Quest

Ransomware prevention

Review your risk mitigation strategy. Protect your endpoints and your backup data from ransomware and related cyberattacks.

Ransomware has been around a long time. And as long as its perpetrators see the opportunity for financial gain, ransomware is surely here to stay.

The FBI's Internet Crime Complaint Center reported 2,084 ransomware complaints in the first half of 2021, a 62-percent year-over-year increase.[1] A Gartner report stated that "in the short term, ransomware can cost companies millions of dollars, and a potentially even greater loss over the long term, impacting reputation and reliability."[2]

Along with the monetary impact of a ransomware attack comes the impact of trying to recover all the compromised data. According to a Forrester survey, only 25 percent of respondents said they were able to recover 75 to 100 percent of their data in the wake of an attack. Far more respondents (39 percent) said they had managed to recover only 50 to 74 percent of their data.[3]

Could you run your business on 50 to 74 percent of the data you used to have?

Ransomware models are changing. So should your data protection strategy.

Facing the high threat levels and high costs associated with ransomware, IT and backup administrators are anxiously re-evaluating their data protection strategies.

Ransomware moves in different forms and guises. Spray-and-pray attacks like CryptoLocker, popular several years ago, cast a wide net to reach as many victims as possible.[4] Models have evolved to take aim at specific industries, such as utilities, universities and health care.[5] Some attacks look like ransomware but are actually intended to simply destroy data and infrastructure.[6]

Even the financial models are changing. The days of hackers asking for $300 worth of Bitcoin to decrypt data are gone. One recent survey revealed an average ransom of nearly $2 million.[7] Also reported was the $4.4 million payment authorized by the CEO of Colonial Pipeline following that company's ransomware attack.[8] Worse yet, perpetrators have adopted tactics such as threatening to publish ransomed data.

The role of endpoint security and backup

When every device connected to your business is a potential vector for attack, endpoint security becomes imperative. That means identifying and safeguarding all devices that access your network, regardless of where they are.

According to the Identity Theft Resource Center (ITRC), the 1,291 data breaches in the first nine months of 2021 amounted to 17 percent more than in all of 2020.[9] Data breaches always start at endpoints, so the risk to your organization from data breaches continues growing as you add devices.

Along with securing your endpoints, consider your backup strategy. Storing a copy of your data on tape, a separate device, or even in a separate location like the cloud helps ensure you can recover after an attack. Many IT organizations replicate their backups offsite for disaster recovery purposes.

The problem is that your backup systems still depend on servers. Those servers depend on potentially vulnerable components like an operating system and Active Directory, which mean that your backups are also vulnerable. Moreover, since network shares are a target for most ransomware, backup products that use shares to store data bring more risk.

To truly protect your organization from ransomware, protect the production data on your endpoints and the data in your backups.

Quest® solutions for protection from ransomware

Quest solutions can help prevent ransomware from attacking your endpoints and backups.

KACE® by Quest Unified Endpoint Manager

KACE Unified Endpoint Manager automates vulnerability scanning, patching and security updating for not only operating systems but also third-party applications and in-place upgrades. Its automated unified endpoint management (UEM) quickly identifies devices that are inadequately patched or that have known Common Vulnerabilities and Exposures (CVEs), then updates them.

From a single dashboard, KACE lets you discover, manage and secure all the endpoints that access your network, including:

- Windows desktops, laptops, servers and mobile devices
- Mac desktops and laptops
- Linux machines and servers
- Chromebooks
- iOS and Android mobile devices
- non-computer devices like printers
- Internet of Things (IoT) devices

Instead of researching, purchasing, learning and maintaining multiple point-solutions, get full UEM in the single KACE console. It centralizes your command of enrollment, wipe/lock, discovery, inventory, hardware/software asset management and scripting. Plus, it offers a built-in help desk for IT service tickets.

Manage your business instead of managing your systems. With KACE Unified Endpoint Manager, you'll have a full overview of your entire endpoint landscape in one place, so that you don't have to cobble together data from different products.

Quest NetVault® Plus

NetVault Plus offers powerful yet easy-to-use enterprise backup along with built-in protection from ransomware. It combines NetVault backup and recovery software with Quest QoreStor® software-defined secondary storage.

On premises and in the cloud, NetVault Plus strengthens your ransomware protection with data encryption for your backups. It provides immutable secondary storage so that backup data written to QoreStor cannot be overwritten, changed or deleted outside of the retention parameters you specify.

NetVault Plus further protects against ransomware attacks by retaining a copy of all deleted backup data in the QoreStor data recycle bin for an administrator-specified time period. For added security, its Secure Connect technology wraps data transfer and control commands in a TLS 2.0 layer to prevent attacks on your backup data.

For data storage, NetVault Plus supports Rapid Data Access (RDA) protocols, which, unlike the Server Message Block (SMB) protocol used for Windows shares, are not open. RDA is not directly accessible by the operating system and has an authentication requirement that sits outside of the local server or domain-controlled constructs.

Finally, NetVault Plus offers robust, role-based access without the need to integrate with services like Active Directory. That offers another degree of separation from the production environment and impedes access by an attacker.

It's time to protect your organization from ransomware

In the end, even the best-prepared organization can't completely protect itself against all ransomware attacks. But you can mitigate risk when you have a solution that not only protects your endpoints, but also allows you to restore all your data quickly and fully.

Quest solutions for ransomware prevention are designed to help you:

- Mitigate the risk of ransomware harming your business
- Reduce the number of core components that can be attacked
- Limit your exposure to data capture techniques
- Protect your backup data from ransomware

Learn more about KACE Unified Endpoint Manager and NetVault Plus.

[1] FBI Internet Crime Complaint Center, "Ransomware Awareness for Holidays and Weekends," September 2021. Complaints numbered 2,084 from January to July 31, 2021.
[2] Gartner, "6 Ways to Defend Against a Ransomware Attack," November 2020.
[3] Forrester Research, "Ransomware Recoverability Must Be a Critical Component of Your Business Continuity Plans," October 2019.
[4] KrebsonSecurity.com, "2014: The Year Extortion Went Mainstream," June 2014.
[5] CyberWire, "Ransomware: healthcare, utilities, and universities. REvil's old sites are stirring," September 2021.
[6] The Register, "Ukraine blames Belarus for PC-wiping 'ransomware' that has no recovery method and nukes target boxen," January 2022.
[7] Ransomware.org, "Ransomware Attacks Ramped Up In 2021," December 2021.
[8] CNN, "Colonial Pipeline CEO admits to authorizing $4.4 million ransomware payment," May 2021.
[9] ITRC, "Number of Data Breaches in 2021 Surpasses All of 2020," October 2021.

Quest, 4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com. If you are located outside North America, you can find local office information on our website.

Quest