Ransomware Protection and Recovery with NetVault® Plus

Organizations need a backup solution that provides additional strength in combatting the ransomware impact. Quest® NetVault Plus does exactly this. NetVault Plus is a comprehensive enterprise data protection solution optimized for most modern data center applications and infrastructure, as well as cloud solutions. It provides a wide range of ransomware protection and recovery capabilities.

Enterprise data protection

NetVault Plus is an enterprise-class backup and recovery solution used by thousands of organizations globally. It protects a wide range of systems, applications and data, on-premises and in the cloud. NetVault Plus accelerates backup and recovery while reducing storage requirements and costs by more than 90%. It provides continuous data protection and instant restore to minimize risk of data loss and damage that causes business downtime.

Protecting your backup data

NetVault Plus includes a software defined storage component that allows for deduplication, compression, encryption, replication and cloud integration. This storage technology relies on an unpublished protocol called Rapid Data Access (RDA) that protects backup data. 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 to ensure data is well protected.

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.

NetVault Plus strengthens your ransomware protection with immutable secondary storage, both on-premises and in the cloud. Backup jobs can be assigned as “immutable” such that backup data cannot be overwritten, changed, deleted or encrypted during the backup retention policy—even by a NetVault administrator. It also supports object locking when using object storage on-prem and in the cloud.

Additionally, NetVault Plus uses source-side deduplication to reduce the amount of data being sent over a network, from a client machine to storage. This further reduces exposure to data capture techniques. 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 offers air-gap backup to tape and cloud for extra protection and provides secure backup replication to enable a 3-2-1 backup strategy for disaster recovery.

Protecting your backup system

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 minimizes 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.

Conclusion

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

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.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks

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.