

Wiederherstellung und Schutz vor Ransomware mit NetVault® Plus

Quest®

Unternehmen benötigen eine Sicherungslösung, die zusätzliche Widerstandskraft beim Kampf gegen die Auswirkungen von Ransomware bietet. Quest® NetVault Plus bietet genau das. NetVault Plus ist eine umfassende Datenschutzlösung für Unternehmen, die für modernste Rechenzentrumsanwendungen und deren Infrastruktur sowie für Cloud-Lösungen optimiert ist. Zudem bietet es umfassende Schutz- und Wiederherstellungsfunktionen im Fall von Ransomware-Angriffen.

Schutz von Unternehmensdaten

NetVault Plus ist eine Sicherungs- und Wiederherstellungslösung der Enterprise-Klasse, auf die Tausende Unternehmen weltweit zum Schutz ihrer Daten vertrauen. Mit diesem Tool ist es möglich, eine Vielzahl von Systemen, Anwendungen und Daten lokal und in der Cloud zu schützen, die Sicherung und Wiederherstellung zu beschleunigen und gleichzeitig die Kosten für den erforderlichen Speicher um mehr als 90 % zu senken. NetVault Plus bietet kontinuierlichen Datenschutz und sofortige Wiederherstellung. Auf diese Weise profitieren Sie von einem geringeren Risiko für Datenverluste und -beschädigungen, die zu betrieblichen Ausfallzeiten führen könnten.

Schutz für Ihre Sicherungsdaten

NetVault Plus umfasst eine softwarebasierte Speicherkomponente für Deduplizierung, Komprimierung, Verschlüsselung, Replikation und Cloud-Integration. Diese Speichertechnologie basiert auf einem unveröffentlichten Protokoll namens Rapid Data Access (RDA), das Ihre Sicherungsdaten schützt. Im Gegensatz zum SMB (Server Message Block), das für Windows-Freigaben verwendet wird, ist RDA kein offenes Protokoll. Es kann nicht direkt über ein Betriebssystem aufgerufen werden

und erfordert eine Authentifizierung, die außerhalb des lokalen Servers bzw. des domänengesteuerten Konstrukts erfolgt. Darüber hinaus bietet NetVault Plus Datenverschlüsselungsfunktionen, damit Sie sich sicher sein können, dass Ihre Daten jederzeit geschützt sind.

Bei Verwendung von NetVault Plus werden die Sicherungsdatenflüsse direkt von der Quelle zum Ziel geleitet. Es sind keine herkömmlichen Medienserver erforderlich. Dadurch wird einerseits die Komplexität und andererseits das Risiko für Datenverluste reduziert, da weniger Kernkomponenten angegriffen werden können.

Mit NetVault Plus stärken Sie den Ransomware-Schutz mit unveränderlichem Sekundärspeicher sowohl lokal als auch in der Cloud. Sicherungsaufgaben können als „unveränderlich“ markiert werden, sodass Sicherungsdaten während der Sicherungsaufbewahrungsfrist nicht überschrieben, geändert, gelöscht oder verschlüsselt werden können – auch nicht durch einen NetVault Administrator. Des Weiteren unterstützt es Objektsperren für Objektspeicher – ganz gleich, ob sich dieser lokal oder in der Cloud befindet.

Zusätzlich verwendet NetVault Plus quellseitige Deduplizierung, um die Datenmenge zu reduzieren, die über das Netzwerk vom Client-Rechner an den Speicher gesendet wird. Somit wird das von Datenerfassungstechnologien ausgehende Risiko weiter gemindert. Darüber hinaus wendet NetVault Plus eine Secure Connect-Technologie an, welche die Datenübertragung und Steuerbefehle in einem sicheren TLS 2.0-Layer verpackt. Dies ist ein wichtiger Schritt zur Beschränkung des Zugriffs auf Ihre Sicherungsdaten durch Ransomware.

NetVault Plus bietet Air-Gap-Sicherungen auf Band und in der Cloud. So profitieren Sie bei Ihrer 3-2-1-Sicherungsstrategie für die Notfallwiederherstellung von zusätzlichem Schutz und wasserdichter Sicherungsreplikation.

Schutz für Ihr Sicherungssystem

Natürlich hat das NetVault Plus System selbst ebenfalls Zugriff auf die Sicherungsdaten, also muss auch das berücksichtigt werden. Bisher waren von Ransomware-Angriffen überwiegend Windows-basierte Systeme betroffen – einerseits aufgrund der Beliebtheit des Systems, andererseits durch die Anzahl vorhandener Benutzer-Clients und Endpunkte, die Ransomware-Angreifer nutzen können. NetVault Plus mindert dieses Risiko durch die Installation unterstützender Systeme unter Linux. Auch wenn es damit nicht komplett unangreifbar ist, wird durch die Installation des NetVault Plus Systems unter Linux die Anzahl potenzieller Bedrohungen reduziert.

Auch die Systemzugriffserteilung sollte nicht außer Acht gelassen werden. NetVault Plus verfügt über zwei Hauptmethoden der Zugriffserteilung: Integration in einen Verzeichnisservice oder eigene rollenbasierte Zugriffsmechanismen. Angesichts des hohen Risikos, das mit den bereits erwähnten Angriffen auf Active Directory-Gruppenrichtlinien und Gruppenrichtlinienobjekte (Group Policy Object, GPO) einhergeht, sollten wir berücksichtigen, dass eine solche Sicherheitslücke den Zugriff auf die Sicherungsanwendung ermöglichen kann, wo es zu systematischen Datenlöschungen kommen könnte. Obwohl Sie Ihren Systemzugriff auch ganz einfach über Active Directory steuern können, bietet NetVault Plus ebenfalls zuverlässigen, rollenbasierten Zugriff – und das ganz ohne die Notwendigkeit, Active Directory zu nutzen. Auch wenn dies etwas weniger komfortabel für die Festlegung von Benutzern und Gruppen ist, wird dadurch eine stärkere Trennung von der Produktionsumgebung erreicht und damit auch potenzielle Zugriffe durch nicht autorisierte Dritte verhindert.

Fazit

Letztendlich können sich selbst die am besten vorbereiteten Unternehmen nicht vollständig gegen Ransomware-Angriffe schützen. Sie können jedoch die Risiken minimieren, indem Sie eine Sicherungslösung verwenden, mit der Sie nicht nur alle Ihre Daten schnell wiederherstellen können, sondern die außerdem die folgenden Vorteile bietet:

- Minimierung der Risiken der Auswirkungen von Ransomware auf Ihr Unternehmen
- Reduzierung der Anzahl angreifbarer Kernkomponenten
- Minderung des von Datenerfassungstechnologien ausgehenden Risikos
- Zugriffsbeschränkung auf Sicherungsdaten für Ransomware

Weitere Informationen zu NetVault Plus finden Sie unter: <https://www.quest.com/products/netvault/netvaultplus.aspx>

Über Quest

Quest stellt Softwarelösungen bereit, mit denen das volle Potenzial neuer Technologien in einer zunehmend komplexen IT-Landschaft ausgeschöpft werden kann. Von der Datenbank- und Systemverwaltung über die Migration zu und Verwaltung von Active Directory und Microsoft 365 bis hin zur Cyber Resilience: Quest hilft Kunden, bereits heute ihre IT-Herausforderungen von morgen zu bewältigen. Weltweit vertrauen mehr als 130.000 Unternehmen und 95 % der Fortune 500 Quest die proaktive Verwaltung und Überwachung der nächsten Unternehmensinitiative an. Quest soll außerdem die nächste Lösung für komplexe Microsoft-Herausforderungen finden, um für die nächste Bedrohung gewappnet zu sein. Quest Software. Where Next Meets Now. Weitere Informationen finden Sie auf www.quest.com.

© 2023 Quest Software Inc. ALLE RECHTE VORBEHALTEN.

Dieses Handbuch enthält urheberrechtlich geschützte Informationen. Die in diesem Handbuch beschriebene Software ist an eine Softwarelizenz oder eine Vertraulichkeitsvereinbarung gebunden. Diese Software darf nur gemäß den Bestimmungen der entsprechenden Vereinbarung genutzt oder kopiert werden. Dieses Handbuch darf ohne schriftliche Genehmigung von Quest Software Inc. – außer zur persönlichen Nutzung durch den Käufer – weder ganz noch in Teilen in irgendeiner Form oder Weise (elektronisch, mechanisch, zum Beispiel durch Fotokopiertechnik oder Aufzeichnung) reproduziert oder an Dritte weitergegeben werden.

Die Informationen in diesem Dokument beziehen sich auf Quest Software Produkte. Dieses Dokument sowie der Verkauf von Quest Software Produkten gewähren weder durch Rechtsverwirkung noch auf andere Weise ausdrückliche oder implizite Lizenzen auf geistige Eigentumsrechte. ES GELTEN AUSSCHLIESSLICH DIE IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT FESTGELEGTEN GESCHÄFTSBEDINGUNGEN. QUEST SOFTWARE ÜBERNIMMT KEINERLEI HAFTUNG UND LEHNT JEGLICHE AUSDRÜCKLICHE ODER IMPLIZIERTE ODER GESETZLICHE GEWÄHRLEISTUNG IN BEZUG AUF DIE PRODUKTE VON QUEST SOFTWARE

AB, INSBESONDERE DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER HANDELSÜBLICHEN QUALITÄT, DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DIE NICHTVERLETZUNG DER RECHTE DRITTER. QUEST SOFTWARE HAFTET IN KEINEM FALL FÜR DIREKTE ODER INDIREKTE SCHÄDEN, FOLGESCHÄDEN, SCHÄDEN AUS BUßGELDERN, KONKRETE SCHÄDEN ODER BEILÄUFIG ENTSTANDENE SCHÄDEN, DIE DURCH DIE NUTZUNG ODER DIE UNFÄHIGKEIT ZUR NUTZUNG DIESES DOKUMENTS ENTSTEHEN KÖNNEN (EINSCHLIEßLICH, JEDOCH NICHT BESCHRÄNKT AUF, ENTGANGENE GEWINNE, GESCHÄFTSUNTERBRECHUNGEN ODER DATENVERLUST), SELBST WENN QUEST SOFTWARE AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE. Quest Software gibt keinerlei Zusicherungen oder Gewährleistungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in diesem Dokument und behält sich das Recht vor, die Spezifikationen und Produktbeschreibungen jederzeit ohne Benachrichtigung zu ändern. Quest Software verpflichtet sich nicht dazu, die Informationen in diesem Dokument zu aktualisieren.

Patente

Wir von Quest Software sind stolz auf unsere fortschrittliche Technologie. Dieses Produkt ist möglicherweise durch Patente oder Patentanmeldungen geschützt. Aktuelle Informationen zu den für dieses Produkt geltenden Patenten finden Sie auf unserer Website unter www.quest.com/legal.

Marken

Quest, das Quest Logo und Quest Software sind Marken und eingetragene Marken von Quest Software Inc. Eine vollständige Auflistung der Marken von Quest finden Sie unter www.quest.com/legal/trademark-information.aspx. Alle anderen Marken sind Eigentum der jeweiligen Markeninhaber.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an: www.quest.com/de-de/company/contact-us.aspx