

Acronis

So verkaufen Sie Disaster Recovery Services

Ein Disaster Recovery-Playbook
für MSPs



Inhalts- verzeichnis

Was ist Disaster Recovery	3
Zukunftsorientierte MSPs steigern ihren Umsatz mit DRaaS	4
Profile der Zielkunden	5
So positionieren Sie Disaster Recovery	6
Häufige Einwände	7
Die Realität	8
Die Bedrohungen	9
10 Gründe, warum Ihre Kunden in Disaster Recovery investieren sollten	11
So begründen Sie inkrementelle Investitionen in vollständige Disaster Recovery	12
Berechnen Sie die Kosten durch Ausfälle	13
Bieten Sie zusätzliche Managed Services mit Disaster Recovery an	14
Marketingmaterialien	15

Einleitung

Einige Ihrer KMU-Kunden glauben wahrscheinlich, dass Backups allein ausreichen, und wissen nicht, wie wertvoll ihre Daten, Systeme und Anwendungen sind – bis es zur Kompromittierung kommt. Disaster Recovery ist der zusätzliche Schritt, den Sie benötigen, damit Ihre Kunden nach einem Ausfall schnell wieder auf die Beine kommen. Es kann mitunter schwierig sein, mit Interessenten über potenzielle Bedrohungen zu sprechen, die sie für sich nicht als relevant ansehen. Das erschwert den Verkauf.

Was ist Disaster Recovery?

Disaster Recovery (DR) funktioniert nicht ohne Backup. DR umfasst aktuelle Kopien der Daten und Verarbeitungsfunktionen auf einer Plattform, die die automatische Verfügbarkeit der wichtigsten Daten, Systeme und Anwendungen der Kunden ermöglicht. DR sorgt dafür, dass voneinander abhängige Prozesse in der richtigen Reihenfolge, auf dem richtigen Recovery-Punkt und zum richtigen Zeitpunkt wiederhergestellt werden.

Zukunftsorientierte MSPs steigern ihren Umsatz mit DRaaS

Es ist bekanntermaßen einfacher, an bestehende Kunden zu verkaufen. Bei Bestandskunden liegt die Wahrscheinlichkeit eines Verkaufsabschlusses bei 60–70 % – bei Interessenten bei lediglich 5–20 %. Mit anderen Worten: Wenn Sie Disaster Recovery nicht per Cross-Selling und Upselling verkaufen, verschenken Sie Geld. Verwenden Sie stattdessen die vorhandenen Daten und Kunden, um Ihre Umsätze und Provisionen zu steigern.

- DRaaS ist kostengünstig.
- Sie können sofort starten, ohne eine weitere Plattform hinzufügen, kennenlernen oder verwalten zu müssen.
- Sie verbessern Ihre Wettbewerbsposition.
- Die Kundenbeziehungen werden gefestigt.
- Die Kundenbindung wird gestärkt, da der Mehrwert der Backup-Daten gesteigert wird.
- Sie steigern den durchschnittlichen Jahresumsatz pro Benutzer (ARPU).
- Im Vergleich zu reinem Backup steigern Sie den Umsatz mit Acronis Cyber Disaster Recovery Cloud um etwa 80 %.

Geschwindigkeit und Umfang der Land-and-Expand-Strategie

Inkrementelle Umsatzsteigerung



■ Recovery nach einem Disaster ■ Recovery vor einem Disaster

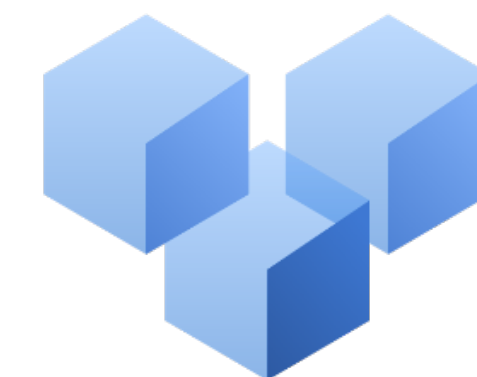
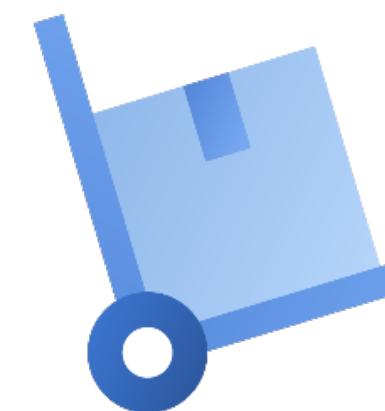
Profile der Zielkunden

Wer benötigt DRaaS? Jeder. Jedes Unternehmen kann einer Katastrophe zum Opfer fallen. Einige Ihrer Kunden haben ihren Standort eventuell in einer katastrophenanfälligen Region oder verfügen nicht über die technischen Ressourcen oder das nötige Fachwissen, um ein Disaster Recovery-Programm umzusetzen.

Zielbranchen

Folgende Branchen sind auf geschäftskritische Anwendungen und Daten angewiesen oder müssen bei Verstößen gegen gesetzliche Vorschriften mit hohen Geldstrafen rechnen:

- Finanzdienstleistungen
- Gesundheitswesen
- Rechtsbranche
- Transportbranche
- Telekommunikation
- Fertigungsindustrie
- Baubranche
- Energiebranche
- E-Commerce
- Versorgungsunternehmen
- Lieferketten und Logistik



So positionieren Sie Disaster Recovery

Die Wiederherstellung des gewohnten Betriebs ist nicht nur für die IT ein Problem. Wenn auch Abteilungen wie Personal, Finanzen, Recht usw. von Ausfällen betroffen sind, wird sie zu einem unternehmensweiten Problem. Passen Sie die Gespräche an die verschiedenen Rollen und Verantwortungsbereiche an.



IT-Abteilung

- Backup und Recovery
- Interne und externe SLAs
- Zufriedenheit der Mitarbeiter
- Audits
- Einhaltung gesetzlicher Vorschriften



Führungsebene

- Pläne zur Gewährleistung der Geschäftskontinuität
- Marktwahrnehmung
- Produktivität der Mitarbeiter
- Einhaltung gesetzlicher Vorschriften
- Versicherung



Finanzabteilung

- Einhaltung gesetzlicher Vorschriften
- Schutz sensibler Daten
- Aufrechterhaltung des Geschäftsbetriebs
- Markt- und ökonomisches Vertrauen
- Audits



Personalabteilung

- Planung für Stellenbesetzung und Belegschaft
- Schulungen
- Produktivität der Mitarbeiter
- Schutz sensibler Daten



Rechtsabteilung

- Einhaltung gesetzlicher Vorschriften
- Schutz sensibler Daten
- Versicherung

Häufige Einwände

Disaster Recovery wird häufig als optionales Extra statt als unerlässliche Funktion betrachtet. Eventuell werden Ihnen viele Gründe genannt, warum Kunden Disaster Recovery nicht im Blick haben.

Dazu gehören Klassiker wie:

- **Das ist zu teuer.**
- **Das ist zu kompliziert.**
- **Das wird uns nie passieren.**

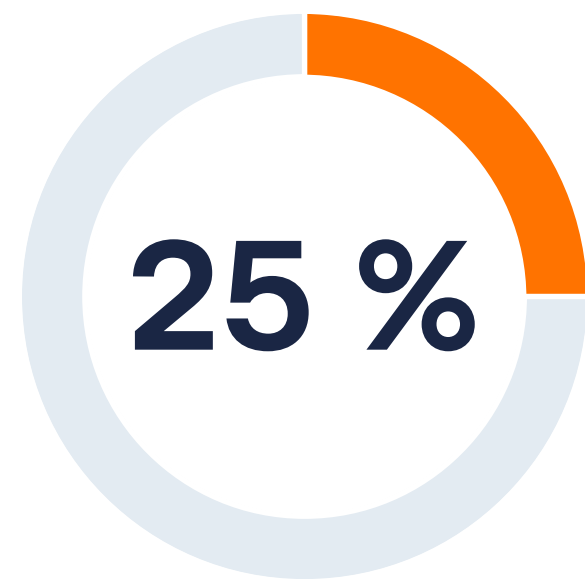
Reagieren Sie auf diese Einwände, indem Sie auf die Fakten zu Disaster Recovery hinweisen, die wir auf den nachfolgenden Seiten aufzeigen: die Realität basierend auf statistischen Daten, die Arten der Bedrohungen, Gründe für die Investition in eine „Versicherung“ für Disaster Recovery und die tatsächlichen Kosten von Ausfallzeiten.

Vergleichen Sie die Kosten für Disaster Recovery mit den Kosten für die Unterbrechungen der täglichen Geschäftsabläufe, um Unterstützung für DRaaS zu gewinnen.

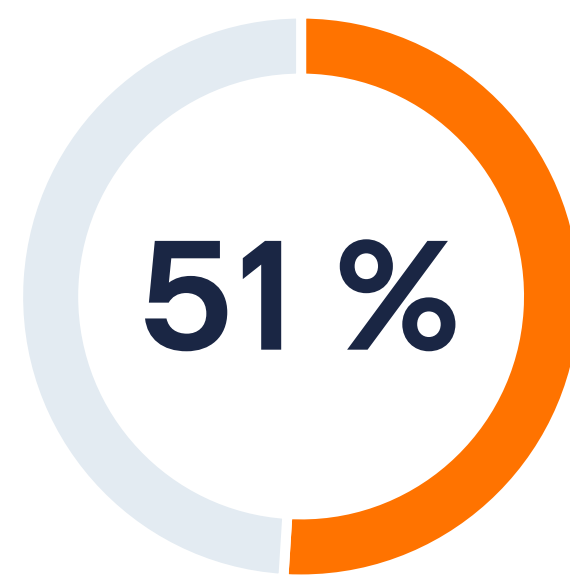


Die Realität

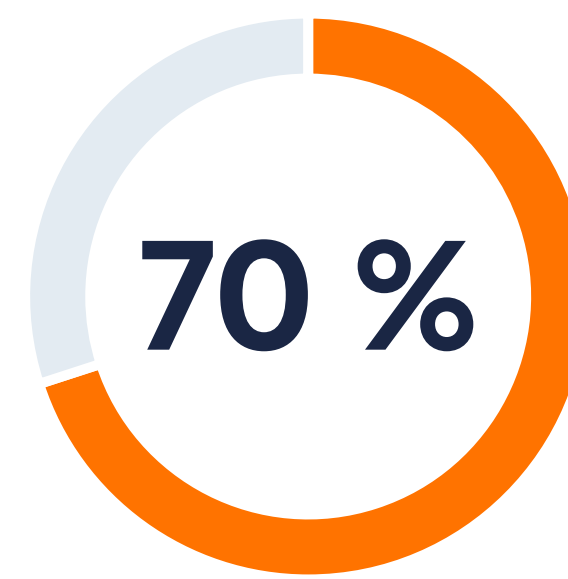
Die Auffassung, dass „uns das nie passieren wird“, lässt sich mit den realen Zahlen schnell widerlegen.



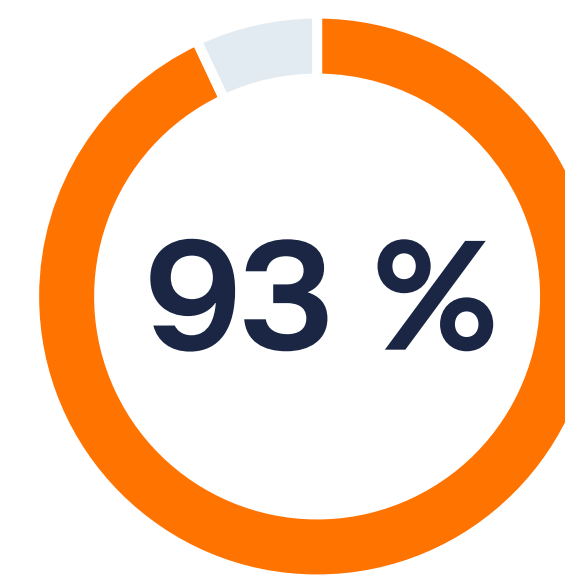
der Datenschutzverletzungen im Jahr 2019 wurden durch versehentliches Löschen oder Überschreiben von Dateien oder Ordnern verursacht¹



der Datenschutzverletzungen im Jahr 2019 wurden durch kriminelle oder böswillige Angriffe verursacht¹



der Unternehmen werden wahrscheinlich bis 2022 Geschäftsunterbrechungen wegen unbehebbarem Datenverlust erleiden²



der Unternehmen haben in den letzten drei Jahren Angriffe erlebt³

2,2 Tage

durchschnittliche
Ausfalldauer²

5.600 \$

durchschnittliche
Kosten pro Minute²

3,92 Mio. \$

durchschnittliche
**Gesamtkosten einer
Datenschutzverletzung²**

1) Ponemon Institute, 2019. 2) Gartner, 2019. 3) IDC, 2019.

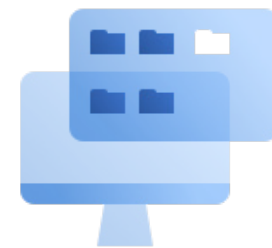
Die Bedrohungen

Beschreiben Sie die Bedrohungen, mit denen Ihre Kunden rechnen müssen. Eventuell glauben sie, dass nur natürliche Desaster zu Unterbrechungen mit Stromausfällen und Hardware-Störungen führen können, doch müssen auch Versagen von Software und Mitarbeitern als Gründe für Ausfälle bedacht werden. Mit der weiteren Entwicklung der Technologie entstehen zudem neue interne und externe Bedrohungen.



Natürliche Desaster

Hurrikane, Tornados und Feuer können schwere Ausfälle verursachen, da sie auch Gebäude und Infrastruktur beeinträchtigen. Viele Kunden verstehen wahrscheinlich nicht, dass nur 6 % der Ausfälle durch natürliche Desaster ausgelöst werden.



Pandemien

Bei dieser Art von Bedrohung sind vor allem die Mitarbeiter eines Unternehmens betroffen. Kommt noch die Arbeit im Homeoffice hinzu, entsteht eine ganze Reihe an Planungsszenarien, die von der IT bisher noch nicht berücksichtigt wurden. Das Sicherheitsrisiko steigt, wenn Daten und Geräte permanent außerhalb der regulären IT-Infrastruktur genutzt werden.



Hardware-Fehler und Software-Beschädigungen

Hardware-Fehler können durch einen Stromausfall entstehen. Software kann durch fehlerhafte Updates oder inkorrekte Formatierung von Laufwerken beschädigt werden.



Menschliche Fehler – unabsichtlich oder böswillig

Menschliches Versagen kommt vor. Viele von uns haben schon einmal etwas versehentlich gelöscht oder überschrieben. Zudem kann auch ein verärgerter Mitarbeiter verheerende Schäden an Daten und Systemen anrichten.

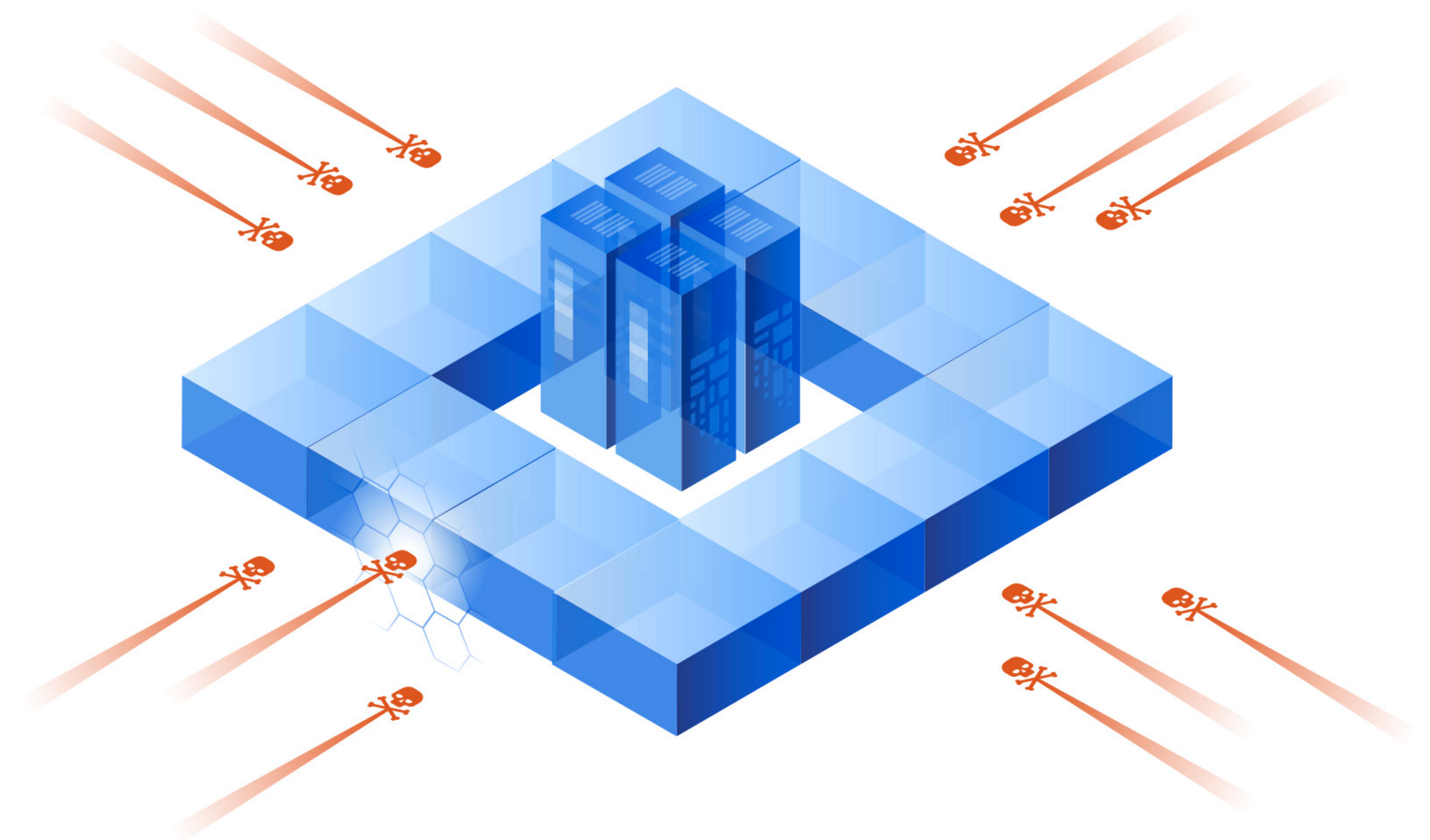


Cyber-Angriffe

Durch einen einzigen kompromittierten Rechner eines Mitarbeiters können ganze Netzwerke anfällig werden. Schnell können Angriffe erfolgen, wenn Mitarbeiter schwache Kennwörter verwenden, auf Phishing-Betrug hereinfliegen oder auf böswillige Links klicken.

Angesichts der Vielzahl von internen und externen Faktoren, die die Systeme und Daten Ihrer Kunden beeinträchtigen können...

stellt sich nicht die Frage, ob Ihre Kunden Datenverluste erleiden werden, sondern eher wann es passieren wird.



10 Gründe, warum Ihre Kunden in Disaster Recovery investieren sollten

Es gibt viele Gründe, warum es sich für Kunden lohnt, über Backups hinaus in Disaster Recovery zu investieren.

- **Geringere Auswirkungen** von Katastrophen
- Gewährleistung ununterbrochener **Mitarbeiterproduktivität**
- **Kosteneinsparungen**
- **Einhaltung der rechtlichen und Compliance-Vorgaben** innerhalb der Branche (Finanz-, Rechts- und Gesundheitswesen)
- Nutzung **sofortiger Wiederherstellung**
- **Kürzerer Ausfall** des Geschäftsbetriebs
- **Weniger** potenzielle **Finanzverluste**
- **Weniger Risiken** durch Haftungsverpflichtungen
- **Geringeres Risiko** für negative Publicity
- **Optimiertes** Krisenmanagement



So begründen Sie inkrementelle Investitionen in vollständige Disaster Recovery

Es ist einfacher als gedacht, Ihren Umsatz zu steigern und gleichzeitig Zeit- und Geldersparnis bei Ihren Kunden zu erzielen. Der wichtigste Vorteil von Cloud-basierter Disaster Recovery ist, dass die Ausgaben zum größten Teil als Betriebsausgaben (OPEX) statt als Kapitalkosten (CAPEX) eingestuft werden.

Die IT-Abteilung spart außerdem viel Zeit, weil die Mitarbeiter nicht mehr die Server kaufen, konfigurieren, testen und bereitstellen müssen, die anschließend meist inaktiv bleiben.

Zu den weiteren Vorteilen einer Cloud-basierten Disaster Recovery-Lösung gehören die Benutzerfreundlichkeit, Agilität, schnelle Wiederherstellung und die beruhigende Gewissheit, geschützt zu sein. Es werden keine zusätzlichen Datenzentren oder Maschinen benötigt.

Acronis Cyber Disaster Recovery Cloud baut auf der Acronis Cyber Backup Cloud auf, sodass Disaster Recovery tatsächlich nur inkrementelle Kosten verursacht.

Sie verfügen also über alle notwendigen Zutaten. Sie müssen sie lediglich aktivieren.



Berechnen Sie die Kosten durch Ausfälle

All diese Faktoren lassen sich auf die Unternehmen Ihrer Kunden anwenden. Um die tatsächlichen Ausfallkosten pro Stunde zu berechnen, werden Zahlen für Aufwand und Kosten aus allen Abteilungen herangezogen. Das Ergebnis: Ausfälle führen zu enormen finanziellen Verlusten.

Verlorener Gewinn + Verlorene Produktivität + Wiederherstellungskosten + Immaterielle Kosten = Ausfallkosten (pro Stunde)

Verlorener Gewinn

Dieser Punkt ist relativ leicht zu verstehen. Steht das Unternehmen Ihrer Kunden still, kann kein Gewinn erwirtschaftet werden.

Berechnen Sie anhand des Bruttojahresumsatzes für jeden Geschäftsbereich den verlorenen Gewinn pro Stunde im Falle eines Ausfalls.

Verlorene Produktivität

Die Kosten durch Ausfälle steigen auch, wenn die Mitarbeiter Ihrer Kunden nicht arbeiten können oder dazu gezwungen sind, nicht gewinnbringende Tätigkeiten auszuführen. Gehälter oder Stundenlöhne sind fixe Kosten und müssen unabhängig von der Produktivität der Mitarbeiter gezahlt werden.

Wiederherstellungskosten

Oft werden die Kosten, die durch Wiederherstellung und Wiederaufnahme des regulären Betriebs entstehen, nicht bedacht. Beispiele für anfallende Kosten:

- Zeitaufwand von Dienstleistern und Mitarbeitern für die Wiederherstellung verlorener Daten
- Physische Tools bzw. Geräte, die repariert oder ersetzt werden müssen
- Kosten durch verlorene Daten

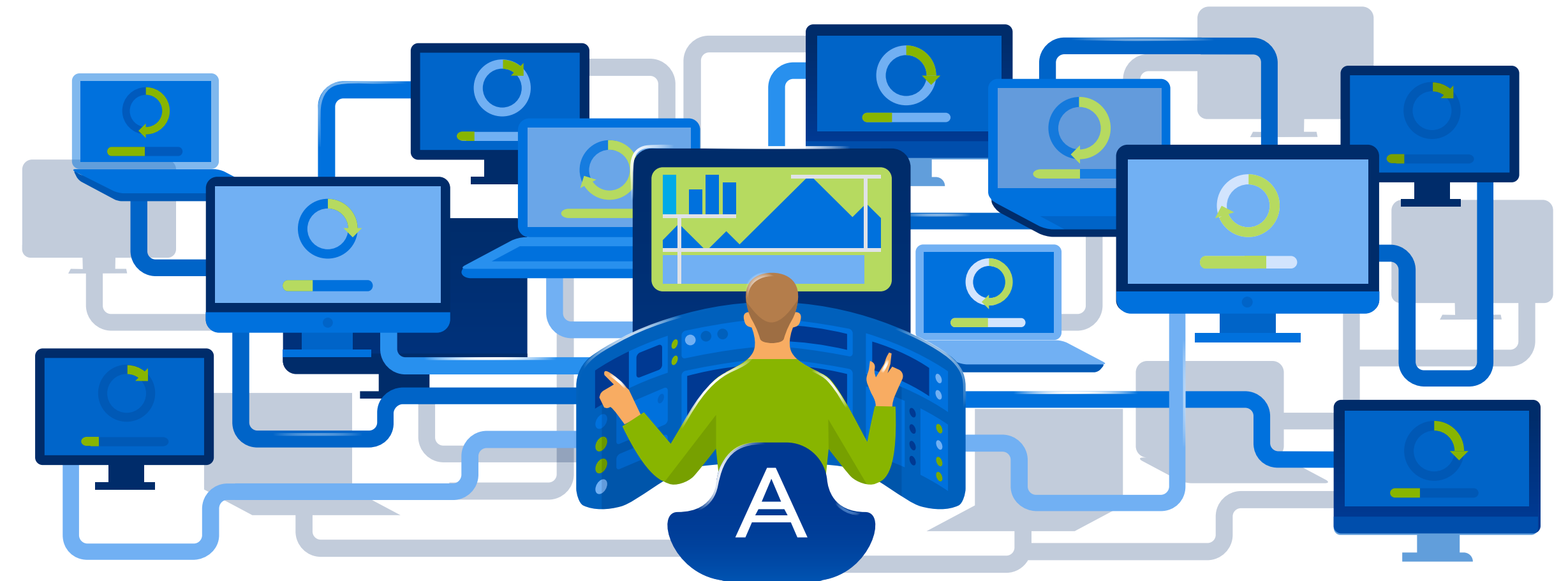
Immaterielle Kosten

Reputations- und Markenschäden führen zu finanziellen Verlusten. Der kleinste Ausfall kann zu unwiderruflichen Schäden für die Unternehmen Ihrer Kunden führen. Wie der Ausfall gehandhabt wird, kann zudem entscheidend dazu beitragen, ob betroffene Unternehmen wieder auf die Beine kommen oder untergehen.

Bieten Sie zusätzliche Managed Services mit Disaster Recovery an

Zur weiteren Steigerung der monatlichen, vierteljährlichen und jährlichen Umsätze können Sie Ihren Kunden zusätzlich zu verwaltetem Disaster Recovery diese Managed Services anbieten:

- Vorbereitung der Mitarbeiter auf Notfälle
- Zuordnung von Workflow-Prozessen vor, während und nach Notfällen
- Offsite-Desktops, Callcenter und Einsatzzentrale für Notfälle
- Dokumentation
- Schulungen
- Wartung und Upgrades
- Tests
- Berichterstellung
- Unterstützung bei Audits



Wenn Sie verwaltete Erlebnisse im größeren Umfang bereitstellen möchten, aber nicht über die nötigen Kompetenzen verfügen, stehen Ihnen Acronis Partner zur Verfügung, deren fachkundige Disaster Recovery Services per White-Labeling einbezogen werden können.

Marketingmaterialien

Ihnen stehen alle Materialien zur Verfügung, um loslegen zu können.

Diese werden per White-Labeling angeboten, damit Sie sie mit Ihrem

Logo und Ihren Produktnamen anpassen können. Die Materialien sind

im Acronis Partnerportal abrufbar:

- DRaaS-Website
- DRaaS-Blog-Beiträge
- Datenblatt
- Multi-Touch-E-Mail-Kampagne
- Banner
- Leicht verständliche Anleitungen

Disaster Recovery bedeutet, das Unerwartete zu erwarten



Disaster Recovery bedeutet, das Unerwartete zu erwarten



DRaaS with <SP name>

<DR product> is an easy and affordable DRaaS solution, built on top of <cloud backup product>, that protects your applications and systems from disaster strikes by instantly spinning up systems in a managed cloud recovery site, enabling them to be restored to anywhere when possible.

APEX

Supports your budget with no investments in an off-site DR facility, or on-premise software and hardware.

DR recovery for any workload

Support all popular workloads – Windows and Linux, major hypervisors, and business applications.

Get More Than Backup for When Disaster Strikes

In today's business world, your data is the single most valuable asset. Our backup solution protects your company's data so we can always restore your critical business systems locally. That means in the case of a serious outage like one caused by a natural disaster, your backup files and systems' images will be safe. But it can still take days or even weeks to bring applications back online.

Downtime Costs You Money



[Insert Image]

When it comes to critical business systems and customer-facing services, each hour of downtime costs money and jeopardizes your reputation. If you've experienced any kind of data loss and system downtime, you know how stressful it can be.

Our integrated disaster recovery as a service (DRaaS)

Call an Expert Before Disaster

There are issues, and there are trusted experts. When it comes to disaster recovery, they go to the dentist. With a broken business, you go to a mechanic. You get the idea.

Consulting an expert typically happens often it's too late. Why wait if it could be avoided? Talking about a business and its operations while it's still running, no matter what happens, costs, cloud storage, and backup files, etc. are all part of a disaster.

Most people think that the "what if" scenario is a disaster. Natural disasters only account for a small portion of the misconception. Most threats to a business are those we have no control over.

We could look at disasters in two ways. One way is to look at the things we can't control. The other way is to look at the things we can control.

The World of Threats

We can't control the weather, but we can control our response. Earthquakes don't cause power outages, but we can have backup generators, alternate power sources, and so on. We can't control the other variable, people. We can take protective and preventative measures.

Avoiding costly downtime

There are known considerations to prepare for if/when disaster strikes. Operations and IT systems must continue with minimal downtime. If systems need to be restored quickly, processes have to be prioritized, and infrastructure has to be up and running without missing a beat.

But what about the unexpected—the things we didn't see coming? New considerations. We're in a new world where remote work is the reality, with teams scattered outside the digital safety of an office. Suddenly, critical data and devices are outside of IT's regular infrastructure. Teams are on different devices. Prioritizing data, systems, and business applications are even more critical. Regulations and compliance still need to be addressed.

Solution Overview

< DR product >

Disaster Recovery as a Service

Enhance your ability to recover data from a disaster and keep your employees productive

Many organizations go beyond backup and implement a Disaster Recovery Program that enables their data, applications, and systems to be available almost instantly in the event of a disaster.

A cloud backup solution protects your company's data so you can always restore your critical business systems, which could take days or weeks to bring the applications back online. In the case of a severe outage like one caused by fire or human error, your systems will be made available rapidly with Disaster Recovery as a Service (DRaaS). When it comes to critical business systems and customer-facing services, each hour of downtime costs money and jeopardizes your reputation. A single unplanned downtime can cost an SMB an average of \$82,200 to \$256,000, according to the IDC.

DRaaS minimizes recovery time by quickly and securely spinning up the defined systems in a cloud data center. That means in case of a serious outage you can count on getting back to business quickly.

	Cloud Backup	Disaster Recovery
Key function	Protect data from loss	Recover applications quickly after a disaster
Application recovery time	Hours to days	Minutes
Storage type	Cold storage	Hot storage (enables rapid application availability after a disaster event)

Managed services:

Our "all-in-one" approach enables multi-layer protection for your entire environment with greater ease-of-use and a lower cost – as compared to purchasing and maintaining separate disaster recovery and backup solutions.

Enable disaster recovery in minutes

Adding disaster recovery capabilities to <cloud backup product> only takes a matter of minutes. The solutions utilize the same agent, replication, backup storage, and cloud infrastructure.

Add disaster recovery with no upfront costs

Charges for compute resources apply only in the event of a production failover or failover testing. If you already back up your machines with <cloud backup product> and store the backups in our cloud, the only additional, on-going cost is for hot disaster recovery storage.

Easier management

<DR product> and <cloud backup product> use the same backup agent. Daily and periodic operations are performed more quickly and easily. Meanwhile, if your team is already familiar with the <cloud backup product> interface, it requires virtually no training to use <DR product>.

Service Provider Logo

Weitere Ressourcen

Von Branchen-Analysten

- Gartner: [Acronis DRaaS erhält Customers' Choice-Auszeichnung von Gartner Peer Insights](#) und wird im „Voice of the Customer“-Bericht hervorgehoben
- Frost & Sullivan: [Auszeichnung für innovative Data Protection-Produkte in Nordamerika 2020](#)
- DCIG: [„Top 5 All-in-One DRaaS Solution Profile“](#) (Profile der Top 5 der umfassenden DRaaS-Lösungen)

Von Acronis

- Partnerportal: partners.acronis.com/de-de/profile/login.html
- Ressourcencenter: www.acronis.com/resource-center/
- Blog: www.acronis.com/blog
- Kostenlose Testversion von Acronis Cyber Cloud: www.acronis.com/business/backup/cloud/trial/#/registration
- Vereinbaren Sie eine individuelle Demo oder Beratung. Senden Sie eine E-Mail an sp@acronis.com





Wenden Sie sich an Ihren Account Manager, um zu erfahren, wie wir Sie dabei unterstützen können, schneller Disaster Recovery Services anzubieten.

Weitere Informationen unter www.acronis.com

Copyright © 2002-2021 Acronis International GmbH. Alle Rechte vorbehalten. Acronis und das Acronis Logo sind eingetragene Markenzeichen der Acronis International GmbH, in den Vereinigten Staaten und/oder in anderen Ländern. Alle anderen Marken oder eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber.

Technische Änderungen, Abweichungen bei den Abbildungen sowie Irrtümer sind vorbehalten. 2021-08