NAKIVO®

Best Practices

for Ransomware Protection and Recovery

Table of Contents

Overview 3

Ransomware Basics

What Is Ransomware? 4
Ransomware as a Service 5
Ransomware Infection Vectors 5

Ransomware Protection

What Is an Incident Response Plan? 7
What Is an Incident in ITIL? 8
Incident Response Steps 9
Best Practices for Ransomware Protection 10
Follow the 3-2-1 Backup Rule 10
Use Multiple Backup Targets 10
Use Replication for Disaster Recovery 11
Create an Appropriate Retention Policy 11
Control Access to Backup Data 11
Verify Backup and Replica Recoverability 11

Ransomware Protection and Recovery with NAKIVO Backup & Replication

Native, Agentless Backups 12
Backup to Multiple Destinations 12
Ransomware-Proof Backups 13
Instant VM Backup/Replica Verification 13
Granular Recovery 13
Flash VM Boot 13
P2V Recovery 14
Replication for Disaster Recovery 14
Disaster Recovery Orchestration and Automation 14

Comprehensive Data Protection with NAKIVO Backup & Replication 15

About NAKIVO 15

Overview

The pandemic has changed how small businesses and global corporations work. It has affected not only how their employees interact and work, but also interactions with customers and customer service. Organizations have increasingly turned to cloud services and platforms to ensure business continuity. The benefits gained from this shift have been great: from improved agility to better visibility. But along with these benefits, organizations have also had to deal with the data vulnerabilities brought about by such sudden change.

The last year has seen an unprecedented surge in ransomware attacks as cybercriminals tried to exploit these new data protection challenges for profit. The first three quarters of 2020 show that 21% of data loss resulted from ransomware attacks[1]. Cybersecurity Ventures has predicted that an organization would be hit by ransomware every 11 seconds in 2021[2]. Ransomware attacks have been one of the leading reasons why businesses lose data permanently. And this data loss leads to loss of productivity, revenue and customers.

Organizations without a ransomware protection plan in place often become hostages of cybercriminals. After launching successful attacks and taking over the data, hackers may demand monetary payments in exchange for restoring access to business data or to avoid leaking it. Under the pressure of potential data loss, public exposure or subsequent attacks, organizations often give in to hackers' demands. According to the latest The State of Ransomware 2021 report from Sophos, 37% of organizations suffered a ransomware attack in 2020, with the average ransom costing USD 170,404[3]. And yet, even when the ransomware was paid, only 65% on average of the data encrypted was recovered[4].

These steep ransom payments indicate that organizations are not always prepared to address the possibility of ransomware attacks proactively. A proactive approach should cover security measures to prevent attacks, steps to take during an incident and a data protection/disaster recovery plan. And no matter the scale of the attack, paying ransomware attackers is not the answer. Possible dangers of paying ransoms to hackers may include further data loss, compromised security, reputational damage and financial losses, not to mention incentivizing cybercriminals to carry out more attacks.

Paying cybercriminals may also entail legal consequences for organizations. In October 2020, the US Department of the Treasury issued an "advisory to highlight the sanctions risks

1 Risk Based Security, 2020
https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020 Q3 Data Breach QuickView Report.pdf
2 Cyber Security Ventures, 2019
https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf
3 Sophos, 2021
https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
4 Sophos, 2021
https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

associated with ransomware payments related to malicious cyber-enabled activities"[5]. Paying the ransom does not guarantee regaining access to business data and can bring about additional losses in the form of legal expenses and fines, further hampering recovery.

No matter the cybersecurity measures in place, hackers find ways of infiltrating systems and putting a lock on their victim's data. But with a holistic approach and a timely response, the chances for full recovery are pretty high. Thus, organizations should look into proven and successful ransomware protection and recovery methods. As of today, third-party companies offer complete backup and recovery solutions ensuring that organizations continue to run even if malicious activity occurs and the first line of defense fails.

Organizations should consider creating an incident response plan (IRP) to tackle ransomware attacks successfully. A good IRP usually covers the range of events from ransomware attacks to data loss and incorporates the best data protection and recovery methods. A workable incident response plan and a top-notch backup solution can ensure data accessibility, recoverability and 99.999% availability.

Ransomware attacks are hitting small and large organizations alike. But one thing is clear – all organizations need to follow smart practices for ransomware protection and recovery to overcome any potential external threats. This paper focuses on the latest best practices for ransomware protection and recovery for organizations in any industry. It covers ransomware, incident response plan (IRP), data protection, disaster recovery and strategies for tackling cyber threats.

Ransomware Basics

What Is Ransomware?

Ransomware is a type of malicious software that encrypts or locks a victim's data. After the data is made inaccessible, cybercriminals can demand a payment in return for making the data available again. The two major types of ransomware are:

- **Crypto-ransomware.** This type of ransomware selects files/folders and then makes them unreadable. Crypto-ransomware scrambles data by using a specific encryption algorithm. To make the data available again, the victim needs to obtain a decryption key.
- **Locker ransomware.** This type of ransomware locks the entire system of a targeted organization. As a result, the user is locked out from the device. A message appears on the screen and may display the price and date by which a payment has to be made to regain access.

The two types of ransomware have different approaches to compromising data and systems. But the result is the same. Once critical data gets blocked, many victims have no other choice

5 Department of the Treasury, 2020
https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

but to pay the ransom. However, even after being paid, hackers don't always follow through with the agreement. As a result, organizations are not able to recover their data. Often the attackers accept bitcoins or other cryptocurrencies as payment, which allows them to cover their tracks and avoid prosecution.

Ransomware as a Service

Today's hackers have gone corporate. They operate websites, hire employees and even issue press releases. In fact, a new ransomware model has emerged recently, with ransomware developers offering malware on a subscription basis. This new "business" model is known as ransomware as a service (RaaS), a spin-off from software as a service (SaaS).

RaaS delivers ransomware in a package that allows cybercriminals with little expertise in developing ransomware to launch malicious attacks in a short period of time. RaaS companies often sell their products on the dark web to attackers looking for quick and ready-made solutions.

Whether ransomware is developed by an individual, state actor or through a RaaS model, all cyber criminals use similar tactics and infection vectors for extortion. Thus, understanding commonly used infection vectors and ransomware behaviours can help you prevent and overcome incidents.

Ransomware Infection Vectors

The majority of ransomware attacks are initiated by unsuspecting users when they visit malicious sites or clicking malicious links. This makes employee awareness a priority in any malware prevention strategy.

The most widespread attack vectors are phishing, exploit kits, downloader and trojan botnets, social engineering and traffic distribution.

- **Phishing.** Phishing is a type of attack that uses messaging to scam users. Cybercriminals send fraudulent emails pretending to be trusted entities. The goal is to trick victims into providing personal information, like bank details or login credentials, or clicking a malicious link.
- **Exploit kits.** These are fully-automated toolsets for stealthy exploitation of targeted environment vulnerabilities, for example a compromised website. Once visitors land on the site, they may inadvertently download a malicious payload and their systems get infected. Cybercriminals often use exploit kits for mass malware distribution.
- **Botnets.** Botnets are computer networks controlled by cybercriminals to distribute ransomware and conduct phishing attacks. Used to launch complex distributed-denial-of-service (DDoS) attacks.

- **Social engineering.** Social engineering uses psychological manipulation instead of technical tricks to persuade users to share their login details or other sensitive information. Attackers use this information to access the system and infect it with ransomware.
- **Traffic distribution.** Traffic distribution is a malicious scheme to redirect victims to infected websites. Any action on such websites can trigger the delivery of a malicious payload.

The ransomware infection vectors vary from basic sophisticated, but their primary goal is to breach security and take over a victim's machine and data. Once ransomware breaches security, it behaves in one or more of the following ways to infect the environment:

- **Payload Persistence.** Payloads are similar to viruses. They are lines of code spread with exploit kits and traffic distribution tactics. Hackers use payloads to establish connections with the victim's device. Hackers can then gain admin privileges and upload malicious files into the user's system. The attacker can hide the code from the user (for example, a registry). This piece of code allows the hacker to gain full control of the user's systems, including data, passwords and network activities[6]. To make sure that payloads are not removed with a simple system reboot, hackers establish payload persistence[7]. This action helps payloads bypass the reboot. Once this is done, the victim's machine becomes available to the attacker at all times[8].
- **Environment Mapping,** During the setup phase, ransomware maps your environment to ensure it is not restricted to a sandbox. A sandbox is a virtual environment that mimics the original environment. It's often used as a security measure against cyber attacks. However, some ransomware can analyze the environment it infects and determine if it's targeting a real environment or a sandbox.
- **Privilege Elevation.** Most of the time attackers explore the system or network with the goal to obtain unlimited access to a certain machine or user account. When they find weak spots in the code, they take advantage of this opportunity and gain full administrative rights for that target machine, application, network or user account. Having full control over a network or any open-source account or software allows the hacker to launch the attack without being detected[9].
- **System Restore Restriction.** As hackers obtain control over admin rights and registry, they can put restrictions on system restore, thereby preventing a device from restoring to

6 A Study on Metasploit Payloads, International Journal of Cyber-Security and Digital Forensics, 2019 https://www.academia.edu/42902811/A_Study_on_Metasploit_Payloads

7 Hacking Articles, 2020 https://www.hackingarticles.in/multiple-ways-to-persistence-on-windows-10-with-metasploit/

8 A note on different types of ransomware attacks, IACR, 2019 https://eprint.iacr.org/2019/605.pdf

9 Vulnerabilities Assessments in Ethical Hacking, AJER, 2016 http://www.ajer.org/papers/v5(05)/A05050105.pdf

its previous state. In this case, the victim won't be able to recover the data and remove the payload from the device[10].

- **Stealth Mode.** Ransomware often enters the stealth mode to prevent detection. It involves communication masking, among other actions, which allows delivering information to attackers and complicates tracking. Operating in the stealth mode, cybercriminals can access data and create doorways on the network without being detected by the security systems.[11] [12]

Ransomware Protection

Cybercrime is continuously evolving, and cybercriminals are finding new vulnerabilities and ways of infiltrating systems. They are also finding new ways to make money with RaaS and targeting high-level organizations with extremely sensitive data. This is why any strategy for ransomware protection should cover data protection/disaster recovery as well as security measures, employee awareness training and detection/containment.

This paper focuses on the data protection and disaster recovery part as part of a holistic incident response plan for a quick and safe recovery from external threats.

What Is an Incident Response Plan?

Ransomware protection and recovery is about ensuring uninterrupted IT service delivery. Whatever the framework used, whether ITIL or something else, you are expected to make sure that systems and data are available and accessible when needed. An incident response plan is the steps to be taken by your IT team to detect, respond and recover from a security incident.

With or without a formal service level agreement (SLA), the expectation is that an IT service should run almost without disruptions and critical systems should be available 99.999% of the time. This standard translates into just 5 minutes and 15 seconds of downtime per year!

Achieving the level of availability required by your organization involves specifying the amount of time needed to bring back systems after an incident and the amount of data that the organization can tolerate to lose, that is, determining your recovery time objective (RTO) and recovery point objective (RPO).

10 TechGenix, 2004
https://techgenix.com/registryhacktodisablesystemrestoreoptionfromxpstartmenuandcontrolpanel/
11 Hackers Wikia
https://hackersthegame.fandom.com/wiki/Stealth_Programs
12 AFCEA, 2019
https://www.afcea.org/content/stealth-attacks-require-stealth-responses

Definitions

RTO is the timeframe during which the operations of the business must be restored to avoid negative or irreversible consequences.

RPO defines the maximum amount of data that can be lost during the incident without serious damage to the business.

NOTE: Ransomware protection requires backing up workloads regularly, and the frequency of the backups depends on your recovery point objective (RPO).

What Is an Incident in ITIL?

Given that ITIL (IT Infrastructure Library) is one of the most used frameworks for IT service delivery these days, let's look at the definition of an incident and the guidelines ITIL provides on managing incidents because they can be applied even without a formal ITIL adoption.

ITIL differentiates between an incident, a problem and a request.

Definitions

An incident is "an unplanned interruption to an IT service or reduction in the quality of an IT service or a failure of a Configuration Item that has not yet impacted an IT service (for example failure of one disk from a mirror set)".[12]

According to ITIL, the main incident management tasks include:

- Restoring the organization's services as fast as possible
- Reducing negative impact of the incident on the organization
- Maintaining high quality of all operations[13]

12 ITIL Service Operation, United Kingdom: The Stationery Office, 2011

13 ITSM Process Description - Incident Management
https://www.alaska.edu/files/oit/ITSM_Program/Incident-Management-Process-Description-v1.pdf

Incident Response Steps

It is recommended that you develop an efficient incident response plan that accounts for your organization's specific needs, RTOs and RPOs. This plan should cover the immediate actions during the ransomware attack and its aftermath. The basic incident response plan involves communicating the incident, containing the damage, clearing the malicious software and recovering data:[14]

- Every organization should determine the chain of command to follow in case of a security incident. The first step is to inform the organization's management and CEO.
- They can estimate the severity of the attack and hire or appoint qualified experts to resolve the situation. The appropriate actions can be taken after the whole picture becomes clear, such as the type of malware used and the underlying causes.
- During the clearing stage, all attacker tools should be wiped out from the systems. It's vital to eliminate malicious malware, remove compromised user accounts and individual files, block phishing emails and run security scans to make sure that all issues have been successfully expunged. It's also recommended to examine all of the machines that could be impacted by the incident and verify that they are not infected.
- Depending on the scale of the attack and whether the organization has a secondary site for disaster recovery, failover can be initiated to that site. Failover of workloads to a disaster recovery site reduces downtime and allows the organization to maintain its operations. Once the attack is contained and systems cleared, a failback can be initiated to the production site.
- Once machines and systems are cleared, it's time to initiate a recovery process. A fast recovery relies on timely and quality backups. Efficient backup strategies should be established and kept maintained prior to any attack as a part of the incident response plan. If an organization has no prior backups or has insufficient backups, the recovery process becomes more complex. There might be a necessity to rebuild the whole working environment which can be expensive and time consuming. Some organizations continue working with fixed versions of old files, for example, and, in this case, there is always a chance that some of the malware has remained in the system.

14 Cyber Security Incident Management Guide
https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

Checklist

Question to answer before formulating your incident response plan:

- How long can your organization survive without its critical systems?
- What is the maximum number of users that can be affected by the incident?
- What are the most critical machines for backup and replication to a secondary location? And what are RTOs and RPOs for these machines?
- What is the most critical data for priority backups and instant recovery?
- What are the responsibilities of the staff during the incident?
- How much data is generated by your business? Does it change often? How important is it?

Best Practices for Ransomware Protection

Organizations are encouraged to follow the best practices for ransomware protection as part of their working process and before the undesired activity takes place. Keeping data in multiple locations and understanding best practices is vital for smooth recovery during and after a ransomware incident.

Follow the 3-2-1 Backup Rule

It's important to remember that even paying the ransom doesn't guarantee that cybercriminals will provide decryption keys. Therefore, backup should be at the core of disaster recovery planning. And the proper way to approach backup is by following the 3-2-1 rule. According to the rule, you should have at least three copies of your data. Two of them should reside on different media and the third copy should be stored offsite.

Although the primary backup can share the same physical location of the production data, make sure it is stored on a different type of media. Even if both backups become unavailable, you can recover critical data from the offsite backup. To further increase your chances of successful recovery, create additional backup copies. The more copies of your data you have, the better your chances of a successful recovery are.

Use Multiple Backup Targets

To put the 3-2-1 rule into practice, store backups on different storage media such as local files, cloud storage, offsite servers, deduplication appliances, tape and NAS devices. The choice of storage media should be based on the type and size of your infrastructure as well as your budgetary constraints. The same applies to the number of backup copies you create, which should not be lower than three. Keep in mind that multiple backup copies can protect

your data not only from ransomware but also from a storage device failure, which is not an uncommon occurrence.

Use Replication for Disaster Recovery

Even the shortest downtime can reduce an organization's productivity and revenue. That's why in addition to reliable backups, you can use replication to bring down RTOs and RPOs to a minimum during and after a ransomware attack. Create replicas of your VMs and maintain them offsite at a secondary location. Of course, it all depends on the number of sites and budget available at the organizations. But this approach can be an added layer of protection where its application is possible.

In case your primary production site is not operational because of a severe ransomware event, simply fail over to the replica and resume your operations. You can failback when your primary site is cleared and running again.

Create an Appropriate Retention Policy

A backup retention policy helps you manage your data efficiently. It allows you to retain backups until a certain point in time and archive or delete backups after a certain period. The backup retention policy is focused on getting maximum recovery points while using minimum space. A well-thought-out retention policy allows you to save storage space by replacing old recovery points with newer ones, so you can still recover the version of your data that you need. Save enough recovery points for each backup and rotate them daily, weekly, monthly, and yearly using the grandfather-father-son (GFS) retention scheme, for example.

With your retention policies set and your data backed up, you get multiple recovery options to perform point-in-time restores of your data. If ransomware hits your organization, use the backups to recover your data without paying the ransom.

Control Access to Backup Data

It's vital to protect your backups and replicas from unauthorized access. You can achieve this by applying the principle of least privilege (PoLP). The principle dictates that you should grant only the bare minimum of permissions for users to get the job done. To apply PoLP, you can use role-based access control (RBAC). RBAC is essential because it offers protection against rogue employees and human error. With access controls, only authorized and authenticated users can have access to your backup data.

Verify Backup and Replica Recoverability

Backing up your VMs is not the end goal by itself. The goal is to be able to restore the data after a ransomware attack. To this end, verify your backups and replicas regularly by running test recoveries. A continually tested backup and recovery mechanism is the number one solution for handling security and disaster related threats. Well planned and timely backups can help retain the versions of data that you need and facilitate a successful recovery process.

Ransomware Protection and Recovery with NAKIVO Backup & Replication

NAKIVO Backup & Replication is a data protection solution that can be used as part of an incident response and disaster recovery plan. The solution delivers all the features to ensure simple and reliable ransomware protection and recovery. This section covers the solution's main features.

Native, Agentless Backups

NAKIVO Backup & Replication provides image-based, application-aware backup for VMware vSphere VMs, Microsoft Hyper-V VMs, Nutanix AHV VMs, Amazon EC2 instances, and Windows/Linux servers and workstations. Application-awareness ensures that backups of app data in Microsoft Exchange Server, Microsoft Active Directory and Microsoft SQL Server are transactionally consistent. As a result, you can instantly recover objects and files such as emails in Microsoft Exchange or users in Active Directory directly from a compressed and deduplicated backup repository.

To perform consistent backups and replicas of Windows-based VMware and Hyper-V VMs, NAKIVO Backup & Replication relies on the Microsoft Volume Shadow Copy (VSS) service running inside VMs. What if your application is not VSS-aware or runs on Linux? NAKIVO Backup & Replication can run custom pre-freeze and post-thaw scripts to enable application-consistent VM backup.

Backup to Multiple Destinations

NAKIVO Backup & Replication allows to put the 3-2-1 rule into practice and store backups on multiple media. The storage options supported by the solution are local folders, CIFS share, NFS share, cloud (Amazon S3, Azure, Wasabi), tape, NAS and deduplication appliances, like HPE StoreOnce and EMC Data Domain. The solution also provides a backup copy feature. You can create as many copies of backups as you need and store them across different media for higher chances of recovery after a ransomware attack.

Ransomware-Proof Backups

NAKIVO Backup & Replication integrates with the S3 Object Lock functionality to protect your backup data stored in Amazon S3 from ransomware and other malicious or accidental data deletions. To enable S3 Object Lock, specify for how long you want to keep your backups immutable right in the solution interface.

Once S3 Object Lock is enabled, objects are stored in S3 Compliance mode using the write-once-read-many (WORM) model. Neither an admin nor a third party can overwrite or modify objects until the expiration of the retention period. Similarly, no one can modify or shorten the retention period. In addition to offering ransomware protection, Amazon S3 Object Lock functionality also allows you to preserve important data for compliance purposes.

Instant VM Backup/Replica Verification

NAKIVO Backup & Replication provides you with automated instant verification of backups. Upon completing your backup job, the solution can test-recover your Hyper-V or VMware VM backup and take a screenshot of the booted OS. You can view the verification results on the solution interface or via email. This way, you can test your Hyper-V or VMware backups and ensure that your VM backups are valid and bootable.

Granular Recovery

With granular recovery, you do not need to perform a full recovery to restore single or multiple backed up items. Instead, you can search and browse through backups to find the objects, files or folders that you need. Once you have selected the item, you can recover it to the source or a custom location, with all the file permissions restored.

NAKIVO Backup & Replication allows you to create up to 4,000 recovery points for each backup, giving you the flexibility of choice when the recovery is needed. The solution uses the grandfather-father-son retention scheme (GFS) and rotates your recovery points according to your preferences, daily, weekly, monthly, or yearly.

Flash VM Boot

If ransomware renders your primary VMs inaccessible, you can recover full VMs with the Flash VM Boot feature. The feature allows booting the VMs directly from compressed and deduplicated backups. Once the VMs are running, you can migrate them to production for permanent recovery, if needed. The feature is fully-functional and does not require any specific setup. With Flash VM Boot, you can bring the full VM to its latest state or to any other point-in-time.

The recovered VM contains all the relevant data, including configuration, OS, applications, associated data and system state. The solution can also recover multiple VMs within a single job. When you run VM recovery, a new VM is created. The source VM is not reverted to the previous state or replaced with the new VM. The feature also allows you to access files, folders, and application objects on any OS.

P2V Recovery

For mixed physical/virtual environments, physical-to-virtual recovery can make recovery during a ransomware incident a simple and swift process. Imagine a scenario where you have to recover a physical machine after a ransomware attack. Your source server is infected, and you don't have a spare one to use for recovery. In this case, you can recover physical machines to VMs, without using third-party conversion utilities. You can do it right from the solution's interface. NAKIVO Backup & Replication allows you to seamlessly boot physical Linux or Windows servers/workstations as VMware vSphere VMs. This feature can be used for both temporary and permanent P2V recoveries.

Replication for Disaster Recovery

Backups are not the only means of recovery after a ransomware attack. You can also use NAKIVO Backup & Replication to create replicas of your workloads at a secondary site. THis way, you can resume your operations by simply failing over to VM replicas if your primary site becomes unavailable.

With NAKIVO Backup & Replication, you can create and maintain exact replicas of your VMs. The solution also allows you to replicate your VMs directly from backups to offload the production environment and free up system resources. There are also other replication-related features in NAKIVO Backup & Replication to simplify the process and ensure recovery. For example, you can use the replication automation feature to completely automate the replication of Hyper-V, VMware VMs and Amazon EC2 instances.

Disaster Recovery Orchestration and Automation

With the Site Recovery feature in NAKIVO Backup & Replication, you get enterprise-grade disaster recovery automation and orchestration. Instead of manually performing VM failover, enable the VM Failover functionality, which offers a smooth path to ransomware recovery and the tightest RTOs. Here's how it works:

- Replicate your VMs to a failover location where you can boot them after a ransomware attack. You can either replicate all of your VMs with a single job or use several jobs for different VM groups and run them on separate schedules.
- Create a single VM failover job and link your VM replication jobs to it. Once done, you can perform VM failover instantly.

Note that new VMs added to replication jobs are automatically included in the failover job. But you can automate the disaster recovery even further with network mapping rules. Upon failover, your VMs will switch from one network to another following previously pre-configured rules. Similarly, create VM re-IP rules to change the IP address of your VM replicas after failover.

To prevent the infection from spreading, automatically power off your source VMs before the VM replicas go online. You can also test the complex series of steps in a disaster recovery plan without any disruptions to your production environment or running data protection tasks. By

testing, you also optimize your disaster recovery plan to ensure a smooth, failure-resistant DR process. So if a ransomware event paralyzes your primary site, you can achieve minimal downtime and zero data loss.

Comprehensive Data Protection with NAKIVO Backup & Replication

NAKIVO Backup & Replication is a data protection solution for virtual, physical, cloud and SaaS environments. The solution delivers backup, replication, instant granular recovery and disaster recovery from a single pane of glass.

Deploy in Under 1 Minute
Pre-configured VMware vSphere VA, Nutanix AHV VA or AMI; 1-click deployment on ASUSTOR, QNAP, Synology, NETGEAR, FreeNAS and WD NAS; 1-click Windows installer, 1-command Linux installer.

Protect Data Across Platforms
Native, agentless, image-based, application-aware backup for VMware vSphere, Microsoft Hyper-V, Amazon EC2, Nutanix AHV; Windows/Linux physical servers and workstations; Microsoft 365; Oracle Database.

Streamline Data Protection
Automatically protect machines matching policy rules, which can be based on machine name, tag, size, location and so on.

Increase Backup Speed
Global backup deduplication, adjustable backup compression.

Reduce Backup Size
Incremental backups with CBT/RCT/CRT, LAN-free data transfer, network acceleration and up to 2x performance when installed on NAS.

Simplify Management
Simple, fast, easy-to-use web interface, accessible anytime and anywhere — even from a mobile device.

Ensure Recoverability
Instant backup verification with screenshots of test-recovered VMs; backup copies offsite, to tape or AWS/Azure clouds.

Decrease Recovery Time
Instant recovery of VMs, files and application objects (Exchange, Active Directory and SQL); Site Recovery; near-instant P2V recovery.

About NAKIVO

NAKIVO is a US-based corporation dedicated to delivering the ultimate backup, ransomware protection and disaster recovery solution for virtual, physical, cloud and SaaS environments. As one of the fastest-growing backup and ransomware recovery software vendors in the industry, NAKIVO boasts 24 consecutive quarters of double-digit growth, 5-star online community reviews, 98% customer satisfaction with support and a network of over 7,000 partners worldwide. Over 22,000 customers in 171 countries trust NAKIVO with protecting their data, including major companies like Coca-Cola, Honda, Siemens and Cisco.