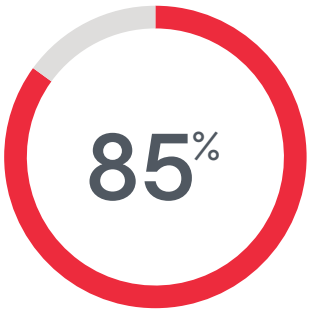
Building a Cyber-Resilient Data Recovery Strategy

Contents

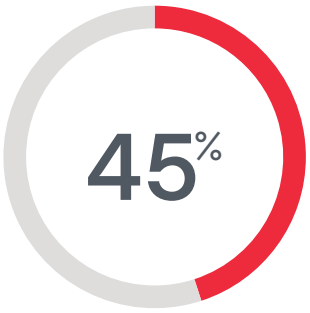
Introduction

Security of data is at the forefront of every organization's strategy because the threat of cyberattacks, primarily ransomware, is a clear and present danger. Unfortunately, 85% of organizations have had at least one ransomware attack in 2022 (2023 Veeam Data Protection Trends Report). Further alarming is the fact that today's ransomware isn't just locking organizations out of their data, they are also exfiltrating, or stealing, the data to be sold, used for future attacks or used as part of one or more extortion schemes.

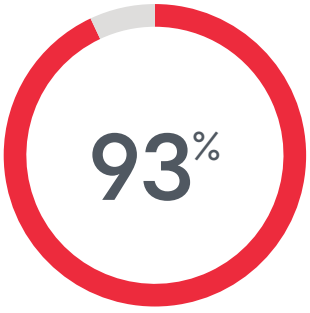
Preventing malicious access to this data should be the top goal of any cybersecurity plan. However, no organization should assume that their defenses will always hold. Therefore, having the ability to recover data as the last line of defense is equally important. Of organizations affected by ransomware, on average 15% of production data was lost (2023 Veeam Ransomware Trends Report), highlighting the importance of having a well-designed and reliable data recovery plan.



of organizations were hit by a ransoware attack in 2023*



of production data was affected by cyber attack*



of ransomware attacks targeted backups*

Source: Veeam Ransomware Trends 2023 report

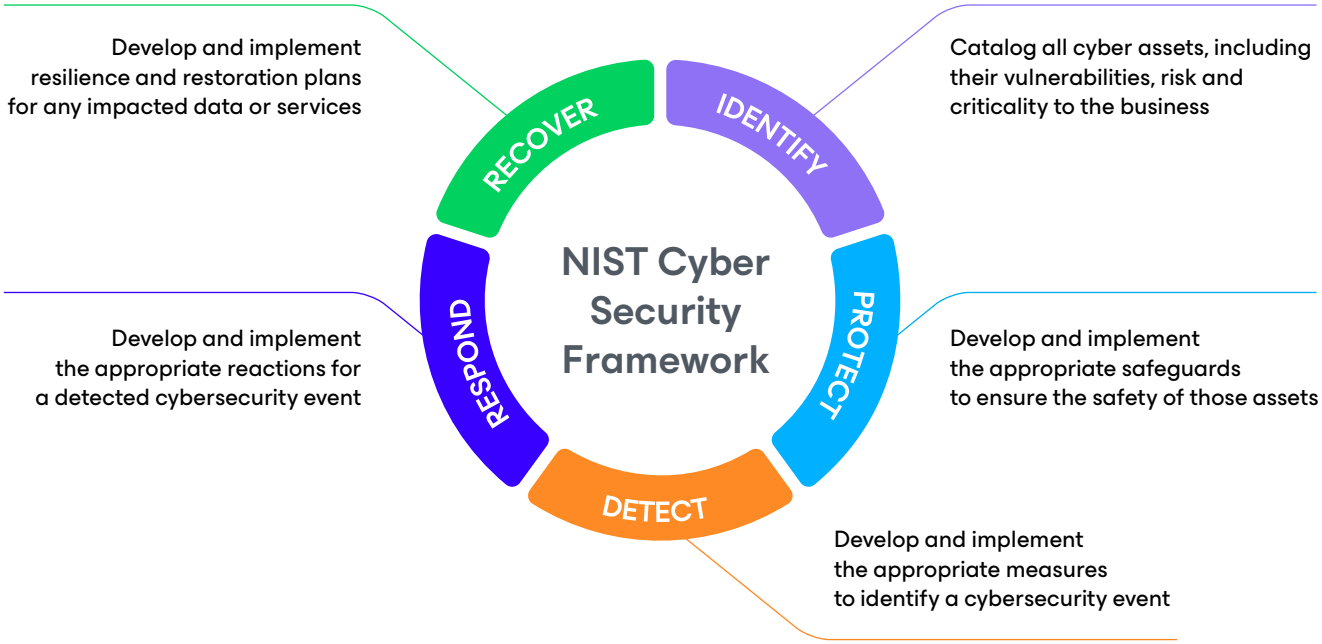
A Reliable Data Recovery Foundation

Data Recovery, as part of a data availability strategy, is often the final backstop of a cybersecurity plan, and therefore needs to be well considered and planned. Utilizing concepts like a 3-2-1-1-0 data protection strategy and having a single tool that can backup data throughout the infrastructure and restore it to a healthy state when and where needed after a cyber incident will provide organizations the proper setup to recover data in any situation.

Veeam customers can accomplish these in a secure, orchestrated and well-documented way with the Veeam Data Platform. Utilizing the full suite, including Veeam Backup & Replication, Veeam ONE and Veeam Recovery Orchestrator, customers are able to accomplish data security goals that align to all stages of the NIST Cybersecurity Framework and go well-beyond data backup and recovery.

A Common Framework for Cybersecurity Planning

The NIST Cybersecurity Framework is a proven framework that organizations can utilize to improve their cybersecurity program. Organized in a repeatable set of stages and functions that can be applied to multiple different IT and business disciplines, the framework is intended to guide organizations to focus on managing cybersecurity risk.



While data availability software is a key component of the Recover phase of the NIST Cybersecurity Framework, most people don't inherently see it being applicable in the other phases of a cybersecurity program. Veeam has been focusing for many years on taking advantage of its place as an enterprise data protection platform to better equip their customers with the information they need to defend their data.

Drawing heavily from the NIST Cybersecurity Framework, this paper will equip IT organizations, security teams and responsible decisions makers with the insights and knowledge to utilize the Veeam Data Platform to provide another rich source of information and capabilities to aid in the identification of critical data, detection of malware, protection of data, quick response to active threats and rapid recovery of clean data, highlighting the key capabilities used to accomplish these goal.

Identify Critical Data

Just like any disaster that could befall a business, planning is job #1. In fact, cybersecurity shares one very core mantra with traditional disaster recovery: **you can't protect what you don't know about**. Cataloging and categorizing assets that need protecting may seem inconsequential compared to the active defense from and reaction to a cybersecurity threat, but knowing what is at risk and the relative priority is the first step. With the following capabilities, Veeam can be an instrumental part of a multi-layered strategy to **Identify** critical data.

Catalog Critical Systems and Data

To create a reliable recovery plan, IT and Security need to work closely with the business to identify, catalog and prioritize all the workloads and data that exist across the organization. A great place to start is with the reports available within Veeam ONE and the catalog of systems being backed up by Veeam Backup & Replication. All critical data should be backed up, and Veeam can make it clear if there are virtual machines or data that are not being protected.

Similarly, the network and security tools used by the Security team will be able to create a list of systems in the environment. Comparing these various systems will often highlight where data is not properly protected within each of the tools, ensuring protection and recovery plans will be as complete as possible.

Identify and Prioritize Data Through Tagging and Classification

Utilizing the tagging and data classification capabilities within Veeam Backup & Replication, customers can start with an existing catalog of workloads — their backups — and begin applying tags to identify system metadata like location, owner and recovery priority. This exercise will sometimes highlight data that is missing, indicating a gap in data protection, as well as identifying key metadata that will be needed to properly plan data recovery.

Once the metadata is applied, the wizard-driven recovery planning within Veeam Recovery Orchestrator can be utilized to create the recovery plan, reducing the time it takes to develop the plan. This plan can then be reviewed with the business as another check to ensure its accuracy and completeness to business needs.

Highlight Gaps and Changes Through Automated Recovery Tests

The single best way to identify that a backup or plan won't be ready for emergency use is to test both. The automated testing capabilities of Veeam Recovery Orchestrator provide a huge benefit to ensuring the complete recoverability of some or all of the infrastructure. Besides the obvious benefits of labor reduction during the test execution, automating the test recovery process can also mean more frequent tests, which will allow these tests to highlight flaws quicker.

One of the flaws that can be identified through frequent testing is when systems are not being backed up or have been left out of plans. Reviewing these test results regularly and quickly remediating any gaps will improve the knowledge of what needs protecting.

Protect Backup Infrastructure and Data

The backup infrastructure is a special place in any IT environment. Not only does it create the final safety net of Data Security, but it contains multiple copies of all data — the more critical, the more copies — including data that may have been deleted in production. This makes it a rich target for criminals to steal data and eliminate the safety net in order to improve the success of their ransom and extortion schemes. This is why it's paramount to **Protect** the backup infrastructure itself.

A Backup Infrastructure That Trusts No One

The first step in protecting backups is to prevent unauthorized access to the backup management system itself. The principles of Zero Trust — verify explicitly, assume breach and least privileged access — should be applied in order to make lateral movement into the backup infrastructure as difficult as possible.

Utilizing multi-factor authentication and having a separate, dedicated data protection Identity and Access Management (IAM) system in place to control user policies will ensure users are properly verified and harder to compromise. Implementing least privilege access, like having separate admin and operational accounts, will prevent unintentional mistakes and minimize privilege escalation. Finally, everything should be configured assuming the rest of the infrastructure has already been compromised by isolating backup components onto a segregated network and restricting access to the Veeam Backup & Replication console itself via a VPN or remote connection.

Every level of the backup infrastructure should incorporate these approaches but may look slightly different at each level. Operating systems, file shares, out of band management and any other applications used to manage them should follow similar principles.

Analyze Backup Infrastructure Compliance

To help customers properly apply the Zero Trust principles, the Veeam Backup & Replication console has a built-in utility called Security & Compliance Analyzer (previously known as the Best Practices Analyzer) that analyzes the Veeam infrastructure and reports on configuration items that have not been implemented per Veeam's recommendations. This analysis should be run on a regular basis and each of the non-compliant items should either be corrected or suppressed. Suppressed items will be noted with the user and date/time it was suppressed. After remediations are completed, the analysis should be run again and the results documented.

Ensure Backups Will Exist When Needed

Deleting backups so that data cannot be recovered is now a common feature of ransomware. Therefore, making sure the backups cannot be modified or deleted is critical.

Immutability is a very old concept in computer science that has recently become a critical feature for backups, especially for backups that need to remain without change or error to satisfy retention requirements. Utilizing Hardened Repositories, Object Storage, third-party deduplication appliances or tape, Veeam backups can be stored in a state where even administrators cannot modify or delete the data. As with any security system, there are often workarounds, so it is critical to consider the entire stack — all the way to the data center floor — to ensure that these workarounds are eliminated or tightly controlled.

It's an old joke in cybersecurity that the most secure system is the one that is powered off, disconnected from the network and stored in a room no one can access. While the joke is completely accurate, it is funny because that system has no reason to exist. This adage, however, can work well when considering the security of backups. As long as it is accessible when necessary, a backup that is stored offline is the least likely to be tampered with. Veeam provides several options to create this air-gapped approach to storing backups that range from on-line systems that require a different authentication to the ultimate off-line storage: tape.

But no plan should ever rely on a single layer of protection. Therefore, Veeam Backup & Replication can enable a "four-eyes" principle to deletion of backups. Similar to the old "nuclear keys" approach, this configuration requires two administrators to authorize the deletion of a backup, protecting backups from accidental or malicious deletion.

Zero Trust Security Model

The goal of the concept of "zero trust" is to eliminate the inherent trust that traditionally has existed within the perimeter security, thus reducing the ability for threats to move easily through an environment. Using the mantra "never trust, always verify" creates a perimeterless security model that does not assume the firewall will take care of stopping cyberthreats. In this model, every system should be verifying every new interaction, making no assumptions they are safe.

The three principles of the Zero Trust Security Model are:

1. Verify explicitly
2. Provide least privileged access
3. Assume breach

Encrypt Your Own Backups

To protect data from abuse after exfiltration, backups can be encrypted by Veeam to prevent anyone being able to access them outside of the Veeam infrastructure. While this won't prevent the data from being taken or locked via ransomware, it will make it very unlikely that it cannot be an avenue for extortion schemes. This encryption can be managed internally within Veeam or tied to a third-party key management system (KMS) to offload and centralize the management of these keys.

Detect Cyberthreats

Once the full landscape of systems and data have been identified, the organization then needs to put into place plans and systems for fast detection of intrusions into those assets. Quick detection will dramatically reduce dwell time and the impact of the threat, which can generally be translated into money lost. Here, too, Veeam's software can be a key component in a multi-layered strategy to **Detect** cyberthreats.

Drawing Attention to Aberrant Behaviors

One of the key strategies of malware is to avoid detection while it escalates privileges and moves laterally within the environment, infecting as many systems as possible. To accomplish this, it may only make small changes at a time to evade notice. Additionally, as they've become savvier at thwarting our efforts to recover the data they want to hold ransom, the malware authors have started deleting backups, reducing backup retention times or disabling backup jobs. Veeam can identify and alert on these types of aberrant behaviors through several alarms and reports within Veeam ONE.

Scanning for Malware During Backup

Using inline malware detection, Veeam Backup & Replication can analyze blocks as they come through the Veeam Proxy nodes for signs of new encryption, a key indicator of active malware. Based on a search of the index of the backup, malicious file names and signatures will be detected and if something suspicious is found, the backup will be flagged as suspicious.

Detect Malware in Backups

The SureBackup feature of Veeam Backup & Replication was originally designed to automate the restoration and validation of backups to validate they are restorable. Since endpoint protection software isn't perfect, which could lead to malware getting into the backups, SureBackup also has a robust set of capabilities that can check backups for malware.

As part of a restorability test, SureBackup can work with malware scanning tools to scan the restored virtual machine. This gives organizations the ability to utilize a secondary malware detection tool in a "trust but verify" approach to detection. As an added benefit, the SureBackup scan will occur with zero impact to the production workload, potentially allowing a more thorough scan. SureBackup can also mount individual disks to a test machine that can then scan the files for malware, providing an even faster and more resource-efficient malware scan when a full restore is not necessary.

If anything is found in these scans, then that particular restore point will be flagged as suspicious.

Regular Recovery Plan Testing to Detect Compromise

Once again, regular testing of recovery plans can be useful to cybersecurity by highlighting the corruption caused by malware. Failures during a complete recovery plan test, including application verification, could highlight areas of the infrastructure where a key file was encrypted or a configuration file was modified inappropriately. This could be especially useful to detect malware that executes during a boot-up sequence.

Centralized Log Reporting and Correlation

Sending log files to an external syslog service provides both a secondary repository of logs and centralization that allows for event correlation across systems. This is the primary function of a Security Incident and Events Manager (SIEM) system for most Security teams. By setting up the SIEM system as a syslog target, indicators of compromise discovered by Veeam can be flagged directly within the system used by the Security team, reducing the time to respond and giving security analysts a more robust view of an event.

Dwell Time

Dwell time — the amount of time the malware exists in the environment before it is discovered — is the time when the malware sits within the environment without executing the primary attack. It may spend this time compromising additional accounts, escalating privileges, embedding itself deeper into the operating system, spreading laterally to other systems and gathering intelligence it can use for current or future attacks.

External Integrations for Data Protection

The Incident API is a set of application programing interfaces (APIs) that cybersecurity tools can utilize to inform the backup infrastructure of a discovered infection and flag backups as either suspicious or infected. Veeam Backup & Recovery can be configured to alert administrators based on this information, allowing them to quickly review, verify and respond with actions like creating an immediate backup, executing a SureBackup action to check for infection and recover clean files, and creating an immutable copy of a backup for forensic purposes. This open integration point between core security tools and the data protection platform greatly enhances communication, which can reduce malware dwell time and will lead to cleaner and quicker recovery.

Respond to Cyberthreats

It is not possible to always be 100% protected, so there also needs to be focus on stopping malware and removing it as quickly as possible. Like planning for recovery from a natural disaster, one of the primary objectives all decisions should align to is the Recovery Time Objectives (RTO). In a cybersecurity event, there is a very similar goal focused on stopping and removing the malware from the environment so that systems can be brought back into service. Being able to reduce the time the malware will have to dwell and exfiltrate data will reduce the clean-up effort and improve the recovery time, which is why it is critical to prepare to **Respond** quickly.

Using Backups for Cyber Forensics

As discussed earlier, SureBackup is a feature that not only tests the restorability of backups but can also detect malware. One of the goals during the Respond phase is to identify dwell time, so using malware flags in the Veeam Backup & Replication console, which will indicate if malware was detected in a restore point or found in that timeframe by a third-party tool using the Incident API, eases the hunting required to find the first point of infection.

Secure Restore is another function of Veeam Backup & Replication which allows for disks to be mounted and scanned for malware prior to full restoration. Iterating this process until an uninfected point is discovered makes it easier to find the point in time when the malware first appeared on a given system, as well as avoiding reinfection by restoring a dormant piece of malware.

With Veeam Recovery Orchestrator, this Secure Restore process can be executed on the entire environment in an orchestrated "clean room" approach. Not only does this add a faster approach to checking for clean restore points, but also quickly adds valuable information to the digital forensics of a cybersecurity incident.

Exfiltration

If data was accessed and modified by malware, then it was likely stolen first. Exfiltrated data is data that is sent from a victim's environment back to the cybercriminals. It could become information released or sold by cybercriminals after a breach, leading to exposed corporate secrets, damaged reputation, and stolen personal information that could lead to future fraud or cyberattacks.

Enhanced Threat Hunting with YARA

A tool familiar to cybersecurity threat hunters, YARA is a rules-based approach to identify and classify malware. As part of a SureBackup or SecureRestore operation, a YARA rule can be identified and executed for both initial classification of the malware and then searching for it across backups.

Incident Tracking with ServiceNow

With direct integrations into ServiceNow, Veeam can automatically create new cases and update existing ones as the situation evolves, helping different teams communicate more efficiently and providing a more automated documentation of the history of the incident.

Recover Safe Data Faster Than Ever

Depending on the nature of the cybersecurity incident, getting clean data restored will be critical to restoring services, particularly with ransomware. If the dwell time is long, then many recovery points may contain malware, and there may be a need to go back far in time to find a clean restore point. Like traditional disaster recovery, it is important to align to goals related to minimizing lost data — the recovery point objective (RPO). Since discovering the start of the infection is important in the Respond phase, many of those efforts will work in parallel with the efforts to **Recover** data.

A Backup is Only Useful if it is Restorable (and Malware-free)

The flagging of suspected or infected restore points during the Detect and Respond phases by features like SureBackup and the Incident API make it very easy to identify right within the Veeam Backup & Replication console if malware was detected in each restore point. This is a great starting point but does not guarantee earlier restore points are completely clean.

To reduce the chances of restoring infected data and minimizing duplicate effort, recovery efforts should work together with the cyber forensics occurring in the Respond phase. A strong working partnership between IT, Security and the business is critical to restore the right data and not reintroduce malware.

Previously undetected malware could be found in earlier restore points when utilizing fully up to date malware detection tools as part of SureBackup and Secure Restore, so it is important to not rely only on malware flags from earlier scans. In the event the clean restore points are further back in time than the defined RPOs, file-level restores can be utilized to restore individual pieces of key data, while avoiding the malware in the full backup.

Backup vs. Replication for Cybersecurity Recovery

Replication may be a part of a cybersecurity recovery plan, but it's important to understand the goals of replication versus backups. Replication is focused on getting data moved as quickly as possible and returning to the most recent good replica. Backups are not continuous, and therefore can be more methodical when ensuring cleanliness and restorability. Cybersecurity recovery needs to be based on dwell time and the cleanliness of the restore point, making backups a more common mechanism.

Restore Uninfected Data as Fast as Possible

Automation is the key to rapidly recovering even the simplest environment, but the mode of restore can make a difference as well. Utilizing storage array snapshots and Instant Recovery, restored backups can be utilized nearly instantaneously.

Veeam Recovery Orchestrator was designed to prescribe the entire restoration process and make it as simple as clicking a single button. Combining the restoration plan with infection flags, Secure Restore, storage array snapshots, Instant Recovery and application verification, Veeam has a very powerful combination of features to restore data quickly and efficiently, while also making sure the data is as malware-free as possible.

Visualizing I/O Anomalies

Sometimes, nothing can highlight trends better than a visual graph. Within the Veeam Backup & Replication user interface, graphs are provided when recovering from a replication job that will help identify the moment where mass encryption began, reducing the effort needed to find a pre-encryption point in time.

Summary

Building a cybersecurity program is no easy task these days. The threats are numerous and the value of a breach to the criminals is potentially huge, so organizations need to use every tool at their disposal to create layers of security so they can maximize their effectiveness at every stage of the NIST Cybersecurity Framework. Veeam can provide value to all stages of the NIST Cybersecurity Framework, improving the organization's overall cybersecurity program:

- The act of creating and regularly testing recovery plans can provide valuable data to be used in the **Identify** phase for ensuring critical data is identified and can be protected.
- Implementing documented best practices and native security capabilities will ensure that the backups and backup infrastructure are addressed in the **Protect** phase.
- Since backups touch all data across the infrastructure, they can be an important second check for malware that may have been missed by endpoint observations in the **Detect** phase.
- Fast access to different points in time and virtual "clean room" environments can be critical to information gathering efforts in the **Respond** phase.
- Backups that are proven to be restorable and malware-free will be available when needed and restorable into a clean and useable state as quickly as possible to support the **Recover** phase.

It's time IT teams become more than just keepers of restorable data and become active participants in the cybersecurity plan. Utilizing the guidance in this document, IT teams should now be able to have a productive conversation with security teams to integrate a Veeam-based data protection platform into the overall cybersecurity program.

For more details on the features mentioned throughout this document, please review the User Guides available in the Veeam Help Center. Many of these features are new with the Veeam Data Platform 23H2 Update.