Lösungsübersicht

Warum HPE Zerto Software für Ransomware-Resilienz?

Einfachheit trifft auf Resilienz

Ransomware-Angriffe sind in den letzten Jahren immer häufiger geworden und richten sich gegen Unternehmen aller Größen und Branchen. Die Folgen von Ransomware-Angriffen können verheerend sein: Unternehmen verlieren den Zugriff auf wichtige Daten und Systeme und müssen mit finanziellen Verlusten und Rufschädigung rechnen. Um die ständig wachsende Bedrohung durch Ransomware zu bekämpfen, setzt HPE eine Kombination aus fortschrittlichen Technologien und Best Practices ein.

Kontinuierliche Datensicherung und journalbasierte Replikation

HPE Zerto Software bietet kontinuierliche Datensicherung (CDP) und eine einzigartige Journaling-Technologie, mit der Unternehmen Änderungen an virtualisierten Daten nahezu in Echtzeit kontinuierlich erfassen und speichern können, sodass nach Datenverlusten oder -beschädigungen eine nahezu sofortige Wiederherstellung möglich ist. Selbst wenn es Ransomware gelingt, Daten auf einem System zu verschlüsseln, kann das Journal die Daten schnell aus einem von Tausenden von Wiederherstellungs-Checkpoints wiederherstellen. Jeder dieser Checkpoints liegt nur 5 bis 15 Sekunden auseinander, was eine granulare Wiederherstellung ermöglicht, anstatt auf eine nächtliche Backup-Kopie zurückzugreifen, die Stunden hinter der Produktion zurückliegt.

Die journalbasierte Replikation ergänzt CDP, indem sie mehrere konsistente Kopien von Daten über verschiedene Datenspeichersysteme hinweg erstellt und so sicherstellt, dass selbst bei Verlust oder Beschädigung einer Datenkopie andere Kopien für die Wiederherstellung verwendet werden können. Diese Methode verhindert auch die Verbreitung von Ransomware, da mehrere Kopien von Daten mehrere Einstiegspunkte bieten, an denen Ransomware isoliert und entfernt werden kann. Darüber hinaus ermöglicht die journalbasierte One-to-Many-Replikation den Unternehmen, ihre Daten überall zu schützen und wiederherzustellen. Dadurch können Daten problemlos von einem Produktionsstandort an mehrere Zielorte kopiert werden, sei es vor Ort, in der Public Cloud oder an einem anderen Standort. Mit der journalbasierten Replikation können Unternehmen ihre Daten über die herkömmliche 3-2-1-Datensicherungsregel hinaus schützen.

HPE Zerto kann auch unveränderliche Kopien aus dem Journal auf Azure Blobs, Amazon S3 oder S3-kompatiblen Datenspeichern erstellen. Dadurch erhalten Sie eine Kopie Ihrer Daten, die nicht geändert oder modifiziert werden kann. Diese Kopie können Sie zur Wiederherstellung auf jeder verfügbaren HPE Zerto Infrastruktur wiederherstellen.

Granulare Wiederherstellung und nahtlose Integration

Ein großer Vorteil dieser Technologien ist die granulare Wiederherstellung. Unternehmen können bestimmte Dateien oder Ordner wiederherstellen, anstatt ein gesamtes System oder einen gesamten Datensatz wiederherzustellen. Diese gezielte und effiziente Wiederherstellung reduziert Ausfallzeiten und minimiert die Auswirkungen auf das Unternehmen.

Unternehmen profitieren außerdem von der nahtlosen Integration von HPE Zerto in andere Sicherheits- und Datamanagementsysteme. Die Verwendung von HPE Zerto APIs bietet eine einfache Möglichkeit zur Anbindung an bestehende Infrastruktur- und Technologieinvestitionen – einschließlich Sicherheitsereignis- und Incident Management sowie Endpunkt-Erkennung und -Reaktion –, um durch Automatisierung einen zusätzlichen Mehrwert zu erzielen. Dies kann die allgemeine Sicherheitslage eines Unternehmens verbessern und ihm helfen, schnell auf Sicherheitsaktionen zu reagieren und sich davon zu erholen.

Erkennung von Verschlüsselung in Echtzeit

Die HPE Zerto Software bietet Verschlüsselungsanalysen, um verdächtige Verschlüsselungsvorgänge auf geschützten Workloads sofort zu erkennen und zu melden. Das neue Inline-Verschlüsselungs- und Warnsystem liefert Ihnen frühzeitig Hinweise auf gefährliche Anomalien. Sie müssen nach der Sicherung nicht wie bei anderen Datensicherungslösungen auf die Erkennung von Ransomware warten. Sie können diese nun innerhalb von Sekunden nach dem ersten Auftreten erkennen.

Sie können Datenverluste auch minimieren, indem Sie es den Incident Response-Teams ermöglichen, bereits während eines Angriffs zu reagieren, anstatt erst Tage oder Wochen später. Mit dem API-First-Ansatz können Sicherheitsteams vorhandene Sicherheitslösungen integrieren und so einen wichtigen Mehrwert schaffen. Durch diese Integrationen können mehrere Erkennungsebenen hinzugefügt werden, um Angriffe zu verhindern und gleichzeitig die Auswirkungen des Angriffs schneller zu lokalisieren sowie saubere Wiederherstellungspunkte rasch zu identifizieren.

Isolieren und Sperren mit HPE Cyber Resilience Vault

Der HPE Cyber Resilience Vault sorgt für Wiederherstellbarkeit selbst nach den schlimmsten Angriffen. Die vollständig isolierte, air-gapped Wiederherstellungsumgebung speichert unveränderliche Kopien auf sicherer, leistungsstarker Hardware. Der HPE Cyber Resilience Vault nutzt eine Zero-Trust-Architektur sowie eine Kombination aus erstklassiger HPE Zerto Software und HPE Hardware, um einen hochsicheren Reinraum zu schaffen – für eine schnelle Wiederherstellung innerhalb von Minuten oder Stunden anstelle von Tagen oder Wochen.

Warum auf HPE Zerto umsteigen?

Alle oben genannten Funktionen von HPE Zerto sind für die Widerstandsfähigkeit gegenüber Ransomware von entscheidender Bedeutung. Hier sind die wichtigsten Gründe, warum Sie sich für HPE Zerto entscheiden sollten, um die Bedrohung durch Ransomware zu minimieren und zu beseitigen.

Stellen Sie alles wieder her, von Dateien bis hin zu Rechenzentren.
Mit HPE Zerto können Unternehmen nicht nur einzelne Dateien und Ordner wiederherstellen, sondern auch ganze VMs, Anwendungen und Rechenzentren.

Halten Sie mit dem Tempo der heutigen Umwelt der digitalen Unternehmen Schritt.
HPE Zerto bietet nahezu Echtzeit-Replikation und Datensicherung durch CDP. Dies ist in der heutigen schnelllebigen Geschäftswelt von entscheidender Bedeutung, in der selbst kleinste Ausfallzeiten kostspielig und störend sein können.

Nutzen Sie, was Sie bereits besitzen, anstatt es zu ersetzen.
HPE Zerto lässt sich über offene APIs nahtlos in die vorhandene IT-Infrastruktur integrieren. Unternehmen können HPE Zerto problemlos in ihre bestehenden Cybersicherheits-Workflows und -abläufe integrieren.

Profitieren Sie von einer auf Ihre Bedürfnisse zugeschnittenen Resilienzstrategie.
HPE Zerto bietet flexible Wiederherstellungsoptionen. Anstatt die Infrastruktur an die Anforderungen einer unflexiblen Lösung anzupassen, können Unternehmen HPE Zerto an ihre individuellen Anforderungen anpassen – unabhängig davon, ob Daten an denselben Standort, an einen anderen Standort oder auf eine cloudbasierte Plattform wiederhergestellt werden sollen.

Vereinfachen Sie Ihre Infrastruktur und Ihren Verwaltungsaufwand.
HPE Zerto ist einfach zu verwenden und bietet intuitive und benutzerfreundliche Funktionen. Selbst Unternehmen mit begrenzten IT-Kenntnissen können HPE Zerto für eine erfolgreiche Wiederherstellung nach Ransomware-Angriffen einsetzen – ohne zusätzliche Rechenzentren oder Personal.

Wählen Sie den Branchenbesten in Sachen Ransomware-Resilienz

HPE Zerto für Ransomware-Resilienz bietet umfassende Wiederherstellungsfunktionen, nutzt Echtzeit-Replikation und -Synchronisierung, lässt sich nahtlos in die bestehende IT-Infrastruktur integrieren, bietet flexible Wiederherstellungsoptionen und ist benutzerfreundlich. Mit HPE Zerto können Unternehmen ihre Daten vor Ransomware-Angriffen schützen und im Falle eines Angriffs ohne Zwischenfälle wiederherstellen.

Erfahren Sie mehr über die schnelle air-gapped Wiederherstellung durch den neuen HPE Cyber Resilience Vault.

Weitere Informationen unter

HPE.com/Zerto

HPE.com besuchen

Jetzt chatten

© Copyright 2026 Hewlett Packard Enterprise Development LP. Die Informationen in diesem Dokument können jederzeit ohne vorherige Ankündigung geändert werden. Neben der gesetzlichen Gewährleistung gilt für Produkte und Dienstleistungen von Hewlett Packard Enterprise ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Dienstleistungen explizit genannt wird. Die hier enthaltenen Informationen stellen keine zusätzliche Garantie dar. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument.

Azure ist in den USA und/oder anderen Ländern eine eingetragene Marke oder Marke der Microsoft Corporation. Alle genannten Marken von Dritten sind Eigentum der jeweiligen Rechteinhaber.

a00129801DEE, Rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com