

5 Ways NetBackup Helps You Defend Against Ransomware

Ransomware continues to make headlines, and for good reason. Businesses will fall victim to a ransomware attack every two seconds by 2031,¹ and half of all IT security professionals say they don't believe their organization is ready to repel a ransomware attack.²

A robust frontline defense is the first step in preventing ransomware attacks, but it's not enough. Every enterprise should develop a comprehensive, multi-layered resiliency framework—one that supports the protect, detect and recover components of an organization's overall cybersecurity strategy. As bad actors grow more sophisticated, companies are realizing it's no longer a matter of "if" ransomware strikes, but "when."

Veritas NetBackup™ can put your organization in a better position to maintain resiliency when that day comes. Here are five ways NetBackup helps you protect against, detect and recover from ransomware attacks.



1. It helps you harden hardware and software.

The complex interconnected nature of IT systems gives ransomware the potential to wreak havoc on all an organization's data through a single point of entry such as a phishing email to one employee.

To fortify against such vulnerabilities, NetBackup can help your organization reduce its IT attack surface through comprehensive hardware and software hardening. With strengthened identity and access management that includes granular role-based access control (RBAC), two-factor authentication and data encryption both in-transit and at-rest, NetBackup has the tools to fortify your environment against increasing threats.



2. It enables you to secure backups with immutable storage.

Backups can be a last line of defense against ransomware. If attackers encrypt your organization's backups, you'll have little recourse against paying a ransom. But when you can arm yourself with immutable storage, which writes data so it cannot be altered or deleted, you have options for how to respond.

Should ransomware penetrate your frontline defenses and across your organization's systems on-premises and in the cloud, NetBackup offers immutable image management and storage to protect your backups from encryption or erasure. As a result, your data becomes impermeable to ransomware's threats of destruction or encryption, so you can ensure a faster recovery.



3. It supports data protection with air-gapping.

Network-connected backups are vulnerable because any physically connected system can be targeted and penetrated. One way to protect data is by creating a physical space between stored data and the networked system—literally, an air gap. These offline backups offer one of the few failproof measures to prevent malicious data access and encryption.

NetBackup can support your air-gapping strategy. With its resiliency capabilities, you can deduplicate and replicate data to storage media that can be air-gapped without requiring a third party.



4. It automatically detects potential threats.

Today's cybercriminals target all aspects of an organization's data and infrastructure. Being aware and in control of your organization's data, infrastructure and user activity is critical to detecting vulnerabilities and threats.

With NetBackup, you'll have a holistic view of your environment and can use the power of artificial intelligence (AI) to detect anomalies and get alerts of suspicious activity whenever backups are made. Your IT team will have a better understanding of baseline behavior for data and infrastructure, including expected data activity and cross-system permissions. When anomalies are detected, the team can act immediately to isolate the affected backups, minimize the impact and ensure your data is always recoverable.



5. It empowers you to implement an automated, orchestrated recovery process.

Although many IT teams build hybrid, multi-cloud infrastructures to satisfy their organization's needs, that complexity can make data more vulnerable and recovery more difficult. Enterprises with hundreds or thousands of servers cannot manually recover data quickly, making automation necessary.

With NetBackup, you have comprehensive options for an automated, orchestrated recovery process that helps you maintain control in the face of a ransomware attack. NetBackup includes Instant Rollback capabilities for VMware, enabling organizations to instantly roll back virtual machines to any point in time. This feature lets you send only the unique blocks needed to roll back the production system, reducing recovery from hours or days down to mere minutes or seconds—and ensuring your business continuity remains unharmed.

Be Confident with Veritas NetBackup

Potentially devastating ransomware attacks are a harsh reality, but NetBackup ensures you'll be prepared when it strikes. As the #1 data backup and recovery solution worldwide, NetBackup provides business-critical resiliency at scale with a single platform that can support any workload, any cloud and any architecture.

With NetBackup, you'll have the tools to protect, detect and recover with a resiliency strategy that reinforces your data and infrastructure against malicious data-damaging threats—and confidently defend against ransomware.

Learn how Veritas NetBackup can help your organization maintain peak ransomware resiliency at www.veritas.com/protection/netbackup.

1. [Cybercrime Magazine](#), "Global Ransomware Damage Costs Predicted To Exceed \$265 Billion By 2031," June 3, 2021.

2. [PurpleSec](#), "10 Cybersecurity Trends You Can't Ignore In 2021," April 29, 2021.

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact
information visit:
veritas.com/company/contact