Building a Cyber-resilient Data Recovery Strategy

Table of contents

Introduction

In today's digital-first world, cybersecurity is a fundamental necessity. It's not surprising that every cybersecurity blog or whitepaper you read today inevitably revolves around ransomware. It's tiresome to hear about (we know!) but ransomware has become the biggest threat to organizations of all sizes and targets our most critical infrastructure and industry sectors. It's a game of cat and mouse, and as new threats emerge, security teams must adapt to keep up. The pervasive digitization of business operations, government functions, and personal activities has exponentially increased the volume of sensitive data that's stored and transmitted online. This shift has unfortunately also broadened the attack surface for cybercriminals, which makes robust cybersecurity measures essential.

Cyberthreats, ranging from data breaches and ransomware attacks to sophisticated state-sponsored cyber espionage, pose significant risks to the integrity of critical infrastructure, the privacy of your personal information, even and the stability of global economies. Therefore, data security should be at the forefront of every organization's strategy since 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[1]. What's even more alarming is the fact that today's ransomware attacks aren't just locking organizations out of their data, they're exfiltrating, stealing, selling or archiving that data for use in other 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. So, having the ability to recover your data is equally important. Of organizations affected by ransomware, 15% of production data was lost on average[2] which highlights the importance of having a well-designed and reliable data recovery plan.

Effective cybersecurity practices protect against unauthorized access to data, ensure the continuity of operations, and maintain the trust between consumers and service providers. As cyber threats evolve in complexity and scale, the importance of cybersecurity in safeguarding digital assets, protecting individual privacy, and preserving national security cannot be overstated. It is a critical pillar in the architecture of our digital society and ensures that we can navigate, innovate, and communicate in this realm with confidence.

The recent update to the NIST Cybersecurity Framework (CSF) 2.0[3] marks a pivotal evolution in he standard approach to cybersecurity and reflects shifting paradigms in a world where digital threats are increasingly complex and pervasive.

This paper explores the updated NIST CSF Framework and discusses places where Veeam Software can assist with implementing this framework.

Background of the NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) was first introduced in 2014 in response to the growing need for a unified approach to managing cybersecurity risks. The framework was developed by the National Institute of Standards and Technology (NIST) through collaboration with both private and public sector entities, and they aimed to provide organizations with a set of industry standards to help protect their information systems. The CSF's objectives were to help organizations understand and improve the management of cybersecurity risk, which would also enhance the security and resilience of critical infrastructures.

The NIST Cybersecurity Framework (CSF) 2.0, released in Feb. 2024, builds on previous versions and brings several significant changes that reflect the evolution of the cybersecurity landscape and feedback received from the community.

CSF 2.0 extends its reach beyond just critical infrastructure sectors; it has been revised to benefit all organizations, regardless of size or type, which makes this guideline more universally applicable.

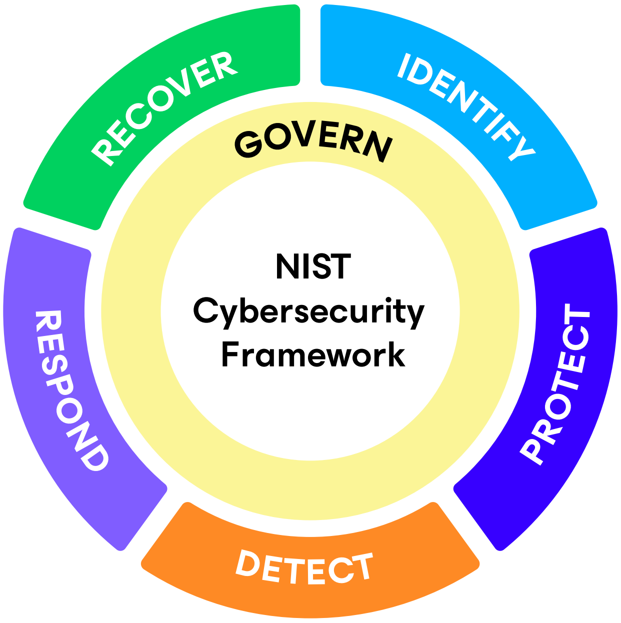

Figure 1 — NIST Cybersecurity Framework 2.0

The core of the CSF is organized around six main functions and when considered together, these features create an all-encompassing recommendation based on the cybersecurity risk life cycle.

- **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. This includes identifying critical business processes and key assets, along with their vulnerabilities and threats.
- **Protect:** Implement appropriate safeguards to ensure the delivery of critical services and limit or contain the impact of potential cybersecurity incidents. This includes identity management, access control, data security, and protective technology.
- **Detect:** Implement measures to identify the occurrence of cybersecurity incidents in a timely manner. Continuous monitoring and threat detection are key capabilities in this function.
- **Respond:** Take action when a cybersecurity incident is detected. This includes incident response planning, analysis, mitigation, and communication.
- **Recover:** Maintain plans for resilience and restore capabilities or services that were impaired due to a cybersecurity incident. Timely recovery to normal operations is the goal.
- **Govern (new):** This new function in CSF 2.0 focuses on the overall management and governance of cybersecurity risk. Here, organizations establish their cybersecurity risk management strategy, policies, and oversight, including defining roles and responsibilities and integrating cybersecurity into enterprise risk management.

The new "Govern" function elevates the fundamental objectives of accountability and transparency and serves as a uniting force to assist organizations in prioritizing and achieving the objectives outlined in the other five functions. It also emphasizes that cybersecurity is not a standalone concern but an integral part of what constitutes enterprise risk. The new function's oversight component in particular helps organizations in complying with regulatory frameworks — like SEC regulations — that emphasize increased accountability for senior management and the Board of Directors when making choices about IT security.

To improve clarity and relevance, the five original functions — Identify, Protect, Detect, Respond, and Recover — have been retained and updated to reflect evolving cybersecurity threats and practices, thus ensuring that organizations can effectively manage and reduce their cybersecurity risks in a dynamic digital environment. Governance-related elements have also been transferred to the newly created "Govern" function. Furthermore, each function's primary objectives are now more clearly stated. By recognizing that these tasks are not sequential but rather interdependent parts of an all-encompassing cybersecurity strategy, this restructuring seeks to enable a more cohesive and linked approach to cybersecurity.

A focus on cybersecurity supply chain risk management is also now more pronounced, with new controls aimed at integrating supply chain risk management throughout an organization's cybersecurity program.

Users of this framework are now provided with implementation examples[4] and quick-start guides[5] that are tailored to their specific needs as well. This includes a searchable catalog of references[6], accessed via the reference tool, that enable organizations to map guidance to over 50 other relevant cybersecurity documents.

Key changes include:

1. CSF 2.0 extends its applicability beyond critical infrastructure sectors. The revised framework is designed to benefit all organizations, regardless of size or industry, by making the guidelines more universally relevant.
2. The addition of the "Govern" function is a significant enhancement in CSF 2.0. This function elevates the core objectives of accountability and transparency while serving as a unifying force to help organizations prioritize and achieve the goals outlined in the other five functions. It emphasizes the integration of cybersecurity into overall enterprise risk management, rather than just treating it as a standalone concern. The oversight component of the "Govern" function is particularly useful for organizations in complying with regulatory frameworks, such as SEC regulations, which stress increased accountability for the Board of Directors and senior management when making decisions related to cybersecurity.
3. A heightened focus on supply chain risk management. CSF 2.0 places a stronger emphasis on managing cybersecurity risks in the supply chain. New controls have also been introduced to integrate supply chain risk management throughout an organization's cybersecurity program. This acknowledges the importance of securing your entire ecosystem of partners, vendors, and service providers.

These enhancements within NIST CSF 2.0 provide organizations with a more comprehensive and adaptable framework to help them navigate the complex cybersecurity landscape. By expanding scope, introducing the "Govern" function, updating core functions, and emphasizing supply chain risk management, CSF 2.0 equips organizations with the tools and guidance they need to strengthen their cybersecurity posture and build resilience in the face of evolving threats.

Users of this framework are now also provided with implementation examples[7] and quick start guides[8] that are tailored to their specific needs. This includes a searchable catalog of references[9], accessed via the reference tool, that enables organizations to map guidance to over 50 other relevant cybersecurity documents.

A Reliable Data Recovery Foundation

Data recovery, as part of a data availability strategy, is often the final stop in 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 your data throughout the infrastructure and restore it to a healthy state after a cyber incident will provide organizations with the proper set up to recover data in any situation.

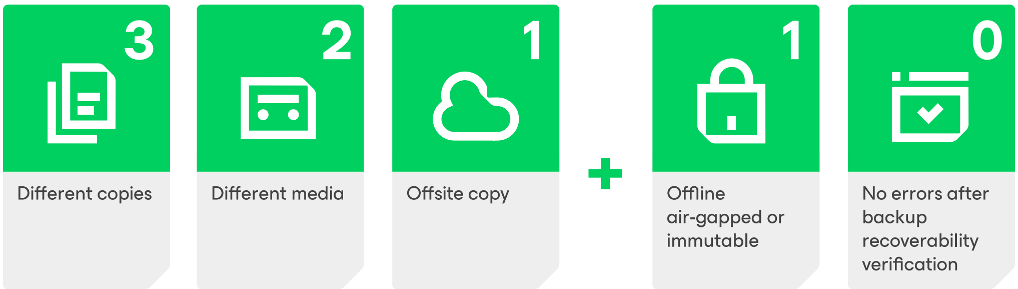
3
Different copies
2
Different media
1
Offsite copy
+
1
Offline air-gapped or immutable
0
No errors after backup recoverability verification

Figure 2 — Veeam's 3-2-1-1-0 Backup Rule

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

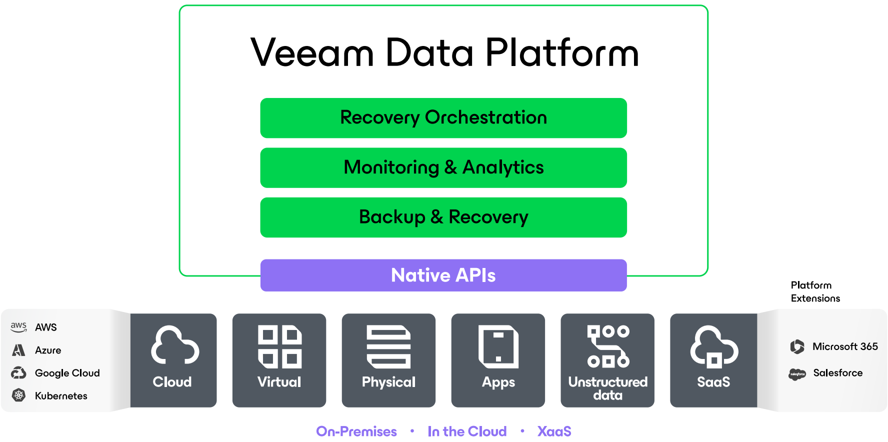

Figure 3 — Veeam Data Platform

Drawing heavily from the NIST Cybersecurity Framework covered above, the rest of this paper is meant to equip IT organizations, security teams, and decision makers with the insights and knowledge they need to effectively use Veeam Data Platform within the framework. We also want to provide you with another rich source of information and capabilities that help identify critical data, detect malware, protect data, quickly respond to active threats and rapidly recover clean data while highlighting the key capabilities that can be used to accomplish these goals.

NIST Function "Identify" (ID)

Desired cybersecurity outcome:

An understanding of the organization's current cybersecurity risks.

Cybersecurity shares one very core mantra with traditional disaster recovery (DR): **You can't protect what you don't know.** Cataloging and categorizing assets that need protection may seem inconsequential compared to actively combatting and reacting to a cybersecurity threat, but knowing what is at risk and its relative priority is the first step. With the following capabilities, Veeam can become 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 in Veeam ONE and the catalog of systems that are backed up by Veeam Backup & Replication. All critical data should be backed up, and Veeam can make it clear if there are virtual machines (VMs) or data that's not being protected.

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

Identify and Prioritize Data Through Tagging and Classification

By utilizing the tagging and data classification capabilities held 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 missing data, indicate a gap in your data protection, and identify key metadata that's needed to properly plan data recovery.

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

Highlight Gaps and Changes Through Automated Recovery Tests

The single best way to identify whether a backup or plan will be ready for emergency use is to test it. The automated testing capabilities of Veeam Recovery Orchestrator provide a huge benefit by ensuring the complete recoverability of some or all of your infrastructure. Besides the obvious benefits of labor reduction during test execution, automating the test recovery process can also mean more frequent tests, which allows flaws to be highlighted 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. Reviewing these test results regularly and remediating any gaps will improve organizational knowledge of what needs protecting.

NIST Function "Protect" (PR)

Desired cybersecurity outcome:

Implement safeguards to ensure the safety of your assets.

The backup infrastructure is a special place for any IT environment. Not only does it make up the final safety net of data security, but it also contains multiple copies of all your data (the more critical, the more copies), including data that may have been deleted in production. This makes it a prime target for criminals to steal your data and safety to improve the success of their ransom and extortion schemes. This is why it's essential that you **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 use least-privileged access — should be applied to make lateral movement into your backup infrastructure as difficult as possible.

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

Each level of your backup infrastructure should incorporate these approaches, but they may look slightly different at each level. This means that operating systems, file shares, out-of-band management, and any applications used to manage them should follow similar principles.

Analyze Backup Infrastructure Compliance

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

Ensure Backups Will Exist When Needed

Deleting backups so that your data cannot be recovered is now a common ransomware feature. Therefore, making sure your 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. Whether you use 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 your 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, truth is, an inaccessible system has no reason to exist. This adage, however, can work well when considering backup security. As long as it's 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 backup storage that range from online systems that require different authentication to the ultimate offline storage: Tape.

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

Encrypt Your Own Backups

To protect your data from abuse after exfiltration, Veeam can encrypt backups to prevent anyone from being able to access them outside of your Veeam infrastructure. While this won't prevent your data from being taken or locked via ransomware, it will make it very unlikely that your data will be used as 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.

Sidebar: Zero Trust Security Model

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

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

NIST Function "Detect"

Desired cybersecurity outcome:

Develop and implement appropriate measures to identify a cybersecurity event.

Once the full landscape of systems and data have been identified, your organization then needs to establish plans and systems for fast detection of intrusions into those assets. Quick detection will dramatically reduce dwell time and threat impact, which can generally translate into money lost. Here, too, Veeam 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 escalating privileges and moving laterally within the environment, thus infecting as many systems as possible. To accomplish this, malware may only make small changes at a time to evade your notice. Additionally, since they've become savvier at thwarting our efforts to recover the data they want to hold ransom, malware authors have started deleting backups, reducing backup retention times, or disabling backup jobs. Veeam can identify and alert you of these types of aberrant behaviors via several alarms and reports within Veeam ONE.

Scanning for Malware During Backup

By using inline malware detection, Veeam Backup & Replication can analyze blocks as they come through Veeam Proxy nodes for signs of new encryption, which is a key indicator of active malware. Based on a search of the backup index, 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 backup restoration and validation to ensure they are restorable. Since endpoint protection software isn't perfect, which could lead to malware getting into your backups, SureBackup also has a robust set of capabilities that can check your backups for malware.

As part of a restorability test, SureBackup can also work with malware scanning tools to scan your restored virtual machine (VM). This gives organizations the ability to use a secondary malware detection tool in a "trust but verify" approach to detection. As an added benefit, the SureBackup scan occurs with zero impact to the production workload, which potentially allows for a more thorough scan. SureBackup can also mount individual disks to a test machine that can then scan files for malware, thus providing an even faster and more resource-efficient malware scan whenever 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 recovery plan testing can be useful since it can highlight the corruption caused by malware. Failures during a complete recovery plan test, including application verification, could call attention to areas where a key file was encrypted, or a configuration file was modified inappropriately. This could be especially useful in detecting 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, thus reducing the time to respond and giving security analysts a more robust view of an event.

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 an infection and flag backups as either suspicious or infected. Veeam Backup & Recovery can be configured to alert administrators based on this information, which allows 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 then creating an immutable copy of a backup for forensic purposes. This open integration point between core security tools and your data protection platform greatly enhances communication, which can reduce malware dwell time and will lead to cleaner and quicker recovery.

Sidebar: Dwell Time

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

NIST Function “Respond”

Desired cybersecurity outcome:

Develop and implement appropriate reactions for a detected cybersecurity event.

It is not possible to always be 100% protected, so you also need to 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 your decisions should align to is the recovery time objectives (RTO). In a cybersecurity event, there is a very similar goal that’s focused on stopping and removing your malware from the environment so that systems can be brought back into service. Being able to reduce the time malware will have to dwell and exfiltrate your data will reduce clean-up effort and improve 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 backup restorability but can detect malware as well. One of the goals in the respond phase is to identify dwell time, so using malware flags in Veeam Backup & Replication that indicate if malware was detected in a restore point or found by a third-party tool, eases the hunting required to find the first point of infection.

Secure restore is another function of Veeam Backup & Replication that allows for disks to be mounted and scanned for malware before full restoration. Iterating this process until an uninfected point is discovered makes it easier to find the point in time when malware first appeared on a given system and helps you avoid reinfection by restoring a dormant piece of malware.

With Veeam Recovery Orchestrator, the secure restore process can be executed on the entire environment with an orchestrated “clean room” approach. Not only does this add speed to checking for clean restore points, but also can quickly add valuable information to the digital forensics of a cybersecurity incident.

Enhanced Threat Hunting with YARA

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

Incident Tracking with ServiceNow

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

Sidebar: 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 then become information released or sold by cybercriminals after a breach, which could lead to exposed corporate secrets, damaged reputations, and stolen personal information that could lead to future fraud or cyberattacks.

NIST Function “Recover”

Desired cybersecurity outcome:

Develop and implement the appropriate activities to recover from a cybersecurity event (plans, process, people, technology)

Depending on the nature of your cybersecurity incident, getting clean data restored will be critical to getting services back online, particularly with ransomware. If the dwell time is long, then many recovery points may contain malware, and you may need to go back far in time to find a clean restore point. Like traditional DR, it is important to align to goals that minimized lost data: Your recovery point objectives (RPOs). Since discovering the start of your infection is important in the respond phase, many of those efforts will work in parallel with the effort to **recover** your 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 if malware was detected in each restore point right within your Veeam Backup & Replication console. This is a great starting point but does not guarantee your earlier restore points are completely clean.

To reduce the chances of restoring infected data and wasted effort, recovery efforts should work together with the cyber forensics that occurs in the respond phase. A strong working partnership between IT, security, and the business as a whole is critical to restoring the right data and not reintroducing malware.

Previously undetected malware could be found in earlier restore points when you’re utilizing fully up-to-date malware detection tools as part of SureBackup and secure restore, so it’s important to not rely solely on malware flags from earlier scans. In the event that clean restore points are further back in time than your defined RPOs, file-level restores can also be used to restore individual pieces of key data, while avoiding the malware that’s in the full backup.

Restore Uninfected Data as Fast as Possible

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

Veeam Recovery Orchestrator was designed to prescribe the entire restoration process and make it as easy as clicking a single button. By combining your restoration plan with infection flags, secure restore, storage array snapshots, Instant Recovery, and application verification, Veeam has a combination of features that can restore data quickly and efficiently while making sure your 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, which reduces the amount of effort needed to find a pre-encryption point in time.

Sidebar: Backup vs. Replication for Cybersecurity Recovery

Replication may be a part of your cybersecurity recovery plan, but it’s important to understand the goals of replication compared to backups. Replication is focused on getting data moved as quickly as possible and returning it 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, which will make backups a more common mechanism.

NIST Function "Govern"

Desired cybersecurity outcome:

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

The introduction of the "Govern" function represents a significant evolution in cybersecurity strategy and oversight. This new function emphasizes the importance of governance in managing cybersecurity risk across an organization. It also underscores the need for establishing clear cybersecurity policies, strategies, and processes that align with your organization's overall goals and risk tolerance. By integrating the "Govern" function, NIST CSF 2.0 encourages organizations to take a more holistic and accountable approach to cybersecurity, thus ensuring that cybersecurity considerations are woven into the fabric of organizational governance. This includes defining roles and responsibilities for cybersecurity, fostering a culture of security awareness, and ensuring that cybersecurity decisions are informed by organizational objectives and constraints. The addition of this function highlights the shift toward recognizing cybersecurity not just as a technical challenge but as a critical component of business management and operational resilience.

As a critical component of data security, your backup infrastructure needs to be demonstrably compliant with company and governmental regulations. To properly "**Govern**" includes the documentation of your organizations' cybersecurity risk management strategy, including configuration and policies, change tracking, and documenting the successes and failures of every test. This helps ensure that expectations and policies are effectively communicated and monitored.

Ensure Everything is Documented

Whether for auditors, cyber insurance, process improvement, or self-assurance, the importance of accurate, thorough, and frequent documentation cannot be overestimated. The accuracy and speed of a fully orchestrated recovery plan will offer the most value to administrators and business owners, but the dynamic documentation created with every full or test run will be a huge for any team that needs evidence that it actually worked, including security and compliance teams.

Beyond that, the number of reports possible out of Veeam ONE will provide you with a wealth of information about your backup infrastructure and its health. Documenting the frequency of backups, change tracking to backup configurations, and more are built-in reports that can be generated either manually or on a schedule and then automatically sent to the proper recipients.

Constantly Monitor to Minimize Risk

Leverage automation to check Veeam configurations and the backup environment to ensure that your devices and software are secure and up to date. With Veeam's Security and Compliance Analyzer, Veeam automatically performs 30+ security checks to ensure you are up to date, patched, and that your old and unsecure protocols are disabled. Additionally, all this information is compiled into a single report for security and IT teams to track adherence to organization policies.

Backup Security Dashboard

Cybersecurity is often about finding patterns across your environment. Given the wide breadth of features that Veeam provides, including new capabilities that focus on cybersecurity, like the Veeam Threat Center dashboard, a single pane of glass that aggregates multiple data sources into Veeam ONE's interface, which gives administrators and security specialists a single view of their entire backup infrastructure.

Conclusion

NIST CSF 2.0 represents a significant milestone in the evolution of cybersecurity risk management and the fight against evolving threats. By building upon the solid foundation of CSF 1.1 and by introducing key enhancements like the "Govern" function and a heightened focus on the supply chain, CSF 2.0 provides organizations with a more comprehensive and adaptable framework to help them navigate their ever-changing cybersecurity landscape.

The expanded scope of CSF 2.0 ensures that organizations of all sizes and sectors can benefit from its guidance, thus fostering a more inclusive and collaborative approach to cybersecurity. The updated framework also recognizes that effective cybersecurity risk management requires the active involvement and commitment of stakeholders across the organization, ranging from senior executives to front-line employees.

Ultimately, the success of implementing NIST CSF 2.0 relies on fostering a culture of cybersecurity awareness, collaboration, and accountability. By investing in training and education programs, organizations can empower their workforce to become active participants in the cybersecurity risk management process. Clear communication and consistent reinforcement of cybersecurity policies and best practices are essential to create a shared sense of responsibility and vigilance.

As we look forward, it is evident that cybersecurity will continue to be a critical priority for organizations worldwide. The increasing sophistication and frequency of cyberthreats coupled with the growing reliance on digital technologies underscore the need for robust and agile cybersecurity frameworks like NIST CSF 2.0. By embracing this updated framework and committing to its ongoing implementation, organizations can strengthen their resilience, protect their assets, and maintain the trust of their stakeholders in the face of evolving cyber risks.

Building a cybersecurity program is no easy task these days. Threats are numerous and the value of a breach to 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 your organization's overall cybersecurity program:

- The act of creating and regularly testing recovery plans can provide valuable data that you can use in the identify phase to ensure 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 serve as 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.
- Everyone plays a role in securing their organization and its data. Establishing, communicating, and monitoring your organization's cybersecurity strategy and policies is critical in the "**Govern**" phase.

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

Please contact us for more detail on Veeam functionalities and capabilities.

About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it. Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data portability, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 68% of the Global 2000, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam.