Don’t become a Ransomware Headline

Data Security in Zeiten wachsender Cyber-Bedrohung

Markus Parzer

Senior Territory Manager

Suchen

Filter | Österreich

https://www.dsgvo-portal.de/sicherheitsvorfaelle

Datum	Betroffene	Land	Sicherheitsvorfall
27.08.2024	WT Gruber Steuerberatung	AT	Ransomwaregruppe stiehlt 120 GB Daten von Steuerberatung . » Details
16.08.2024	Hiesmayr Haustechnik	AT	Unternehmen für Haustechnik offenbar mit Ransomware attackiert. » Details
13.08.2024	XPERT Business Solutions	AT	32 GB Daten von österreichischem IT-Dienstleister kompromittiert. » Details
19.07.2024	Albona Nova	AT	Hotel in Österreich auf Opferliste von Ransomwaregruppe gesetzt. » Details
05.07.2024	Europlast Kunststoffbehälterindus-trie GmbH	AT	Hacker stehlen 2,9 Mio. EUR innerhalb weniger Stunden. » Details
02.07.2024	Hauptmann	AT	Hacker kompromittieren Daten von Unternehmen. » Details
10.05.2024	Kuhn Rechtsanwälte	AT	Hacker kompromittieren 180 GB an Daten von Wirtschaftskanzlei. » Details
07.05.2024	Syntax Architektur	AT	Cyber-Angriff von LockBit Erpressergruppe auf Architekturbüro. » Details
02.04.2024	TUBEX Aluminium Tubes	AT	Ransomware-Gruppe kompromittiert 476 GB Daten von Tubenhersteller. » Details
13.03.2024	Forstinger Österreich	AT	Autoteilehändler von Ransomware-Gruppe angegriffen. » Details

Zeige Vorfall 1 bis 10 von 47 Vorfällen. 10 ▲ Vorfälle pro Seite.

← 1 2 3 4 5 →

veeam

Das „perfekte Chaos" aus Komplexität und Bedrohungen:

Daten Explosion

150+ ZB

erstellt 2024
verdoppelt sich jedes Jahr ...

Komplexität der Infrastruktur

92%

Unternehmen verfolgen eine Multi-Cloud-Strategie

Anbieter Anbieterbindung

Alle 3 Jahre

IT-Hardwaremodernisierung

Zunahme der Komplexität von Ransomware

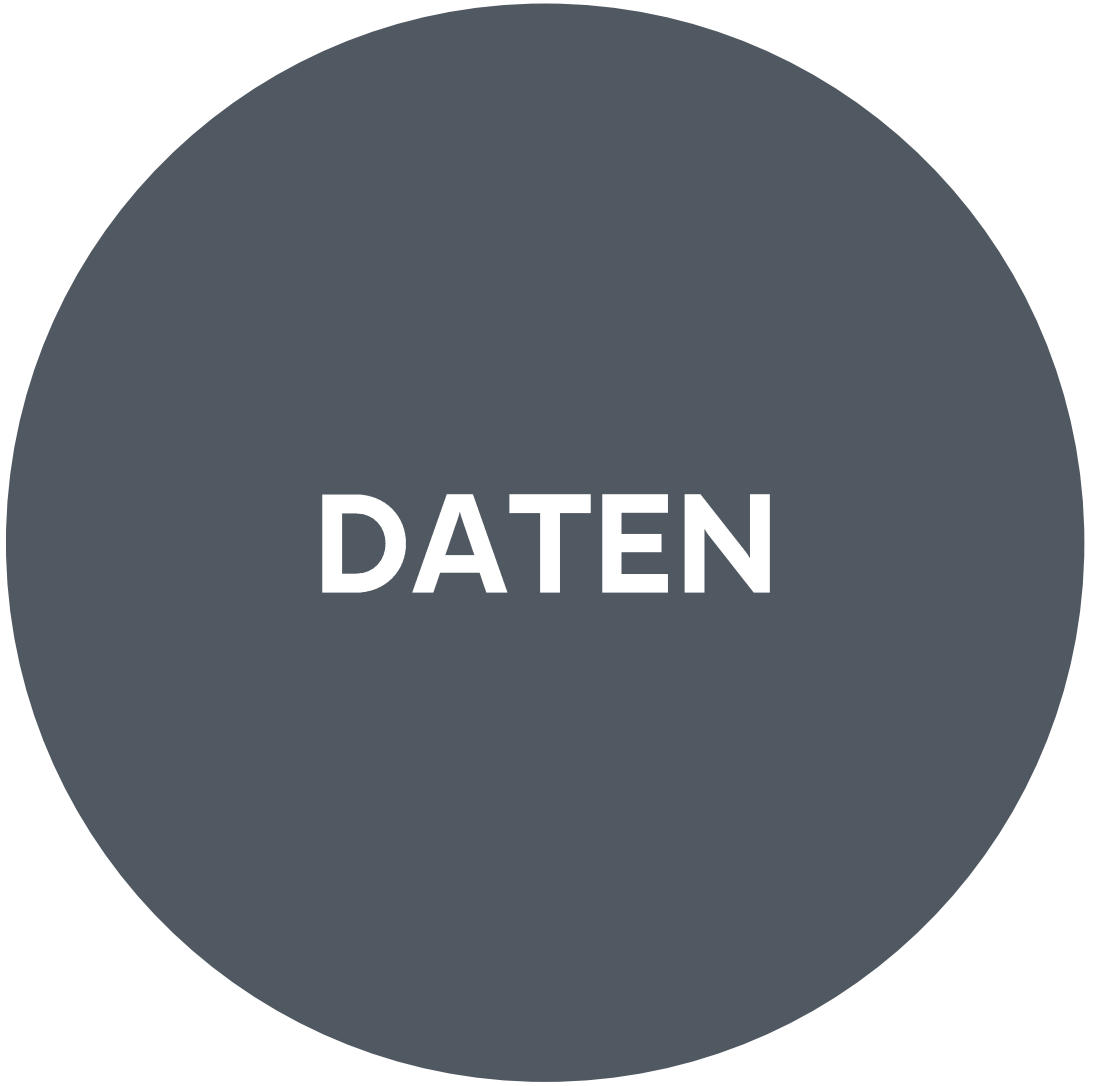
1 von 4

27% der Unternehmen konnten ihre Daten trotz Lösegeldzahlung nicht wiederherstellen

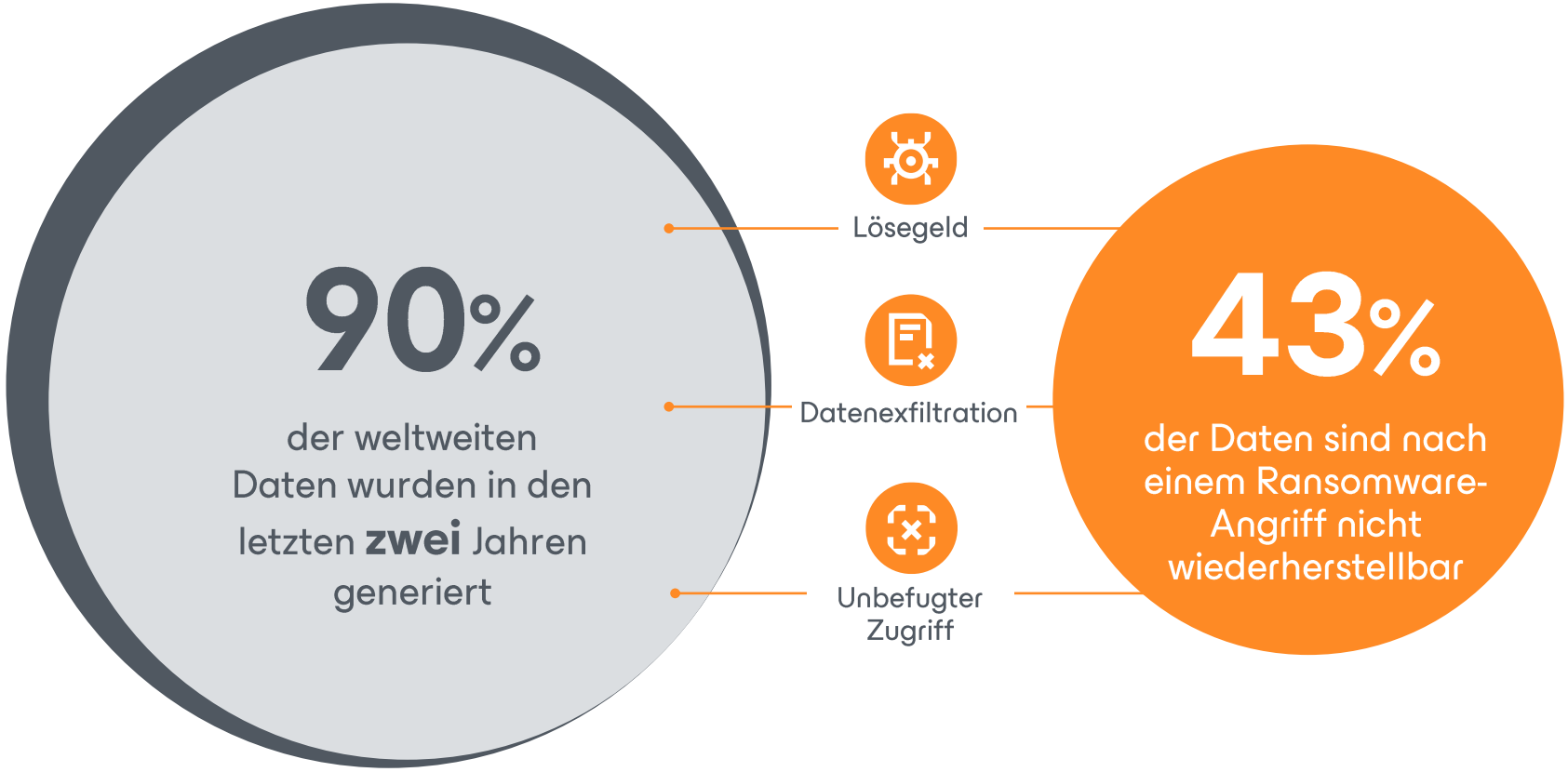
Komplexität

Bedrohungen

Daten sind das Lebenselixier des Business und **immerzu bedroht**



Daten sind das Lebenselixier des Business und **immerzu bedroht**

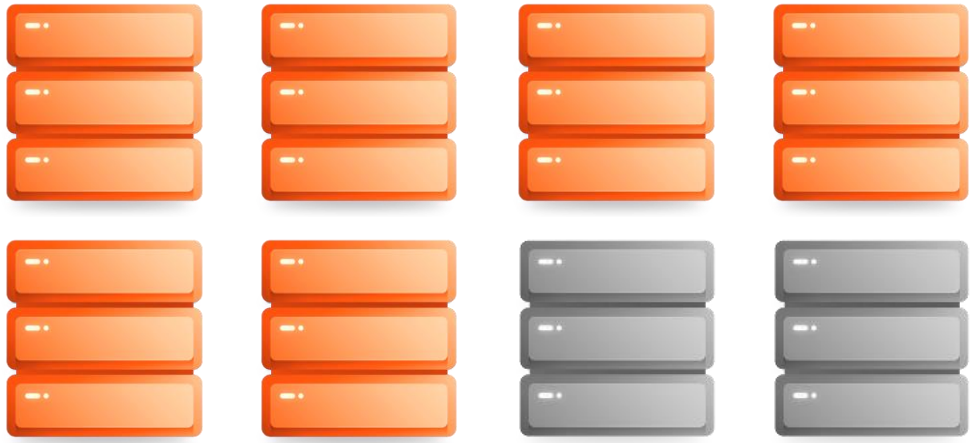


„Auf dem digitalen Schlachtfeld sind System-Backups die letzte Verteidigungslinie.

Cyberangreifer wissen das, und sie haben es darauf abgesehen, diese wichtigen Sicherheitsmechanismen zu untergraben. Als CIOs dürfen wir Backups nicht als bloße Kopien betrachten, sondern müssen sie als strategische Ressourcen einordnen.“

John O’Neill Sr.
CIO, Molded Fiber Glass Companies

Herkömmliche Strategien zur Datenwiederherstellung gefährden Ihr Unternehmen



Backups sind das Ziel von **96%** der Ransomware-Angriffe und wurden in **76%** der Fälle erfolgreich infiltriert.

Die Wiederherstellung nach einem Ransomware-Angriff ist nicht einfach

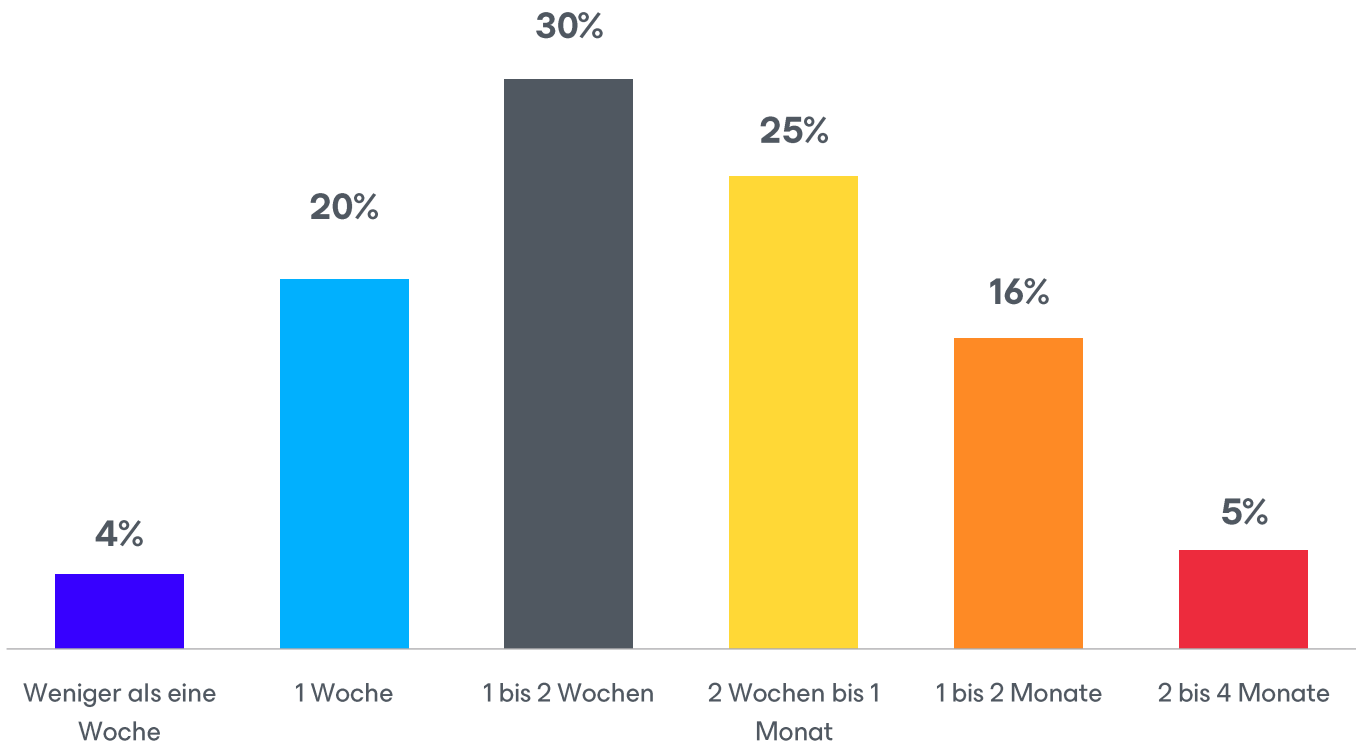
Wie lange dauerte die Wiederherstellung?

Die Wiederherstellung dauert durchschnittlich

drei Wochen

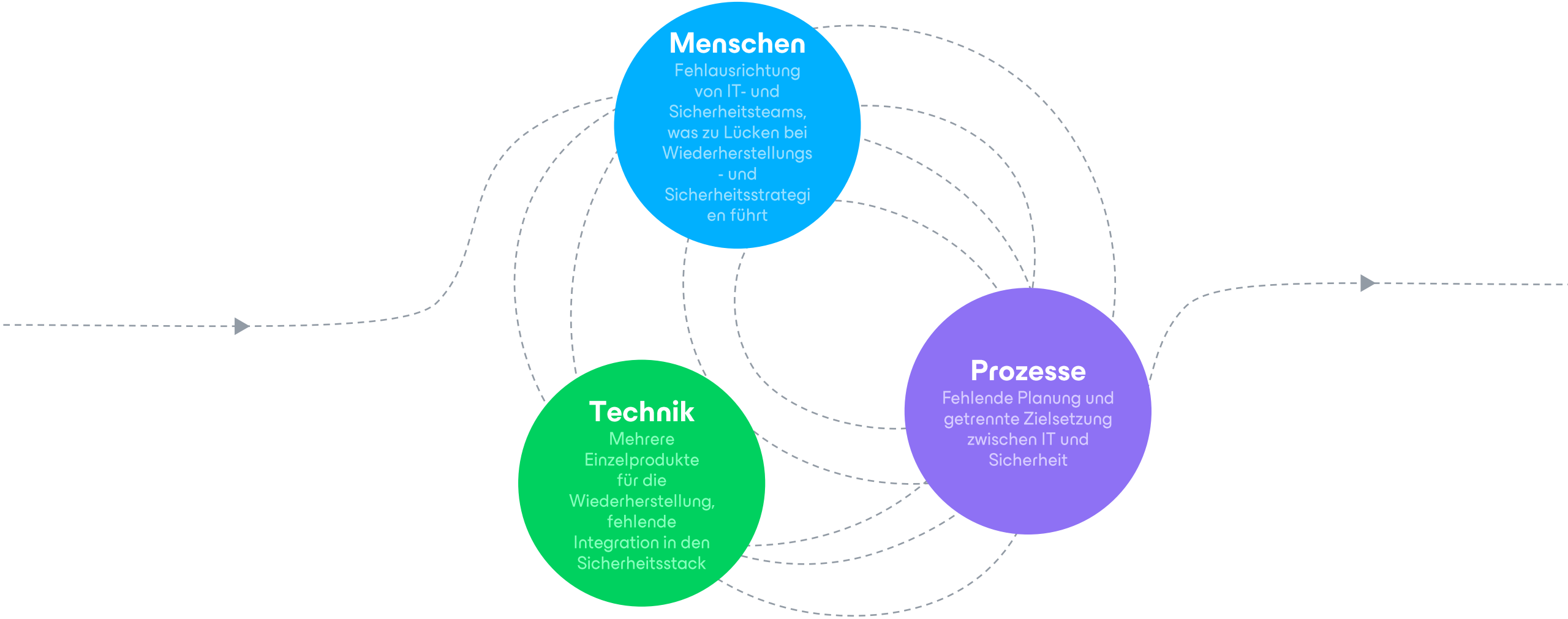
(pro Angriff) – nach Priorisierung der Maßnahmen

Wie lange dauerte die komplette Fehlerbehebung/Wiederherstellung, bis das gesamte Unternehmen das Problem als gelöst betrachtete?*



*Quelle: 2024 Ransomware Trends Report

Technologie allein reicht nicht aus, um echte **Resilienz zu gewährleisten**



Neue Ansätze zur Wiederherstellung sind nötig für echte **Datenresilienz**

aufeinander abgestimmte Sicherheits- und IT-Teams

schnelle und saubere Datenwiederherstellung in großem Umfang

Menschen
Prozess
Technik

AUSGERICHTET

Resilient bleiben und den Geschäftsbetrieb aufrecht erhalten

Maßnahmen zur Vorbeugung von Ransomware und zur Erkennung von Bedrohungen

UNSER ZIEL:

Wir sorgen für Datenresilienz, damit jedes Unternehmen am Laufen bleibt

Voraussetzung für Cyberresilienz ist eine gute Planung

Datensicherung ist Ihr Rettungsanker bei einem Ransomware-Angriff

Identifizierung

Welche Daten sind für Ihr Unternehmen unerlässlich?

Schutz

Wie sichern Sie unternehmenskritische Daten?

Erkennung

Werden Datenverlust und Datenkorruption rechtzeitig erkannt?

Reaktion

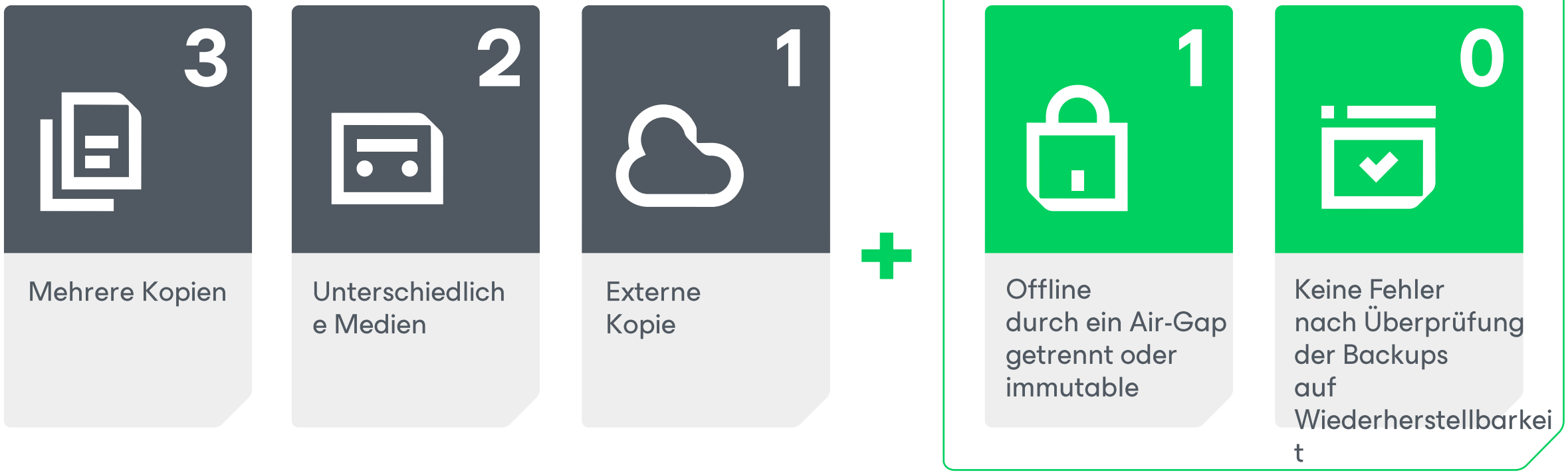
Sind Sie in der Lage, Daten schnell und präzise wiederherzustellen?

Wiederherstellung

Sind Ihre Disaster-Recovery-Pläne auf dem neuesten Stand und wurden sie getestet?

Umfassende Datensicherung

Lückenlose Immutability und vollständige Transparenz



Mehrere Resilienz-Domains, einzeln abgesichert

Objektsperre, echtes Air-Gap, branchenbewährte Verfahren

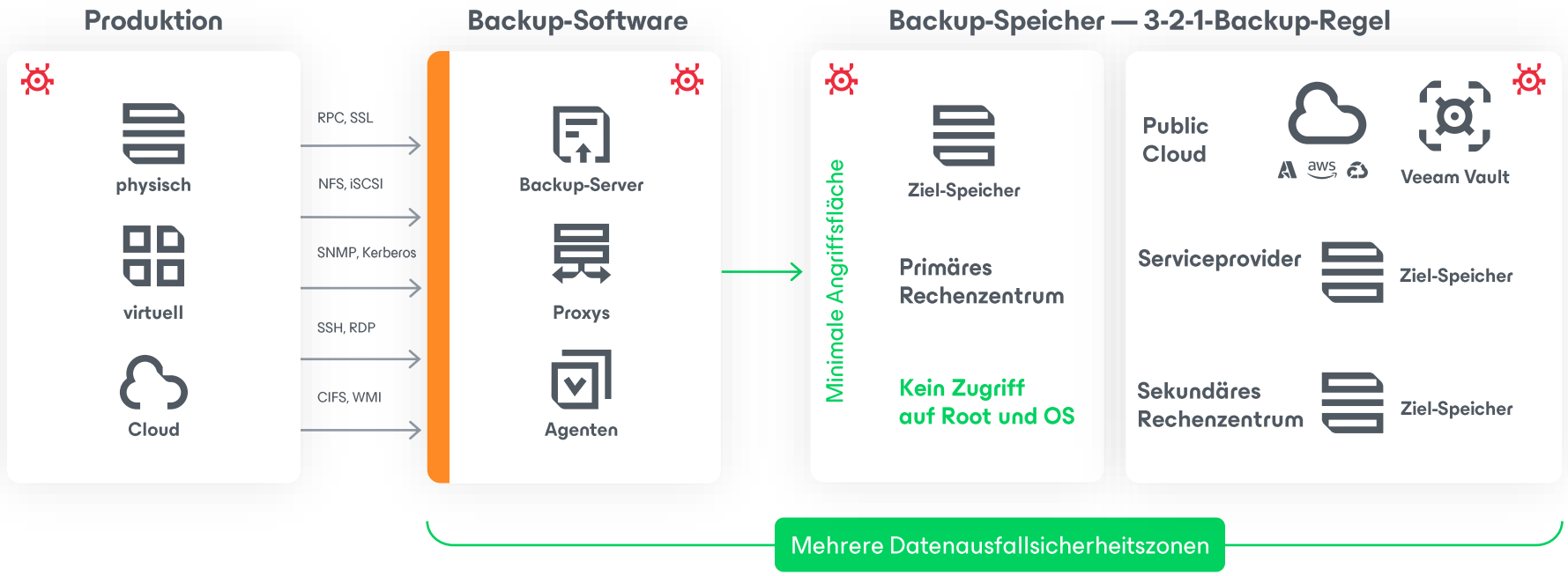
Security und Compliance Analyzer

Daten werden während der Übertragung und bei der Speicherung verschlüsselt

Keine Festlegung auf einen bestimmten Anbieter

Hardwareunabhängige Sicherheit mit Zero-Trust-Datenresilienz

Auf Sicherheit ausgelegt mit Zero-Trust-Architektur



Segmentierung von Software und Speicher

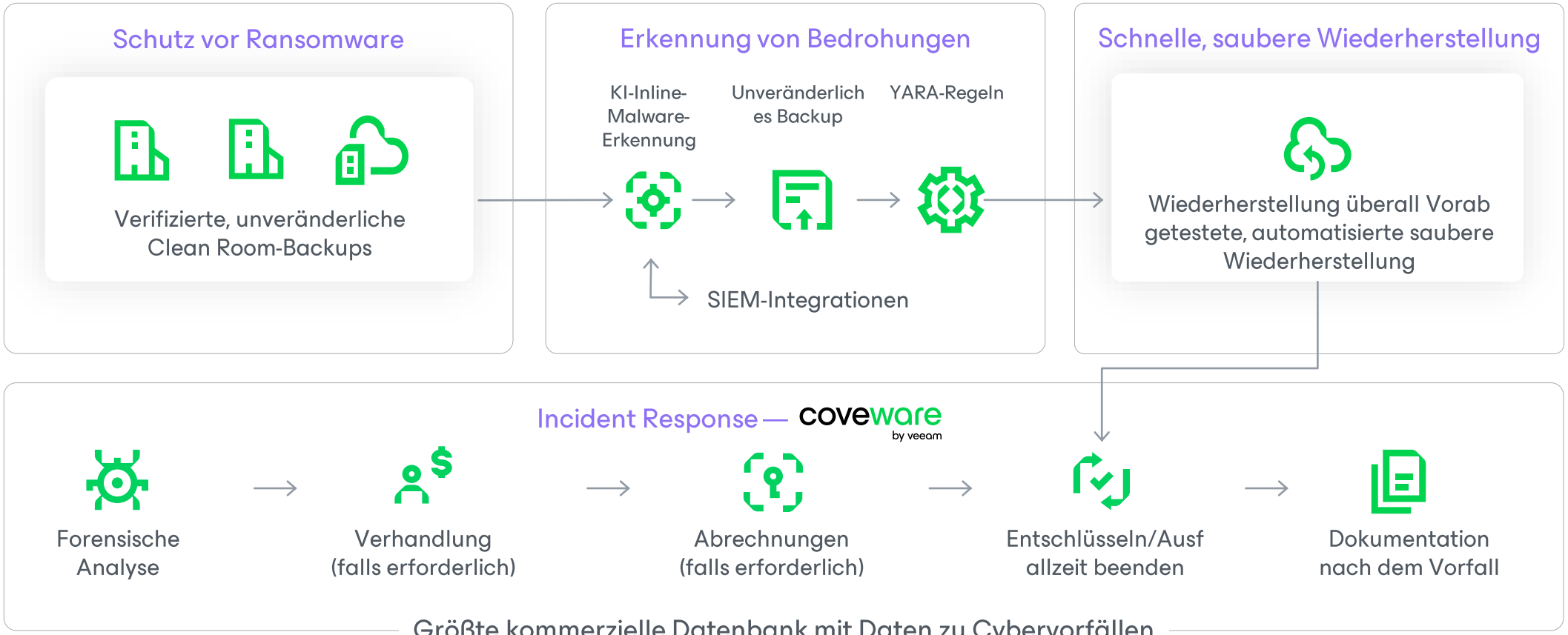
Mehrere **Datenresilienzzonen**

Unveränderlicher Backup-Speicher

Veeam bietet die umfassendsten Funktionen für den End-to-End-Schutz vor Ransomware und Wiederherstellung

Veeam Cyber Secure-Programm

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



Orchestrierte DR-Bereitschaft und Wiederherstellung

Dynamische Dokumentation

Automatische aktualisierte Reports zur Kontrolle, zum Test und zur Ausführung helfen, Probleme mit der DR-Bereitschaft zu korrigieren

Tests durchführen, ohne den Betrieb zu beeinträchtigen

DataLab-Tests sorgen für Gewissheit, indem sie die Disaster Recovery simulieren, ohne das Produktivsystem zu beeinträchtigen.

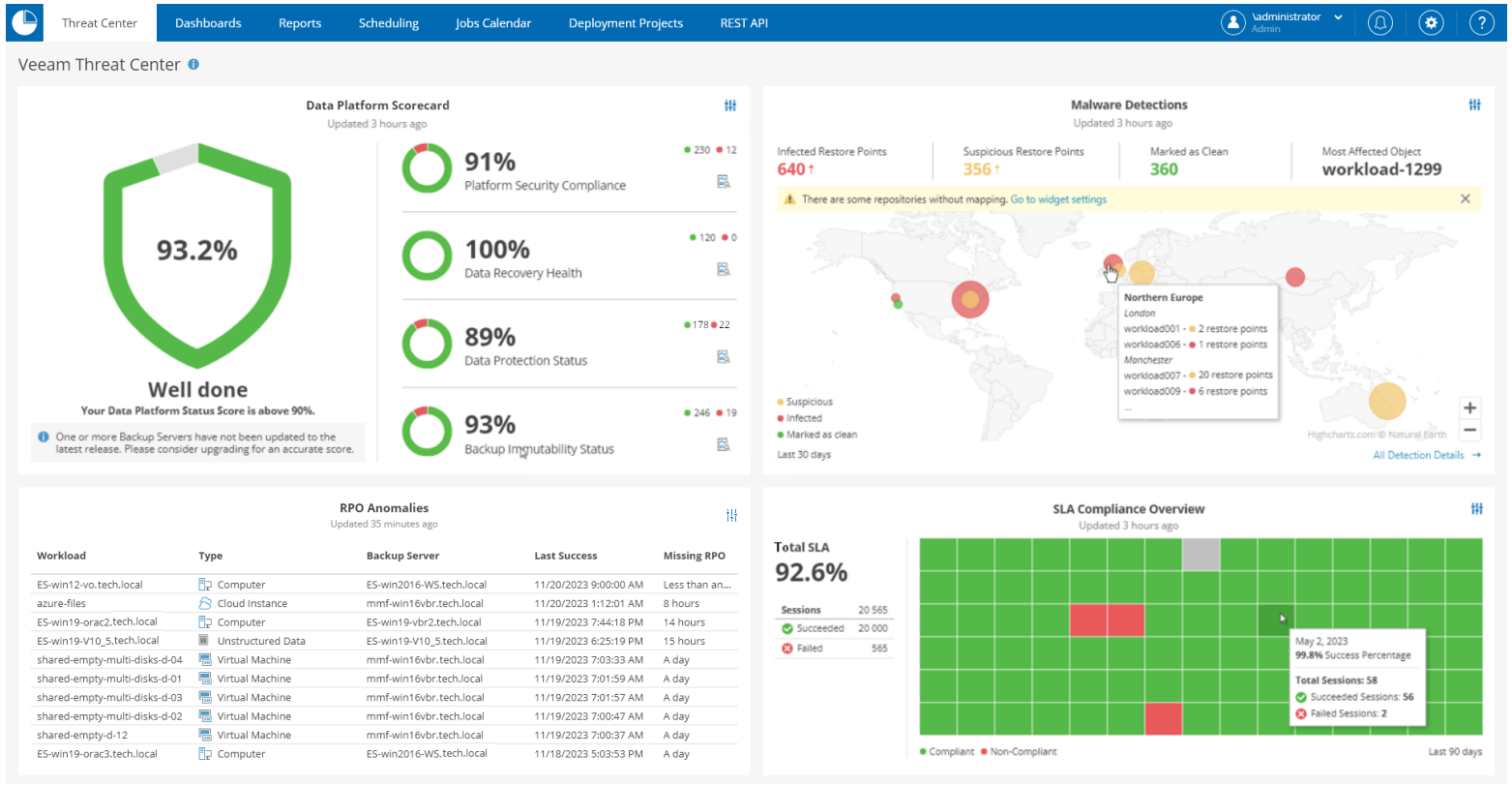
Compliance

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

Umfassende 1-Klick-Wiederherstellung

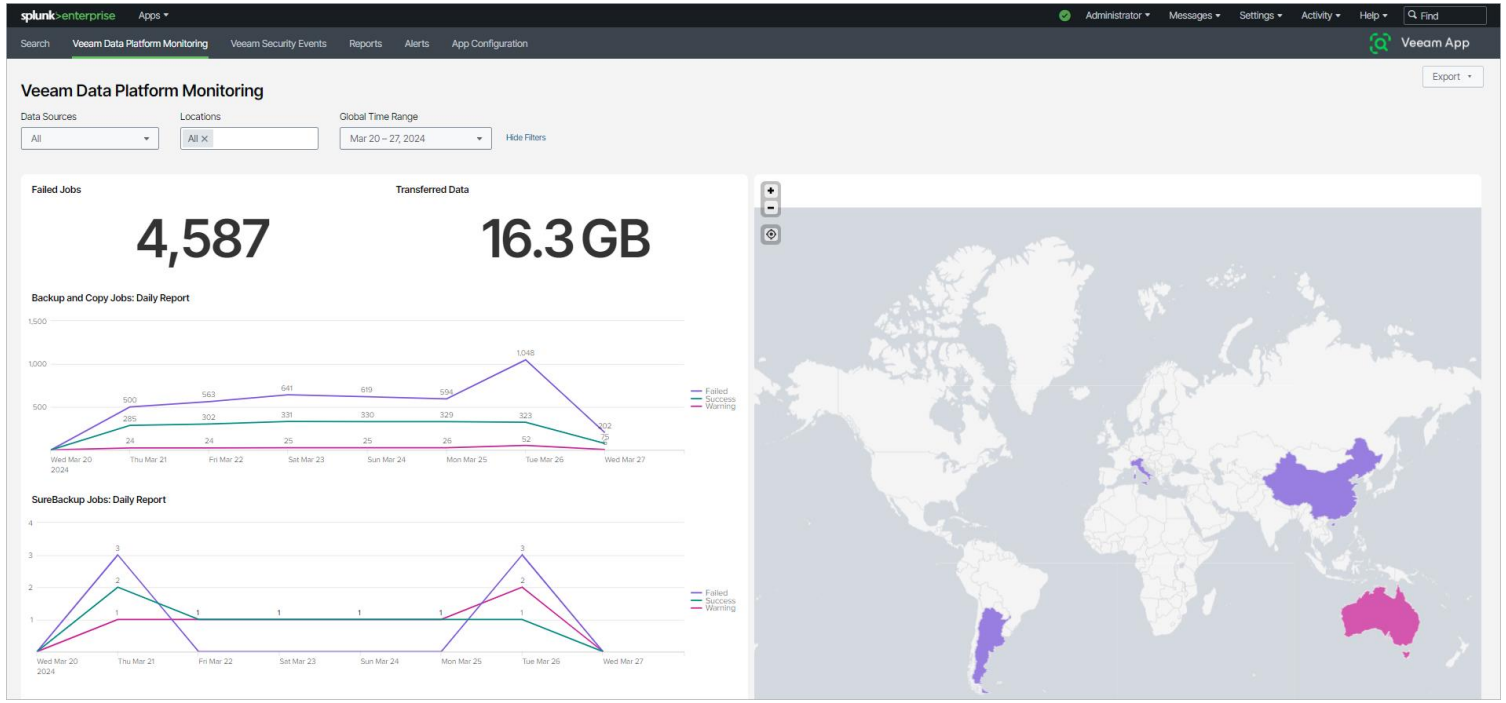
Wiederherstellung einzelner Anwendungen oder ganzer Standorte mit nur einem Klick und mit zuverlässigem Schutz durch rollenbasierte Zugriffskontrolle

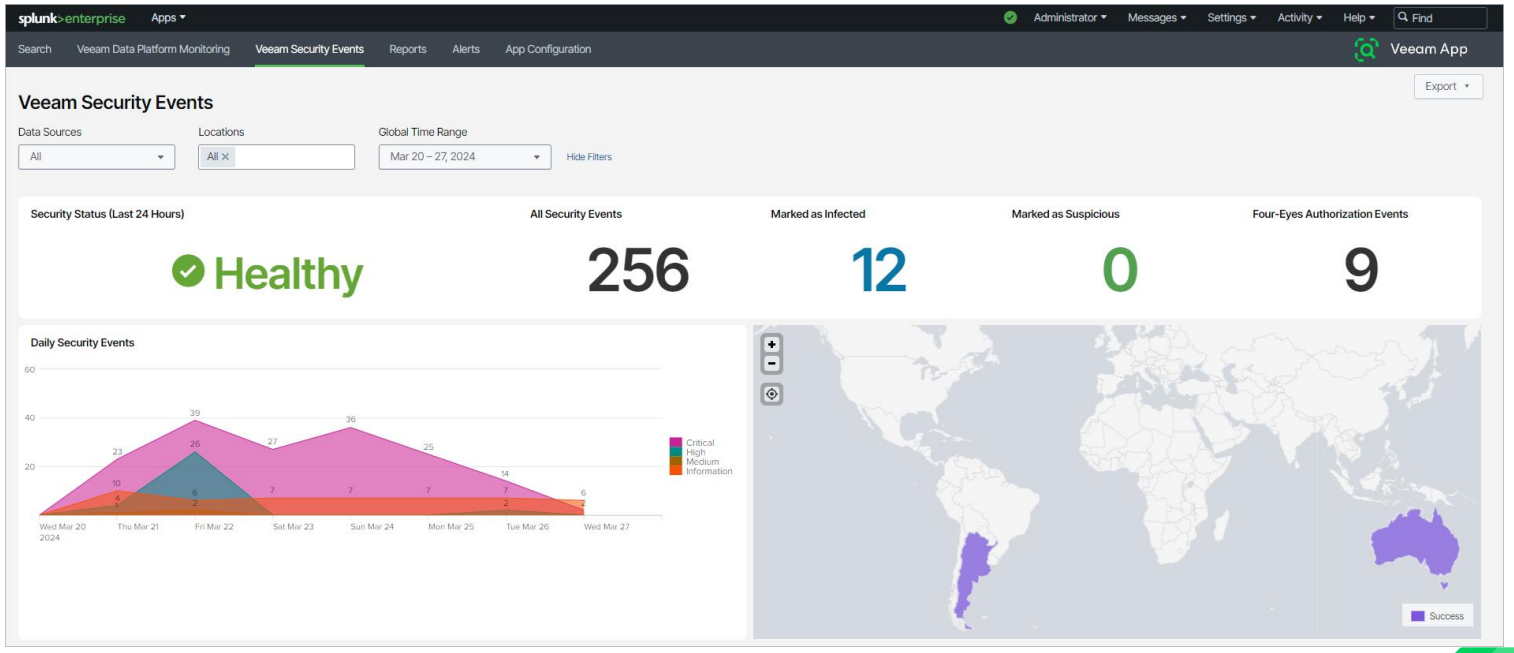
Veeam One Threat Center



Veeam App for Splunk

https://vee.am/splunk



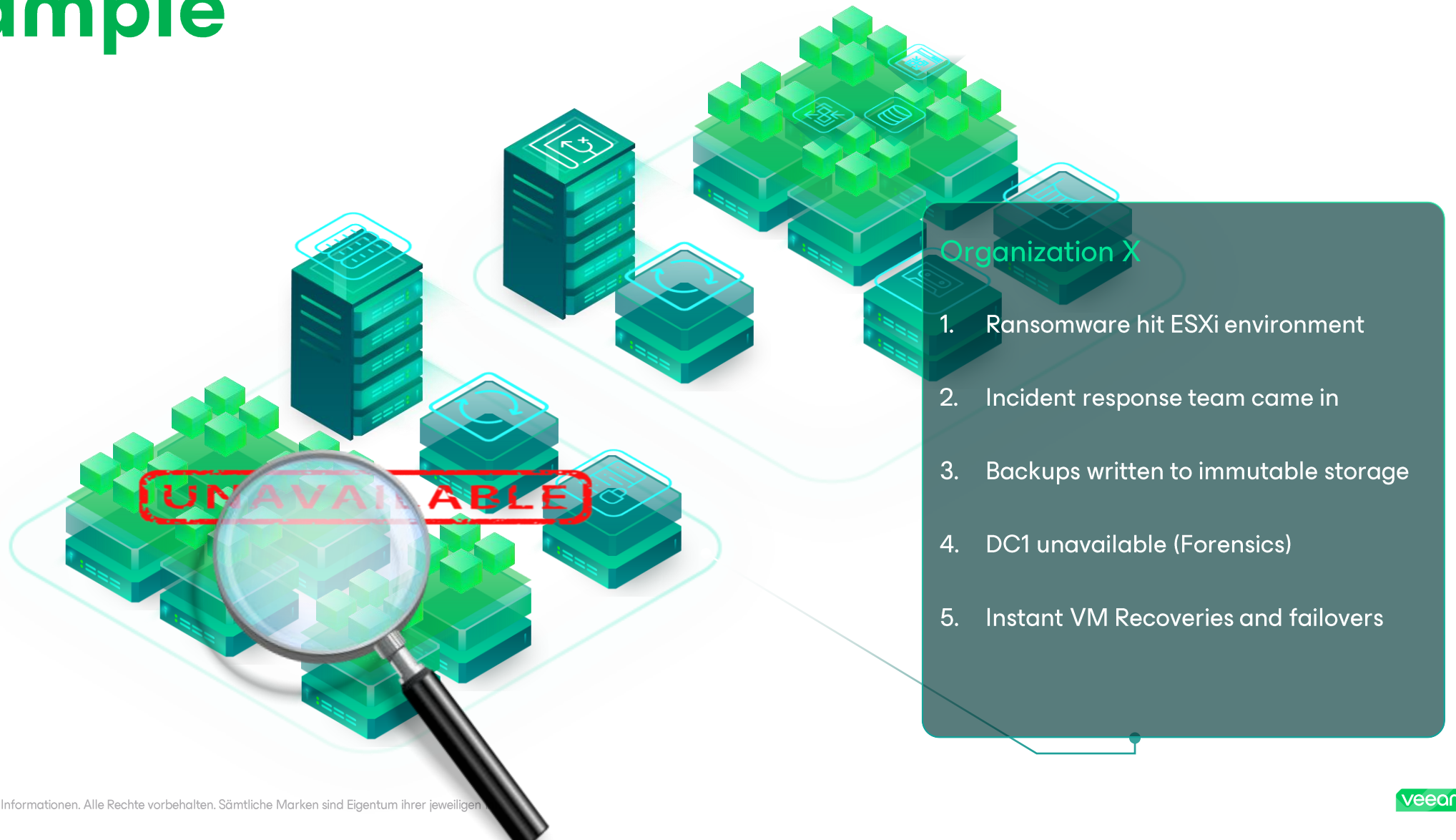


Veeam App for Palo Alto XSOAR 1.0

https://vee.am/xsoar

Lassen Sie sich nicht auf Verhandlungen mit Kriminellen ein, sondern gehen Sie schnell wieder zum Alltagsgeschäft über

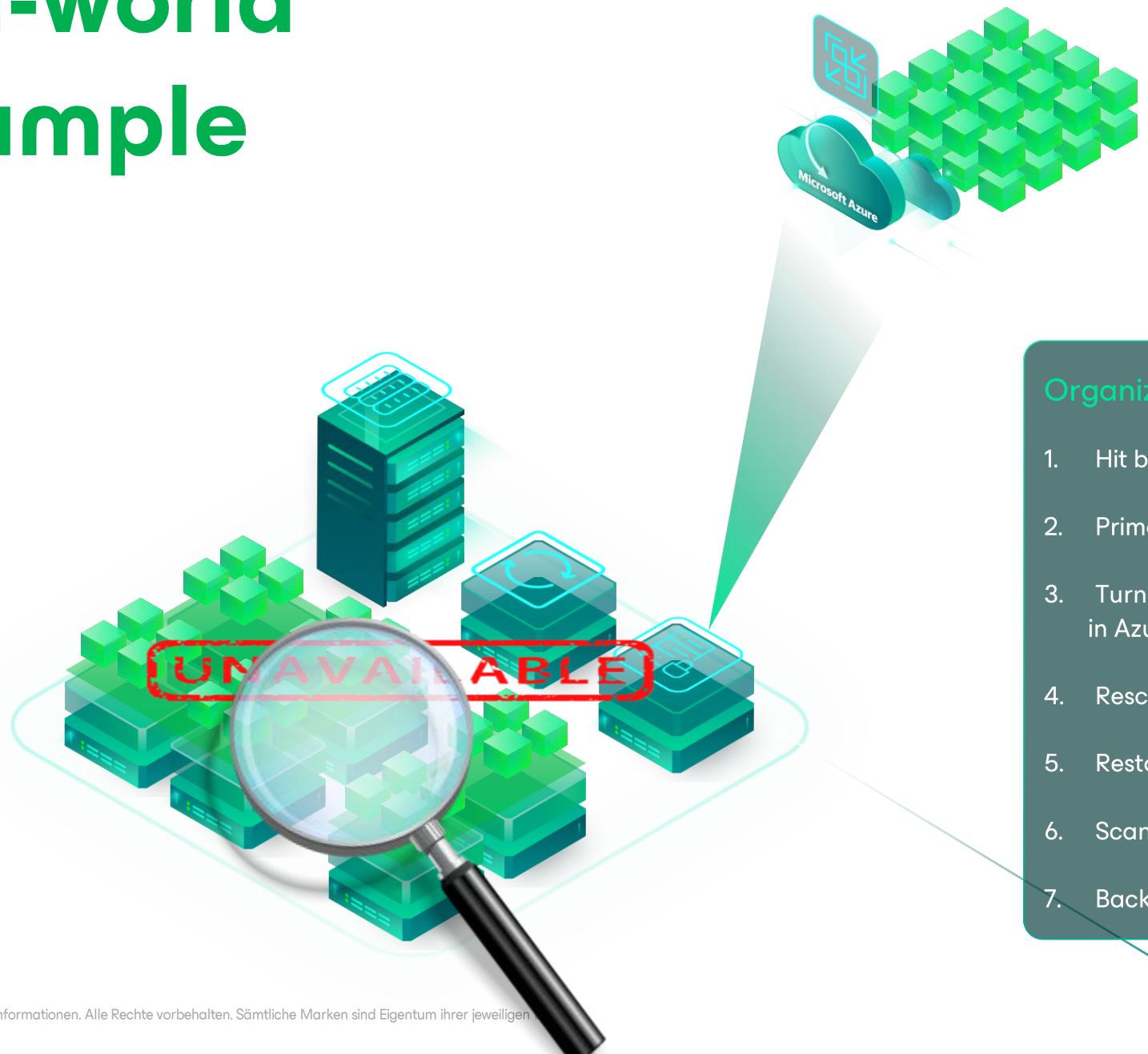
Real-world example



Organization X

1. Ransomware hit ESXi environment
2. Incident response team came in
3. Backups written to immutable storage
4. DC1 unavailable (Forensics)
5. Instant VM Recoveries and failovers

Real-world Example



Organization Z

1. Hit by Conti ransomware group
2. Primary DC offline for incident response team
3. Turned on Veeam Backup & Replication in Azure
4. Rescanned offsite copies in Azure
5. Restored VMs into Azure VMs
6. Scanned for malware
7. Back online

Backup ist wichtig, Wiederherstellung ist alles. Veeam kann beides.

Veeam ist weltweit führend bei Datenresilienz

#1
globaler Marktanteil für Datenreplikation und -sicherung
IDC

#1
Zuverlässige Wiederherstellung, fünfmal schneller
IDC

#1
Daten Portierbarkeit

#1
Microsoft 365

#1
Kubernetes

#1
Multi-Cloud-/Hybrid-Umgebungen
aws

#1
Magic Quadrant, Umsetzungsfähigkeit
Gartner

veeam

Take Away

Ransomware Trends Report 2024

- http://vee.am/NGpsGwq

Cyber Extortion: Protection and Rapid Recovery Guide

- https://vee.am/tj3GLwq

Folgen Sie uns!

Werden Sie Mitglied des Community-Hubs: