Ransomware:

6 Capabilities You Need for Rapid Recovery

Dave Russell,
Vice President,
Enterprise Strategy,
Veeam Software

Jeff Reichard,
Senior Director,
Enterprise Strategy,
Veeam Software

Chris Hoff,
Data Protection &
Ransomware Marketing
Manager, Veeam Software

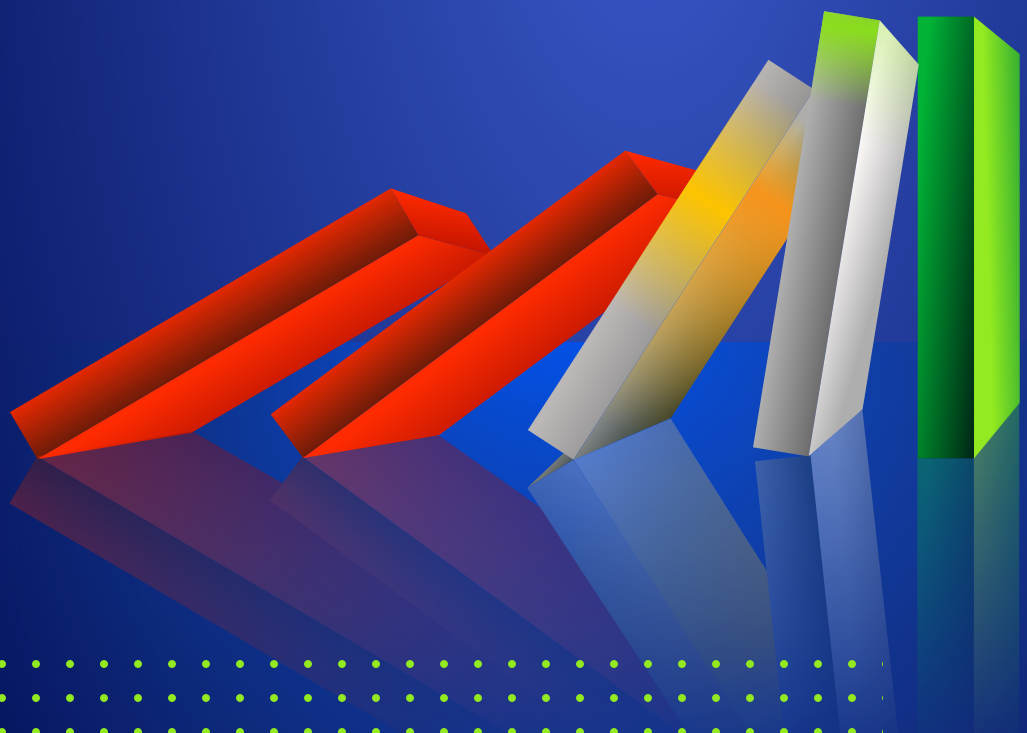


Table of Contents

Businesses can't prevent a cyber attack

The growth and evolution of ransomware is one of the most destructive trends of the last decade. This explosion has moved ransomware from an economic crime to one with immense global security implications. NATO, the US federal government and military, and the G7 have all recently acknowledged the severity of the ransomware threat and the need for large-scale coordinated response from government and industry.

Coordinated government and industry response takes time. In the meantime, organizations of all sizes need to protect themselves and their customers and constituents today. Fortunately, concrete steps using readily available tools and security frameworks can assist.

The sophistication and adaptability of ransomware and other cyber threats today require an agile, layered defense. Yet many organizations still maintain standalone security products that are focused on a single attack vector, which can easily be bypassed. Compounding the technology issues is a lack of security expertise on staff. One recent estimate puts the number of unfilled cybersecurity positions at over three million worldwide. The staffing issues go beyond technical skills to knowing how to apply policies that create consistency and provide a way to measure your organization's overall effectiveness.[i] These gaps in people, process and technology make attacking your data easier than ever for sophisticated cybercriminals.

Organizations can't prevent a cyber-attack, but they need to take the necessary steps to be prepared to effectively protect their data when an attack occurs.

Ransomware growth 2016-2021

Global cost: $325M to $20B USD

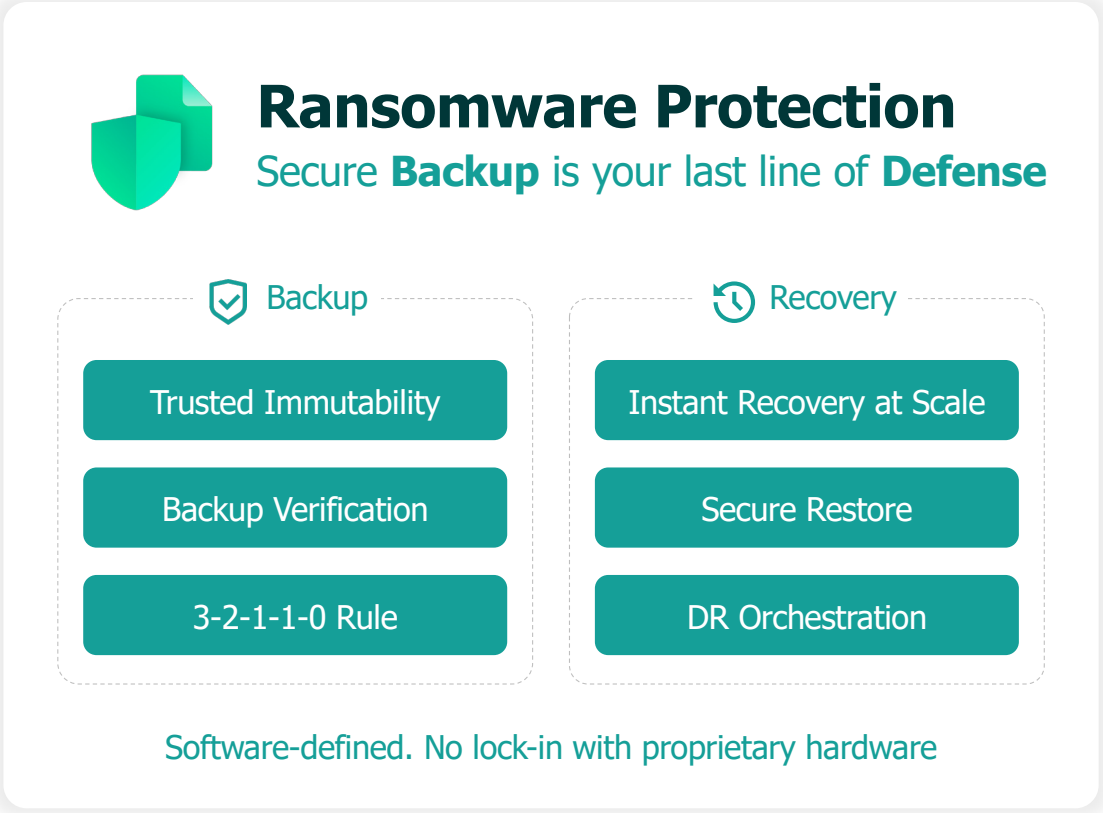
Frequency: Every 2 minutes to every 11 seconds

Innovation: Bitcoin, ransomware-as-a-service, double/triple extortion

Building a framework for resilient recovery

Effective security programs start with structure to understand what should be protected and the cost to the business if that asset were lost to determine how protection should be implemented. Many organizations start their security journey by trying to protect every asset in the same way and with the same level of importance, but as they grow best practices are applied that allow for risks to be categorized and responses to be better defined and measured. As frameworks are implemented, security teams and allowed to mature and understand the threats they face as well as the methodologies used by their attackers which allows teams to defend against attacks and recover quickly if an attack is successful. This organized approach can also help justify investments in cybersecurity by clearly illustrating the outcomes of those investments. And the process is iterative, allowing for a phased implementation and for learning from previous implementation cycles.

Without a structured way to manage cybersecurity risk, it would be easy to focus all your efforts into detection-based defenses such as firewalls and anti-virus while neglecting the processes and tools that are mandatory to effectively respond to, and recover from, a successful attack. Put another way, the best offense is a solid defense including having a robust strategy for backing up and protecting your data and workloads. Successful backups are the last line of defense for cyberattacks and can be the deciding factor to prevent considerable downtime, data loss and paying a costly ransom. To that end we've put together these best practices guide to provide real world advice on securing your data.



Veeam ransomware best practices and selected capabilities

Since 2019, every release of Veeam's® Modern Data Protection platform has delivered significant cyber resiliency and secure ransomware protection capabilities, helping organizations reliably recover from any cyberattack in minutes. Our software-first approach gives you the flexibility to maintain resilient, immutable storage on premises and in the cloud without being locked into proprietary hardware. These best practices allow you to have the appropriate safeguards to ensure the delivery of reliable backup and recovery for your critical infrastructure services and ensure your data will be there when you need it.

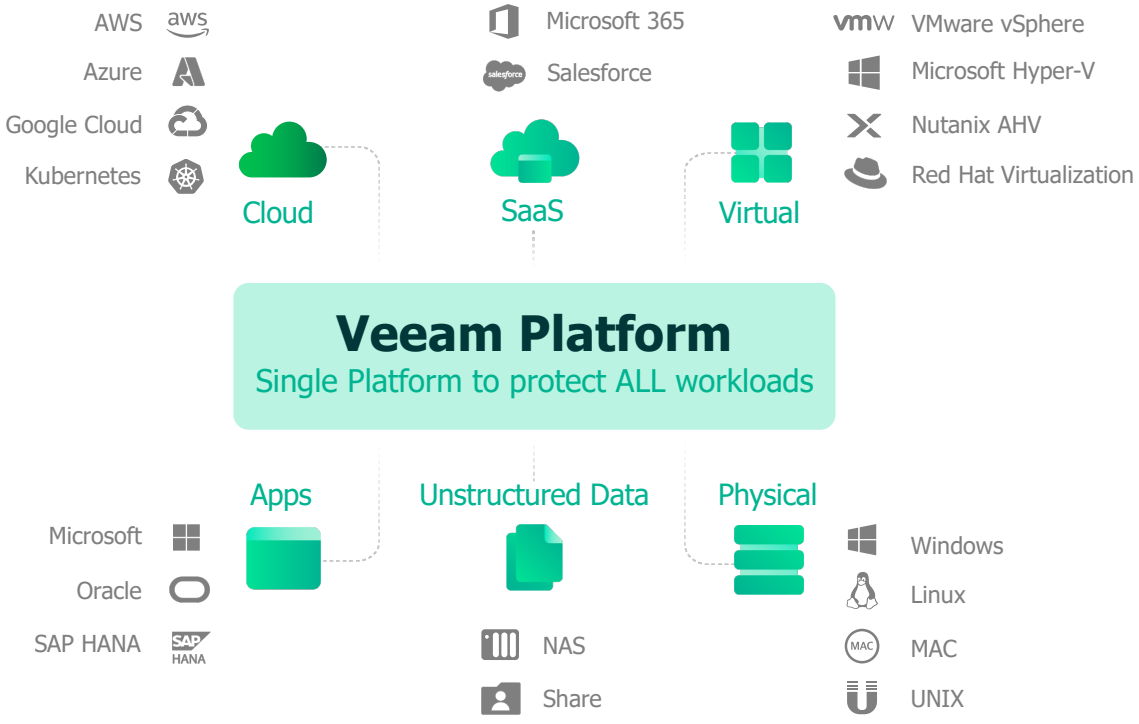
Secure Backup is your last line of Defense

The availability solution deployed should be capable of protecting the breadth of all mission critical workloads, be they physical, virtual or container based. Regardless of if workloads are deployed on premises, in the cloud with IaaS or as SaaS, mission critical data now resides in many locations, and needs to be portable to account for future requirements. The protection platform should have the ability to scale up or down, depending on requirements and workloads being protected. The backup solution should be capable of capturing data via a multitude of methods, including backup, replication, continuous data protection (CDP) and storage array integrations.

Veeam offers a horizontally scalable software defined storage (SDS) architecture. On the front end, Veeam can easily be extended to ingest more data as your backup volumes, or performance needs change. On the back end, our Scale-out Backup Repository™ (SoBR) is a software-defined construct that pools different types of storage devices for backup data. Through Veeam's policy engine, data can be placed on the most appropriate devices, including on-premises direct attached storage (DAS), deduplication appliances, network attached storage (NAS), object storage and the cloud; automatically managed over time or via a Service Provider.

The Veeam Platform delivers on all these capabilities, allowing for a solution that scales and extends as your business and its requirements evolve over time. Veeam's approach is modular and extensible, with no point solutions required, no dictated hardware dependencies and no worry of outgrowing the solution.

Veeam's software-defined ransomware remediation capabilities work with any infrastructure, today and in the future. Proprietary infrastructure should not be required, allowing the business to deploy on the hardware or cloud that it selects. Infrastructure flexibility not only allows an organization to determine what hardware their backup solution runs on, but also protects your backups from ransomware, no matter where vital data resides.



1. Trusted Immutability

Cyber criminals now routinely attempt to encrypt or delete an organization's backups as part of any ransomware attack. Success for the adversary is critical here, because without backups the victim must pay handsomely to recover their data.

Resilient backups are simply backups that cannot be destroyed by an adversary — even one who has acquired administrative credentials.

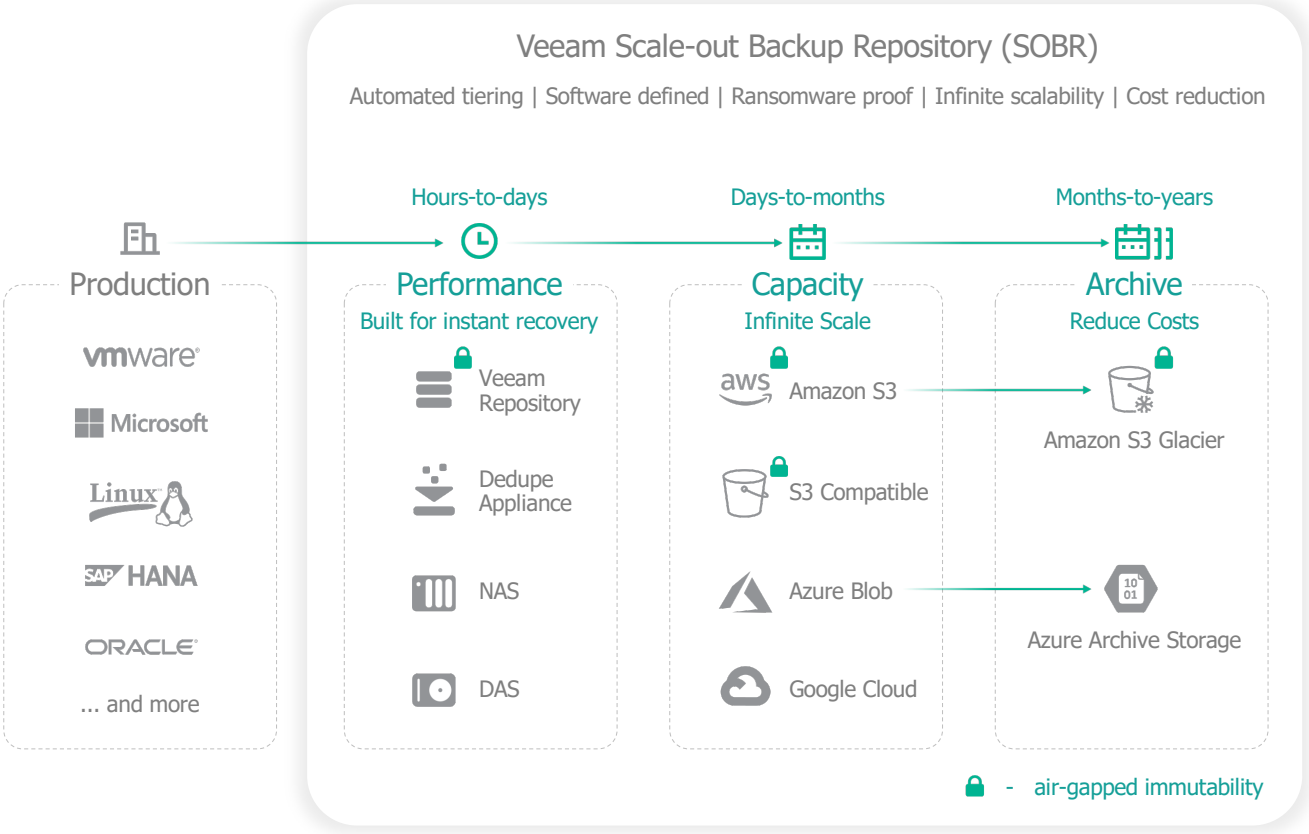
At the simplest level, robust resiliency can be achieved by backup to removable drives or to tapes which are then removed from the tape library. Having offline, air gapped backups is step one.

Veeam offers a bulletproof, policy-driven approach for data management across various resilient storage options. Enhancing overall resiliency, certified storage solutions[ii] from Veeam[iii] and via our broad partner ecosystem guarantee *immutability* (the inability to delete or change data for a prescribed time). **These options include our Veeam Hardened Repository, which delivers a robust immutable option for your on-premises backups.** If you prefer to keep your data in the cloud, Veeam provides immutability using AWS Amazon S3 and other approved S3-compatible object storage providers, using their object lock capability.

Backups written to resilient storage will be one of the most critical defenses for ensuring ransomware resiliency. Resilient backup storage would mean that you have one or more copies of your backup data on any combination of the following media:

- Backups on tape (and removed from the library or marked as WORM)
- Immutable backups in S3 or S3-compatible object storage
- Air-gapped and offline media (i.e., removable drives, rotating drives)
- Backups in Veeam Cloud Connect with Insider Protection (a services-lead capability)
- Immutable backups in a hardened repository

The Veeam Platform includes a complete set of ransomware remediation capabilities in its core product that are easily customer-deployable, and flexible enough to work with any infrastructure, on-premises or in the cloud.



Policy-driven Backup Data Lifecycle Management

Some Veeam customers seek to implement immutability via a double or triple immutability approach. This can include leveraging the Veeam Hardened Repository for on-premises, first level backups, then leveraging the immutability capabiltiy in the automatically managed Veeam Capacity Tier with S3 Object Lock for cloud or on-premises object storage, and/or automatically writing backups to WORM (write one, read many) physical tape media; noting that Veeam natively supports physical tape without the need for third party integrations.

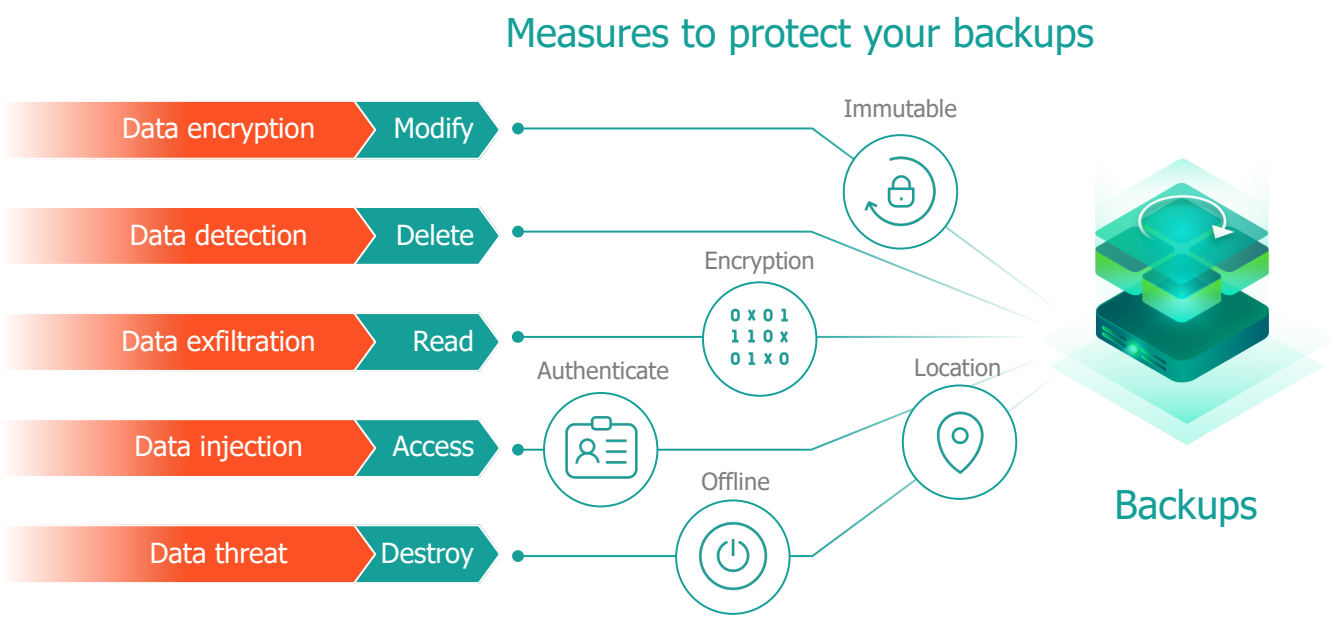
While immutability, whether implemented as a single, double or triple immutable approach is very helpful in remediating cyberthreats, it is only the beginning of a comprehensive ransomware protection practice.

Encryption end-to-end is needed to fend of data exfiltration. Today, one of the fastest rising cyberthreats is data leakage and data exlfiltration, whereby a ransom must be paid in order to avoid sensitive data from being shared on the dark web.

Proper authentication, and 'digital hygiene' regarding least privilige access, are needed to remediate against data injection. Data also needs to be protected against being altered such that records and entries that appear valid have not been maliciously changed to be invalid.

Other digital hygiene best practices include:

- Unique passwords for every login source. This way you can ensure that if one password or machine gets breached, the stolen password won't give hackers access to other accounts.
- A password manager. A robust password manager can help manage all of your login information, making it easier to create and use strong, unique passwords.
- Multi Factor Authentication (MFA). You can configure multi-factor authentication for additional security of your accounts, which will require continual secondary validation at every login.
- Remove unused devices, applications and non-essential programs and utilities from all servers.
- Patch management — make sure all software, hardware and firmware in use are running up-to-date software levels that have shored up any known vulnerabilties.



2. Backup Verification

A robust, comprehensive cyber defense strategy always starts with valid backups. Reliable, verified and tested backups are the first step to any successful recovery success. Busy IT teams need a way to automatically verify the integrity of backup data as backups are taken. If there is any issue, another backup can be taken while production data is still available, thus ensuring that there are no issues in data availability that are discovered after the production data is no longer available, has been compromised or is deemed to be untrustworthy and lacking integrity.

Veeam SureBackup® pioneered automated backup verification, and it's a key capability in our ransomware resiliency best practices. SureBackup automatically brings up servers and applications in a network-isolated environment and executes health checks that include many built in application verification means, such as executing specific Active Directory or SQL commands to verify application integrity. This automated testing capability can be extended and customized to fit your requirements and can be scheduled to execute when you feel it is most appropriate, sending a status report to your mailbox once the testing has concluded.

3. 3-2-1-1-0 Rule

Veeam recommends following the 3-2-1-1-0 backup rule, which is our enhancement to the well-known industry 3-2-1 rule.

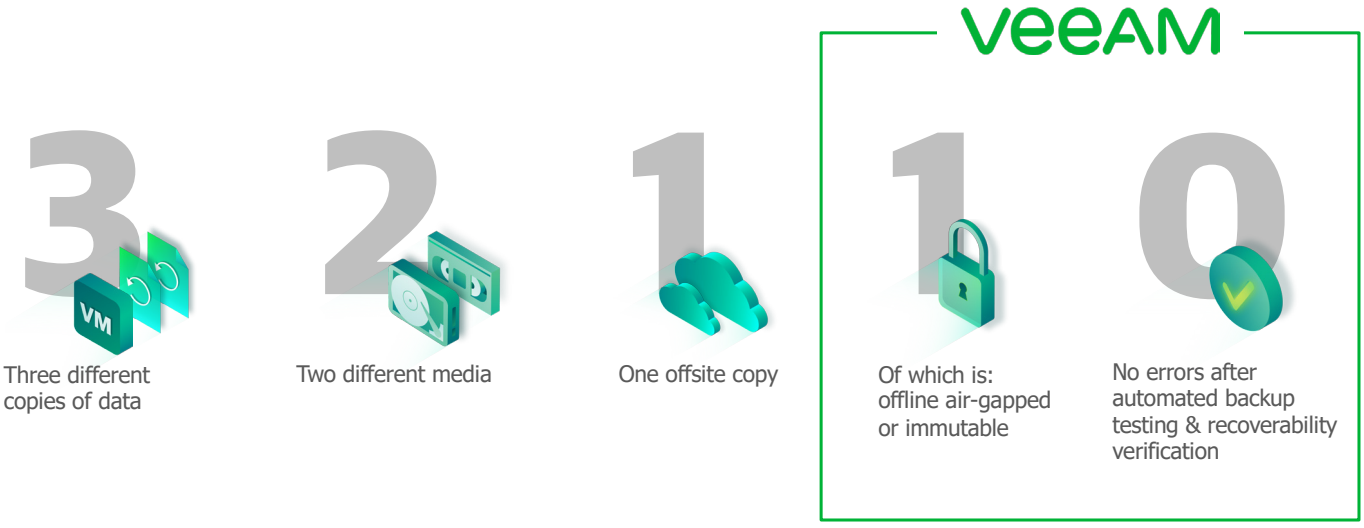
For many years, Veeam has advocated for the 3-2-1 Rule as a general data management strategy. The 3-2-1 Rule recommends that there should be at least three copies of important data, on at least two different types of media, with at least one of these copies being off site. The 3-2-1 Rule does not dictate or require any specific hardware and is versatile enough to address nearly any failure scenario.

As the threat of ransomware has advanced, Veeam has emphasized that at least the "one" copy of data be resilient (i.e., air-gapped, offline or immutable).

This recommendation is imperative for becoming resilient against ransomware.

The modern application to the 3-2-1-1-0 rule addresses the need for the resilient copy requirement and is one of the most important concepts that an organization can implement to be better prepared to fend off and remediate against cyberthreats.

Offline copies of data are needed to combat insider threats, including destruction of data. Insider threats are a rising concern, with some analyst firms stating that the majority of cyber threats over the next three years could come from employees of the business.



4. Instant Recovery at Scale

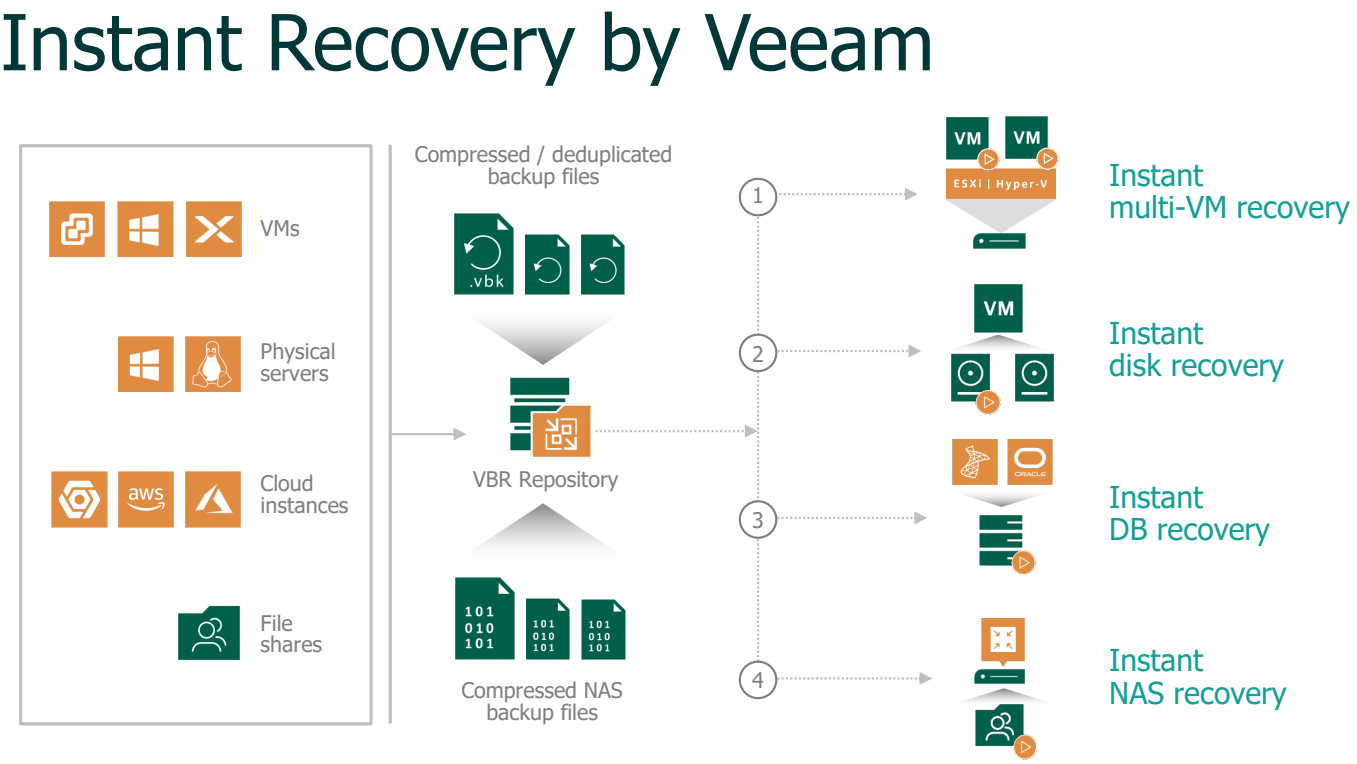
Before ransomware, organizations typically only restored 3-5% of their backed-up data over a one-year time frame. But in a ransomware attack, 100% of your production data may be encrypted or contaminated with malware, and you need to get it all back, fast. Fast access to data is critical, with the goal being more of a resume than a restore for all vital operations.

Veeam pioneered instant recovery of data in 2010 and has refined and extended this capability ever since. Today Veeam is optimized to quickly restore multiple machines simultaneously to handle even the largest enterprise recovery needs.

Veeam delivers instant recovery of data:

- Without requiring costly, proprietary appliances or solid-state drives
- Without being limited to only the most recent backup data
- Providing the ability to recover physical and virtual files and workloads to a virtualized environment (such as VMware vSphere, Microsoft Hyper-V, and Nutanix AHV), even migrating from one hypervisor to another automictically, with just two mouse clicks
- Providing the ability to recover physical and virtual files and servers to a cloud environment (such as AWS, Azure and Google Cloud Platform), with just two mouse clicks
- Providing the ability to instantly recover key enterprise applications, such as Oracle and SQL Server databases for immediate use
- Providing the ability to rollback entire Network Attached Storage (NAS) and file shares to a known good, pre-infected state so that your business gets back to normal operations quickly

Instant recovery of data, that can leverage a portable data format to deliver cross platform access to data ensure fast recovery, when and where you need it. From AHV, Hyper-V, or vSphere to physical Windows or Linux, to Azure, AWS or GCP, the Veeam Platform has you covered.



5. Secure data recovery

Ransomware dwell times (the time an adversary is on a victim's network before activating an attack) can be many months. Because of this, you need automation to ensure that you never restore malware back into your cleansed or new environment.

One of the versatile aspects of a SureBackup job (described above in item #2) is the ability to leave the job running so that additional verification and forensics can be performed on the system from the backup restore point. This can include doing a manual inspection to see if the ransomware threat is still in place, investigating specific files.

Building upon the Instant Recovery capability mentioned earlier, Veeam integrates with leading anti-malware solutions to deliver an automated recovery process to check and clean infected backup data, ensuring that backup data recovered into production is free of cyberthreats, eliminating re-infections.

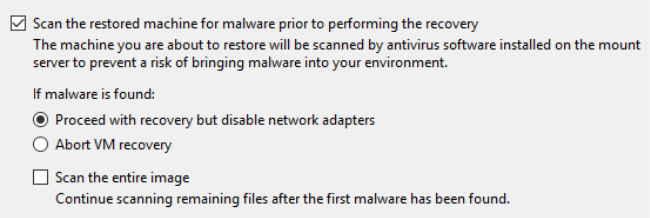
Veeam Secure Restore provides users an optional, fully integrated anti-virus scan step as part of any chosen recovery process. This feature addresses the problems associated with managing malicious malware by providing the ability to assure any of your copy data that you want or need to recover into production is in a good state and malware free. **Secure Restore was another industry first, patent-pending method of remediating an attack arising from malware hidden in your backup data.** Secure Restore provides additional confidence that a threat has been properly neutralized and no longer exists within your environment.

Secure Restore is fully configurable through PowerShell, which means that if you automate recovery processes via a third-party integration or portal, that you are also able to take advantage of this capability to ensure that threats are not reintroduced into your production environment.

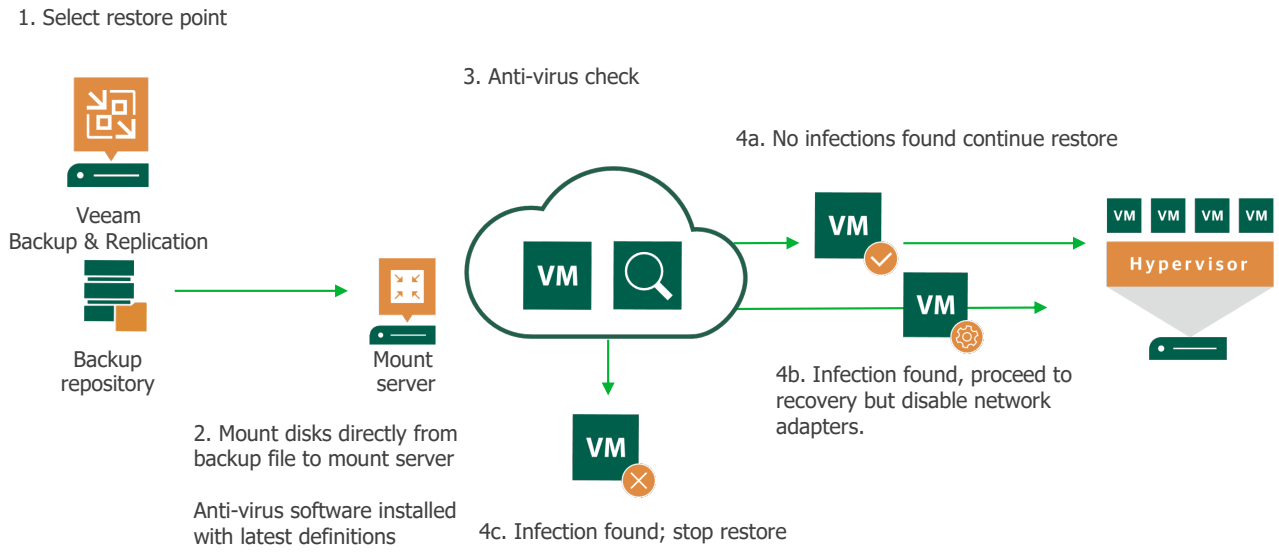
This powerful capability is useful for:

- Detecting "sleeping" ransomware in backup data and invoking anti-virus remediation to disinfect data before it lands back into the production environment
- Verifying backups from locations with less IT control, such as remote and branch offices (ROBO), prior to restoring them into the primary data
- Scanning backup data with additional anti-virus solutions to better detect rare or zero-day malware

As with all Veeam Platform capabilities, implementing Secure Restore is fast and easy to configure with only a couple of mouse clicks:



Veeam DataLabs: Secure Restore



6. DR Orchestration

Make no mistake, cyberattacks are disasters. In an emergency, your team needs automated, repeatable results. Your tool set must allow regular tests and audits of how quickly you could recover from a disaster, including automated testing of server and application accessibility and usability post-restore. And the testing process and results should be self-documenting to satisfy management and external security auditors.

Veeam's industry leading **Veeam Disaster Recover Orchestrator** (VDRO) **lets you fully automate and document complex workflows, including non-disruptive, large-scale recovery testing with dynamic documentation.** Incident response/recovery documentation can also be updated with non-Veeam information, such as contact lists and other mission-critical response information.

Reliable recovery

- Reliable, scalable orchestration
- Application-centric

Automated testing

- Non-disruptive
- Scheduled and on-demand
- Readiness checks

Dynamic documentation

- Audit trails
- Compliance reporting
- Built-in change tracking
- Proactive remediation

Most organizations have many types of Business Continuity (BC) and Disaster Recovery (DR) plans. Here are a few examples:

- Application-level failure
- Site-level failure
- Infrastructure component failure
- Mission-critical applications
- Dev/test applications

Much like automated backup verification, such as Veeam's SureBackup, is important in daily backup operations, so too is regular testing of your overall cyber resiliency recovery plan. After creating a recovery plan, the most important thing you can do is test it. You need to know if the plan you put together works. There is a tendency to not fully test disaster recovery plans, or not test them at all. At best, most organizations partially test their DR plans once or twice a year.

Continuous testing is important, especially since applications are constantly changing. To respond to changes and configuration drift, recovery plans must be updated any time a change is made to an application, such as adding more servers for additional capacity, or removing older servers. When testing, be sure to pay special attention to what did not go as desired. This is the only way your disaster recovery plan will improve. The true purpose of a test is to find out if your plan works or not.

Cyber resiliency, and ransomware remediation need to be part of your overall disaster recovery plan. One of the clearest ways you can prepare for cyber security incidents is to draw up an incident response plan. Creating a clearly defined incident response plan will enable you to outline procedures for detecting, communicating, controlling and remediating security incidents so that employees know how to respond to cyber security events in case they happen.

Further, this plan needs to be capable of being automatically tested, dynamically updating critical documentation, and allow for integration with other necessary tools and workflows that will ensure resumption of critical business operations.

1-click site recovery and DR testing

Veeam Disaster Recovery Orchestrator

Conclusion

A company's data is its most valuable asset; however, ransomware is a rising threat for organizations of all sizes, industries and geographic locations that puts critical data at risk. It is imperative that companies continue to improve their security programs to ensure that data is properly and securely protected, and that robust capabilities are at every organization's disposal to recover from an incident quickly and safely. Building a comprehensive security program requires the merging of people, processes and technology in ways that focus on continuous improvement while providing the best defenses possible. No matter the methodology companies choose the framework needs to define measurable outcomes that allows IT teams to defend against attacks and recover quickly if an attack is successful.

The response to threats like ransomware requires the implementation of a comprehensive remediation strategy. Veeam's broad set of ransomware remediation capabilities provide the most complete set of capabilities on the market and the most expertise in ensuring data is available during a crisis. We do this by taking a software first approach which gives you the flexibility to maintain resilient, immutable storage on premises and in the cloud without being locked into proprietary hardware. By following best practices, and deploying Veeam's modern data protection platform, Veeam can help your organization achieve digital resiliency which will minimize downtime after a ransomware attack using fully automated processes to provide ransomware free restore and DR orchestration no matter where your data resides.

No matter if your data resides on premises or in the cloud, having a complete set of ransomware remediation capabilities is key. Bringing these best practices into your security program simplifies the response to cyber-attacks and avoids data loss or paying a costly ransom.

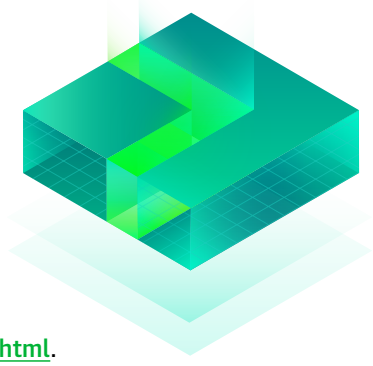
About Veeam Software

Veeam® is the leader in backup, recovery and data management solutions that deliver Modern Data Protection. We provide a single platform for cloud, virtual, SaaS, Kubernetes and physical environments. Our customers are confident their apps and data are protected and always available with the most simple, flexible, reliable and powerful platform in the industry. Veeam protects over 400,000 customers worldwide, including more than 82% of the Fortune 500 and over 60% of the Global 2,000. Veeam's global ecosystem includes 35,000+ technology partners, resellers and service providers, and alliance partners and has offices in more than 30 countries. To learn more, visit www.veeam.com or follow Veeam on LinkedIn @veeamsoftware and Twitter @veeam.

Veeam Products for Your Ransomware Remediation Practice

Veeam products for your ransomware remediation practice

- Veeam Backup & Replication
- Veeam ONE
- Veeam Disaster Recovery Orchestrator
- Veeam Backup *for AWS*, *Azure*, and *Google Cloud Platform*
- Veeam Backup *for Microsoft Office 365*
- Kasten K10 by Veeam



More information regarding Veeam's ransomware capabilities can be found at this dedicated web site: https://www.veeam.com/ransomware-protection.html.

A detailed, long form technical white paper of ransomware best practices and in-depth coverage of Veeam's cybersecurity capabilities is available at: https://www.veeam.com/wp-protection-yourself-from-ransomware.html?wpty.

About the Authors

Dave Russell is a 32-year veteran in the storage industry, serving as Veeam's Vice President of Enterprise Strategy, responsible for driving strategic product and go-to-market programs, spearheading industry engagement and evangelizing Veeam's vision for Modern Data Protection. Prior to Veeam, he held the role of Vice President and Distinguished Analyst at Gartner for 13 years and spent 15 years at IBM in product development for mainframe & open systems backup/recovery.

Jeff Reichard is Senior Director of Enterprise Strategy at Veeam, where he focuses on risk, compliance, and partnerships. Jeff has 25 years of experience in data protection/availability, business continuity, and regulatory compliance solutions. His previous roles have ranged from designing SAN and data backup solutions to systems engineering and engineering leadership serving public sector and enterprise customers. Prior to Veeam, Jeff most recently led Commvault's federal civilian SE team. At Veeam, Jeff works with partners, customers and industry analysts to evangelize Veeam's vision for cloud data management and digital transformation.

Chris' career has been deeply rooted in cyber security with over 15 years of diverse technical experience. He is currently driving the Security and Data Protection Marketing effort at Veeam. Before joining the team, Chris has held various engineering, sales, and product management roles. During his career, he's helped numerous organizations manage cyber risks by designing solutions that align with industry frameworks, programs, and compliance mandates.

i https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-1/

ii Technical certifications for immutable storage came in response to the world of financial industry regulation. Numerous government rules are designed to ensure that regulated organizations retain unaltered copies of financial records for a prescribed time (for example in the US, see SEC Rule 17a-4(f), FINRA Rule 4511 and CFTC Rule 1.31 (c)-(d)). Fortunately, the same control certifications that guarantee financial probity can also guarantee undeletable and unalterable backup data.

iii See https://www.veeam.com/blog/hardened-repository-passes-compliance.html for the recent compliance certifications of Veeam's Hardened Linux Repository