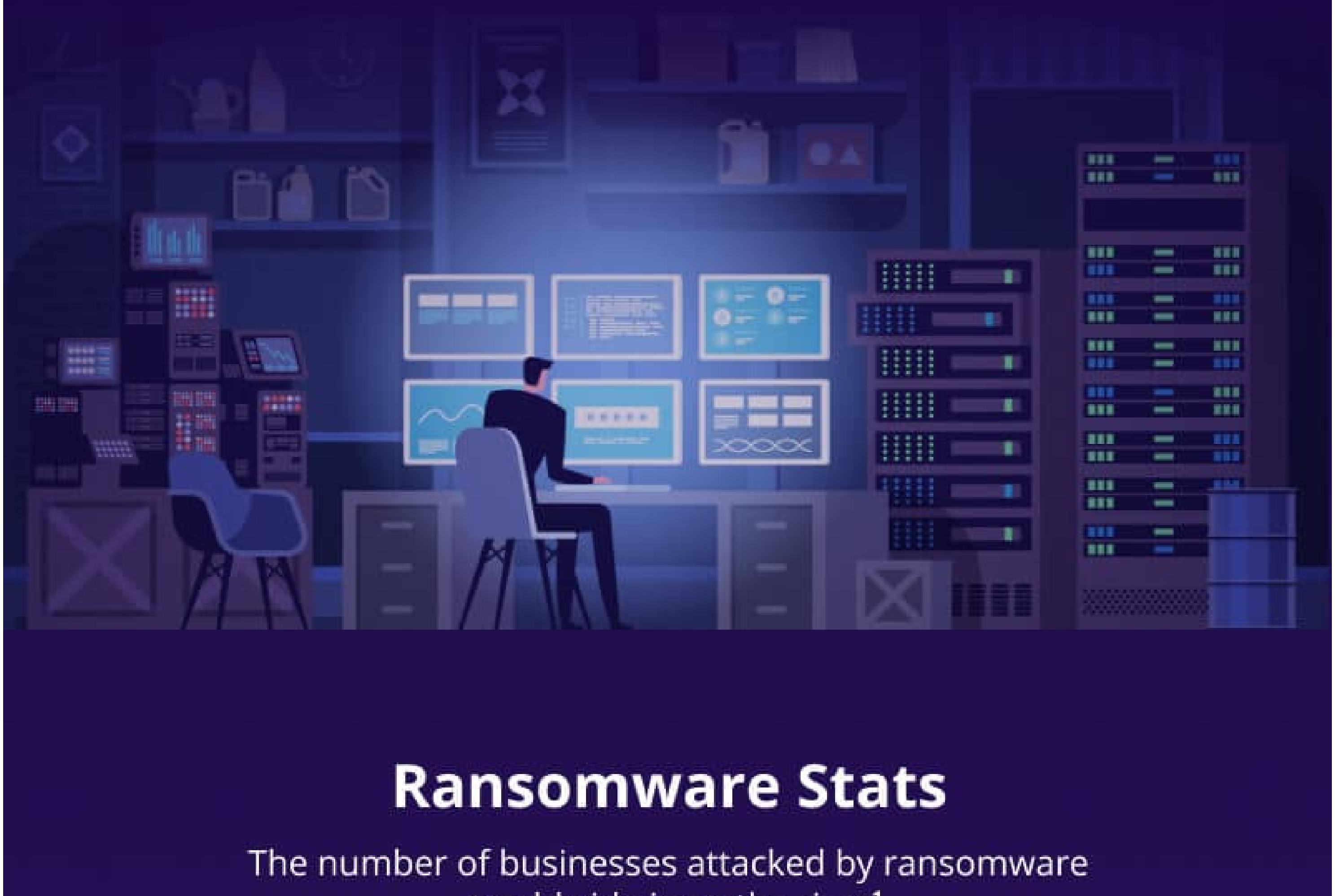
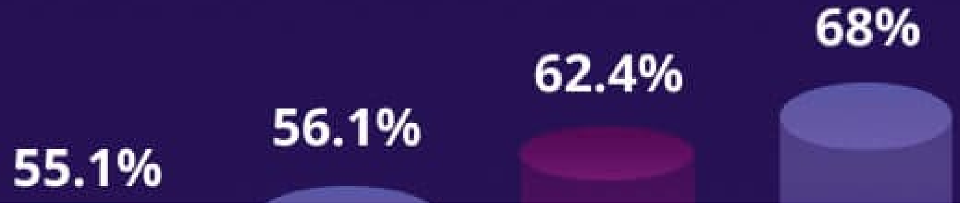
NAKIVO®

# How to Recover
from a Ransomware Attack



Ransomware Stats

The number of businesses attacked by ransomware worldwide is on the rise:[1]



2018
2019
2020
2021

Most Common Types of Ransomware

1 Locker Ransomware

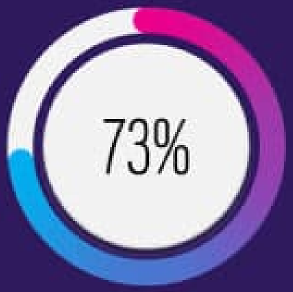
- Infects the system with a payload
- Entirely locks the user out of the system
- Displays a massage with demand to pay a ransom

2 Crypto Ransomware

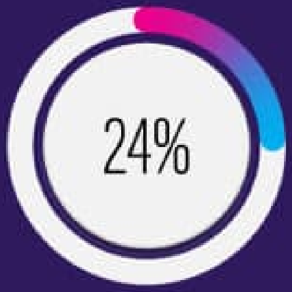
- Infects the system via a phishing mail or infected website
- Encrypts files with or without a warning massage
- Demands a ransom in return for a decryption key

Cyber Attacks Success Rates

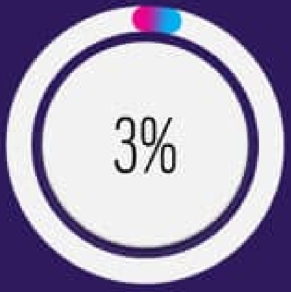
2020 Global Survey Of 5,000 IT Managers Revealed: [2]



of attackers successfully encrypted data

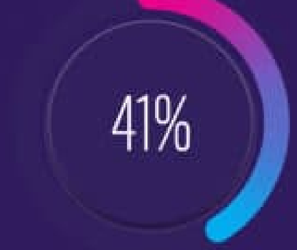


of attacks stopped prior to data encryption

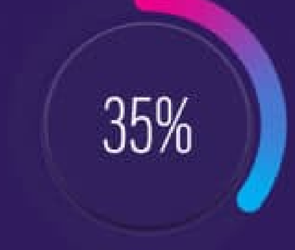


of businesses paid a ransom even though their data was not encrypted

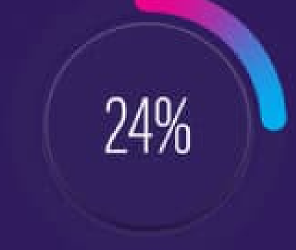
The Growing Need For Data Protection [2]



of IT managers report



say the attack took



of attacks involve data

attacks on premises and in private clouds

place in a public cloud

on-premises, in a public cloud and in a private cloud

How To Recover From A Ransomware Attack

#1 Backup

Backups are the best method to tackle ransomware-related concerns. By backing up your physical, virtual, cloud and SaaS environments, you can ensure full recoverability of your data after a ransomware attack. The more backup locations you have, the greater your chances of a complete data recovery. The 3-2-1 rule recommends keeping at least 3 backup copies — two copies on different media and one copy offsite. By having efficient backups, you can restore your objects, files and folders instantly. In fact, you can boot your machines directly from a backup to bring your downtime to a minimum.

#2 Replication to a Secondary Site

You can create replicas of your VMs and store them on a target host. If hit by ransomware, you can instantly fail over to your replicas and resume your business operations. Your replicas

business operations. Your replicas remain powered-off until needed and don't require any resources. Once the ransomware attack is contained and systems are restored, you can perform failback to your production environment.

#3 Business Continuity Planning

Create an incident response plan. The main steps include:

- Identifying which systems and processes are critical to your organization's operations
- Determining how much downtime can be tolerated for these critical systems, i.e. your RTO
- Prepare all components essential for recovery: hardware, software, staff

Recap: Ransomware Protection And Recovery

Prepare

Be prepared for ransomware attacks and implement a reliable

attacks and implement a reliable data protection solution as part of an incident response plan to avoid losing data and systems functionality.

Test

Regularly test your backups/replicas, secondary locations, recovery staff preparedness.

Recover

Ensure efficient recovery of files/app objects, full physical/virtual machines, disaster recovery

---

Ransomware Recovery With NAKIVO Backup & Replication

NAKIVO Backup & Replication is a comprehensive data protection solution for virtual, physical, cloud and SaaS environments. With NAKIVO Backup and Replication you can:

- Perform incremental backups for all your data using GFS scheme
- Benefit from app-aware and consistent backups
- Remain in compliance with 3-2-1 rule by storing backups locally

rule by storing backups locally, offsite and in the cloud

- Verify recoverability of your backups
- Perform granular recovery of single files, folders and objects
- Recover full virtual and physical machines
- Initiate automated disaster recovery

Why NAKIVO Backup & Replication

Deploy in under 1 minute

Pre-configured VMware VA, Nutanix AHV and Amazon Machine Image; 1-click deployment on ASUSTOR, QNAP, Synology, NETGEAR, FreeNAS-based and WD NAS; 1-click Windows installer, 1-command Linux installer

Protect Data Across Platforms

Native, agentless, image-based, application-aware backup for VMware, Hyper-V, Amazon EC2, Nutanix AHV; Windows/Linux physical servers and workstations; Microsoft 365 data; Oracle Databases.

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

Exclusion of swap files and partitions, global backup deduplication, adjustable backup compression.

Reduce Backup Size

Incremental backups with CBT/RCT/CRT, LANfree data transfer, network acceleration; up to 2X performance boost 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 Amazon S3, Wasabi or Microsoft Azure.

Decrease Recovery Time

Instant recovery of VMs, files, and application objects (Exchange, Active Directory and SQL); automated Site Recovery; instant and full P2V recovery

Sources:

1. Percentage of organizations victimized by ransomware attacks worldwide from 2018 to 2021, Statista
2. The State of Ransomware 2020, Sophos