Essential Eight Maturity Level Three Compliance for Federal and State Agencies

October 2024

Table of contents

NOTE

Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement

Introduction

This white paper is designed for Australian federal and state agencies and aims to provide assistance to help these agencies reach Essential Eight maturity level two and three compliance for backups and comply with other mandates specified for other components of the Essential Eight. The white paper also includes additional guidance on how to best protect against various cyberthreats, as highlighted by the Office of the Australian Information Commissioner, Australian Cyber Security Centre (ACSC), and the Australian Signals Directorate (ASD).

Achieving maturity levels two and three within the Essential Eight, especially in backups, enhances security for federal and state agencies by improving data protection and disaster recovery (DR) while reducing vulnerabilities from internal and external threats. Backups act as the last line of defense to ensure accessibility, availability, business continuity, and data integrity. An effective and tested business continuity strategy with a robust backup plan can help ensure a reliable recovery process. The ASD Essential Eight provides guidelines to help agencies achieve both maturity level 2 and 3, though other elements are considered too if they contribute to a hardened backup solution.

- Ensuring you have three copies of important data (one production and two backup copies), on two separate media types (i.e., disk, cloud, or tape), one of which is offsite, with one or all of them immutable/offline, and data integrity verification that ensures zero errors. This is the 3-2-1-1-0 Rule.
- Ensuring your backup environment supports end-to-end ISM-compliant 256-bit data encryption both in flight and at rest, with the ability to integrate into enterprise KMS platforms to ensure encryption key policies are met for key rotations.
- Ensuring that access to encryption keys is still available even if your key is damaged or misplaced.
- Automated backup and DR failover testing with reporting and auditing on service level agreements (SLAs), as well as recovery point objectives and recovery time objectives (RPOs/RTOs).
- Ensuring that your data protection infrastructure supports deployment into different isolated resiliency domains or zones off the production network, as well as directory services if production administrator credentials are compromised. This includes implementing a zero-trust data resilience framework to restrict the cyberattack blast radius and ensure your backup infrastructure is not only hidden, but impervious to production credential leaks.
- Ensuring that you have one or several early alerting mechanisms within your backup environment including bi-directional integration into third party XDR/MDR incident alerting platforms when potential ransomware events may be occurring.
- Ensure your backup solution can identify file-type anomalies or changes via built-in alerting capabilities, including when known malicious file types or abnormal file modifications occur within production systems.
- Ensuring you have visibility into what recovery points are clean vs infected when recovering from a cyberattack.
- Ensuring you can automatically scan test or production recoveries or failovers via automated or ad-hoc spot-checks with technologies such as YARA rules and/or third-party AV solutions. These can identify dormant threats that are still sitting inside recovery points to avoid reinfections from inactive or dormant ransomware threats.

- Ensuring that, in the case of ransomware recoveries or compromised platforms, your existing recovery solution allows for a re-platform or bare-metal recovery for your physical and virtual workloads into a different hypervisor or cloud.
- Ensuring that efficient logging and monitoring events can be captured into enterprise SIEM tools (e.g., Splunk, Azure Sentinel, or any SIEM tool supporting Syslog standards like RFC 5424).
- Automated monthly or more frequent checks for hardening recommendations, Essential Eight compliance, or best practice implementation when performing audits on your backup environments as new workloads are added.
- Leveraging backup policies to dynamically protect new workloads as they're added at scale instead of via manual processes.
- Internal or external threat actor protection with four-eyes authorization and a second security approval framework for potentially malicious activities attempted through backup platforms.
- The ability to verify your current backup environment's security posture ad-hoc or on a schedule. As more and more workloads are added and environments are altered, ensure your environment is architected to both internal and industry best practices regarding hardening standards.
- Unfortunately, not all backup solutions are created equal, and the reason behind this is explained below as we look at what we're protecting against, especially within modern ransomware attacks. Based on Veeam's Ransomware Trends Report published last year, in 2023.

over

93%

of ransomware attacks explicitly target buckups

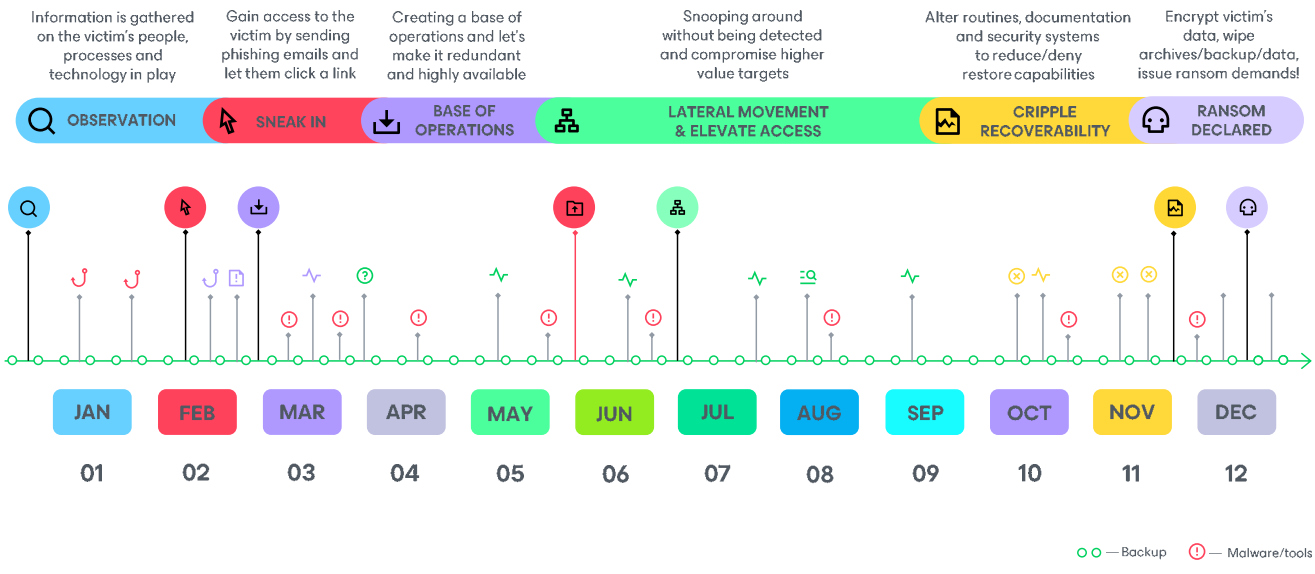
93% of all cyberattacks involved some type of attempt to cripple backup platforms and data. Attackers attempt to make recoveries impossible and increase ransom payments even for those with a no-ransom payment policy, since it leaves victims with no other way out. Furthermore, this report found that, even in cases where the ransom was paid, one in four organizations still could not recover their data.

The Anatomy of a Ransomware Attack

Let's look at what we are protecting against and discuss why traditional backup and recovery solutions struggle to meet modern cyberthreats, especially when it comes to ransomware recovery. Modern variants of ransomware and cyberthreats are highly advanced and have the primary goal of crippling your recovery operations or backup files to make paying the ransom your only option. This is a multi-trillion dollar industry, so ransomware variants have significantly evolved.

With ransomware-as-a-service and reusing tooling making it easier for threat actors to reappear and/or affiliate with other threat actors that appear on the dark web, we're seeing many of the same actors reappear and spin-off following law enforcement disruptions. So, let's look at what a modern cyberattack might look like. Note that this timeline may be longer or shorter depending on your organization's ICT security tools and safety nets (e.g., intrusion detection platforms in use, firewalls, perimeter security processes, OSes, and application vulnerability patching processes, etc.). A good stance of preparation is to prepare now for when you get attacked. If you don't, by the time you incur a cyberattack, it'll most likely be too late and you'll be left defenseless. According to ASD's 2023 Cyber Threat Report, ASD responded to over 1,100 cybersecurity incidents from Australian entities. Separately, nearly 94,000 reports were made to law enforcement through ReportCyber — which is about one every six minutes.

An example of an advanced ransomware attack looks something like this:



1. **Observation:** Social engineering and finding information on an organization's people, processes, and technologies.
2. **Sneaking in:** Phishing attempts, brute force attacks on external web-facing systems, and gaining access to endpoints/mobile devices or other unpatched external-facing systems.
3. **Establishing a base of operations:** On unpatched systems, bad actors can disable firewalls, alert mechanisms, and create a highly available base of operations via multiple systems. According to Elastic Security Labs's global threat report in 2024, adversaries are also tripling down on defense evasion techniques to hinder sensor visibility.
4. **Elevate access and lateral movement:** Credential scanning, gaining access to heightened production AD credentials, creating admin accounts, resetting passwords on existing domain admin accounts, and searching for high-impact DNS hostname scans and naming conventions. This includes internal file shares, servers with file shares or databases, virtualization infrastructure scanning, backup infrastructure naming conventions, etc.) Bad actors may also place time bombed threats into high-value targets that can sit dormant and hidden for months, often masked as system files or common file types.
5. **Crippling recovery:** After a breach, we found this process is sometimes offloaded to third party threat actors that are experts in backup and recovery systems. This could include production and backup file exfiltration, malicious deletion/encryption attempts on backups, or even remote access of backup servers via remote RDP, remote registry, SSH, and disabling or changing passwords for critical backup services and service accounts.
6. **Ransom declared:** Encryption begins for heightened targets, usually before a long weekend or holiday to ensure the most damage can be inflicted while going unnoticed. Ransom notes are left, and by this point, backups have more than likely been impacted, since recovery points that span days, weeks, or months have already been encrypted by threat actors, rendering them useless.

If you come in on a Monday and you're facing that dreaded ransom note, your network has been compromised for some time, and traditional backups may not be enough to recover your data. Chances are, they have been disabled, deleted, or destroyed, unless you already put together strategies to isolate or harden your backup environment. If they are still available, however, recent backups may also contain encrypted files and make it difficult to work out the best point in time to start recoveries from.

Moreover, when successful, exfiltration may add to the pain and the fear of customer/citizen data being leaked to the Dark web, which we increasingly saw in 2023. Again, backup data contains all an organization's important data all in one place. If your backups are not encrypted while in-flight and at-rest, they become an easy target for threat actors to exfiltrate and extort for ransom.

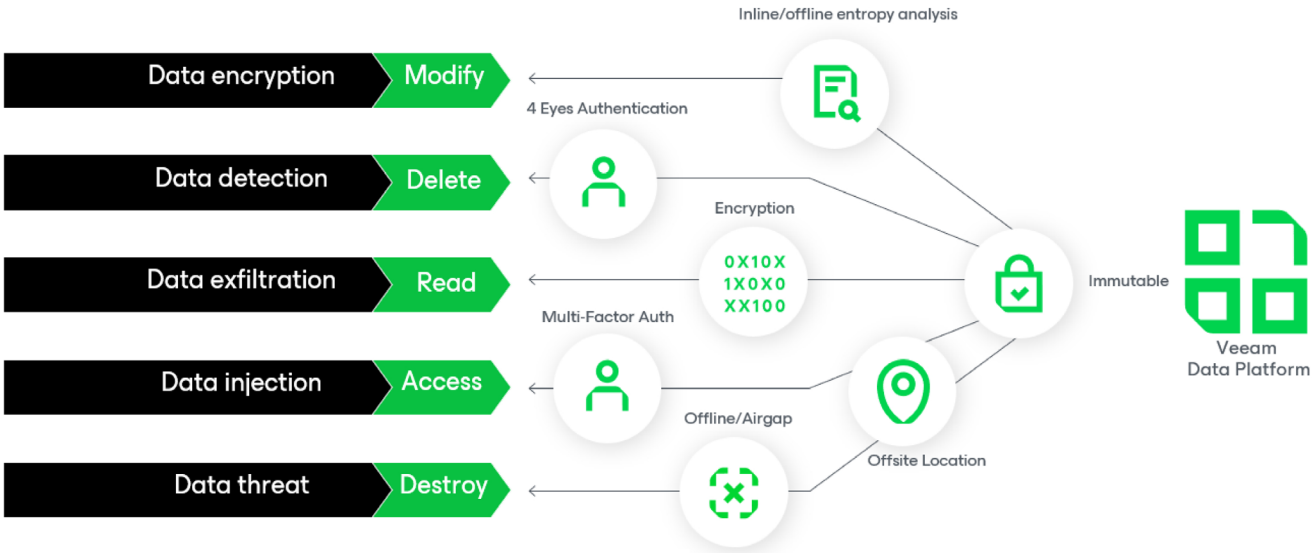
Going back to what a hardened backup should look like, ask yourself the following questions:

- Do I have isolated copies of my backups in multiple locations under my control? If so, are they secured, offline, isolated, or immutable and impervious to internal and external modification or deletion?
- Can my backup environment/server run without direct access to the internet?
- Are my backups using 256bit AES encryption, protecting me from data exfiltration whether in-flight or at-rest?
- If KMS policies are unavailable, am I still able to retrieve access to encryption keys and ensure data recoverability in an outage?
- Is my backup infrastructure connectivity certificate-based to minimize the risk of man-in-the-middle attacks?
- Can I automate, test, and measure my service level agreements (SLAs) for recoveries and perform disaster recovery (DR) failover testing non-disruptively with production-identical data in an isolated environment?
- Can I scan my backup recovery points or replicas during restore/failover testing with YARA rules? Or, can I use third party antivirus software to identify potentially malicious files or dormant ransomware during full recoveries and recovery/failover testing to reduce reinfections?
- Is my backup infrastructure and repository in an isolated domain? Is my resiliency zone/workgroup inaccessible from the production domain's administrator account?
- Is multi-factor authentication (MFA) implemented to safeguard login access to my backup server?
- Does my backup infrastructure integrate with security intrusion detection tools (e.g., XDR/MDR)?
- In the event of a cyberattack, can my backup environment quickly and reliably identify clean recovery points for all my workloads?
- Does my existing backup solution allow me to recover to a different virtualization, cloud platform, or a clean, uncompromised network if my production environment were to be seized for triage by cyber recovery teams or law enforcement?
- Can my existing backup solution integrate into log management event tools and parse security events into enterprise SIEM tools like Splunk or Azure Sentinel? Can I automate system tickets into ServiceNow or similar solutions for automated responses to cyberthreats?
- Can I schedule or easily see at-a-glance whether my backup environment is meeting strict security mandates for Essential Eight audits on my backups?

- Can I automatically and dynamically protect new workloads as they are created by adding them to my backup schedules and policies to ensure compliant protection at scale?
- Does my existing backup solution identify and alert me of anomalies in my production servers and backups? Can it identify abnormal behavior or abnormal incremental backup sizes via inline/offline entropy analysis? (e.g., can you identify malicious known file types/extensions or abnormal encryption on production file servers)?
- Can I scan backups to proactively identify and remediate corrupted blocks inside my backups?
- Can my backup solution restrict potentially accidental or malicious activity from occurring in case of malicious internal or external threat actors (e.g., backup data deletion, repositories, modify access, modify time, and date settings)? Can my solution pass authorization to a second backup or security administrator for a second authority before allowing potentially destructive events?

If you answered no to any of the above, you may be at a higher risk for ransomware/cyberattacks. At minimum, you should implement the above if your backup solution provides this functionality. At Veeam, we've been fighting the good fight against ransomware and cyberthreats and cover all the above right out of the box. Since 2023, we added over 500 security enhancements to our platform to better protect customer and citizen data.

It's also important to understand that there are so many safeguards required to implement a hardened ICT strategy. The information securities manual covers a lot about hardening government citizen and data platforms, and the ACSC Ransomware Emergency Response Guide outlines what to do in the case of a cyberattack on government systems. What Veeam excels at is protecting that last line of defense — your backups and overlay protection strategies that secure your organization against data encryption, detection, exfiltration, injection, and other internal and external data threats to help you recover fast and prevent reinfection.

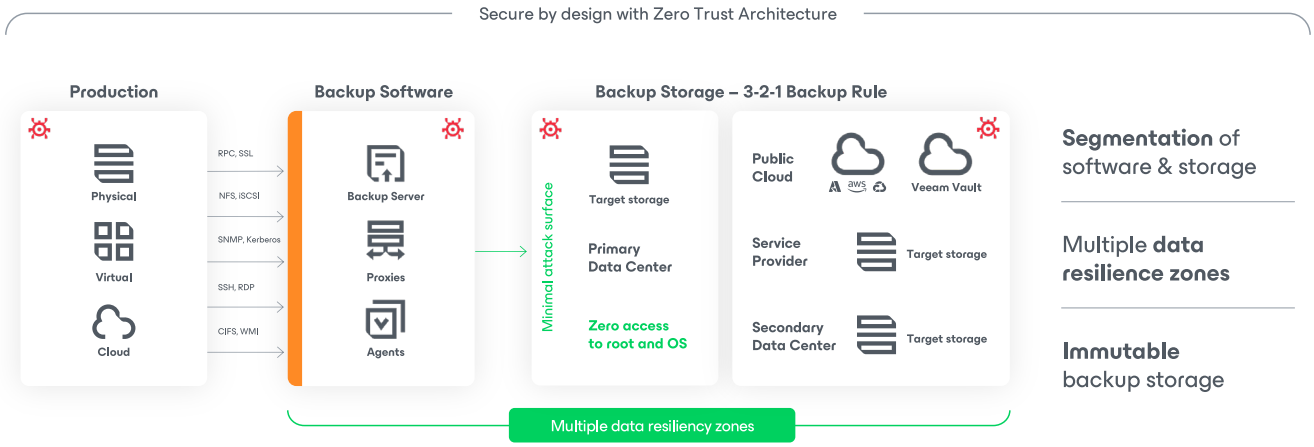


What About My Workloads in the Cloud?

Cloud platforms and data residing in the cloud is still the organization's responsibility to secure, manage, access, and protect. Cloud providers manage high availability and uptime for their cloud services, but all data and access adhere to a shared responsibility model. Therefore, data control and protection falls under the customers' responsibility. But cloud and PaaS platforms don't always allow customers to employ existing legacy protection scenarios like those used on-premises. They also don't provide the same level of access to hypervisors, APIs, networks, or integration to cloud-native apps. Additionally, you need to contend with obstacles like network throttling, egress costs, API call costs, and limited deployment options. First-party cloud protection options from hyperscalers, while available, can also end up costing a lot more through the lack of features they have. For example, they lack important features like in-built deduplication or compression, the flexibility to leverage cheaper cloud backup storage, and the agility to run backup schedules that are in line with application-specific recovery point objectives (RPOs) or internal business requirements.

The good news is, Veeam fully supports the native data protection practices mentioned above in the cloud and on-premises, including multiple cloud resilience zones due to Veeam's flexible building block approach. We can also do this in an extremely cost-effective manner, thanks to components like ephemeral workers, which can be spun up and down on-demand. This process avoids the risk of having a heavy backup infrastructure just sitting around consuming compute costs and allows customers to choose the most cost-effective location to store their backups in. Our cloud-native approach keeps within Veeam's mantra of simple, native protection for cloud workloads that offers the flexibility to achieve a zero-trust framework that reduces the blast radius of cyberattacks from within production. This empowers you to protect your last line of defense from internal/external threats at a much lower price point, ensuring recovery when and where you need it.

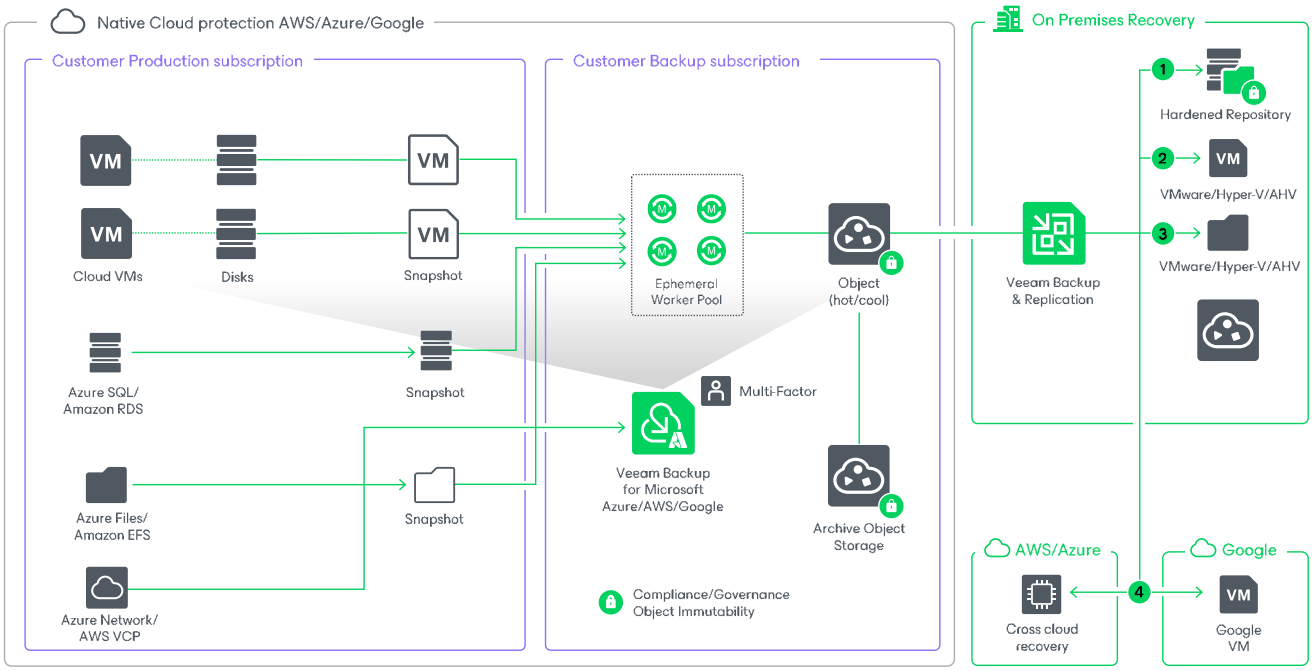
Veeam's data freedom approach also allows users to recover to other clouds or back on-premises. If the worst should happen, this also gives customers additional resiliency options if they need to draw on Plan B, or C from a recovery platform or cloud perspective.



We do this via separate backup subscriptions inside customer cloud accounts that can help provide the same level of native protection for hybrid workloads. Additionally, customer data will never leave a customer's secure network boundary while providing full end-to-end backup encryption, compression, and deduplication. This can result in you saving 50% or more in storage space when compared to native cloud backup solutions while leveraging much cheaper storage tiers.

In addition, Veeam provides full data freedom, so your workloads can be recovered cross-platform, cross-cloud, or to a different cloud ecosystem altogether. Again, this includes providing different resiliency domains to isolate backups from production credentials and networks and providing full immutability, MFA, and recovery testing wherever and whenever you need to run it.

Hybrid Cloud Multi-layer protection support



Veeam Support for Essential Eight Maturity Levels

Prevent attacks

- Patch application
- Application control
- User application hardening
- Configure MS office Macro settings

Limit Impact of cyber attacks

- Patch operating systems vulnerabilities
- Restrict admin access
- Implement multi-factor authentication (MFA)

Data recovery and system availability

- Daily backups

The Essential Eight, a joint effort of both the Australian Cyber Security Centre (ASCS) and Australian Signals Directorate (ASD), is a framework that agencies and other organizations can adhere to via different maturity levels. Following this framework helps bolster and harden both Government ICT and other critical infrastructure systems.

This covers three main components:

- Attack prevention
- Limiting the impact of cyberattacks
- Data recovery and system availability

Veeam Data Platform, while allowing for full Essential Eight maturity level 2 or 3 backup support, also allows organizations to raise their maturity levels within other parts of the Essential Eight.

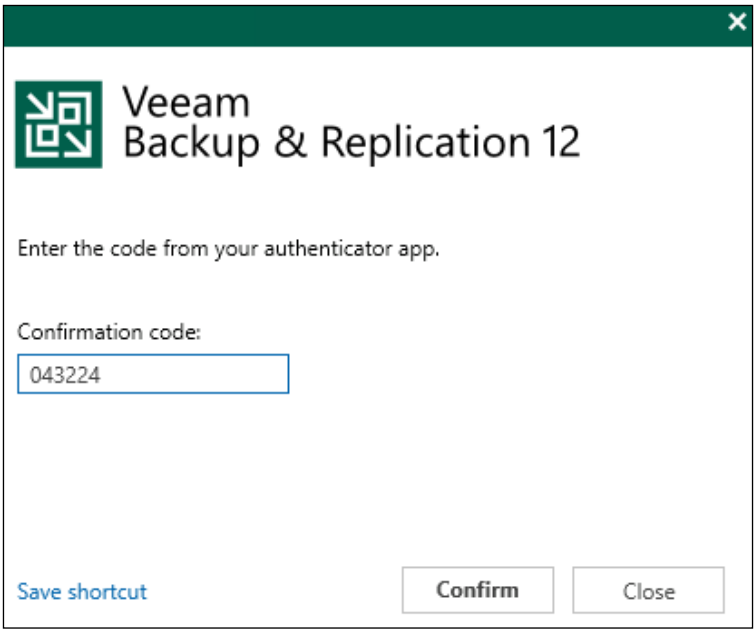
Essential Eight Maturity Level Three Capability	Status	Details
MFA	✔	Veeam amplifies your security posture with robust MFA capabilities into consoles, including self-service user web-based portals. This creates an added barrier against credential compromise and enhances your defense-in-depth strategy to reduce the attack vector of the backup applications you have in use, as well as self-service restore MFA support for end users.
Patch Applications and Operating Systems	✔	Veeam's proprietary capability enables a proactive approach to patch management by creating secure, isolated environments and leveraging backup data to create sandboxes. This allows complete application ecosystems to mirror production workloads and assist with patch management. By scanning these workloads and applications within a sandbox with third-party antivirus tools, organizations can identify dormant threats in their backups before recovering systems back into production. This "Shift-Left" approach also allows IT teams to preemptively mitigate vulnerabilities and system instabilities and enables resilient operations in an era of increasing cybersecurity threats
Restrict Admin Privileges	✔	Veeam employs a principle of least privilege model with its role-based access control (RBAC), allowing for non-backup admins to see, protect, and recover what belongs to them. Accomplished through a HTTPS web portal, this restricts access to backup consoles, mitigates insider threats, and enhances governance by restricting high-level privileges to the minimum necessary for to perform a task. Veeam also supports and recommends having backup infrastructures and repositories in separate resiliency zones to protect against production domain admin or other credential leaks. Additionally, Veeam offers four-eyes authorization to force secondary security confirmation for potentially disastrous events within the backup platform, preventing malicious attempts to cripple recovery from within your backup platform.

Essential Eight Maturity Level Three Capability	Status	Details
Regular Backups	✔	Veeam's backup solutions empower organizations with automated, scheduled, and routine application-aware backups and DR workload replication. This drives operational continuity and data integrity across hybrid cloud and PaaS/SaaS workloads by aligning to extremely granular per-application RPOs. The solutions validate the success of your backups as desired, providing IT leaders with confidence in the integrity of their digital assets. This is augmented with powerful monitoring, reporting, and dashboards that can help you ensure compliance is met. This includes schedulable DR failover orchestration and non-disruptive recovery testing at-scale, always leveraging production identical data. As part of recovery testing, additional scanning for dormant threats residing in backups/replicas is possible via YARA rules or third-party antivirus software.
Backups of Important Data, Software, and Configuration Settings are Retained in a Secure and Resilient Manner	✔	Veeam provides a secure and encrypted mechanism to protect its configuration and backups can be scheduled and written directly to an offsite location. Veeam also fully supports ISM-compliant and industry-standard in-flight and at-rest encryption and immutable storage. This includes common industry standards like S3 Object Lock across both AWS S3 and S3-compatible storage as well as Microsoft Azure Blob immutability. These options offer tight configuration and retention based on individual requirement settings per application. As an additional safety net to protect against ransomware or malicious insiders, Veeam also offers Linux-based immutability via a hardened repository for immutability that goes everywhere. Veeam also supports proprietary immutability provided by storage snapshot providers and enterprise deduplication appliances by Dell and HPE. Additionally, Veeam includes SIEM log parsing to enterprise SIEM tools for security events, and integrates with logging tools such as Splunk, Azure Sentinel, or any SIEM tool that leverages RFC 2454, enabling enterprise security event monitoring.

Essential Eight Auditing and Remediation to Raise Maturity Levels

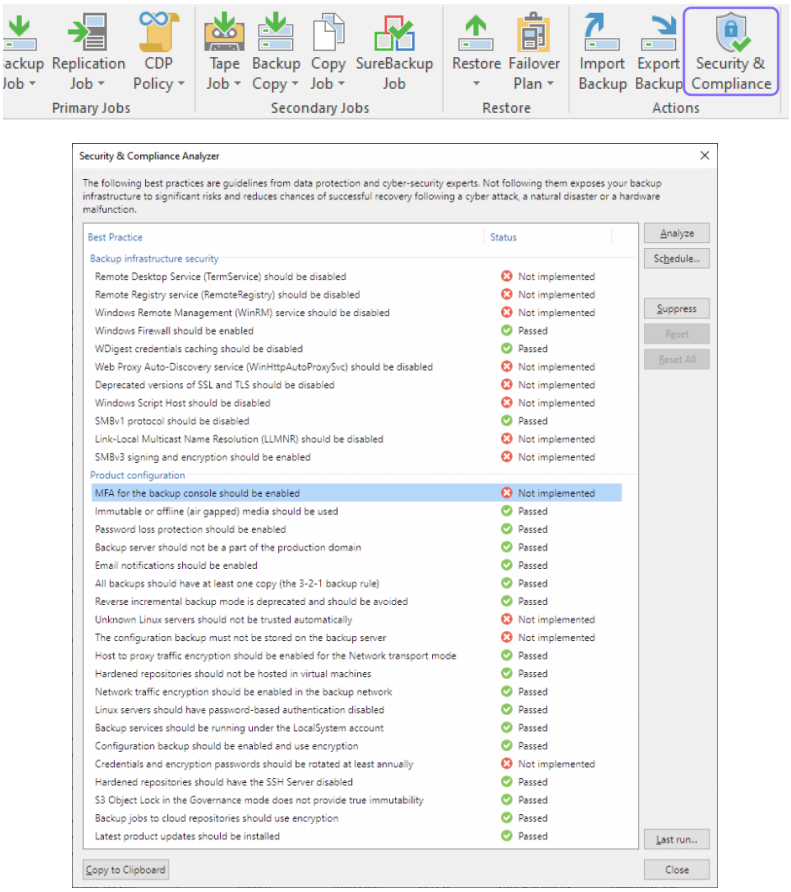
Essential Eight audits are often considered a difficult task. It can take weeks of triage, and often consists of clicking on each job to check configurations like retention settings, finding reports that tell you what workloads are protected, or what workload backups are or are not immutable. During Essential Eight audits, backup administrators can be burdened for weeks while trying to prove compliance. When applicable, remediation efforts and hardening recommendations can take equally as long to put in place. Good news is, Veeam makes it easy to check what your security posture is within your backup and data recovery environment at a glance. A more extensive list of configurable compliance-based reports is also available, enabling customers to ease their audit process.

This process starts with logging onto your backup server using MFA. The Veeam console supports mobile authenticator apps that adhere to time-based one-time passwords (TOTP) as per RFC 6238. Example applications include Microsoft Authenticator, Google Authenticator, DUO, and others.



Security and Compliance Analyzer

Once you authenticate into the backup server, you'll see that the security and compliance analyzer is built into the Veeam Backup Console UI v12, which is an isolated, schedulable, and reportable service to ensure you have an at-a-glance view of your data recovery and backup environment's current security posture. Additionally, this console provides a guide for admins and security teams to see what can be implemented to ensure industry best practices are maintained over time and achieve greater adherence to security and compliance frameworks. No internet connectivity to the outside world is required, so the solution is also suitable for dark or isolated sites.



This will provide an immediate snapshot of your data protection platform in seconds, ensuring you are meeting many of the Essential Eight mandates and industry best practices like:

- MFA to the backup console
- Deployed immutable backup targets
- Applied applications and updates
- Enabled in-flight and at-rest encryption for backups and configuration backups
- Potential security vulnerabilities are turned off, like depreciated unsecure protocols
- Remote registry and SSL that's disabled to the backup infrastructure
- And many others!

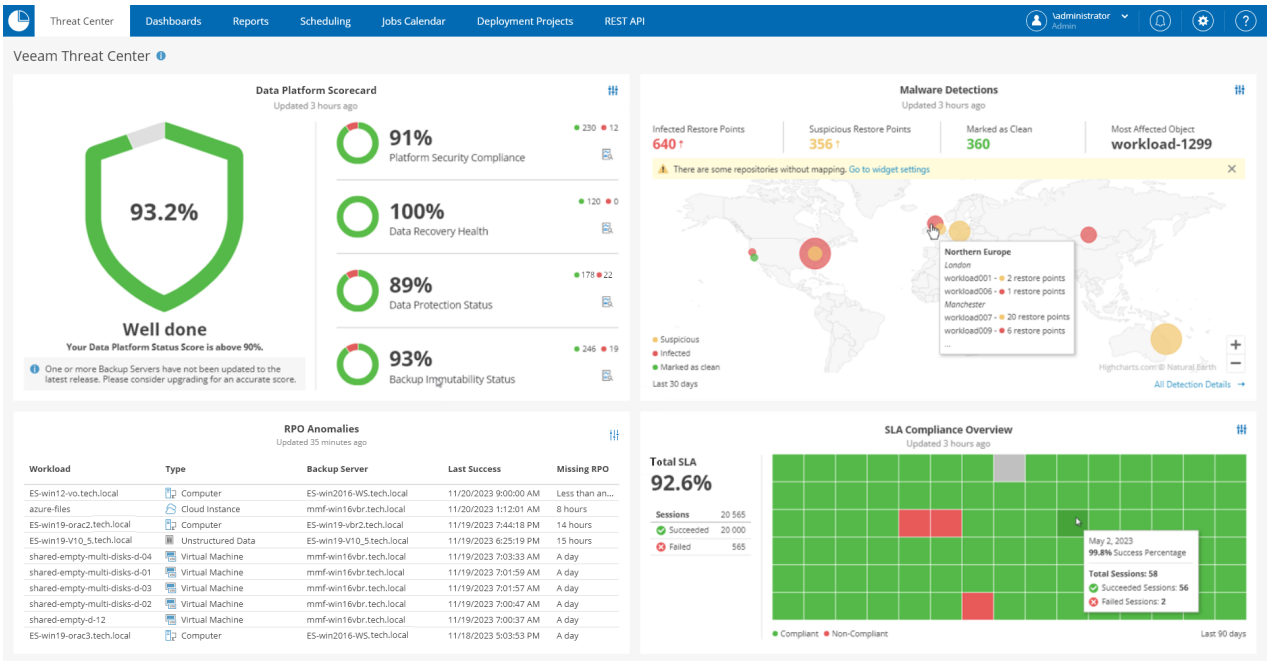
Enhancements and additions are continually being delivered to the analyzer with each new release. These enhancements can be activated when applicable, but events can also be suppressed if they are not applicable. When an event is suppressed, detailed information is captured so administrators can review who made the change and when that change was implemented.

Veeam Threat Center

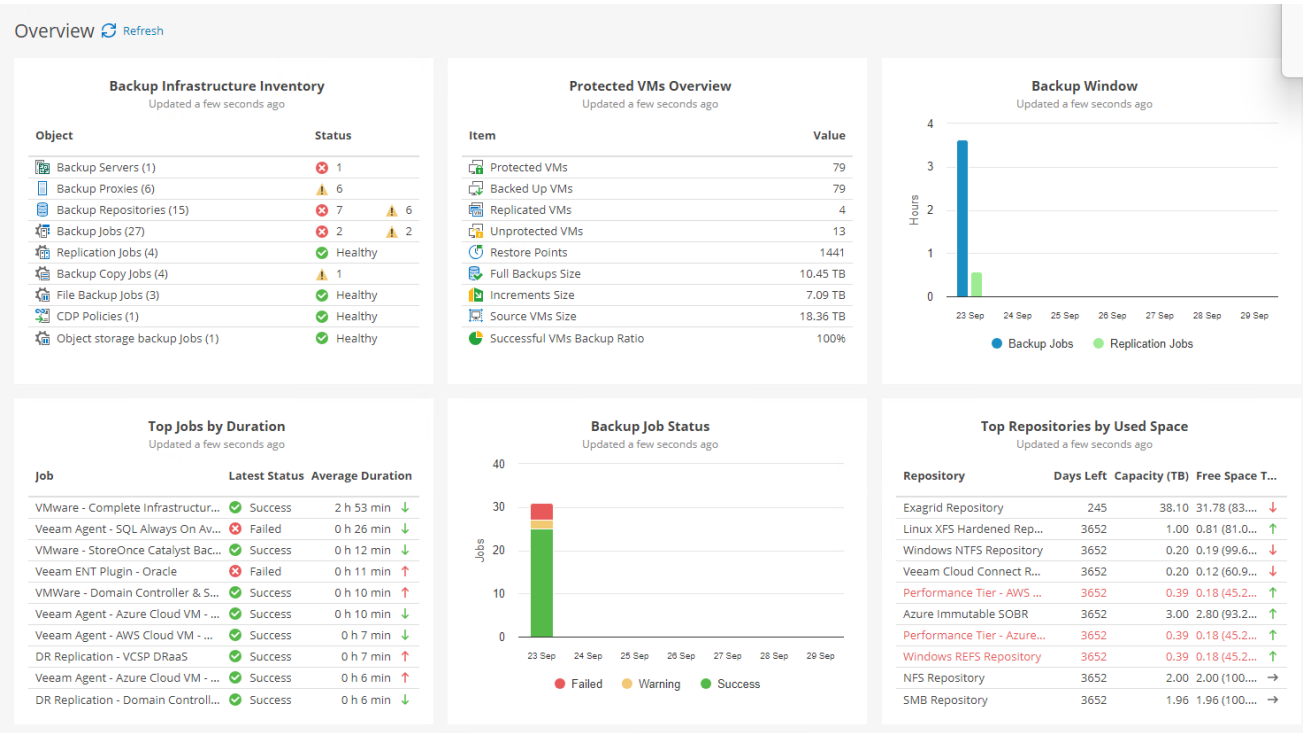
This is an extremely powerful addition to V12 and is offered as a part of Veeam Data Platform Advanced and Premium editions, delivering critical information at-a-glance. This features covers the workloads that are or are not leveraging immutable backups, what workloads are violating your data protection rules or recovery SLAs, and disclosing potentially infected workloads sitting in your backups.

Infected restore point data is generated via multiple methods, including:

- Inline entropy scans during backup
- File system activity analysis
- Rule-based YARA detection
- Antivirus scans
- Integrations with third party XDR/MDR solutions (like those from Sophos, Cisco, or Palo Alto)
- Veeam Recovery Orchestrator SLA compliance for recovery and failover testing



A direct link into Veeam ONE's customizable dashboard provides key metrics like protected and unprotected virtual machines (VMs), whether your pre-defined backup windows are being met, and projected repository capacity growth that's based on analytics and historical data.



Veeam ONE provides over 300+ predefined, customizable reports and alerts and integrates into ServiceNow service management to allow for remediation automation.

Veeam Recon Scanner

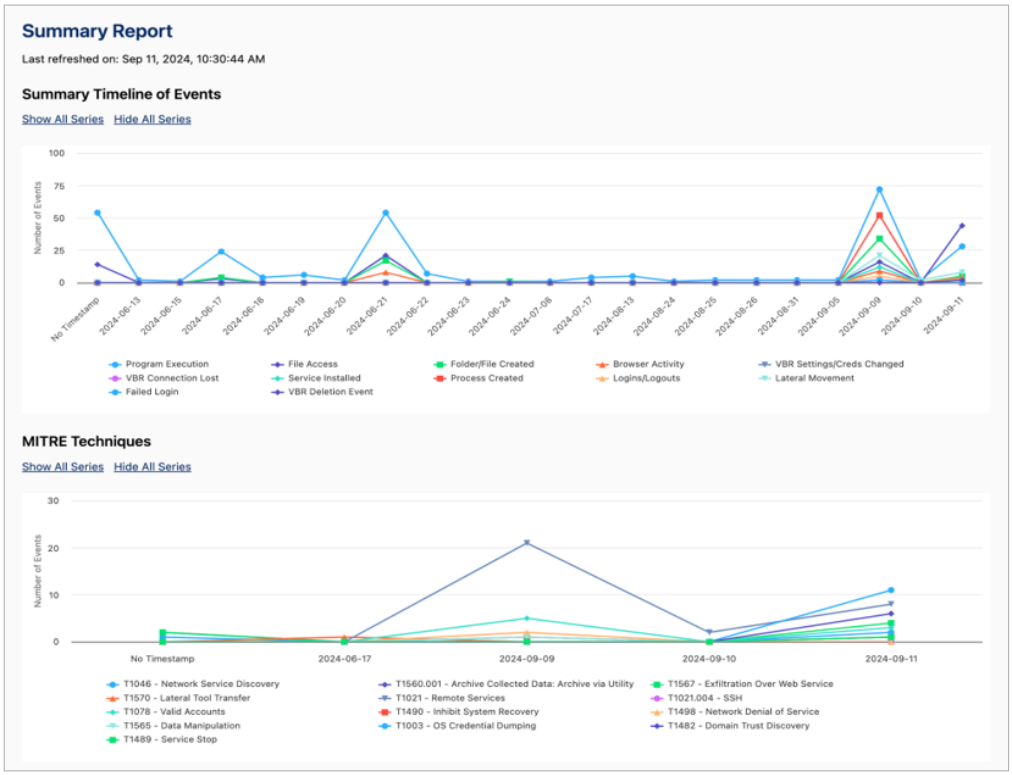
As over 93% of ransomware attacks are now targeting backup infrastructure, building on Veeam's innovative data resilience offerings from Veeam Cyber Secure to TTP Analysis , we have now added in Veeam Recon Scanner technology to the Veeam Data Platform for deep forensic analysis across the backup infrastructure.

Coveware by Veeam, is the leader in cyber-extortion incident response with best-in-class ransomware assessment, negotiation, and recovery capabilities through patent-pending technology and expert services, brings us the Recon Scanner. It is a groundbreaking addition to the Veeam Data Platform, leveraging technology used in thousands of ransomware incidents and boasting an extensive database of such incidents.

Now, we're bringing this technology, honed over years of combating ransomware, to every Veeam Data Platform Premium deployment. This technology is designed to identify, help triage, and prevent cyberattacks and direct attacks across the backup environment.

Imagine being able to spot potential cyberattacks before they happen! With the Recon Scanner, this is now a reality. By collecting and analysing data proactively, the Recon Scanner can identify unexpected network connections, unusual user behavior, suspicious file activity, data exfiltration attempts, and even potential brute force attacks on the backup infrastructure inline with the MITRE ATT&CK framework.

The unpredictability of dwell time — the period between compromise and attack — makes traditional threat detection and mitigation challenging. That's why we're integrating the Recon Scanner with the Veeam Data Platform, using technology and years of experience assisting organisations respond to cyberattacks to not only combat cyber threats early, but to also assist with internal and government led forensics of compromised systems.



High Findings from Sep 11, 2024, 10:21:36 AM

Sep 11, 2024, 12:16:41 PM	APP-01	Program Execution (T1003)	C:\Users\vagrant\Downloads\t\mimikatz-master\mimikatz-master\x64\mimikatz.exe **User:** vagrant	8
Sep 11, 2024, 12:17:40 PM	APP-01	File Access (T1003)	C:\Users\vagrant\Downloads\t\mimikatz-master\mimikatz-master\x64\2.txt Show File Details	8
Sep 11, 2024, 12:18:51 PM	APP-01	File Access (T1482)	C:\Users\vagrant\Downloads\t\AdFind\AdFind.exe Show File Details	7
Sep 11, 2024, 12:18:52 PM	APP-01	File Access (T1482)	This PC\{088E3905-0323-4B02-9826-5D99428E115F}\t\AdFind **User:** vagrant	7
Sep 11, 2024, 12:19:29 PM	APP-01	File Access (T1482)	C:\Users\vagrant\AppData\Roaming\Microsoft\Windows\Recent\AdFind.lnk	7
Sep 11, 2024, 12:19:29 PM	APP-01	File Access (T1482)	C:\Users\vagrant\Downloads\t\AdFind\password.txt Show File Details	7
Sep 11, 2024, 12:19:35 PM	APP-01	Program Execution (T1482)	C:\Users\vagrant\Downloads\t\AdFind\AdFind.exe **User:** vagrant	7
Sep 11, 2024, 12:53:13 PM	APP-01	Browser Activity (T1567)	temp.sh Visit Count: 2 (Source: \\?\C:\Users\vagrant\AppData\Local\Microsoft\Edge\User Data\Default\History)	8
Sep 11, 2024, 12:53:21 PM	APP-01	File Access (T1567)	C:\Users\vagrant\Downloads\MEGAsyncSetup64.exe Show File Details	8

Orchestration and Essential Eight Recovery Testing Made Simple

Veeam pioneered non-disruptive testing for backups and DR recoveries over nine years ago, with Veeam's in-built DataLabs, SureBackup, and SureReplica that allow for schedulable recovery testing for backups and replicas inside a pre-defined, isolated sandbox on any vSphere or Hyper-V host. This feature alone provides other Essential Eight benefits, including:

- **Application and OS patch testing** uses production-identical systems for more accurate testing on production systems as of the last backup.
- **Veeam Data Integration API**, Veeam Backup & Replication PowerShell module subset. This presents Veeam backup(s) as block storage mounts for filesystems, log-level interrogations, and triages from cyberattacks.
- **Off-production UAT testing** for development and testing.

Over time, Veeam also built many additional functionalities into this process, such as:

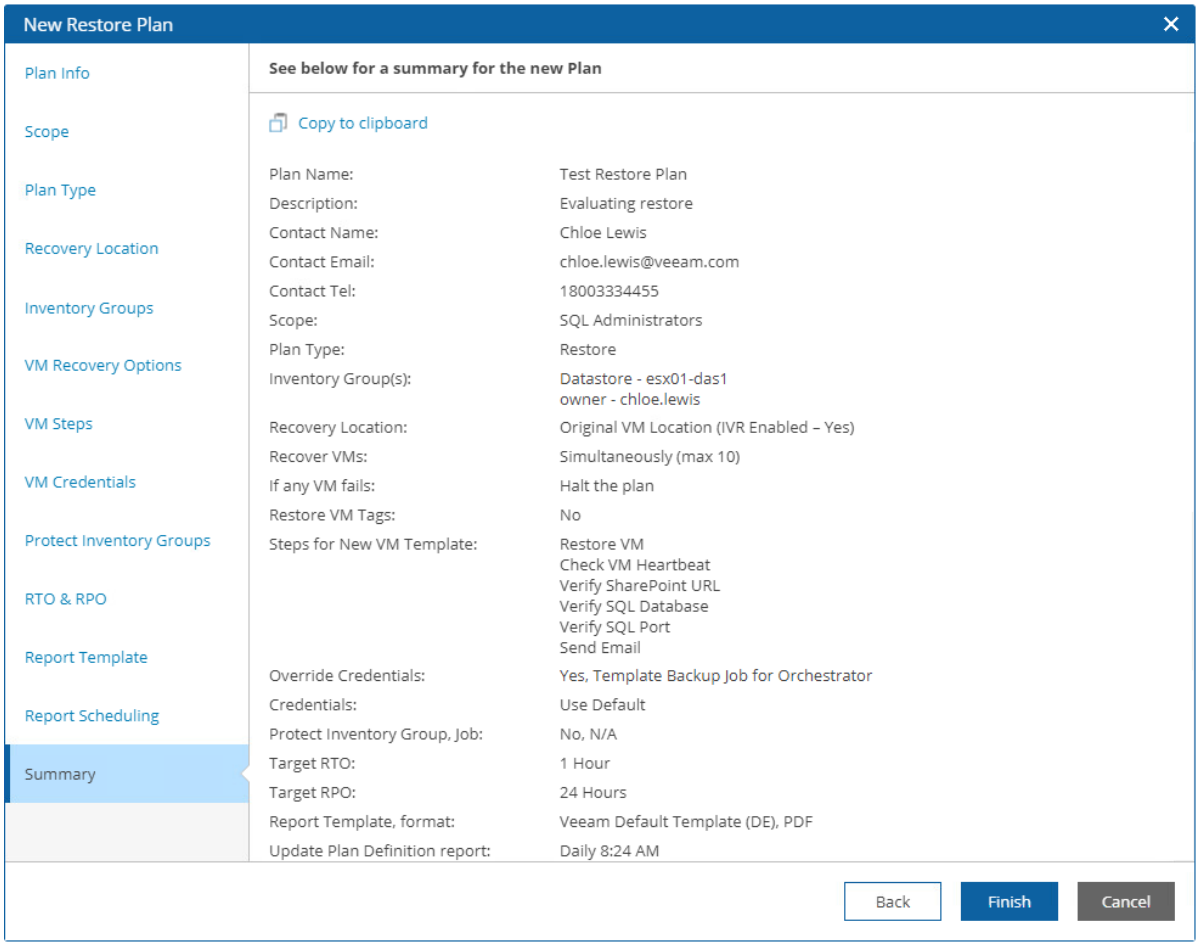
- **Full recoverability testing.** Veeam Backup & Replication runs machines in an isolated sandbox via Veeam DataLabs directly from backups and performs tests against production-identical applications. This mode ensures the recoverability of your production workloads in a DR event.
- **Backup verification and content scans only.** Veeam Backup & Replication performs backup integrity checks and content analysis to detect traces of malware or any other unwanted or sensitive data. These tests do not require you to set up a virtual lab or application group.
- Available via Veeam Data Platform Premium licensing is orchestrated testing at scale via Veeam Recovery Orchestrator.

Providing simple, non-disruptive Essential Eight recovery and DR failover testing, Orchestrator extends the functionality of Veeam Data Platform by orchestrating traditional manual recovery processes with one-click recovery plans for mission-critical applications. This includes rich features for dynamic DR documentation handling and testing for applications that are mapped to specific recovery time objectives (RTOs) and RPOs.

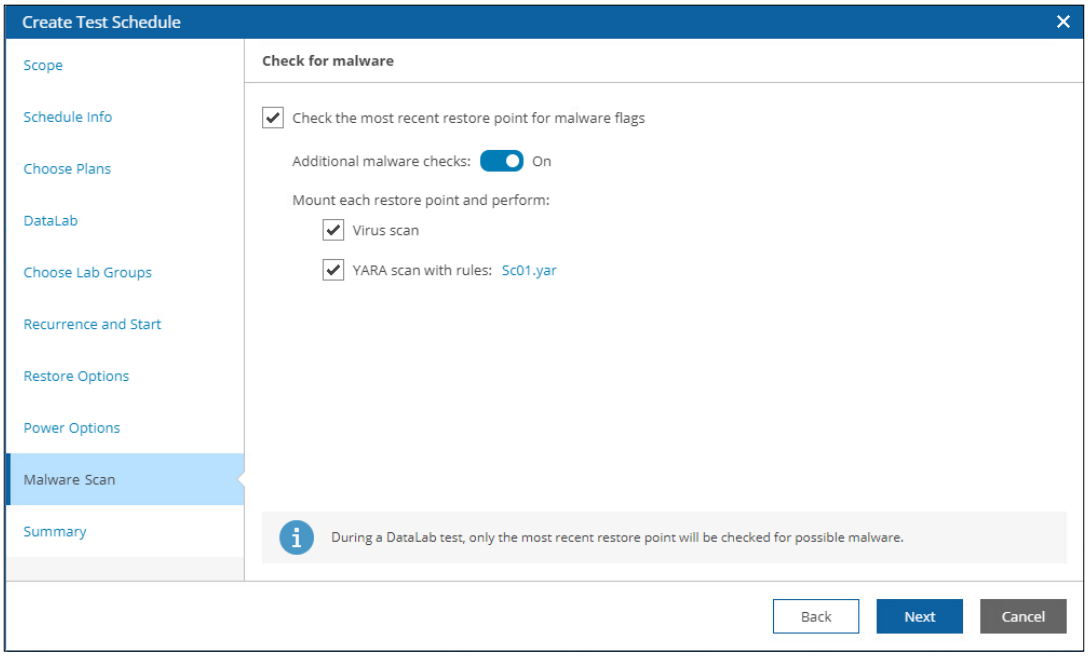
Orchestrator leverages the recovery capabilities of Veeam Backup & Replication to build straightforward DR workflows, automate recovery processes, and eliminate error-prone manual steps. Orchestrator also provides reporting capabilities that let enterprises document their DR plans to meet industry compliance requirements for critical infrastructure and Essential Eight maturity levels.

With Orchestrator, you can:

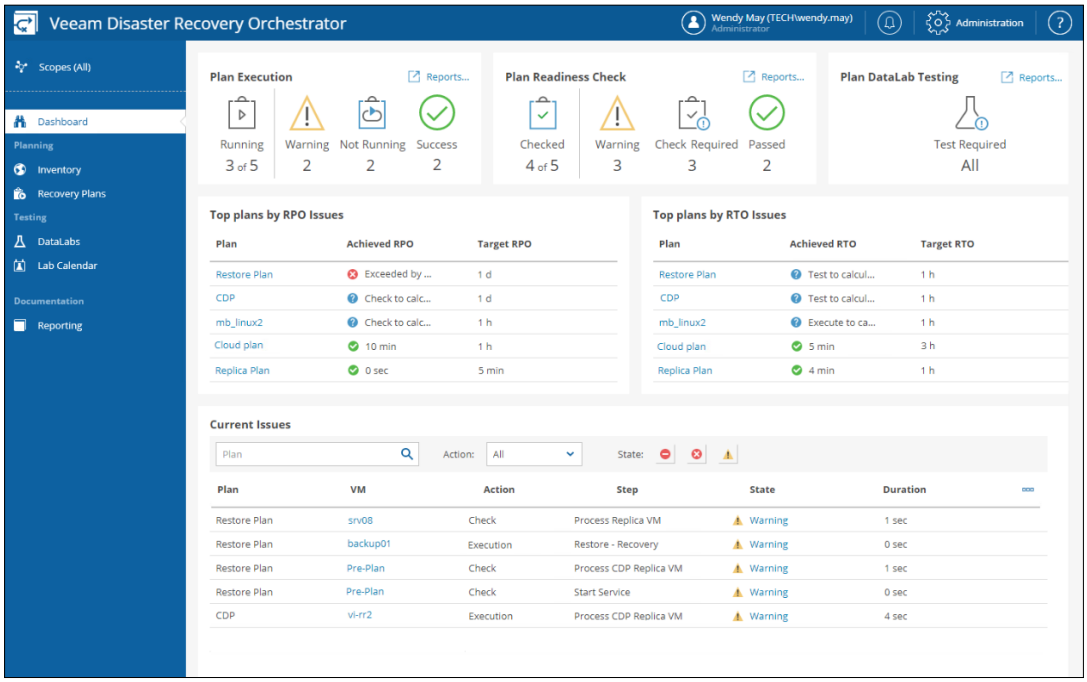
- **Orchestrate recovery.** Create simple or complex workflows to orchestrate recovery operations for both virtual and physical machines to VMware vSphere and customer's internal Microsoft Azure environments.
- **Automate simple to complex checks and tests.** Schedule checks and tests to automate the verification of your recovery plans, with features such as isolated test labs and comprehensive readiness checks at each phase.
- **Meet Essential Eight compliance requirements for backup and failover testing.** View RPO and RTO achievements on the dashboard and generate automatically updated reports for recovery plan checks, tests, and executions. This feature helps ensure that requirements for compliance and audits are met.



Recovery plans are easy to set up via Orchestrator's wizard-based approach and are not disruptive to production.

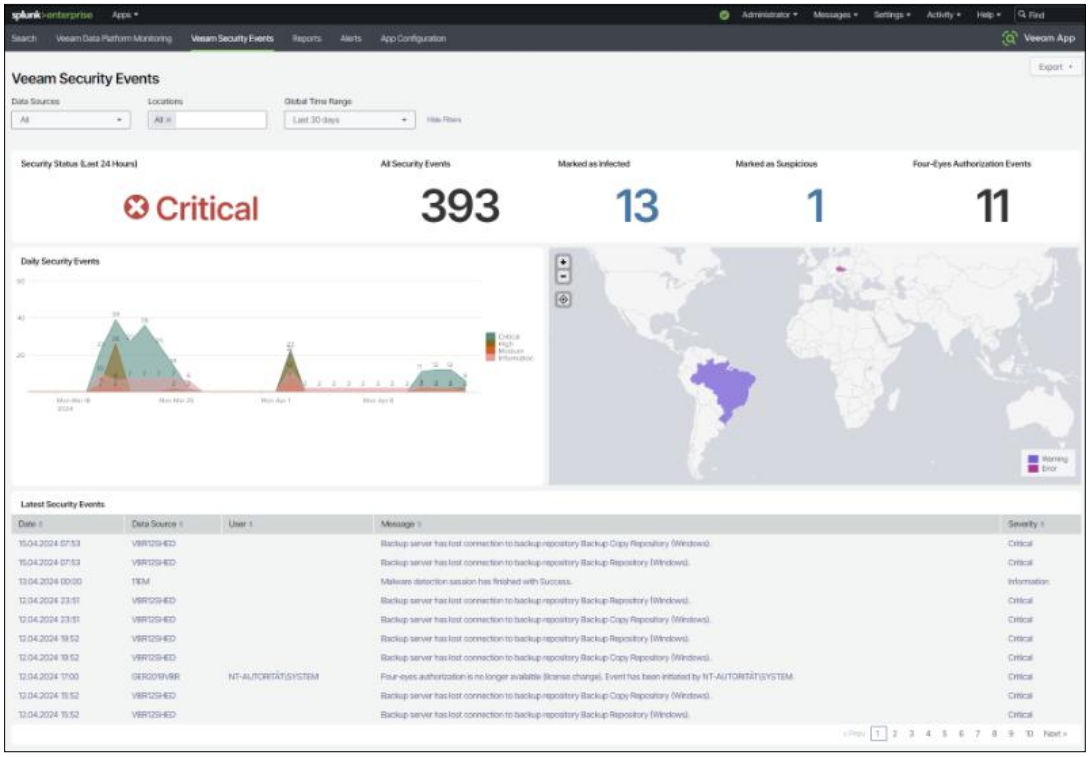


All recovery and failover plans include the ability to verify and check for malware via YARA rules or third-party anti-malware platforms.



To help with ongoing recovery testing efforts, Orchestrator provides feature-rich dashboards and reports to enable simple maintenance on recovery plans, in line with pre-defined RPOs and RTOs. This helps ensure compliance, and issues are resolved before they need to be actioned in production.

Syslog output allows for additional Syslog integrations into enterprise SIEM platforms. Veeam App for Splunk can parse and capture important Veeam security events into existing log management and alerting platforms.



Veeam's Cyber Secure Program

As a part of Veeam Data Platform v12, Veeam announced the Cyber Secure Program, which is an optional add-on to Veeam Data Platform Premium edition. This program protects customers against ransomware threats and provides a 24.7.365 SWAT team and proactive incident hardening analysis. Veeam's incident response team provides 1:1 best practice training for our customers under this program to proactively plan a robust incident response blueprint.

Backed by experienced cybersecurity experts and an industry-leading ransomware warranty, Veeam is unique in the market with how complete its enterprise data resilience is, period.

REACTIVE Incident Response Service

Assessment

- Understand Client Impact
- Identify Ransomware
- Identify Threat Actor Group
- Provide Data on Threat Actor

Settlement

- 100% Transparency
- Payment Facilitation
- Compliance Checks
- Documentation/Attestation

Negotiation

- Secure & Safe Negotiations
- Transparency
- Risk & Outcome Analysis
- 24/7/365 Coverage

End Downtime

- Recovery Support Tools
- Post Incident Documentation
- Insurance Documentation
- Industry Expert Support

Veeam's reactive incident response service is hyper-focused on providing best-in-class assistance and support to victims of ransomware and cyber extortion attacks. With a database of thousands of cyber incident data, Veeam's incident response team can assist with:

Assessment: Assessing the overall impact, identifying the ransomware and threat actor involved, and forecasting possible outcomes based on historical case data and real time data collection through our recon agent.

Negotiation: Secure and transparent negotiations with data-driven tactics and strategy performed by incident response experts to work toward agreed-upon deliverables and outcomes.

Settlement: If necessary, facilitating cryptocurrency acquisition and all necessary compliance checks and documentation, including delivery to the threat actor in exchange for negotiated deliverables. This is a $0 profit business model, as the only cost to the victim from Veeam is the cost of the cryptocurrency acquisition.

Veeam Cyber Secure: Proactive Protection, Swift Response, and Comprehensive Recovery

In today's digital landscape, it's vital to prepare for cybersecurity attacks since you're bound to face one at some point. Having the right planning and safety nets in place early will lead to a much better outcome since it can minimize the damage blast radius and provide much faster and cheaper business continuity. With the right strategy in place, organizations can stay ahead of attackers and recover quickly if the worst happens. Veeam offers a suite of robust services that are designed to protect your business before, during, and after a ransomware attack.

Before a Ransomware Attack: Building a Strong Defense

Advanced Onboarding Support

Veeam provides a personalized onboarding experience to ensure that your backup and security strategy has a proper start. Whether your data infrastructure is large or small, our team of experts can help you set up the foundation you need to stay protected.

Architectural Design and Implementation Services

Every organization's DR requirements and infrastructures are unique. Veeam experts work with you to define your architectural design and offer implementation services for that design so your Veeam Data Platform environment is deployed according to best practices.

Quarterly Security Assessments

Your infrastructure and user base evolve as Veeam Data Platform continues to improve with new features, including security capabilities and enhancements. Veeam conducts quarterly security assessments to ensure your environment remains up-to-date with the latest protection measures. These assessments help identify any potential gaps in your defenses to enable swift remediation. These assessments cover a lengthy checklist of recommendations.

Priority Incident Routing by Veeam's SWAT Team

With Veeam Cyber Secure, Veeam offers priority incident routing to ensure our specialized SWAT team and a dedicated support account manager can address your issue without delay. This means faster response times and increased peace of mind.

Personalized Training and TTP Analysis

Cyberattacks evolve constantly, and staying informed is key to staying protected. Veeam provides personalized training, including quarterly updates for the latest techniques, techniques, and procedures (TTPs). This equips your team with the knowledge to recognize and respond to new and emerging threats.

During a Ransomware Attack: Swift Incident Response

If a ransomware attack does occur, having the experts on your side is crucial to minimizing damage and downtime. Veeam offers 24.7.365 expert incident response to manage the situation quickly and effectively.

24.7.365 Incident Response with a 15-Minute Response SLA

When minutes matter, Veeam Incident response experts provide around-the-clock support with a 15-minute response SLA. This ensures that your business can receive expert support when needed by reacting immediately to the attack.

Patent-pending Assessment Technology

Veeam's innovative, patent-pending technology provides a rapid assessment for your systems during an attack, giving you clear insights into the extent of the breach, encryption information, and even the threat actor group. All this information and our experience in thousands of cases allows us to have enough information to forecast resolution and start negotiations.

Negotiation, Settlement, and Decryption Services

Should the need arise, Veeam's expert team can assist with negotiating with attackers, managing settlements, and facilitating the decryption process to ensure that your organization recovers as quickly as possible. Expert negotiations on cybercrimes work with you step-by-step to gather information and make informed decisions.

After a Ransomware Attack: Recovery and Documentation

Recovering from a ransomware attack is a multi-step process, and Veeam ensures your business can bounce back stronger.

Ransomware Recovery Warranty for Up to $5 Million

Veeam stands behind Veeam Data Platform and its services by offering a ransomware recovery warranty of up to $5 million. This provides financial assurance and reinforces Veeam's commitment to your recovery.

Post-incident and Insurance Documentation

After an attack, having detailed post-incident documentation is vital for both recovery and cyber insurance claims. Veeam provides comprehensive documentation to help you navigate the post-incident process with ease, ensure compliance, and support necessary insurance claims if required.

With Veeam Cyber Secure ransomware preparedness and recovery services, you can safeguard your organization before an attack, respond swiftly during an incident, and recover confidently afterward. Let Veeam help you stay resilient in the face of growing cyberthreats, since when it comes to ransomware, preparation is the best protection.

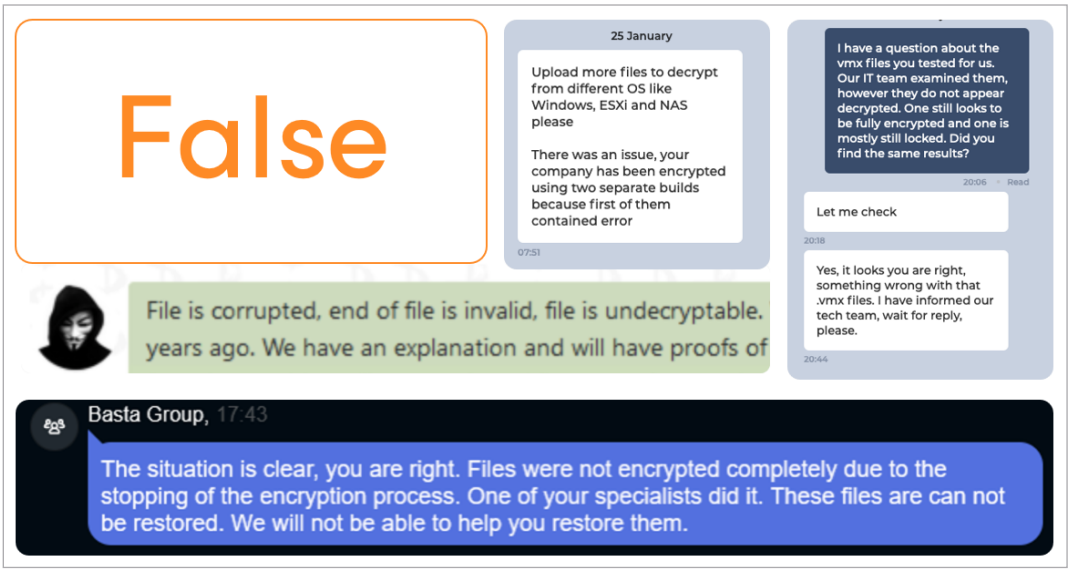
The Australian Signals Directorate and Australian Cyber Security Centre have advised users to never pay a ransom, as there is no guarantee your data will be recovered and not sold to the dark web. Rather, it's recommended that you engage professionals to ensure the fastest recovery and lowest impact of a cyberattack or data leak. Don't assume that threat actors will store your data securely, be able to decrypt it, or delete it once a ransom is paid.

End downtime. Whether the encryption is vulnerable to "cracking" or we receive a decryption key from a threat actor, our teams and tooling will assist your organization to recover encrypted data in a safe, secure, and performant manner if recoveries or decryption are unavailable.

Myth: Threat Actor's handle, store and delete files properly.

Myth: Threat Actor's will credibly delete any stolen data.

Myth: Threat Actor's decryptor is the fastest and best recovery option.



Don't assume that threat actors will store your data securely, be able to decrypt it, or delete it once a ransom is paid.

End downtime

Whether the encryption is vulnerable to "cracking" or we receive a decryption key from a threat actor, our teams and tooling will assist your organization to recover encrypted data in a safe, secure, and performant manner if recoveries or decryption are unavailable.

Veeam 2024 Ransomware Trends Report

To stay on top of industry trends and be a leading force against ransomware and cyberthreats, Veeam commissioned independent analysts or research firms eight times over the past 10 years to produce an industry report on the evolving data protection landscape. This report aims to affect product strategy as well as help the market be better informed.

The latest report, sanctioned in 2024, covers the opinions of 1,200 unbiased global organizations on a variety of data protection trends, with the most notable insights being:

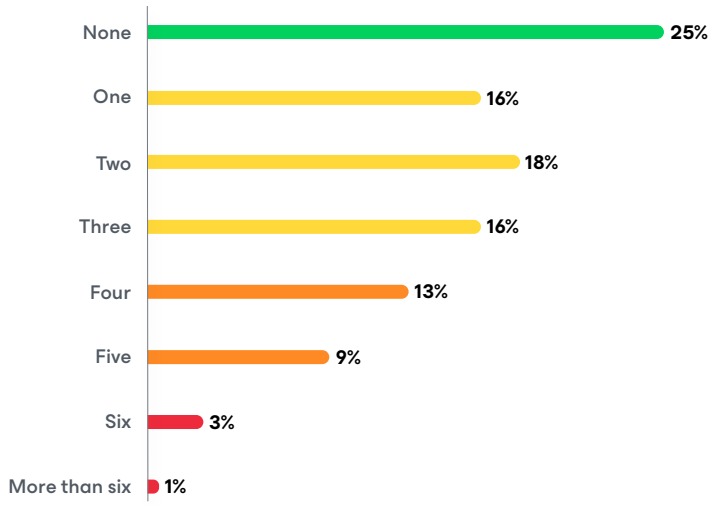
- **Reliability and consistency** for protecting IaaS and SaaS protection alongside datacenter servers are the key drivers for improving data protection in 2024.
- **Ransomware** is both the most common and most impactful cause of outages, but in many cases, insider or user error is the cause of many affected outages too.
- **Cloud-based services** seem nearly inevitable for organizations of all sizes. But, just like how there isn't just one type of production cloud, storage, OS, or application ecosystem, there isn't always one protection scenario either. Veeam allows customers to choose the right tool for the job.

Since 2019, consistent data analysis by analysts formerly at Gartner and ESG were added to the report to enable year-over-year comparisons and statistically defensible regional, vertical, and segment analyses. These research endeavors were conducted using "double-blind" surveys, where the research firms' respondents were unaware of who was seeking the data. Additionally, Veeam had no visibility or effect on who responded to the survey, beyond defining the target persona of an IT leader or implementer that's responsible for data protection strategies within their organization. Some of the most insightful statistics pulled out of the survey are listed below:

Cyberattacks are more common than you think. Out of the 1,200 organizations surveyed, 25% reported that they had not suffered a cyberattack in 2023, but a staggering 60% reported two or more cyberattacks in the calendar year of 2023. With long dwell times and dormant malware now being the norm, these may indicate that the environment had already been infected, but an attack hadn't started yet.

75% suffered ransomware attacks in 2023

How many ransomware attacks has your organization suffered in the last 12 months?



Large-scale recoveries can take a long time. Organizations also reported major recoveries of more than 50% of their environment, 32% reported that a large-scale recovery would take less than five days, and 63% reported that a large-scale recovery would take between six to fourteen days, and 5% reported a large-scale recovery RTO of 15–28 days.

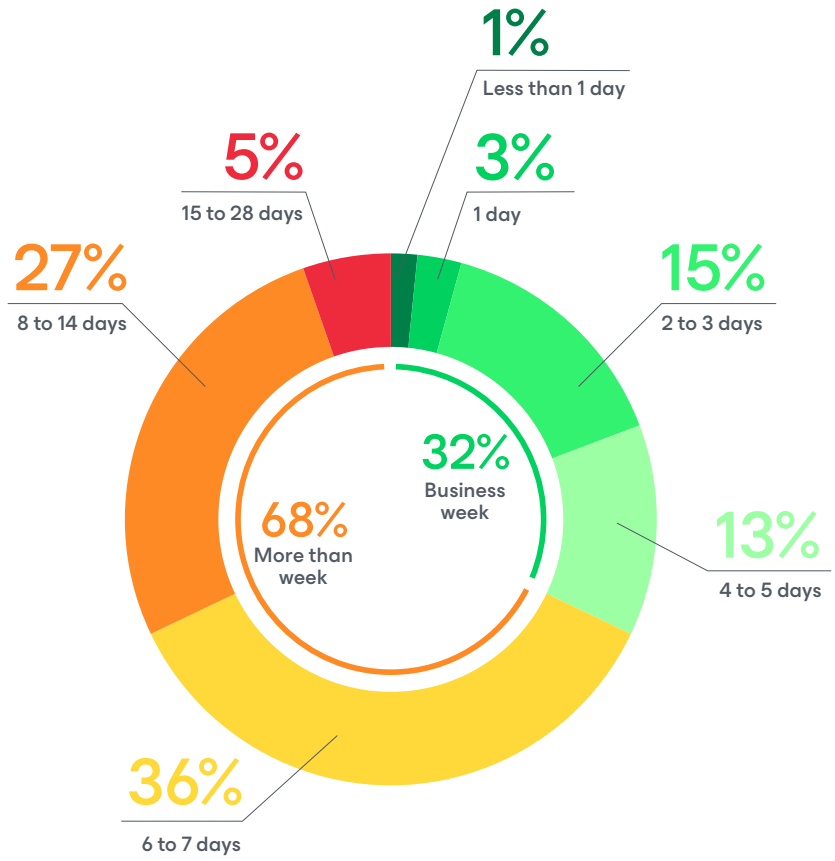
Closer to home, according to The Office of the Australian Information Commissioner (OAIC), government systems were the second-most breached sector in Australia over the first six months of 2024, with 63 incidents reported in total. As reported by the OAIC, most breaches — around 87 percent took more than 30 days to identify. The healthcare industry still retains the top spot as the most-hit sector, with 102 breaches.

Overall, 354 malicious or criminal attacks were reported, equating to 67 percent of all reported breaches. More than half of these were cyber security incidents.

In the OAIC report, human error accounted for 30 percent of reports or 156 incidents. The takeaway here is that providing orchestration for many manual human-based tasks and having built-in safety nets for human error or internal threats is vitally important.

Most organizations can't recover within a week

If your organization had to fail over 50 servers due to a disaster or cyber event, how long do you estimate it would take from starting the recovering of the first server until the last server was online?



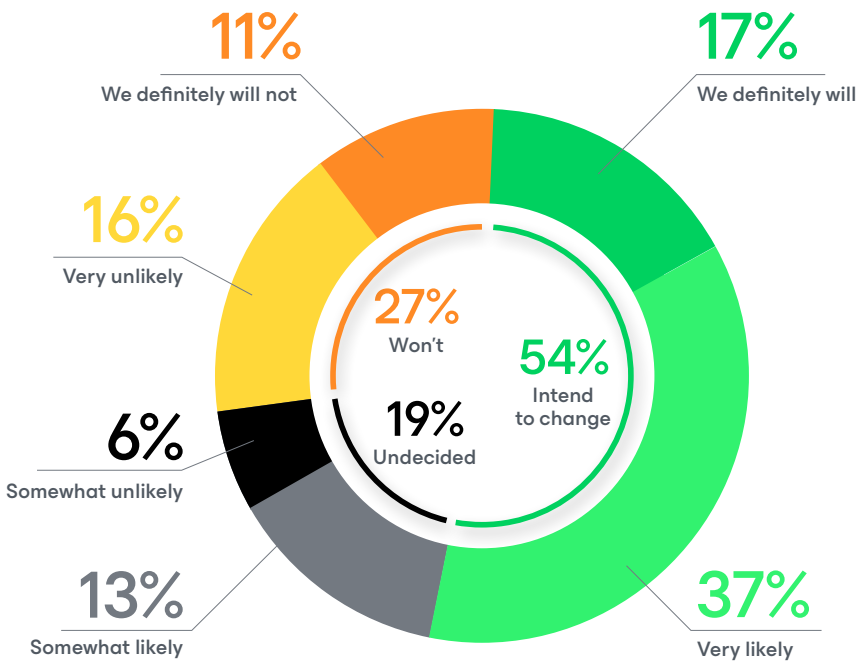
Forces for change. Thinking of moving to a modern, agile, and hardened backup solution that focuses on lightning-fast recovery? You're not alone. As a result of market drivers for organizations to provide a reliable, highly resilient data protection solution, over 54% of those surveyed were very likely or are actively planning to change backup providers. This is largely driven by the fact that their existing provider simply can't protect them or was unreliable when they needed to recover from outages.

If your existing data protection solution doesn't provide the reliability, security, and resiliency your organization requires, there's still hope! Veeam has pioneered modern, native data protection for hybrid workloads that help ensure not only compliance with strict government mandates, but makes it easier to stay that way too. Veeam is easy to adopt too, since we remove many moving parts and legacy architecture roadblocks and can leverage virtually any hardware or cloud platform that's in use today.

As for deployment, management, and day-to-day operations like platform upgrades, these require much less time as well with Veeam, and most of our customers upgrade within an hour.

You no longer need to wrestle with slow, unreliable recoveries from legacy backup solutions that have been in place for years. As environments change and evolve, Veeam has you covered with many resources and partners that can ensure your valuable data is hardened, protected, and recoverable now and in the future without vendor or cloud lock-in. We call this data freedom, and it allows customers to use the right platforms for their applications and replatform as required, often without a forklift upgrade to your data protection and recovery strategies.

54% are very likely to change backup solutions



What is the likelihood that your organization will switch its primary backup solutions or services within the next twelve months?

Veeam Data Platform: Recommended Licensing

If you're choosing the compliance path, Veeam makes it easy to look at all the recommended compliance features that make up the Essential Eight maturity levels for backups. This is meant to assist federal and state agencies with their next Veeam renewal, or simply identify what platform edition to consider depending on your current security posture.

Veeam offers flexible licensing options for Veeam Data Platform that's tailored to your business needs, whether on-premises, in the cloud, or in hybrid environments. These options are offered in three main categories: Foundation, Advanced, and Premium editions.

Many of the Essential Eight mandates Veeam sees as non-negotiable, meaning we build this into every edition and not as an add-on, since we see these as vital for all organizations, not just the larger ones. Features including governance and compliance-based immutability, backup file encryption, direct recovery to cloud/other hypervisors, security and resiliency zone support, and MFA form a standard baseline of protection as a minimum. The table below highlights where Veeam can help raise agency maturity levels and operational efficiencies across both cyber resilience and within Essential Eight compliance across the board.

Veeam Data Platform

	Secure Foundation			Cyber Resilience					Enterprise Resilience			
	Zero Trust Data Resilience	Generative AI	Detect + Identify Threats	Security and Observability					Recovery Orchestration and Compliance			
	Data Protection & Verified Recovery	AI Assistant	AI-powered Malware Detection	Proactive Threat Hunting	Security Integrations	Analytics, Discovery & Reporting	Intelligent Diagnostics & Remediation	Threat Health Center	Orchestrated Recovery & Validation	Ess 8 Audit Documen-tation	Forensic Triage	Veeam Recon Scanner
Foundation	✓	✓	✓	—	—	—	—	—	—	—	—	—
Advanced	✓	✓	✓	✓	✓	✓	✓	✓	—	—	—	—
Premium	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

\+ Veeam Cyber Secure

- Coveware Incident Response Subscription
- Up to $5M Ransomware Warranty
- 24/7/365 SWAT Team with 30min SLA to help
- Onboarding, Implementation, Quarterly Health Assessments for Security Best Practices

References

1. ASD 2023 Cyber Threat report
2. IT News Article - Office of the Australian Information Commissioner Bulletin
3. Cyber.gov.au Essential 8 Maturity Model
4. ACSC Ransomware Emergency Response Guide
5. Cyber.com.au Strategies to mitigate cyber Security Incidents
6. Veeam 2024 Data Protection trends report
7. Veeam 2023 ransomware trends report
8. The Commonwealth Cyber Security Posture in 2023
9. DTA Digital Government Strategy
10. OAIC Notifiable data breaches report 1H 2024
11. 2024 Elastic security labs global threat report

About the author

Rob Johnston,
Senior Systems Engineer, ANZ Veeam Federal Team

Based in Canberra, Rob Johnston has been working in and around Australian federal agencies for over 20+ years in various architecture, and technical sales roles with Tier 1 vendors, integration partners, and directly within federal agencies. He works with a core focus that surrounds robust data protection and recovery technologies, including cloud, virtualization, and data protection compliance

About Veeam Software

Veeam, the #1 global market leader in data resilience, believes every business should control all their data whenever and wherever they need it. We're obsessed with creating innovative ways to help our customers achieve data resilience. We do that by offering purpose-built solutions that provide data backup, data recovery, data freedom, data security, and data intelligence. Headquartered in Seattle, with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, who trust Veeam to keep their businesses running. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

Learn more: veeam.com