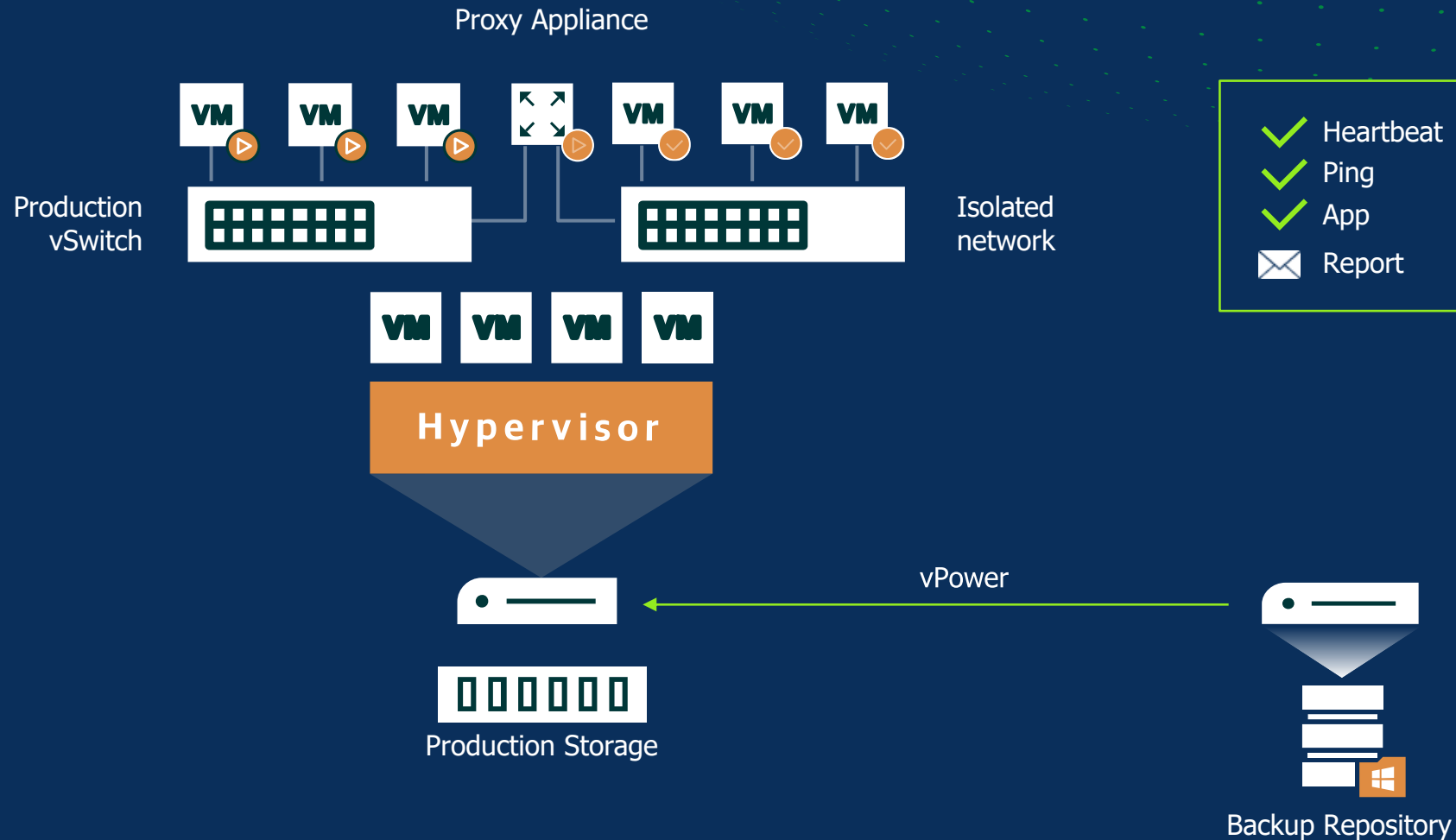
Tape

+

+(+)

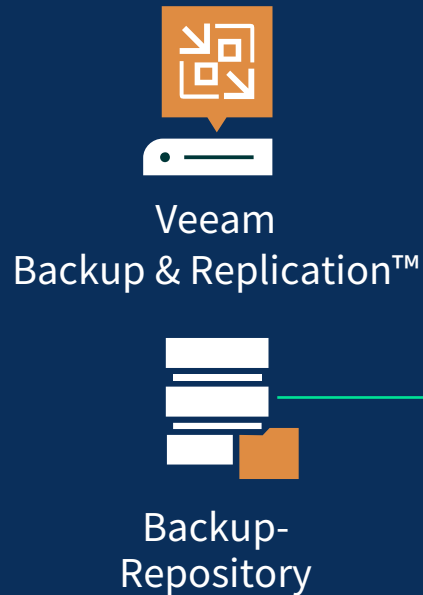
+++

Überprüfung der Backups



Secure Restore

1. Wiederherstellungspunkt auswählen



2. Backup-Dateien direkt als Laufwerk einhängen

Antivirensoftware mit aktuellen Definitionen installiert

3. Antivirus-Check



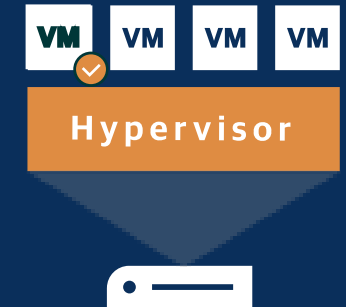
4a. Keine Infektion gefunden;
Wiederherstellung fortsetzen



4b. Infektion gefunden;
Wiederherstellung fortsetzen,
aber Netzwerk trennen



4c. Infektion gefunden;
Wiederherstellung
stoppen



Microsoft Windows Defender



ESET NOD32 Smart Security

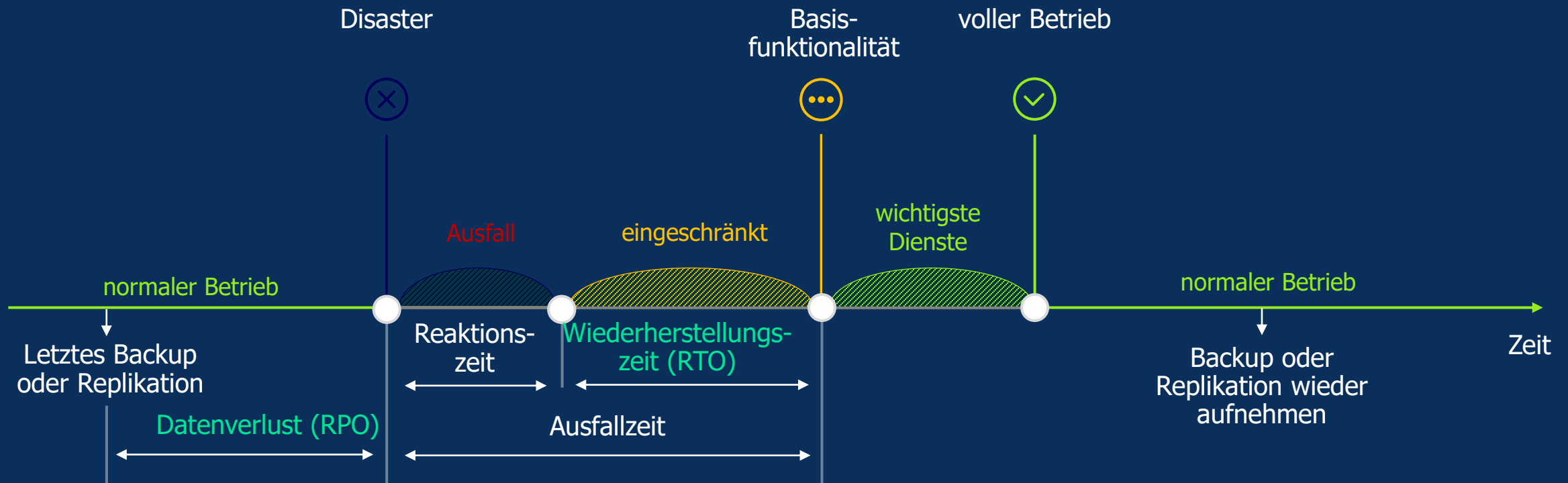


Symantec Protection Engine

Oder jede andere Antivirensoftware mit CMD-Unterstützung

Wiederherstellungsprozess

Was passiert, wenn eine Katastrophe eintritt?



Veeam Recovery Orchestrator



Dynamische Dokumentation

Sich automatisch aktualisierende Reports für Pre-Check, Test und Ausführung minimieren das Risiko von Fehlern im DR-Fall



Zero-Impact-Tests

DataLab-Tests erhöhen die Zuverlässigkeit, indem sie die Wiederherstellbarkeit im Katastrophenfall prüfen, ohne die Produktivsysteme zu beeinträchtigen



Compliance

RTO- und RPO-Reports unterstützen bei der Einhaltung von Compliance-Standards und SLA-Zielen



1-Klick-Wiederherstellung

Wiederherstellung einzelner Anwendungen oder eines ganzen Rechenzentrums mit einem Klick, gesichert durch rollenbasierte Zugriffskontrolle

Unterstützte Plattformen und Anwendungen:



Azure, vSphere



Agents:
Windows & Linux



Apps:
Exchange, SQL, SharePoint



Storage:
NetApp, HPE, Lenovo



Custom Scripting

Fragen?



Marc Heuser

Senior Systems Engineer – Germany NorthWest

marc.heuser@veeam.com



Dr. Christian Hillebrand

Atos Expert Community

hillebrand.christian@atos.net

