Business-Whitepaper

Die Breite und Tiefe der modernen Datensicherung verstehen

Warum man modernen Datenbedrohungen einen Schritt voraus sein muss, wenn man Datensicherheit und -sicherung vom Edge bis zur Cloud gewährleisten will

Kurzübersicht

Daten sind das wertvollste Kapital eines Unternehmens. Dennoch gelingt es vielen Unternehmen nicht, Daten die gebührende Sorgfalt zukommen zu lassen. Die Bedrohungslandschaft wird immer ernster. Daher werden Daten im Rahmen von Modernisierungs- und Transformationsbemühungen in ein Wirrwarr von isolierten Lösungen und neuartigen Hosting-Umgebungen gesteckt – und zwar vom Edge bis zur Cloud. Diese Komplexität hat zur Folge, dass die Daten anfälliger für Angriffe durch die raffinierten Hacker von heute werden.

Bestehende Ansätze für die Datensicherung reichen immer öfter nicht aus. Der Grundansatz bestand früher darin, die veränderten Daten aus jeder Produktionsumgebung zu kopieren und diese Kopie an einem sekundären Standort aufzubewahren. In der Regel geschah dies einmal am Tag außerhalb der Spitzenzeiten, oftmals spät nachts, um Beeinträchtigungen der Leistung der Infrastruktur zu vermeiden. Dieser periodische Ansatz lässt in der heutigen schnelllebigen Welt voller Cyber-Bedrohungen einiges zu wünschen übrig, und bei dem Versuch, die enorme – und immer weiter wachsende – Datenmenge zu schützen, wiederherzustellen und zu sichern, werden IT-Organisationen mit einer Reihe von Herausforderungen konfrontiert:

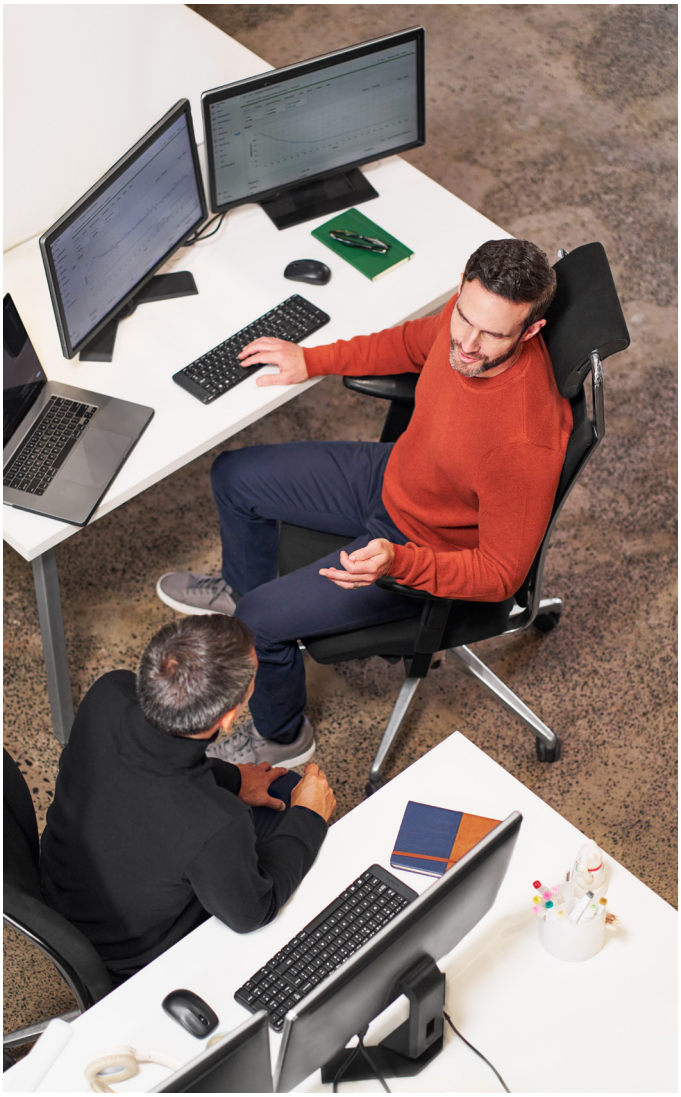
- Unfähigkeit zur schnellen Abwehr von Cyberangriffen wie Ransomware und Malware
- Komplexität im Management und im Betrieb mit mehreren Kontaktstellen für die Administration und der Wartung der Datensicherungssoftware und -hardware vor Ort oder in Hybrid-Cloud-Umgebungen
- Isolierte Datenbestände mit fragmentierten Einzellösungen
- Erhöhte Kosten, Überbereitstellung von Kapazität und unzureichende Ressourcenauslastung aufgrund von ineffektiver Planung für das Datenwachstum oder – im schlimmsten Fall – Unterbereitstellungen, die zu erhöhten Risiken führen
- Ein schnell wachsendes Datenvolumen, anspruchsvolle Service Level Agreements (SLAs) und eine sich ständig verändernde Bedrohungs- und Compliance-Landschaft, die immer höhere Kosten und größere Risiken mit sich bringen
- Datenverlust zwischen dem aktuellen Wiederherstellungspunkt und der letzten einwandfreien Datenkopie
- Lange und komplexe Wiederherstellungszeiten, die die Wiederaufnahme des Normalbetriebs behindern

Es wird eine umfassende und konsistente Datensicherung benötigt, mit der die Datenintegrität und -verfügbarkeit dauerhaft gewährleistet ist – unabhängig von Standort und Hosting-Plattform. Eine robuste Lösung, die rund um die Uhr in Betrieb ist und die Daten vollständig sichert und für eine sofortige Wiederherstellung bereitstellt, ist der Schlüssel, um die potenziellen Schäden durch Ransomware und sonstige böswillige Angriffe einzudämmen.

Einführung

Die gute Nachricht: Fortschrittliche Technologien machen eine konsistente und effektive Datensicherung möglich. Moderne Sicherungs- und Disaster-Recovery-Lösungen (DR) können isolierte Datenbestände, sogenannte Silos, aufbrechen und die Daten sowohl bei Inaktivität als auch bei ihrer Verschiebung von Standort zu Standort in ihrem gesamten Lebenszyklus schützen.

In diesem Whitepaper wird erörtert, wie wichtig eine sichere Datensicherungsstrategie mit einem umfassenden, einheitlichen und kontinuierlichen Ansatz ist, um Datenverluste oder -kompromittierungen durch unerwünschte Eindringlinge, insbesondere durch Ransomware oder durch von Malware veränderten Code, zu verhindern. Zunehmende Cyberkriminalität betrifft sämtliche Branchen, Versorgungsbetriebe und Behörden, daher dürften IT-Organisationen zu keinem Zeitpunkt unachtsam werden.



Datensicherung und Datensicherheit

In diesem Whitepaper wird wie folgt zwischen Datensicherung und Datensicherheit unterschieden:

— **Datensicherung:** ein umfassendes, ganzheitliches Programm von Kontrollen, Prozessen und Gegenmaßnahmen, das die Verfügbarkeit und Integrität von Daten gewährleistet, unabhängig davon, wo sie sich befinden.

— **Datensicherheit:** spezielle Prozesse und Protokolle, die Daten vor Bedrohungen, Angreifern oder sogar versehentlicher Löschung schützen – am Speicherort, bei Datenbewegungen und während der Datenverarbeitung.

Explosionsartiges Datenwachstum, erhöhtes Risiko

Die meisten IT-Organisationen werden mit mehr Daten als je zuvor überschwemmt, und dennoch wird von ihnen erwartet, dass sie diese Daten mit veralteter Technologie sichern. Die technologische Katastrophe ist damit praktisch vorprogrammiert. Eine aktuelle Umfrage von IDC, die von Zerto, einem Unternehmen von Hewlett Packard Enterprise, gesponsert wurde, ergab, dass 93 % der befragten Unternehmen von datenbedingten Geschäftsunterbrechungen betroffen waren und 68 % von ihnen mehr als vier Ereignisse erlitten, die zu einer Geschäftsunterbrechung führten.[1]

Angesichts der Häufigkeit von Cyberangriffen ist die Wahrscheinlichkeit einer Datenschutzverletzung sehr hoch geworden und stellt ein erhebliches Risiko für den Geschäftsbetrieb dar. In derselben Umfrage wurde festgestellt, dass die Befragten in den letzten 12 Monaten durchschnittlich 19,3 Cyberangriffe (jeglicher Art) und 2,3 Ransomware-Angriffe erlebt hatten. Von den Befragten, die einem Angriff zum Opfer gefallen waren, gaben 83 % an, dass mindestens ein Angriff zu einer Datenbeschädigung geführt hatte. Noch besorgniserregender sind die 60 %, bei denen es innerhalb desselben 12-monatigen Zeitraums zu einem nicht wiederherstellbaren Datenverlust gekommen war.

Daher ist es auch kein Wunder, dass die Stärkung der Datensicherheit und -sicherung für die IT-Organisationen von heute oberste Priorität hat. Isolierte Datenbestände, Datenwachstum, zunehmende Ransomware-/Malware-Bedrohungen und die Ausbreitung von Daten im Kern, in der Cloud und am Edge haben zu einer noch nie dagewesenen Komplexität und einem höheren Risiko von Datenverlusten für Unternehmen weltweit geführt.

Folgen von böswilligen Datenangriffen

Angesichts des „virtuellen Ausnahmezustands", der durch die zunehmenden Cyberangriffe entsteht, müssen Datenschutzverletzungen von vornherein vermieden und Datenschäden durch unbefugte Änderungen verhindert werden. Die Folgen böswilliger Angriffe auf Daten können sein:

— Schädigung des Rufs von Unternehmen
— Kurz- oder längerfristige Funktionsunfähigkeit oder sogar permanente Abschaltung
— Hohe Kosten für Behebungsmaßnahmen
— Strenge Strafen für die Einhaltung von Vorschriften (z. B. Datenschutzgesetze)
— Potenzieller Verlust von Wettbewerbsvorteilen auf dem Markt

[1] „State of Ransomware and Disaster Preparedness for 2022", IDC, Mai 2022

Eine umfassendere Strategie für größere Bedrohungen

Es liegt auf der Hand, dass jedes Unternehmen einen anderen Ansatz verfolgen muss, um das zunehmende Risiko von Datenverlusten effizient zu beseitigen, die Bedrohungen durch immer raffiniertere Ransomware einzudämmen und eine schnelle Datenwiederherstellung nach einem kleinen oder großen Vorfall zu erzielen. Dies verlangt nach einer breit angelegten und sicheren Datensicherungsstrategie, die sich auf das gesamte Unternehmen und darüber hinaus erstreckt und alle Außenstellen des Unternehmens (Zweigstellen), Außendienstmitarbeiter und Partnerunternehmen einbezieht, die im Rahmen gemeinsamer Projekte und der Zusammenarbeit Zugriff auf Daten erhalten.

Eine umfassendere Strategie beinhaltet auch geschützte Sicherungen in der Hybrid Cloud in Verbindung mit schnellen Wiederherstellungsprozessen, um das Risiko von Ausfallzeiten zu verringern und die Cyber-Resilienz angesichts der ständigen und sich weiterentwickelnden Ransomware-Bedrohungen zu verbessern.

Wie funktioniert Datensicherung?

Die Datensicherung umfasst die Datensicherheit, aber auch Sicherung, Wiederherstellung und Archivierung sowie DR und Business Continuity. Ebenso muss eine erfolgreiche Datensicherung kontinuierlich und ganzheitlich sein – einfach, stark und nahtlos. Daher sind Mehrpunktlösungen einfach unzureichend. Da sich Speicherort und Verwendung von Daten ständig ändern, muss die Datensicherung mit der Entwicklung Schritt halten, um das Risiko von Datenverlusten zu reduzieren, eine schnelle Datenwiederherstellung zu ermöglichen, zusammen mit der Automatisierung zu skalieren, um sich vor neuen Bedrohungen zu schützen, und die Datenmobilität über den gesamten Lebenszyklus der Daten abzudecken.

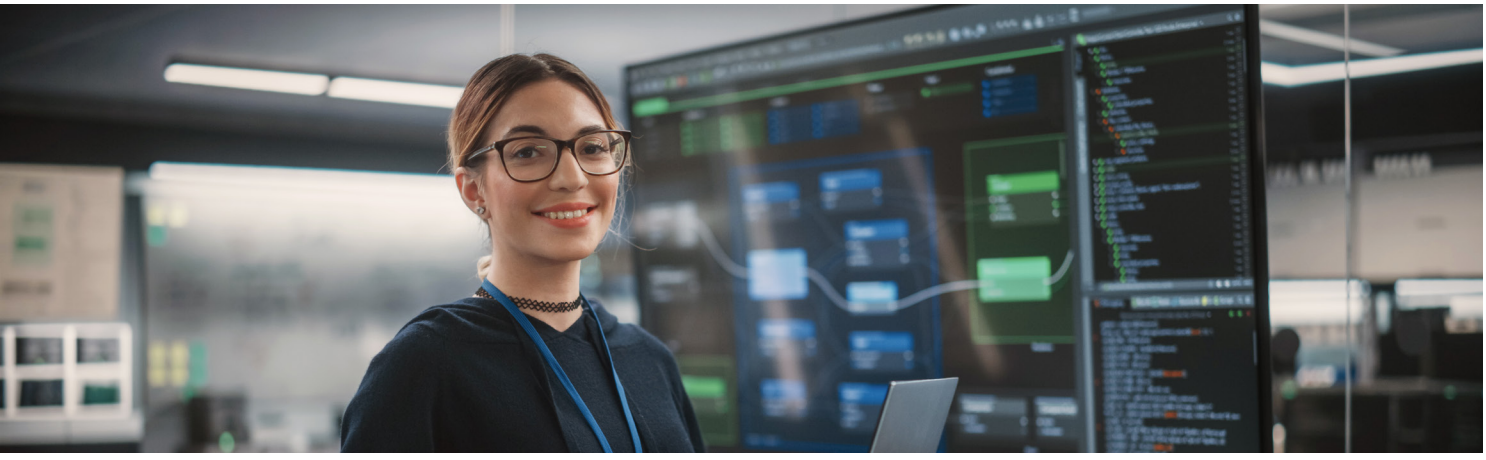
Datenschwachstellen – Schließen der Ransomware-Lücke

Da sich Unternehmensdaten heute an unzähligen Orten außerhalb der traditionellen Firewall befinden, sind sie ernsthaften Schwachstellen ausgesetzt, was zu einer immer größer werdenden Sicherheitslücke führt, die es zu schließen gilt. Beispiel:

- In einer Umfrage von 2022 wurde aufgedeckt, dass 94 % der Angreifer auf Sicherungs-Repositorys abzielen und dass 72 % der Angriffsversuche zumindest teilweise erfolgreich sind.[2]
- In derselben Umfrage sprachen 52 % der Befragten von einem Mangel an Interaktionspunkten zwischen den Cyber- und Business-Continuity-/Disaster-Recovery-Strategien ihrer Unternehmen und merkten an, dass Verbesserungen erforderlich waren.
- Im Jahr 2023 wurde berichtet, dass 43 % der Cyberangriffe auf kleine Unternehmen abzielten und 60 % der Betroffenen innerhalb von sechs Monaten das Geschäft aufgaben.[3]

Dieser Grad der Gefährdung öffnet zukünftigen Angriffen Tür und Tor und erschwert die Datenwiederherstellung.

Auch Zero-Day-Malware kommt immer häufiger vor, sodass Antivirensoftware nicht unbedingt vor diesen sich entwickelnden Bedrohungen schützt. Die Sicherung Ihrer Daten ist von entscheidender Bedeutung, aber der Schlüssel zu einer effektiven Wiederherstellung vor Ransomware liegt in der Granularität. Herkömmliche Backup-Methoden bieten diese Granularität nicht, wodurch die meisten Unternehmen mit unregelmäßigen Backups einem erhöhten Risiko ausgesetzt sind, wenn ihre Systeme infiziert werden. Es kann sogar passieren, dass Daten für mehrere Tage verloren gehen, was für das Unternehmen katastrophale Folgen und hohe Kosten bedeuten kann.



[2] „Paying the ransom is not a good recovery strategy", Help Net Security, Mai 2022

[3] „30 Surprising Small Business Cyber Security Statistics", Fundera, 2023

Eine ideale Lösung zur Vermeidung von Schäden durch Ransomware verwendet kontinuierliche Datensicherung (Continuous Data Protection, CDP) mit unterbrechungsfreier Replikation und granularem Journaling, um eine möglichst schnelle und effektive Wiederherstellung zu gewährleisten. CDP ermöglicht eine schnelle Wiederherstellung nach einem Angriff ohne übermäßige Datenverluste. Die Zahlung eines Lösegelds in der Hoffnung, dann alle Daten entschlüsseln zu können, ist hingegen kein Weg zu einer schnellen oder zuverlässigen Wiederherstellung. Zahlreiche Unternehmen entscheiden sich für die Zahlung des Lösegelds – mit gemischten Ergebnissen: Der Umfrage von 2022 zufolge war ein Drittel der zahlenden Unternehmen[4] dennoch nicht in der Lage, alle Daten wiederherzustellen.

Keine Branche ist vor Hackern und Bedrohungen der Cybersicherheit sicher. Daher ist es für alle Unternehmen wichtig, eine Bestandsaufnahme ihrer bestehenden Cybersicherheitsprogramme vorzunehmen, indem sie eine Datenrisikobewertung durchführen, um Lücken zu ermitteln, und dann Maßnahmen ergreifen, um diese Lücken zu schließen.

Trends und Herausforderungen der Cybersicherheit

Prognostiker sagen voraus, dass die Cyberkriminellen nicht nachlassen werden. Ganz im Gegenteil, sie erhöhen damit die organisatorischen Herausforderungen für die IT. Nach Angaben von Cybersecurity Ventures:[5]

- Ransomware wird die Weltwirtschaft bis 2031 jährlich 265 Milliarden Dollar kosten.
- Cyberkriminalität wird in den nächsten fünf Jahren jährlich um 15 % zunehmen.
- Cyberkriminalität wird bis 2025 10,5 Billionen US-Dollar erreichen.
- Bis Ende 2023 wird es voraussichtlich 3,5 Millionen unbesetzte Stellen im Bereich der Cybersicherheit geben.

Weitere Trends deuten auf Folgendes hin:

- Bis 2025 werden nur 55 % der Unternehmen eine Cloud-orientierte Datensicherungsstrategie implementiert haben.[6]
- 51 % haben mit dem Schutz komplexer und sich dynamisch verändernder Angriffsflächen zu kämpfen.[7]
- 50 % haben mit Komplexität und der Unfähigkeit zu kämpfen, Sicherheitslösungen zu integrieren, wodurch Lücken in der Verteidigung entstehen.[8]

Vorteile der modernen Datensicherung

Die Implementierung einer modernen Datensicherung bietet Unternehmen jeder Größenordnung viele unbestreitbare Vorteile – insbesondere angesichts der immer weiter zunehmenden Datenflut und Fragmentierung, die einen effektiven Schutz der Daten in der Cloud, im Kern und zunehmend auch am Edge erschweren.

Eine Modernisierung der Datensicherung kann dazu beitragen, isolierte Datenbestände aus der Vergangenheit aufzubrechen, um die sich immer weiter verschlimmernden Datenrisiken einzudämmen. Durch einen neuen, integrierten Ansatz können Daten vor Ransomware geschützt werden, indem Sicherungs-, Replikations- und Wiederherstellungsvorgänge vereinfacht und automatisiert werden, sodass eine schnelle Datenwiederherstellung ermöglicht wird. Wichtig ist, dass verschlüsselte Datenkopien Ihre gesicherten Daten für Cyberangriffe unzugänglich machen – sogar für Ransomware. Weitere Vorteile sind Langzeitdatenspeicherung, Datenmobilität, unveränderliche Sicherungen und regelmäßige Tests der Ausfallsicherheit.

Datensicherung as-a-Service

Im Zusammenhang mit den vorherrschenden, abonnementbasierten As-a-Service-Cloud-Umgebungen ist eine moderne Datensicherung in der gesamten Hybrid Cloud ein weiteres Angebot, das in Betracht gezogen werden sollte.

- Datensicherung as-a-Service (DPaaS) – Eine cloudbasierte oder webbasierte Software-as-a-Service, die Ihnen hilft, die Daten und Anwendungen Ihres Unternehmens zu schützen, indem sie Ihr Netzwerk sichert und Wiederherstellungsoptionen bietet.
- Disaster Recovery as-a-Service (DRaaS) – Verlagert die Computerverarbeitung Ihres Unternehmens in Ihre Cloud-Infrastruktur im Falle einer Katastrophe.
- SaaS-basierte Sicherung – Optimiert Sicherungsvorgänge mithilfe einer globalen Schutzrichtlinie für den konsistenten Schutz von On-Premises- und Cloud-nativen Workloads in der gesamten Hybrid Cloud.

Den Schutz Ihrer Unternehmensdaten den Fachexperten zu überlassen ist eine gute und kosteneffiziente Idee, um Ihr wertvollstes Kapital zu schützen: Ihre Daten.

[4] „Paying the ransom is not a good recovery strategy", Help Net Security, Mai 2022

[5] „2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics", Cybercrime Magazine, Mai 2023

[6] „State of Ransomware and Disaster Preparedness for 2022", IDC, Mai 2022

[7, 8] „The 2022 Study on Closing the IT Security Gap", Forschungsbericht des Ponemon Institute, gesponsert von HPE, Januar 2022

Die richtigen Services mit den richtigen Technologien und den richtigen Experten

Hewlett Packard Enterprise und Zerto bieten Datensicherungslösungen vom Edge bis zur Cloud, die Sie beim Risikomanagement unterstützen. Unsere Sicherheitsexperten wissen, dass die Frage nicht lautet, ob Sie angegriffen oder von Hackern infiltriert werden, sondern wann.

HPE und Zerto bieten neue Möglichkeiten, Innovationen agiler einzuführen, ihre Kosten zu handhaben, Daten zu schützen und ausgeklügelte Ransomware- und sonstige Cyberangriffe zu bewältigen. Die flexiblen Cloud-nativen Datenservices und Datensicherungslösungen der nächsten Generation umfassen:

— Ransomware-Ausfallsicherheit, Disaster Recovery und Multi-Cloud-Mobilitätsservices mit Zerto

— SaaS-basierte Wiederherstellung mit HPE GreenLake for Backup and Recovery

Zusammen bieten sie die nötige Flexibilität zur Modernisierung der Datensicherung. Die Innovationen reichen von der schnellen Wiederherstellung über den Schutz vor Ransomware und die Langzeitdatenspeicherung bis hin zur Unveränderbarkeit für On-Premises und die Public Cloud bei einfacher Bedienung. Sie tragen dazu bei, den Wandel von HPE zu einem Unternehmen für Cloud-Services weiter zu beschleunigen. Ziel ist es, Ihnen eine größere Auswahl und Freiheit für Ihre Geschäfts- und IT-Strategie zu bieten, mit einer offenen Plattform, die unabhängig vom Standort nahtlos das Beste der Cloud ermöglicht.

Dank der Möglichkeit, Daten und Workloads in die Cloud und aus der Cloud zu migrieren, werden Sicherung und Datenwiederherstellung für On-Premises-, Cloud-native und SaaS-Workloads möglich gemacht, sodass Sie Ihre Lösungen flexibel optimieren können.

HPE und Zerto sind bereit, Datensicherungsprobleme in den folgenden drei wichtigen Bereichen zu lösen:

1. **Umfassende und konsistente Datensicherung**

   Moderne Edge-to-Cloud-Datensicherung stellt durchgängige Verfügbarkeit über einfache, schnelle Wiederherstellung nach Störungen, umfassenden konsistenten Betrieb sowie nahtlose Anwendungs- und Datenmobilität über Clouds hinweg sicher.

2. **Effiziente Sicherung und Wiederherstellung**

   Optimieren Sie den Betrieb und mindern Sie Risiken mit einer zentralen Managementkonsole und einer globalen Schutzrichtlinie für konsistente Orchestrierungsfunktionen für alle Ihre lokalen virtuellen Maschinen oder Cloud-nativen Workloads wie beispielsweise Amazon EBS-Volumes, EKS-Cluster und EC2- oder RDS-Instanzen.

3. **Schutz vor Ransomware-Angriffen**

   Mit einer vollständig orchestrierten Failover- und Failback-Lösung zur Unterstützung der Wiederherstellung infizierter oder beschädigter Anwendungen und Daten helfen HPE und Zerto Unternehmen dabei, sich vor den Folgen von Ransomware zu schützen. Ausfallzeiten können auf Minuten und Datenverluste auf bloße Sekunden eingegrenzt werden.

Modernisierung der Datensicherung gemeinsam mit HPE und Zerto

Es ist Zeit, isolierte Datenbestände aufzubrechen und die Daten Ihres Unternehmens vor Ransomware zu schützen, die Wiederherstellung nach jeder Unterbrechung zu ermöglichen und VM-Workloads vor Ort, in der Hybrid Cloud und in Multi-Cloud-Umgebungen zu sichern. Unsere Experten helfen Ihnen dabei, Ihren Sicherungs- und Wiederherstellungsprozess mühelos mit der Einfachheit und Flexibilität der Cloud neu zu definieren und zu verwalten – und letztendlich eine moderne Datensicherung zu erzielen, um Cyber-Bedrohungen und Ransomware-Angriffen die Stirn zu bieten. Sie erhalten die richtige Mischung aus DR, Sicherungen und Archiven, die automatisch konfiguriert und verwaltet werden, um Ihre Unternehmensdaten und -anwendungen zu schützen.

Kein Unternehmen ist von der Bewältigung der täglichen Bedrohungen für Daten ausgenommen, und wie Untersuchungen gezeigt haben, wird dies auch in Zukunft so bleiben. Unternehmen können es sich nicht leisten, den Status quo beizubehalten, wenn es um die Datensicherung für eine wachsende Anzahl (Zehntausende) von Geräten und Standorten, einschließlich der Cloud, geht.

In einer hochgradig verteilten Betriebsumgebung muss ein umfassenderer Ansatz zum Schutz von Daten berücksichtigen, wo sie gespeichert sind, wo sie genutzt werden und wem sie gehören. Stärkere, besser integrierte Maßnahmen sind notwendig, um diesen technologischen Krieg zu gewinnen, der in immer größerem Ausmaß geführt wird. Ebenso brauchen Unternehmen die Flexibilität, um sich zu modernisieren und ihre digitale Transformation fortzusetzen, ohne dass ihnen Steine in den Weg gelegt werden oder Innovationen verhindert werden, die sie voranbringen.

Eine moderne Datensicherung – von Schutzmaßnahmen gegen Ransomware bis hin zur schnellen Datenwiederherstellung und Langzeitdatenspeicherung – wird entweder vor Ort oder in der Public Cloud benötigt. Sie muss einfach und effizient zu betreiben sein und jedes Service Level Agreement (SLA) kostengünstig erfüllen, damit Unternehmen sie ohne zu zögern übernehmen können.

Fazit

Es ist nie zu spät für eine robuste Datensicherungsstrategie, um weltweit verteilte Unternehmensdaten kontinuierlich zu schützen und im Falle einer Kompromittierung schnellstmöglich wiederherzustellen. Die richtige moderne Datensicherung kann sogar der Schlüssel zum Überleben eines Unternehmens im 21. Jahrhundert sein.

Weitere Informationen unter

Schützen Sie all Ihre Daten. Zu jeder Zeit. Zerto, ein Unternehmen von Hewlett Packard Enterprise

Schützen Sie Ihre Daten mühelos mit HPE GreenLake for Backup and Recovery

Visit HPE.com

Chat mit Vertrieb

a50009795DEE, Rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com