

RANSOMWARE FÜRCHTET RESILIENZ



Veritas NetBackup gewährleistet die Wiederherstellung geschäftskritischer Daten in jeder Größenordnung und schützt weltweit die meisten Exabytes an Daten. Die Lösung ist mit ihren neuen, modernen Funktionen führend im Wettbewerb und unterstützt Unternehmen dabei, die Lücken in ihrer Strategie für Ransomware-Resilienz zu schließen.



SCHUTZ

Mehrstufiger, proaktiver Schutz

Die Unterstützung für unveränderbaren Speicher auf AWS S3 stellt die Einhaltung der Compliance-Vorgaben sicher und verhindert, dass Ihre Daten kompromittiert werden.



ERKENNUNG

Vollständige, aktive Erkennung

Die Anomalie-Erkennung mithilfe von KI/ML ist Teil einer umfassenden Strategie, die sicherstellt, dass Daten sich stets wiederherstellen lassen.



WIEDERHERSTELLUNG

Automatisierte Orchestrierung der Wiederherstellung

Ressourcenschonende CDP-Backups und Instant-Rollback-Funktionen für VMware bieten integrierten Schutz ohne Ausfallzeiten.



Ransomware wird die Opfer mehr als **265 MILLIARDEN USD JÄHRLICH** kosten¹.

Unternehmen werden **BIS ZUM JAHR 2031 ALLE 2 SEKUNDEN** Opfer einer **RANSOMWARE-ATTACKE**¹.

BEISPIELLOSE DIGITALE TRANSFORMATION



Die Pandemie hatte tragische Folgen für Millionen von Menschen auf der ganzen Welt... doch diese Krise hat auch die digitale Transformation der Weltwirtschaft enorm beschleunigt.“

Dejan Ljustina, CEE TMT Industry Leader, PWC



Wir waren gezwungen, die digitale Transformation zu forcieren – nur, um zu überleben. Unsere 3-Jahres-Strategie für die Transformation wurde in ein 3-Monats-Fenster gezwängt. Das war schmerzhaft, aber wir haben es geschafft.“

Fortune 2000-Unternehmen und Veritas-Kunde



64 %

der IT-Führungskräfte sagen, dass ihre Sicherheitsmaßnahmen mit der IT-Komplexität NICHT Schritt halten konnten².



66 %

folgen dem 3-2-1-Backup-Prozess NICHT².



38 %

der IT-Führungskräfte berichten, dass sie nach einem Angriff mehr als 5 Tage nicht erreichbar waren².

DIE SORGEN ÜBER RANSOMWARE STEHEN IM VORDERGRUND

Hinsichtlich der Ransomware-Resilienz gibt es große Diskrepanzen in den Unternehmen.

> 96 %

der Führungskräfte stufen Ransomware als kritische Bedrohung für ihr Unternehmen ein².

Die Teams sind jedoch nicht im Einklang.

Die Kluft zwischen der wahrgenommenen Ransomware-Readiness der Unternehmensleitung und der ihrer IT-Teams ist erheblich.

> 25 %

der Unternehmen geben an, mehr als einmal Opfer eines Ransomware-Angriffs geworden zu sein².

Die Infrastruktur spielt dabei keine Rolle.

Untersuchungen ergaben, dass Ransomware-Angriffe in jeder Infrastruktur auftreten – auch in der Cloud.

1. <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/>
2. https://www.veritas.com/content/dam/Veritas/docs/ebook/V1117_GA_EB_2020-ransomware-resiliency-report_EN.pdf

WAPPEN SIE SICH GEGEN RANSOMWARE >