BECHTLE

| EBOOK

Veeam Backup : the ultimate solution againts ransomware

Discover 5 ways to protect yourself from the threat of ransomware

VEEAM

The threat of ransomware is real and every organisation must be prepared for potential attacks on its data.

To leave nothing to chance, it is highly recommended to establish a reliable security strategy, especially by protecting the sensitive data of your organisation.

To best build your strategy, we suggest you discover 5 good security practices against ransomware through our dedicated ebook: Identify, Protect, Detect, Respond and Recover.

The purpose of a back up solution is to avoid considerable downtime, the loss of your data and the payment of a costly ransom.

Withthetechnicalguidanceprovided, thisdocument will be of great use to Backup Administrators, Site Reliability Engineers and all IT professionals in charge of security or operations management.

SUMMARY

1 | Identify with an overview of employees, equipment use and safety processes

2 | Protecting to ensure the delivery of critical infrastructure services

3 | Detect intrusions immediately to limite the impact of cyber attacks

4 | Respond effectively to cyber threats through the implementation of an incident response plan

5 | Recover your sensitive data correctly to quickly restore operations

1 IDENTIFY WITH AN OVERVIEW OF EMPLOYEES, EQUIPMENT USE AND SAFETY PROCESSES

In order to be sufficiently armed against cyber attacks it is very important to put yourself in the shoes of cybercriminals and understand the way they try to achieve their goals.
To do this, it is advisable to have a global view of the company's personnel, the use of computer equipment and your security processes.

The following are best practices for identifying risks:

1. The human firewall

Technology alone cannot strengthen your organisation's cyber security. With the increasing complexity and threat of cyber-attacks, organisations must be prepared to put in place a multi-layered defence. This means that everyone must be aware of security risks and potential incidents and report anything suspicious. The importance of this human layer of protection lies in the fact that many attacks are due to mistakes made by employees. Successful hacks are often due to negligence, simple mistakes or a lack of knowledge of cyber threats and cybercriminal practices.
Knowing that phishing, remote access (RDP) and software updates are the three main entry mechanisms for a cybercriminal, is invaluable in determining where you should invest the most effort from an attack vector perspective.

OUR EXPERT ADVICE

Identify potential knowledge gaps within your staff by conducting a cyber security awareness program, assess your organisation's level of cyber security awareness maturity.

2.Have a business continuity plan (BCP) that is always available and up to date

Who should be contacted in the event of a disruptive event? Ensuring that the business continuity plan (BCP) is always available, even if everything is lost and locked, is crucial to an organisation's survival. Best practice is to ensure that your BCP is stored in a separate location, that it is immutable and that it is available 24 hours a day, 7 days a week, 365 days a year. A BCP should outline how the business will continue to operate in the event of an unforeseen service disruption.

3. Tagging digital assets

Knowing what assets are critical to your organisation and how to effectively protect them is essential to creating an effective cyber security response plan. Before you start protecting, you need to identify and tag assets to put the most effective plan in place.

Tagging digital assets can be the difference between looking for a needle in a haystack and finding the specific asset you need through a simple search.

Veeam solutions for identification

Data labelling : Labelling virtual machines (VMs) paves the way for good organisational constructs in the data centre. Ideally, all new VMs should be created with a label describing their data protection strategy. These can be simple levels such as backup only, but it is also possible to allow labels to be subject to disaster recovery (DR) or additional protection.

Data localization: Assigning locations to backup storage allows organisations to control the location of their data. In **Veeam Backup & Replication**, key infrastructure components can be assigned locations to provide visibility into where your data is located and where it can be backed up and/or restored. This can provide greater control and visibility when needed in the response and recovery functions of the framework.

Business View: **Veeam ONE** provides a business view, which is a great way to use categories and groups for visibility into business stakeholders by tagging technology assets assigned to them. Groups in the business view can be synchronised with vSphere and Hyper-V tags. This can synchronize the creation of tags based on **Veeam ONE** categorisation, which improves visibility and manageability.

Reports on protected VMs and computers: This **Veeam ONE** report provides users with an excellent view of what is and is not backed up in the environments being assessed. The backup VM alert can be used in conjunction with **Veeam ONE** remediation actions to automatically add systems that are not backed up to a backup job.

2 | PROTECTING TO ENSURE THE DELIVERY OF CRITICAL INFRASTRUCTURE SERVICES

The protection function is essential as it contributes to the development and implementation of appropriate protective measures to ensure the delivery of critical infrastructure services.

It proactively supports the ability to limit or contain the impact of a potential cyber security event. Successfully protecting your organisation against ransomware requires an understanding of the current attack vectors: what threats and opponents are you protecting your digital systems/services against? If you know what you are protecting against, it is easier to take the right countermeasures.

SPECIALISTS ADVICE

The backup strategy 3-2-1

The 3-2-1 rule is an industry standard on how to protect data and is the ultimate line of defence in the fight against ransomware. This rule requires that you ensure you keep at least three copies of every important piece of data, store your backup data on two different types of media and replicate one copy of your data off-site.

Best practices in protection are as follows:

1. Secure by design

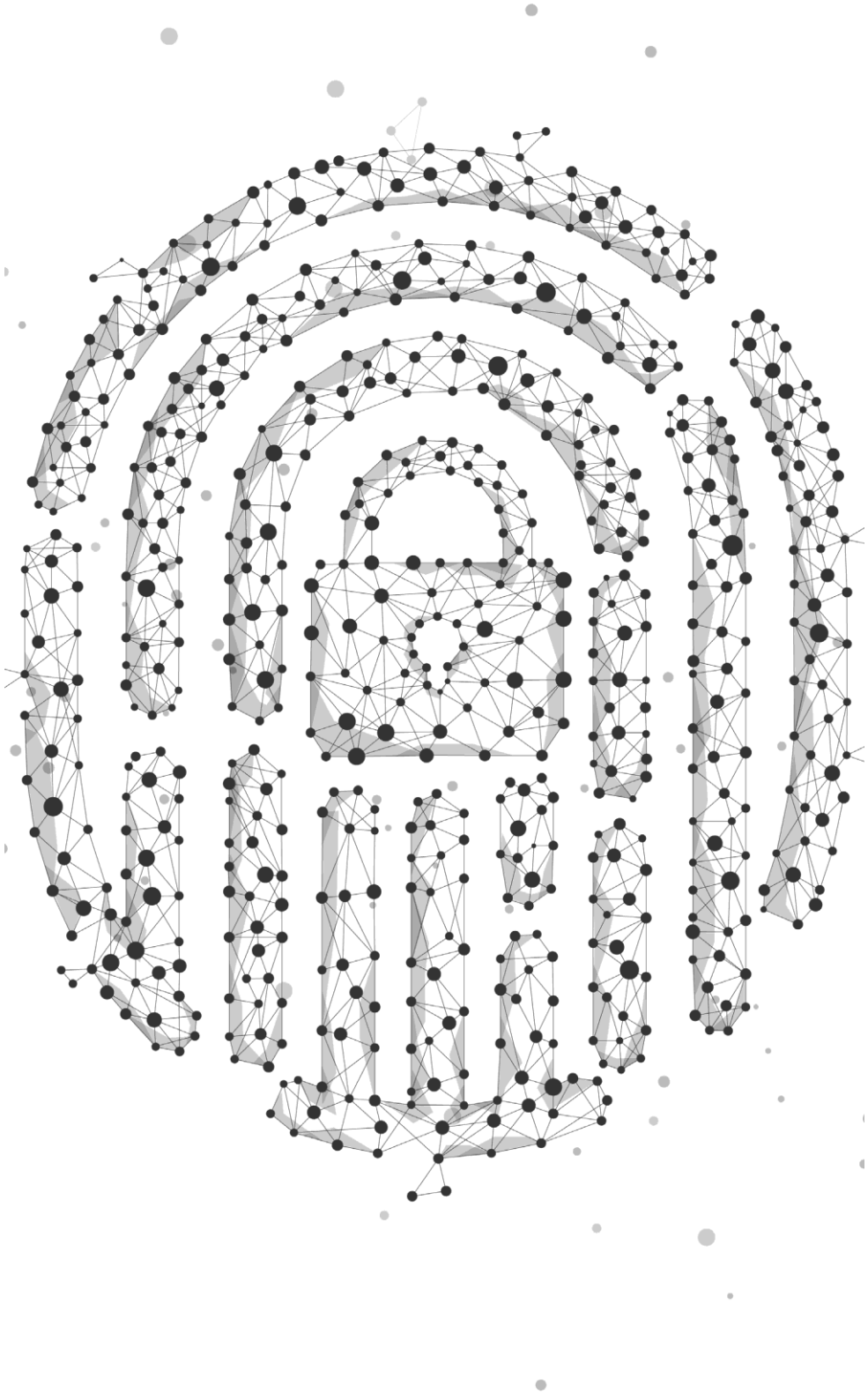
It is much more difficult and costly to add a security layer to an existing infrastructure than to think about it at the design stage of the infrastructure. It is good practice to remove all known attack vectors and only open access when components are added that require specific openings or additional software to function properly.

2. K.I.S.S. principle

Overly complex designs become more difficult for IT teams to manage, making it easier for an attacker to exploit weaknesses and remain in the shadows. Having more manageable designs are inherently more secure, use K.I.S.S. (keep it simple and straightforward) for your designs.

3. Principle of least privilege

This principle consists of granting a user account or process only those privileges that are absolutely essential to perform its intended function. The principle of least privilege is widely recognised as an important design element that enhances the protection of data and functionality against malicious behaviour and failure.



4. Segmentation

Segmentation is the process of dividing your infrastructure into zones where objects are grouped into logical zones by looking at the level of access needed, common restriction policies and connectivity within and outside that zone.

A zone is an area with a specific characteristic, purpose, use and/or set of restrictions. By using zones, you have an effective strategy for reducing many types of risk.

5. Separating duties

Separating duties is a basic element of sustainable risk management and internal control in an organisation. The idea behind it, is to divide the tasks and privileges for security tasks among several people.

One person should not be able to control everything, which means that one person should not be able to suppress everything either.

6. Digital hygiene

With the proliferation of threats, vulnerabilities and digital contacts, you are always at risk of catching the digital flu. By adopting good digital hygiene practices such as creating unique passwords for each login source or multi-factor authentication (MFA), it is possible to maintain the health of your data, your privacy and your security.

7. Backups

Ransomware prevents you from accessing your own data by encrypting your files. As such, proper backups are an excellent way to recover from this type of attack. With backups, it becomes easy to replace your encrypted files with copies you have in your recent backup savings.

8. Encryption

Encryption ensures that only authorised parties can access the information. As soon as information leaves a defined security domain, make sure it is encrypted to an appropriate predefined level. Encryption itself does not prevent interference, but it does prevent unauthorised parties from reading your information. Encryption helps protect sensitive data if other security measures fail.

Veeam solutions to improve protection

Veeam provides backup solutions for a wide range of virtual, physical, file, Software as a Service (SaaS), container and cloud platforms. Focusing on **Veeam Backup & Replication**, the capabilities listed below align with the protection function of the framework.

Backups to highly resilient storage media are one of the most important mechanisms for ensuring resilience against ransomware. Organisations should choose the approach (storage type) that best suits their data type and business process.

Backup drive

Every IT organisation has an opinion on tape media, but the acquisition cost, offline capability and portability of tape are hard to beat. Tape drive that is ejected or removed from a library is automatically taken offline. Veeam supports WORM (write-once read-many) media for additional resilience against ransomware, and has broad, native tape support, including writing files and full backup drives.

Organisations fighting ransomware forget that drives are not always removed from the library. If the threat actor running the ransomware takes control of the control planes on the network, the deletion of backup storage can be an attack vector.

Veeam solutions to improve protection

Backups in Veeam Cloud Connect with insider protection

Veeam Cloud Connect Insider Protection has been created to provide additional resilience for backup data against the risk of ransomware, malicious administrator activity or accidental deletion. With Insider Protection, an additional out-of-band copy of the backup data will be retained by the service provider and exposed through interventions such as a support call. This process will allow the backup data to be re-entered into the **Veeam Cloud Connect** repository and then conduct onsite restores.

Encryption

Customers can use a single encryption method, or a combination of both, to protect against unauthorised access to important data throughout all stages of the data protection process.

3 DETECT INTRUSIONS IMMEDIATELY TO LIMITE THE IMPACT OF CYBER ATTACKS

The detection function is an essential step in a robust cyber security programme, the sooner a cyber threat is detected, the sooner the impact can be mitigated.

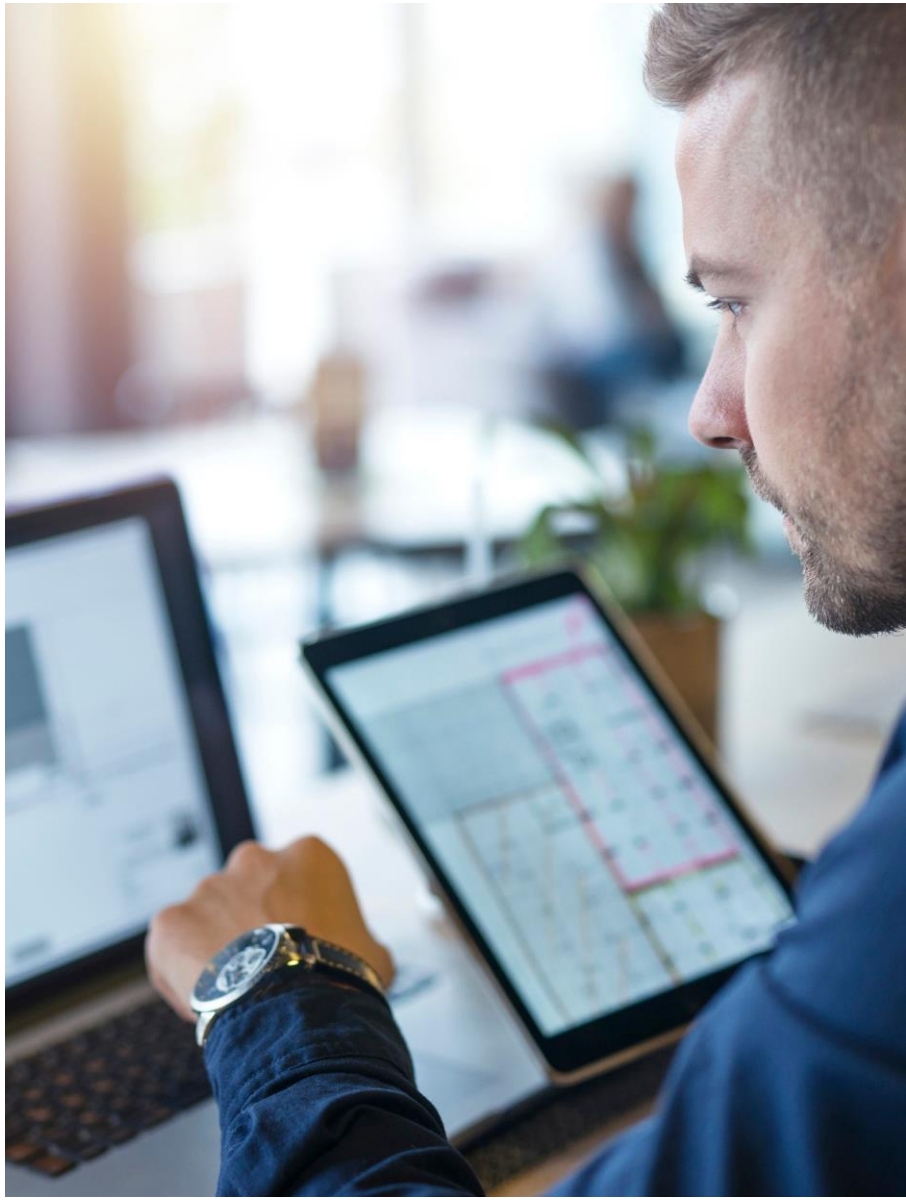
The 2 best cybersecurity practices for detection :

1. Detection system

There are several systems that can alert you to suspicious behaviour so that you become aware of an intrusion and attempt to access your infrastructure. It is important to receive alerts as soon as possible to defend against other attacks such as viruses, malware and ransomware. The biggest risk of these attacks is that they can spread quickly to other systems. It is therefore essential to have visibility of potential ransomware activity.

2. Trap devices

Create virtual triggers, such as an unused administrator account with alarms linked to it. When activity on this account is observed, a red alert is triggered instantly.



Veeam solutions to improve detection against ransomware

The **Veeam ONE™** alarm detects a combination of high processor activity of sustained write I/O to a drive or a high network transmission rate. This alarm is customizable. The default values are a good starting point for possible ransomware activity, but can be adjusted to be more conservative in triggering this particular alarm.

Veeam recommends several actions that are built into the alarm to provide more important notifications to IT staff. This includes sending text messages, alerting security teams, and potentially extreme measures such as powering down a VM or disconnecting the network interface via the **Veeam ONE** alarm actions.

This alarm applies to **Veeam ONE** when monitoring **Veeam Backup & Replication** in the data protection view.

As with most **Veeam ONE** alarms, there are configurable rules for choosing the depth of the scan. By default, it will scan three restore points and indicate a warning at a 150% rate of change and an error alarm at a 200% rate of change.

4 | RESPOND EFFECTIVELY TO CYBER THREATS THROUGH THE IMPLEMENTATION OF AN INCIDENT RESPONSE PLAN

The response function helps develop techniques to contain the impact of a cyber attack by ensuring that you develop and implement the appropriate actions to take in the event of a detected cyber security incident. The faster and more effectively you respond to the potential detection of a cyber incident, the sooner you can stop the threat in its tracks or mitigate its damage and reduce any potential financial impact.

SPECIALISTS ADVICE

Create a response plan

One obvious way to prepare for cyber security incidents is to create an incident response plan. Creating a clearly defined incident response plan will allow you to outline procedures for detecting, communicating, monitoring and correcting security incidents so that employees know how best to respond to cyber security events when they occur.

Veeam solutions to improve ransomware response

Response to ransomware is a course of action that often leads to recovery scenarios. Having the response function ready for action will ensure the success of the recovery function. The reality is that any response will depend on the nature of the incident, but one thing will remain consistent across all recommendations: it is time to prepare a robust response plan.

Veeam Disaster Recovery Orchestrator is a powerful extension to **Veeam Backup & Replication**. It provides essential capabilities for the response functions needed to recover from cyberattacks of many types, including ransomware. There are four types of plans available that can provide organisations with a clear path to an optimal response. These four plan types are based on **Veeam Replication**, Backups, Supported Storage Snapshots and **Veeam Continuous Data Protection (CDP) Replication.**

It is essential to test DR plans to ensure that they can be used successfully to recover from ransomware. Automated auditing and reporting can be part of internal and external compliance initiatives.

Also have a list of security experts ready to be contacted if needed. These experts can be internal or external to your organisation. If you use a Veeam service provider, you may want to consider adding additional services to their core offering (such as **Veeam Cloud Connect Insider Protection**).

5 | RECOVER YOUR SENSITIVE DATA CORRECTLY TO QUICKLY RESTORE OPERATIONS

The recovery function allows you to quickly restore normal operations to reduce the impact of a cyber attack event. This function ensures that you develop and implement appropriate activities to maintain resilience plans and restore any capabilities or services affected by a cyber incident.

As the number of cyber attacks continues to grow, organisations will inevitably face a security incident at some point.

1. Recover strategy

Before you realise that your infrastructure has been attacked, you need to know what to do in the event of an attack. Defining a list of priority action points that can be used to undertake recovery activities is essential for rapid recovery and for limiting the damage of an attack.

Back up your data and ensure that backups are not within reach to hackers. It is strongly recommended that you make an off-site or read-only copy of the data on any device to survive a ransomware attack. Remember the 3-2-1 rule to protect your data.

Veeam's solutions to improve recovery against ransomware

Veeam Backup & Replication backups provide a versatile set of recovery options. This versatility starts with the portable data format of the backup files that can be restored to new locations if necessary. This is important in a scenario where the source platform cannot be relied upon for recovery.

NAS devices are one of the most popular targets for ransomware, as they store large amounts of sensitive data. Add to that insider threats, device failures or accidental deletions, and there are many reasons why file data should also be considered a threat target.

Veeam Backup & Replication support for NAS backups provides a recovery option for file share data if a ransomware has compromised the contents of that file share. It's hard to predict exactly how a cyber attack will play out, but having multiple options for dealing with a threat is a sound approach. One of the versatility of Veeam backups is the absolute portability of backup data.

There are three types of organisations in the world: those that have been hacked, those that are about to be hacked and worst of all, those that don't know they have already been hacked. The only thing you can and should do is buy as much time as possible by deploying the right countermeasures in terms of people, processes and technology

Below are some additional considerations for restoration :

Ready to recover: When conditions are right to recover, implement additional security checks before putting the systems back on the network. A few additional steps can be included when recovering your network access disabled for a final check on data integration.

Recover options: Depending on the situation, a full VM restore may be the best option. In other cases, a filelevel restore may be preferred. Knowing your recovery options in advance will greatly assis in choosing the optimal recovery method and reduce resolution time.

For more information contact our specialist:

Nagy Gabriella
Software Specialist
+36 1 882 7394
gabriella.nagy@bechtle.com

Montevideó u. 3/A HU-1037 Budapest
+36 1 882 7391
www.bechtle.com/hu

https://www.bechtle.com/hu