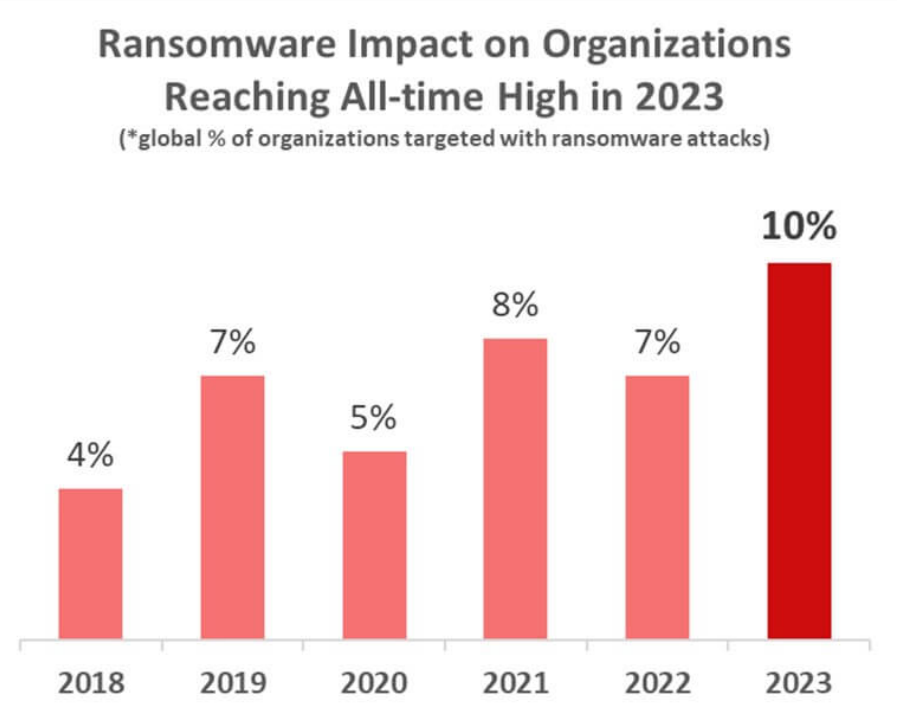
Ransomware Resilience with NetVault® Plus

Ransomware attacks continue to plague companies and non-profit organizations globally, causing irreparable harm and high cost. Add the negative impact to brand reputation and customer service, and you have a perfect storm.



Source: Checkpoint Research Blog January 2024[1]

According to Checkpoint Research, a staggering 1 in every 10 organizations worldwide were hit by attempted ransomware attacks in 2023, surging 33% from the previous year. Throughout 2023, organizations around the world have each experienced over 60,000 attacks on average - that's 1,158 attacks per organization per week.

Organizations need a backup solution that provides ransomware resilience in the face of this growing risk, to minimize data loss and business downtime. Quest® NetVault Plus does exactly this. NetVault Plus is a comprehensive data protection solution developed for most modern data center applications and infrastructure, as well as cloud solutions like Microsoft 365. It provides a wide range of ransomware protection, recovery and optimization capabilities.

1 Checkpoint

PROTECT

Preparing for ransomware attacks involves a multilayered approach, and a solid backup and recovery solution is your last line of defense to minimize business risk. Cyber-attackers target both your production data stores as well as your backups, so your backup solution needs to protect both!

To start, NetVault Plus provides enterprise-class backup and recovery that is used by thousands of organizations globally. It protects a wide range of systems, applications and data, both on-premises and in the cloud. NetVault Plus offers continuous data protection (CDP) that performs incremental forever backups of VMware virtual machines and Microsoft 365 data to help speed backup and reduce risk of data loss and damage.

NetVault Plus includes a software-defined storage component that provides deduplication, compression, encryption, replication and cloud connection. To protect backup data, this storage technology uses an unpublished protocol called Rapid Data Access (RDA). Unlike Server Message Block (SMB), used for Windows shares, RDA is not an open protocol. It is not accessible directly by an operating system and has an authentication requirement that sits outside the local server or domain-controlled constructs.

NetVault Plus also provides data encryption during transmission and at rest, to ensure data is well protected both on-premises and in the cloud. By encrypting your data, you can reduce risk of unauthorized use and disclosure of confidential information. To address government data security requirements, NetVault Plus crypto module is certified for FIPS 140-2 Level.

NetVault Plus strengthens your ransomware protection, as backup jobs can be assigned as “immutable” such that the backup data cannot be overwritten, changed, deleted or encrypted during the backup retention policy—even by a NetVault administrator.

When using NetVault Plus, backup data flows directly from source to destination. There is no need to have traditional media servers. This reduces complexity and helps to reduce risk by having fewer core components that could be attacked.

On top of that, NetVault Plus employs Secure Connect technology that wraps the data transfer and control commands in a TLS 2.0 secure layer. This is a great step to restrict access to your backup data from ransomware.

NetVault Plus also provides object locking and cloud locking to ensure backups that are stored in object storage on-prem and in the cloud are made immutable, to prevent unauthorized changes and deletion.

With NetVault Plus, you can quickly and safely replicate backup data to enable a 3-2-1 backup strategy for disaster recovery. And for extra protection, NetVault Plus also offers air-gap backup to tape.

Of course, the NetVault Plus system itself has access to backup data, so we also need to consider that. Ransomware has been known to predominately target Windows-based systems, partly due to popularity, but also due to the number of existing user client/user endpoints that ransomware perpetrators can take advantage of. NetVault Plus reduces that threat by supporting system installation on Linux. While not completely invulnerable, installing the NetVault Plus system on Linux reduces the number of potential threats.

Another consideration is how system access is granted. NetVault Plus has two main methods for granting access: Integration with a directory service or its own role-based access mechanism. Given the risk of Active Directory Group Policy and Group Policy Object (GPO) attacks, we must consider that this level of compromise could allow access to the backup application where systemic data deletion could be achieved. While you can leverage Active Directory to control system access, NetVault Plus also provides robust role-based access without the need to use Active Directory. While this might be less convenient for user and group control, it does offer another degree of separation from the production environment and potential access by an unauthorized

third party.

RECOVER

NetVault Plus makes recovery quick and easy. With powerful search and catalog tools, adminstrators can easily find what they need and immediately start recovery. When using NetVault Plus CDP for VMware, you get Instant Restore that allows you to instantly recover a virtual machine by mounting a VM snapshot image directly from the NetVault Plus deduplicated secondary storage repository. With NetVault Plus, you will reduce business downtime that affects all parts of the organization, including your reputation.

OPTIMIZE

NetVault Plus includes powerful automation to simplify data protection and increase IT staff productivity. It provides global source-side data deduplication and compression that accelerates backup and recovery while reducing storage requirements and costs by up to 93%. NetVault Plus' deduplication is far from ordinary. To start, it performs deduplication and compression across all your backup jobs for true global deduplication. It combines a variable-block deduplication chunking methodology with a content-aware algorithm that identifies patterns in the data, despite the shifting that results from additions or deletions in the data stream. In the end, you attain the best possible storage reduction available in the industry. This source-side deduplication also reduces the amount of data being sent over a network, from a client machine to storage, further reducing exposure to data capture techniques.

NetVault Plus' cloud tiering also helps optimize your backup data by keeping more recent backups on-prem and moving older backups to cloud. That way you can save money by using cloud storage versus on-prem storage. Cloud tiering will also help you recover your data faster as it will deliver the more recent backups from local disk while it's acquiring what it needs from the cloud.

KEY BENEFITS

In the end, even the most prepared organization can't completely protect itself against ransomware attacks. But you can limit the risks when you have a backup solution that not only allows you to restore all your data quickly and fully, but also:

- Mitigates the risks of ransomware impacting your business
- Reduces the number of core components that can be attacked
- Limits exposure to data capture techniques
- Restricts your backup data from ransomware

NetVault Plus provides ransomware resilience and delivers the protection, recovery and optimization capabilities demanding IT managers and executives seek in today's challenging high-risk environment.

For more information about NetVault Plus, visit www.quest.com/products/netvault-plus.

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
20 Enterprise, Suite 100
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.