

The background of the slide is a night-time aerial view of a city, likely Brussels, featuring the Atomium structure and other illuminated buildings. A blue network overlay with glowing nodes and connecting lines is superimposed on the cityscape.

VERITAS™

# Veritas Solution Day

Benelux

VERITAS PRESENTS:

**RANSOMWARE'S  
GREATEST FEARS**



# Agenda

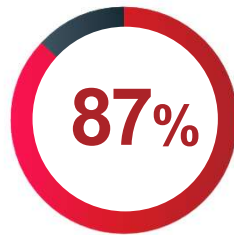
- 9'30 - Welcome - Overcoming the Fear of Ransomware & Benelux results – Vulnerability Lag Survey  
Tim Van Honsté, Managing Director, Veritas Technologies Benelux
- 9'45 - Achieving Ransomware Immunity with Protect, Detect, and Recover  
Ola Rehnberg, TS Director, Nordics & Benelux, Veritas Technologies
- 10'30 - Break
- 11'00 - Are you Prepared for When Ransomware Strikes? A Readiness roadmap  
Alain Pelegrin, Distinguished Sales Engineer, Veritas Technologies
- 11'45 - Best Practices for Hardening SaaS Applications like Microsoft 365 Against Ransomware Threats  
Frédéric Assuncao, Technology Sales, Veritas Technologies
- 12'30 - Wrap up & Lunch



# Veritas in Numbers

**Gartner®**  
**16x**  
**LEADER**

Enterprise  
Backup &  
Recovery  
Software  
Solutions



Fortune Global 500  
Trust Veritas



Customer Peer  
Rating  
**98%**  
Recommended

**Gartner®**  
**14x**  
**LEADER**

Enterprise  
Information  
Archiving



**6,000+**  
Employees  
Worldwide



**20,000+**  
Global  
Partners



**80,000+**  
Global  
Customers



**2,000+**  
Developers  
Worldwide



**2,200+**  
Global  
Patents



**800+**  
Supported  
Workloads

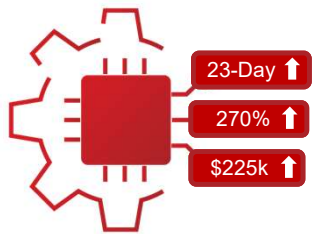


**100+ EB**  
Data Under  
Management

Gartner is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

**VERITAS™**

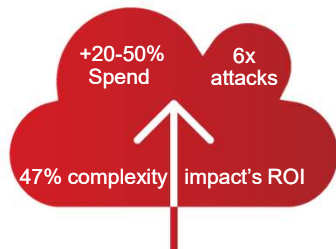
# Customer Tension Data Points



## CYBER

**Protect  
Recover  
Detect**

**Resiliency** in the face of  
a ransomware attack



## CLOUD

**Transform  
Protect  
Optimise**

**Standardise** data  
management across clouds



## COMPLIANCE

**Capture  
Archive  
Discover**

**Abide** by new data regulations



## COSTS

**Consolidation  
Optimise (ROT)  
Automate**

**Innovation** delivering  
sustainable cost savings





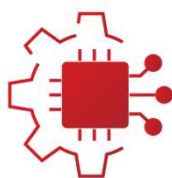
VERITAS™

# Benelux results The Vulnerability Lag Research



VansonBourne

# What is causing the Vulnerability lag?



## CYBER RISK

Security (40%) & Resiliency (42%) are within the highest reported gaps.

**Organizations are unable to keep pace.**

**94 %** of senior IT decision makers admit that at least one gap now exists in their organization's IT strategy\*



## COMPLIANCE

**There is a lack of clarity on what needs to be protected.**

On average, respondents' organizations' data is made up of 35% dark data, 53% redundant, obsolete, or trivial (ROT) data, and only 12% business critical data



## CLOUD

Cloud technology (40%) is a key reported gap because **there is a lack of clarity around what technology has been introduced.**

Only 68% of surveyed senior IT decision makers believe that they can confidently and accurately state the exact number of cloud services that their organization is currently using



## COST

**Organizations would need to spend an average of \$2.14 million (USD) to close the gaps in their technology strategy within the next 12 months.**

On average, respondents think that their organization would need to hire 17 full-time IT employees to close the gaps in their technology strategy within the next 12 months

# What is causing vulnerability and risk?

The Vulnerability Lag | Benelux

## How vulnerable are businesses as a result?

92%

of Benelux organizations  
have experienced downtime  
in the last 12 months



2.84

The average organization  
has experienced 2.84  
ransomware attacks that led  
to downtime in the last 12  
months, with 22% having  
been hit five times, or more



54%

report that their organization's  
focus on software updates  
and upgrades has  
changed/increased for  
security purposes as a result  
of COVID

VERITAS™



“30% of ITDMs surveyed said that their organization’s security measures have slightly or significantly lagged since the implementation of COVID-led digital transformation initiatives over the last 18 months.”





“ **22%** admit to five or more ransomware attacks causing downtime in the last year – higher than the global total of 14%.”



## What customers wants to know

**How can I reduce the chance an attack is successful?**

**If an attack is successful, how can I limit any disruptions?**

**How do I know I am recovering from clean data?**



VERITAS™

# Achieving Ransomware Immunity with Protect, Detect and Recover

Ola.Rehnberg@veritas.com, Technical Sales Director,  
Veritas Nordics & BeNelux





A sign telling shoppers that this Coop store is temporarily closed. Credit: Lisa Abrahamsson/TT

#### IT SECURITY

## ▶ Coop supermarkets reopen after ransomware attack on US tech provider

4:26 min [My playlist](#) [Share](#)

Published torsdag 8 juli kl 15.03

- Supermarket chain Coop says it will open all of its stores on Thursday, after they closed due to last week's extensive IT attack.
- Since the attack last Friday, technicians have worked to restart every checkout at all of the chain's 800 stores.
- "Coop is one of the businesses hit hardest. To not be operating at full capacity for nearly a week is quite remarkable," says Swedish Radio's IT expert Sven Carlsson.



# Feedback from our BeneLux Customers

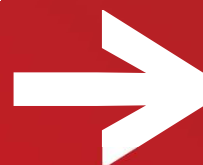
Source: Vulnerability Lag Survey, Nov 2021



**40%** admit that their organization's security measures have lagged since the implementation of COVID-led digital initiatives\*



**54%** of BeNeLux companies mention cloud as one of the major contributors



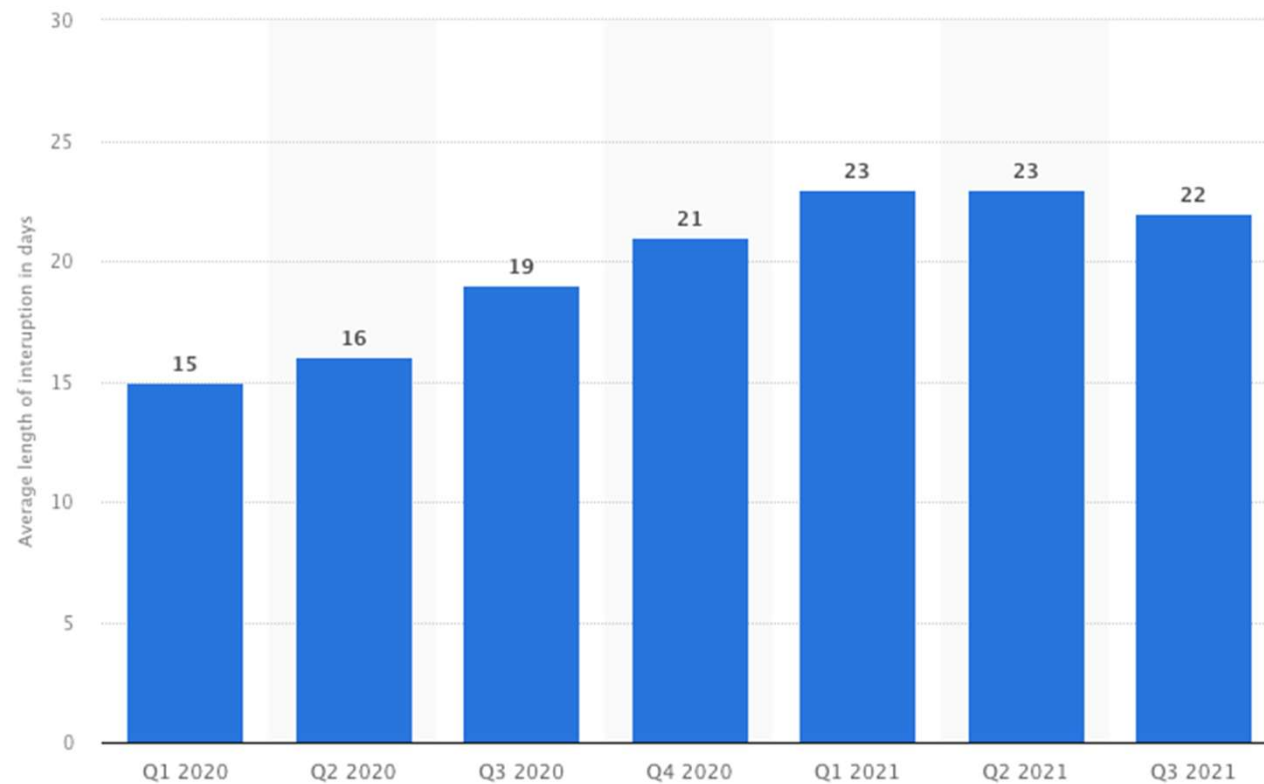
**59%**



experienced at least one **ransomware attack** that caused downtime last year

*\*over the past 18 months*

# Average Time To Recover from a Ransomware attack



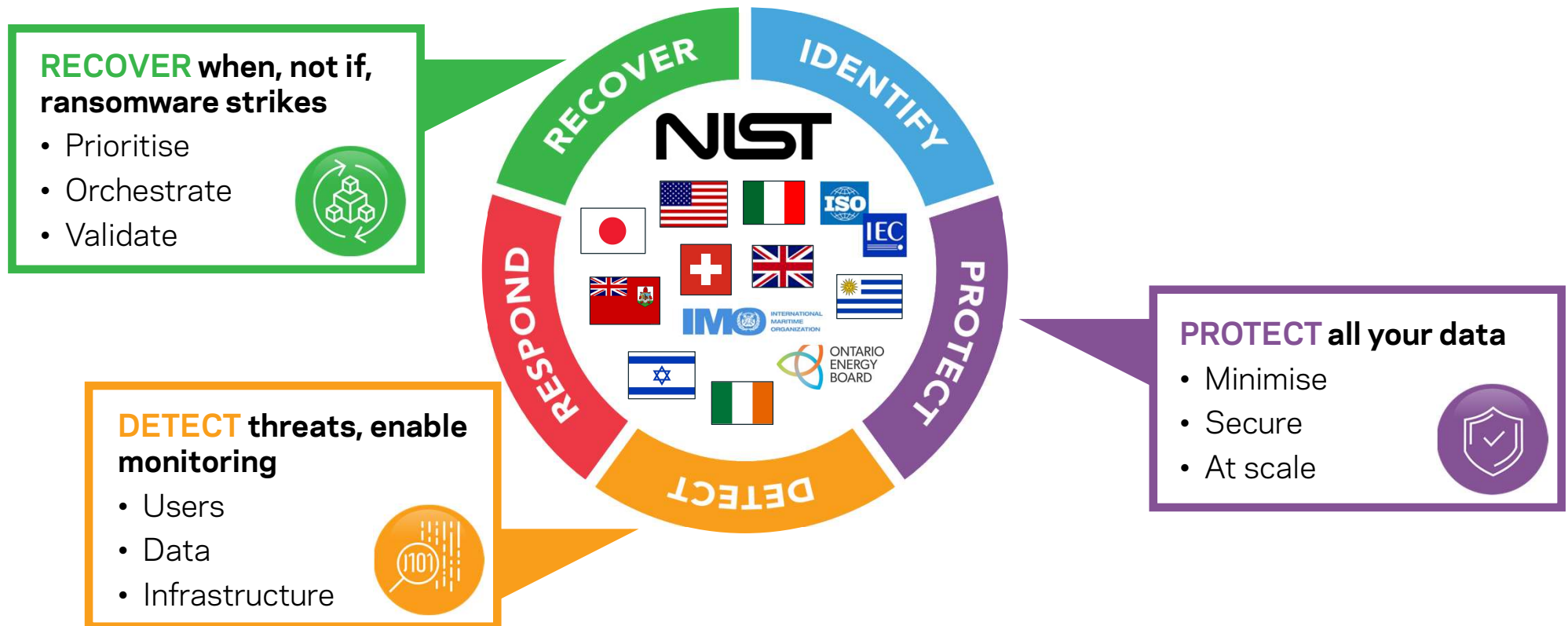
© Statista 2022

Copyright © 2022 Veeva Technologies LLC

[Show source](#)

# Effective Data Management

A key to closing the resiliency gap





## Comprehensive Platform and Workload Support

- Protect 800+ different sources
- Automated discovery
- Performance and Scale
- Optimized backup, data transfer and storage



## 3 – 2 – 1 Principle

- Automated Storage Lifecycle Policies
- Optimised duplication
- Virtual air-gap between storage pools



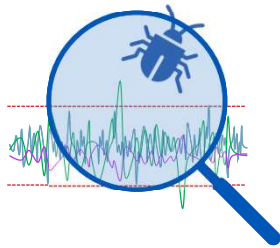
## Bullet-proof Platform

- Hardened, SELinux-based, containerised OS
- Role-based access control – Principle of Least Privileged Access
- Immutable & indelible storage with hardware compliance clock
- Robust network controls



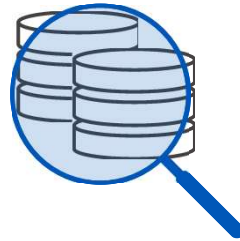


# Detect



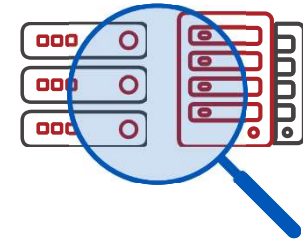
## Backup / Recovery Anomaly & Malware Detection

- Machine learning algorithm creates a baseline of backup activity
- Incidents outside of the baseline are flagged as potential anomalies
- Malware detection of high-risk backup data and prior to data restore



## Anomaly Detection in Primary Storage

- Identify anomalous user activity or irregular activity on sensitive data
- Detect over 700+ sensitive data patterns & potential malware file types
- Activity metrics identify anomalies and trigger responses against policy
- Multi-dimensional analysis of permissions, deviations and alerts



## Actionable Insights into your Infrastructure

- Identify partial or failed backups that report as successful by the backup software
- Unprotected data discovery—automatically identify clients and data sets that aren't protected under a backup policy



# Recover



Granular File  
Recovery



Bare Metal  
Recovery



Bulk/Instant  
Recovery



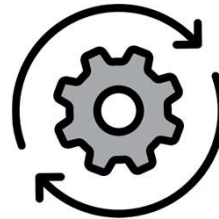
Instant  
Access



CDP  
Rollback

## Comprehensive Recovery Options

- Size for restore, not for backup
- Use a layered recovery strategy
- Select the right recovery option for the situation



## Automated Recovery & Testing

- Automated bulk failover, failback & rehearsal
- Pre-define dependencies between application components



## Cloud Recovery

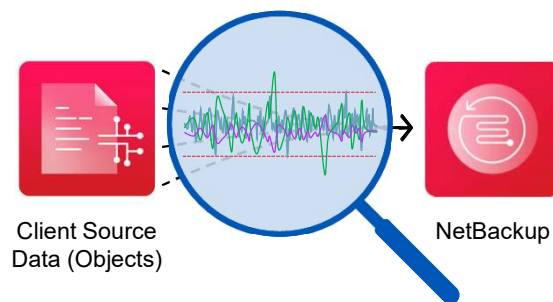
- Fully automated recovery in the cloud
- Recover from deduplicated backup copy of data in cloud object storage



DETECT

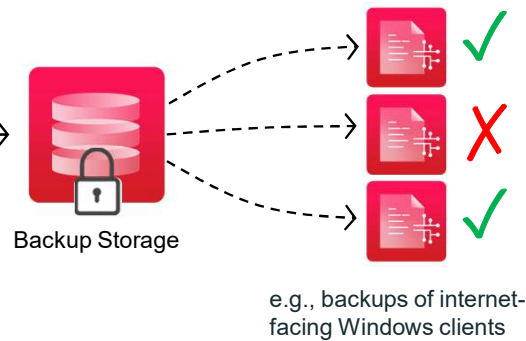
# New NetBackup Active Anomaly Detection and Malware Scanning

## During Backup



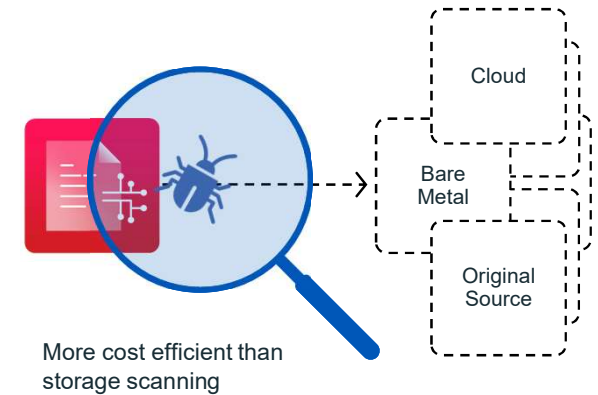
AI Anomaly Detection  
Near Real-Time

## Post Backup



Automatic Malware Scanning  
Based on Anomaly Detection

## Before Restore



Scanning Prior to Restore  
Ensures Clean Data

nbprime2 - NetBackup Administ

Not secure | https://nbprime2/webui/dashboard

Veritas NetBackup™

1

?

⚙

R

«

Dashboard

Activity monitor

Recovery

Protection

- Protection plans
- Policies

Workloads

Storage

- Storage configuration
- Storage lifecycle policies

Catalog

Detection and reporting

- Anomaly detection
- Malware detection
- Usage

Credential management

Hosts

- Host properties

Hello, root

JOBS

Last 24 hours

0

Active

0

Queued

6

Failed

59

Success

3

Partial success

0

Retries

MALWARE DETECTION

Last 24 hours

1

Impacted

0

Not impacted

0

Pending

0

In progress

0

Failed

ANOMALY DETECTION

Last 24 hours

0

Not reviewed

0

High severity

0

Medium severity

0

Low severity

CERTIFICATES

NetBackupExternal

3

All

1

Revoked

2

Valid

0

Expired

TOKENS

1

All

1

Not valid

0

Valid

SECURITY EVENTS

Access historyAudit events

Tuesday

Feb 8

04:28:32 pm

R

User 'root' authenticated successfully from 192.168.2.70

04:27:58 pm

R

User 'root@nbprime2' is logged out

04:22:35 pm

R

User 'root' authenticated successfully from 192.168.2.70

02:12:29 pm

R

User 'root' authenticated successfully from 192.168.2.70

Monday

Feb 7

10:13:27 am

R

User 'root' authenticated successfully from 192.168.2.70

Friday

Feb 4

05:08:55 pm

R

User 'root' authenticated successfully from 192.168.2.70

Veritas™ NetInsights Console

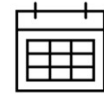


# NetBackup Recovery Vault

## Seamless Cloud Storage-as-a-Service



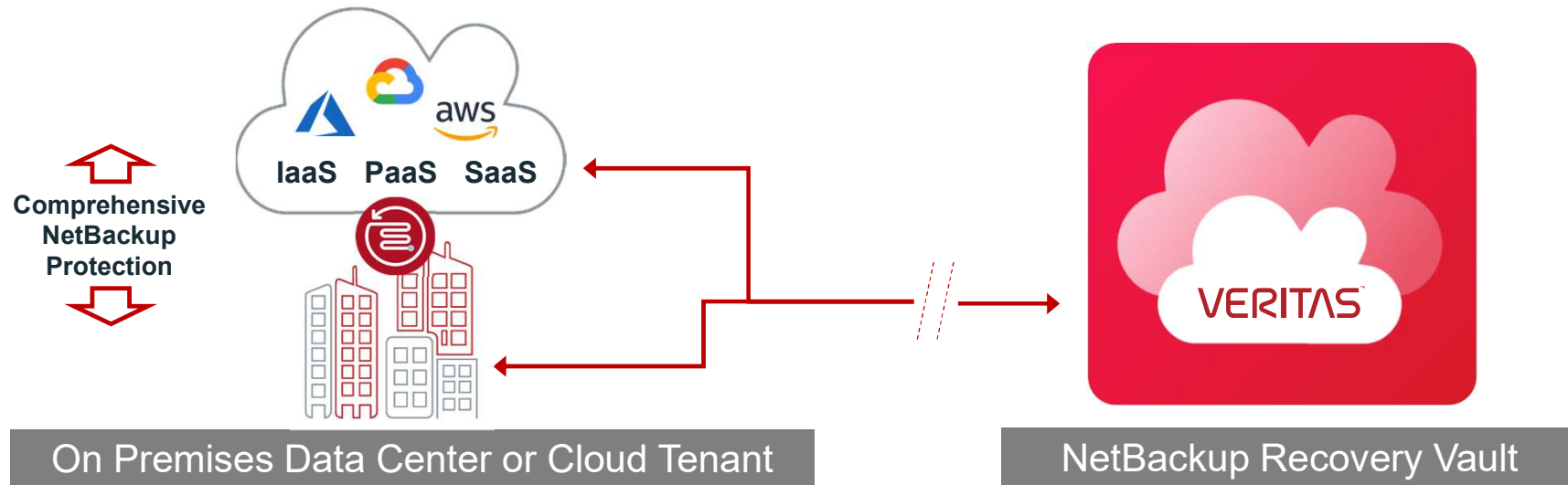
BETB




1 or 3  
years



Includes  
data  
transfer



- Provisioned Securely in NetBackup
  - RBAC Authentication
  - Subscription based
  - Consumption reporting
- Automated Resiliency

- Air-Gapped ransomware protection
- Recover to cloud or data center
- Limitless scale
- Predictable costs
- Powered by Azure 

Note: Additional monthly billing may apply if overages are measured for storage consumption or data operations.

# Summary



Ransomware attacks are on the increase.



Organisations are more vulnerable than ever, as Digital Transformation outpaces resiliency measures.



Protect



Detect



Recover



Effective data management is a critical ransomware resiliency measure.

A night cityscape with a network overlay. The background shows a city at night with lights and buildings. Overlaid on the city is a network of blue lines and dots, representing a digital or cyber network. The network lines connect various points across the city, some of which are highlighted with blue dots. The overall theme is digital security and network immunity.

VERITAS™

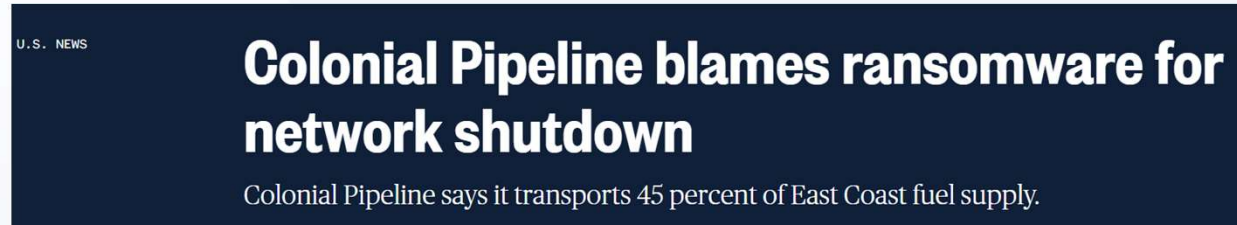
# Achieving Ransomware Immunity

with **Protect, Detect, and Recover** Best Practices

Alain Pelegrin, Distinguished Engineer



The Colonial Pipeline event was not the first nor the last but garnered enough attention for CEOs globally to question whether they have done enough to prepare



Economy | Oil and Gas | **Bloomberg**

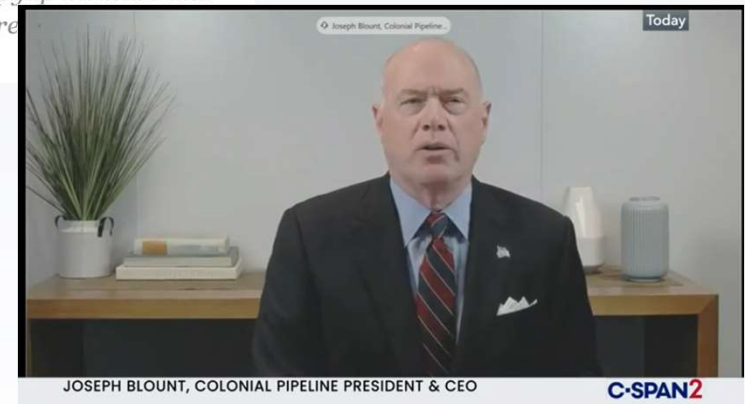
## Petrol shortages sweep US as Colonial Pipeline remains down

*Four days into the crisis, Colonial Pipeline Co has only managed to restart a small segment of its pipeline as a stopgap measure and*

**Colonial Pipeline Co. paid nearly \$5 million to Eastern European hackers on**

Friday, contradicting reports earlier this week that the company had no intention of paying an extortion fee to help restore the country's largest fuel pipeline, according to two people familiar with the transaction.

The company paid the hefty ransom in difficult-to-trace cryptocurrency within hours after the attack, **underscoring the immense pressure faced by** the Georgia-based operator to get gasoline and jet fuel flowing again to major cities along the Eastern Seaboard, those people said. A third person





# Business impact of Ransomware



## Direct

Production / Services impact by unavailability of IT resources

Loss of business because of Brand and reputation damage

Publicly traded companies stock value impact

## Indirect

Inability to deliver contractual obligations to 3<sup>rd</sup> parties leading to litigation

Legal compliancy impact – possible loss of data and records

Closures, layoffs, loss of talent



# The Main Ransomware Challenges Articulated by Customers

**How can I reduce the chance an attack is successful?**

**If an attack is successful, how can I limit any disruptions?**

**How do I know I am recovering from clean data?**

**Solved by a multi-layered strategy based on best practices**

Protect

Detect

Recover

# What is ransomware?

- Ransomware

- Encrypts your data
- Will try to disable ability to restore data from backups
- Opens ability to download the customer's data – threat to publish private records, financial and business records, contracts
  - Will allow attackers to also blackmail the victim's business partners and their customers

- Why isn't it just detected by corporate security frameworks?

- Sophisticated signature changing payloads
- Targets weakest link – a user or an application
- Most ransomware had ability to remain “dormant” and propagate before going active

- Paying?

- No guarantees exist you'll get a decrypt key, or your data no longer being used
- No guarantees about decryption algorithm performances



# What is The Zero Trust Security Model?

**Not trusting** any devices—or users—by default, even if they're inside the corporate network.

‡ **Institute Identity and Access Management (IAM)**

controls (for both users and machines)

- Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC)

‡ **Encrypt data** both in-flight and at-rest to reduce data exfiltration leverage (use data loss prevention software).

‡ **Limit access to backups** (no one with access to primary data should also have access to backups).

‡ **Implement security analytics** to monitor for and mitigate malicious activity.

“

Zero Trust... is useful as a shorthand way of describing an approach where implicit trust is removed from all computing infrastructure. Instead, trust levels are explicitly and continuously calculated and adapted to allow **just-in-time, just-enough-access** to enterprise resources.”

**Neil MacDonald**

VP Analyst, Gartner



# Effective Data Management

A key to closing the resiliency gap

Stop Ransomware by  
implementing a Prevention and  
Detection first strategy

**RECOVER** when, not if,  
ransomware strikes

- Prioritise
- Orchestrate
- Validate

**DETECT** threats, enable  
monitoring

- Users
- Data
- Infrastructure



**PROTECT** all your data

- Minimise
- Secure
- At scale

# A Multi-Layered Approach Based on Zero-Trust Principles

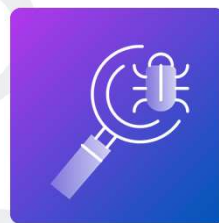
1



## Protect

- ✓ Support more enterprise workloads than any other ISV
- ✓ Bullet-proof intrusion prevention
- ✓ Industry-leading immutable storage options

2



## Detect

- ✓ Cost-efficient malware scanning
- ✓ Near real-time, AI-based anomaly detection
- ✓ Total infrastructure visibility edge to core to cloud

3



## Recover

- ✓ Automated recovery orchestration to anywhere, cloud & bare metal
- ✓ Non-disruptive recovery testing
- ✓ Instant access recovery and roll-back

STEP 1:

# Protect



# Protection Basics Prevention

2/3

Do not follow basic data protection prevention best practices

Source: Veritas Ransomware Resiliency Report, Oct 2020

## 3 – 2 – 1 Backup Rule



3 backup copies on

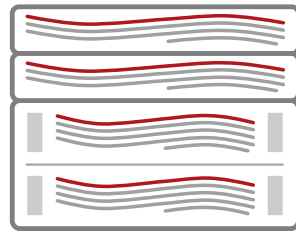


2 types of Media



And 1 offsite copy

## Hardened Backup Infra

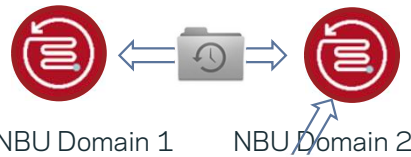


Appliances

Hardened  
Linux OS  
Intrusion Detection /  
Protection  
Firewalled  
Secure

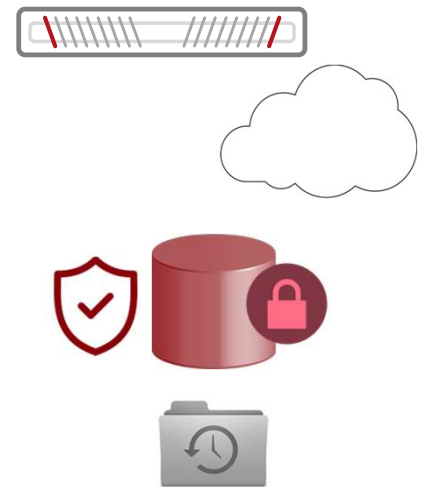
## Air GAP

Auto Image Replication



One to One  
Many to One  
One to Many

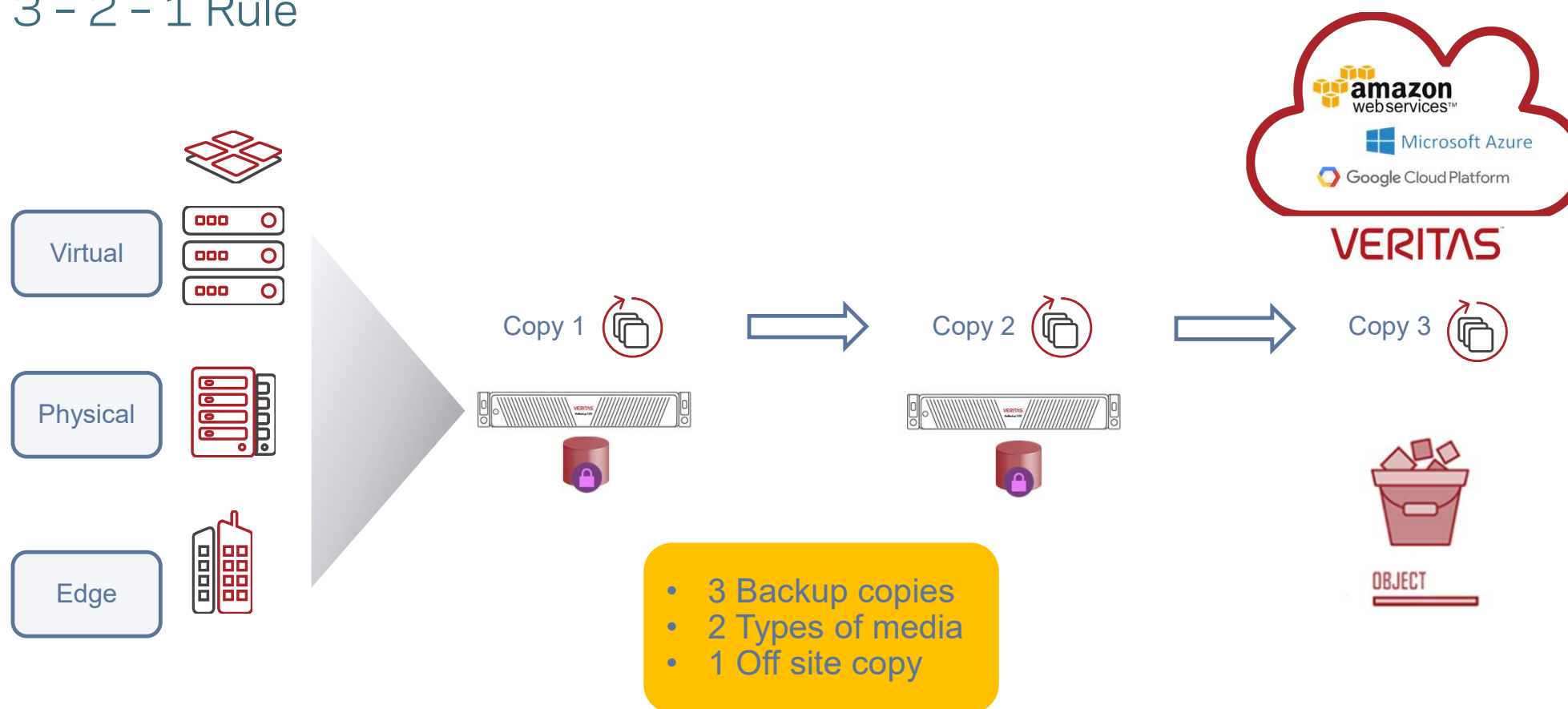
## Immutable backup Storage



Immutable Storage  
Flex Appliance / Cloud  
Indelible Storage

# Protection basics

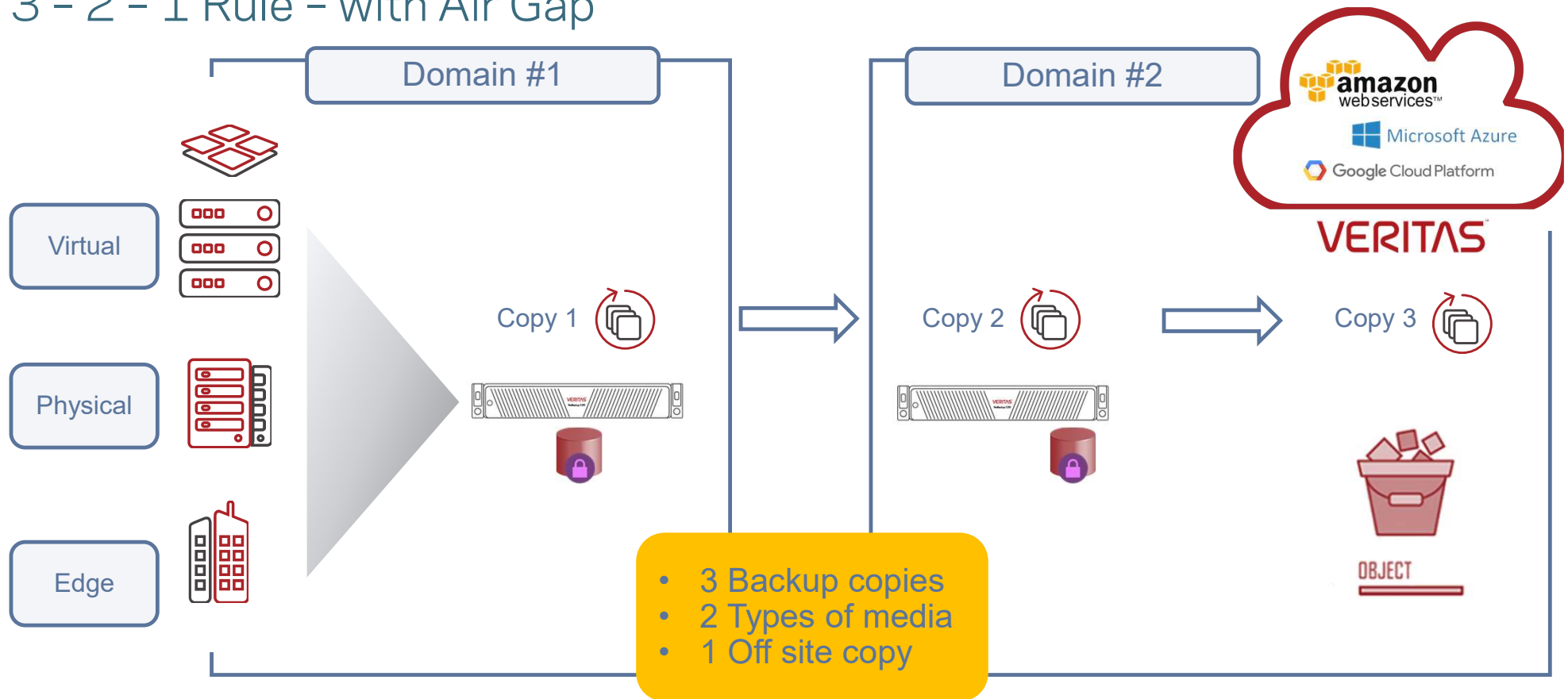
## 3 - 2 - 1 Rule



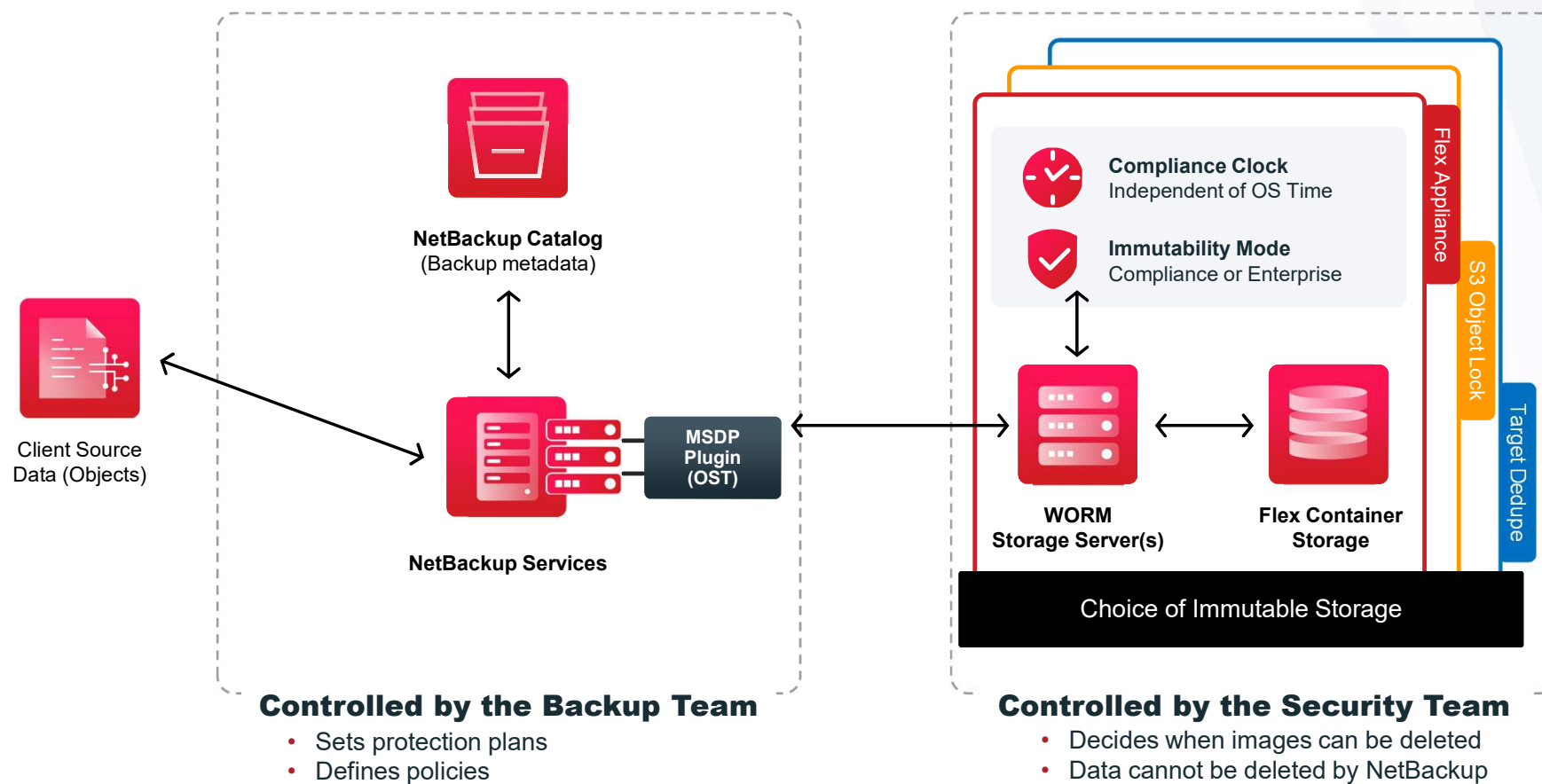


# Protection basics

## 3 - 2 - 1 Rule - with Air Gap



# Immutable Storage



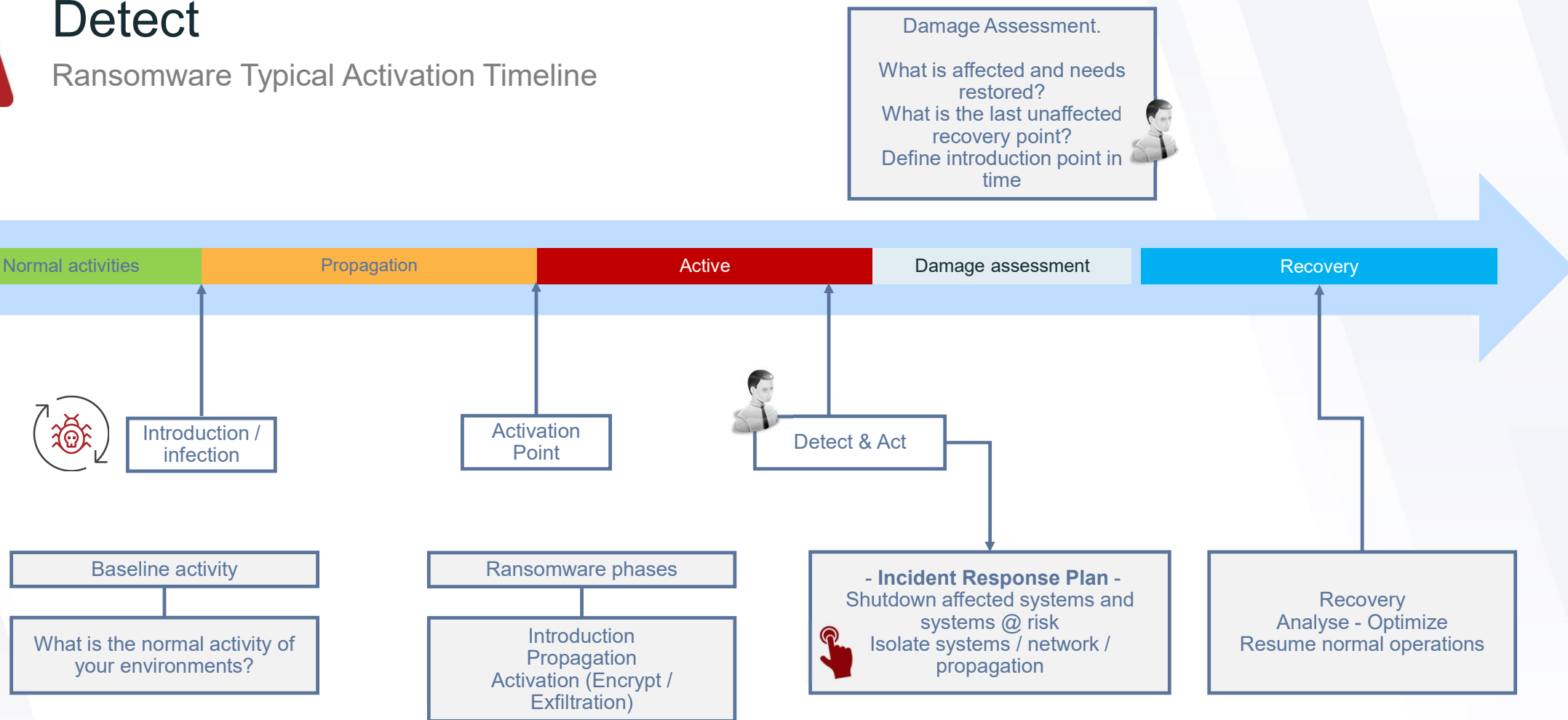


STEP 2:

# Detect

# Detect

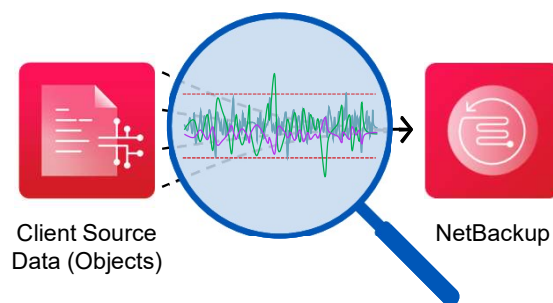
## Ransomware Typical Activation Timeline





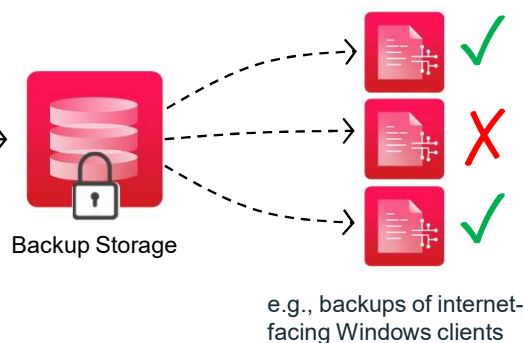
# High-Level Overview of Malware Detection in NetBackup

## During Backup



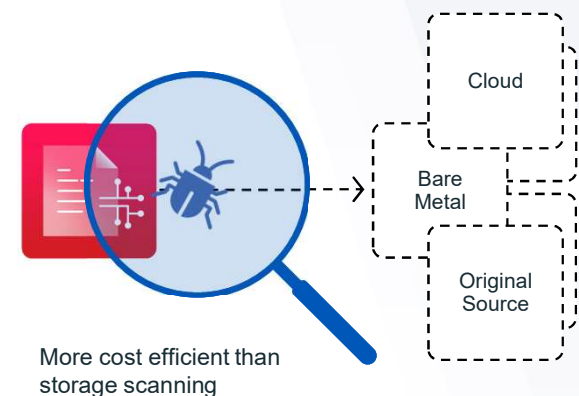
Anomaly detection in near real-time

## Post Backup



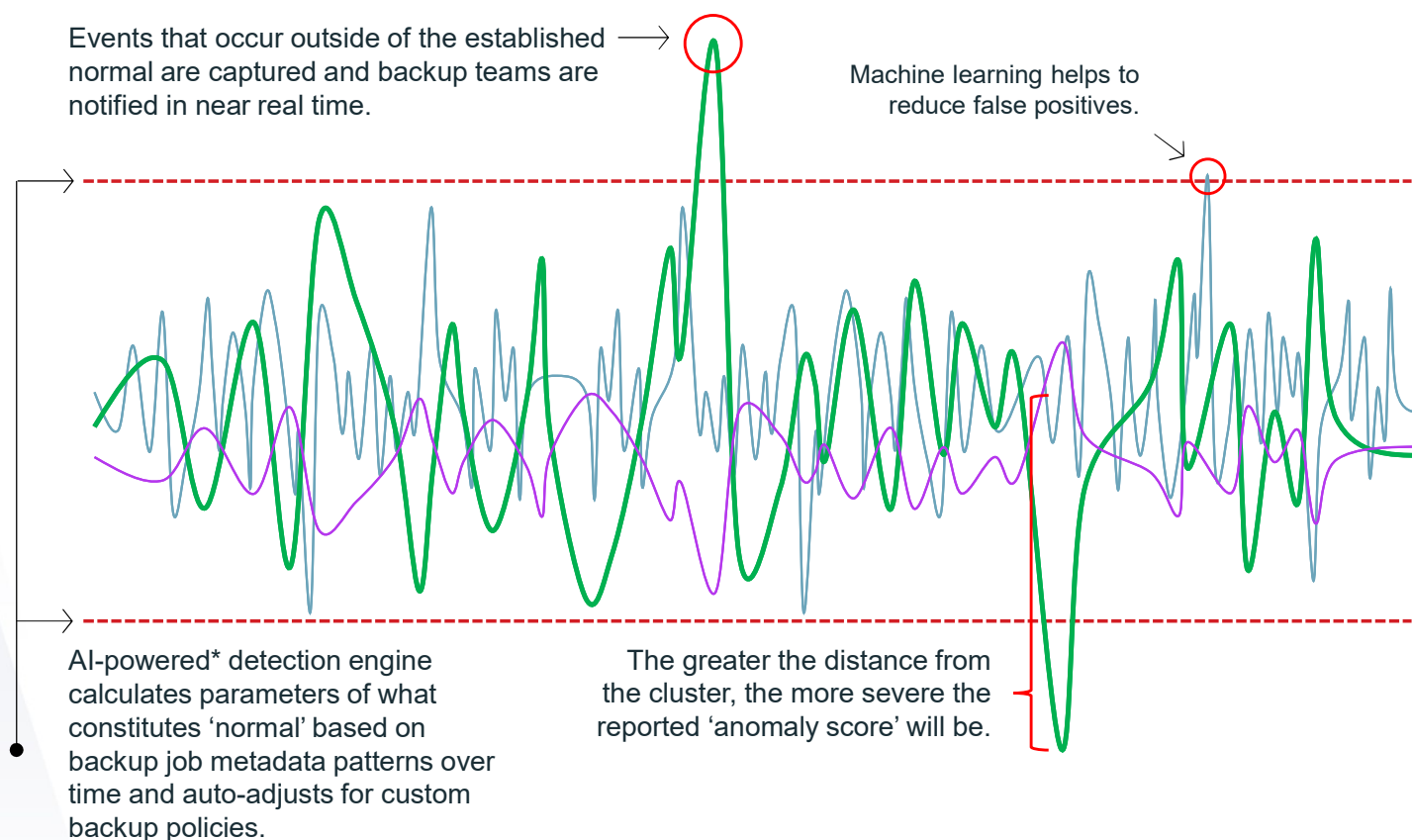
Spot-checking of known high-risk areas

## Before Restore



Scanning before restore to ensure clean data

# Understanding Anomaly Detection



## AI-Powered Anomaly Detection Engine in NetBackup

- Mine enormous amounts of data
- Automate monitoring and reporting
- Gain actionable insights
- Report based on several criteria
- Establish early warning of an attack

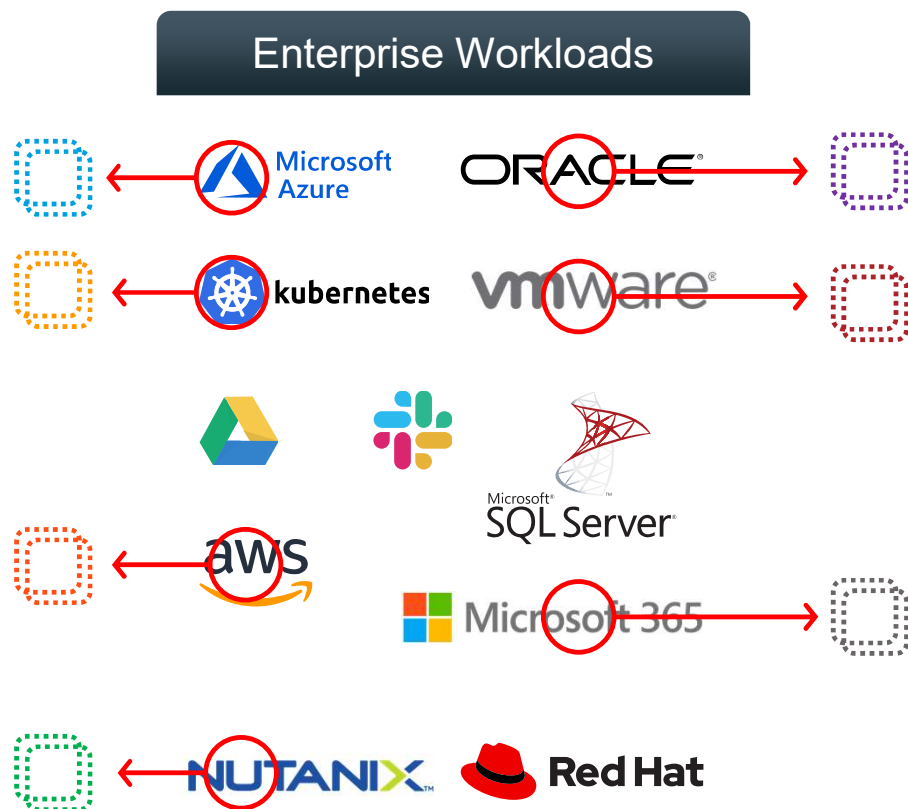
\* Machine learning model takes advantage of data pre-seeding using nbdeployutil. AI is powered by DBSCAN algorithm.

STEP 3:

# Recover



# Optimizing for Recovery, Not just Backup



Copy of important data? ✓

Optimized recovery experience? ✗

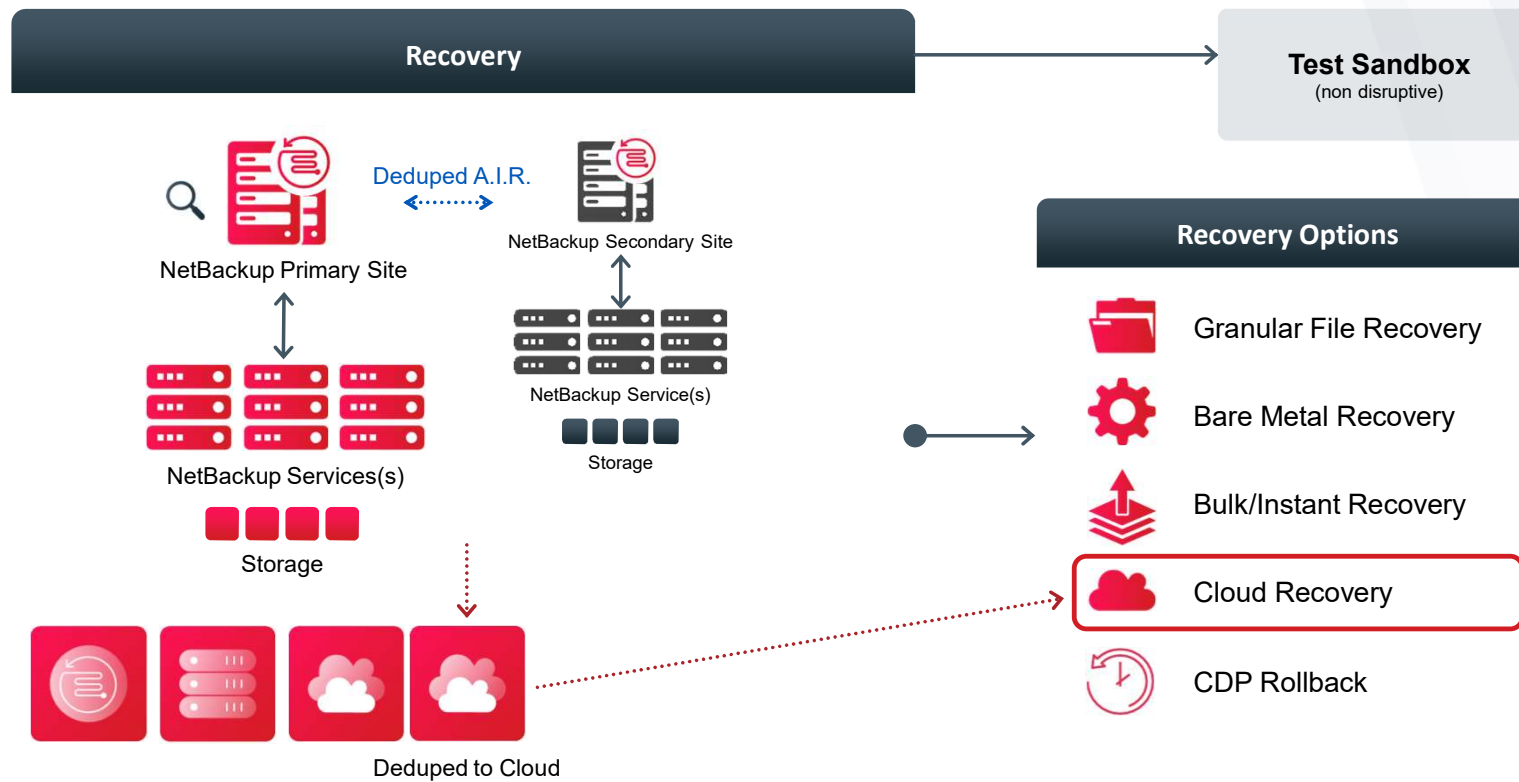
Multiple disparate backup solutions by design create a **complicated recovery experience**—especially when multiple systems are compromised.

Additional considerations:

- Skills/training gaps
- Lost storage dedupe efficiencies
- No global data visibility/oversight



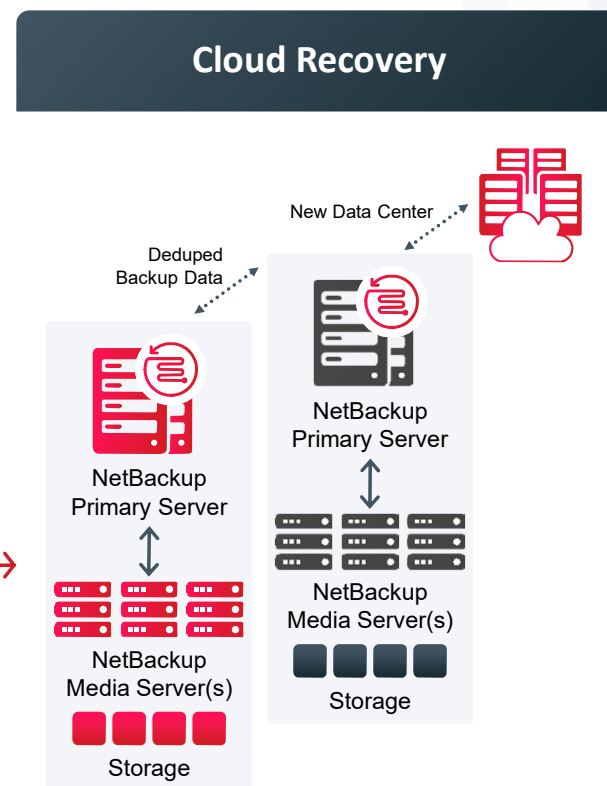
## Step 3: Recover



## Step 3: Recover

### Maintain Control

- Completely automated recovery orchestration
- Fast recovery direct from deduplicated data stored in the cloud
- Recover an entire data center in the cloud on demand



## Case Study

# Steelcase

### Use Case

Backup & Recovery

### Industry

Manufacturing

### Customer

Global office furniture producer with **\$2.6 billion** in annual revenue and **11,000 employees** worldwide.

## CHALLENGE

Facing a growing cybersecurity threat, Steelcase wanted to ensure it was prepared.

## SOLUTION

Steelcase has long trusted Veritas to support its disaster recovery and business continuity needs. When the company recently refreshed its data protection infrastructure, it selected Veritas NetBackup™ and NetBackup Appliances because of their resiliency, ease of use, centralized management, and support for automation.

## OUTCOMES

- **93% reduction in recovery times**
- **Standardized on NetBackup**

*"We have been able to build an air-gapped data protection system for images, which helps protect us from cybersecurity losses as well as ensuring that data is portable and recoverable in the event of a facility disaster."*

**Raul Coste**, Infrastructure Engineer at Steelcase Inc.

# Case Study



## Use Case

Backup & Recovery

## Industry

Manufacturing

## Customer

Global insurer company with **more than 5,000 employees** headquartered in **Johannesburg, South Africa**.

## CHALLENGE

Liberty needed to be ransomware and compliance ready, optimize data management time, transform to new technologies and evolve tape-based long-term data retention.

## SOLUTION

With NetBackup, Liberty's typical data restore of 48 hours was reduced to just 6 hours. They made the transformation to cloud-native and the need for offsite storage was significantly reduced.

## OUTCOMES

- **88% reduction in recovery time from a ransomware attack**

*"In every circumstance we've faced, NetBackup has delivered the protection we've required. This was particularly crucial when we experienced a ransomware attack. Because we had all the data in Veritas NetBackup, we were able to completely recover from the attack in just six hours."*

**Jayson Martin**, Head of IT Data Storage, Liberty Group Ltd.

# Your Plan is Only as Good as Your Last Test!

# 57%

of organizations haven't tested their DR plans within the last two months.<sup>1</sup>

**Don't be them.**

<sup>1</sup> Source: Ransomware Resiliency Report, Veritas, 2020

## Veritas can help you:

- Set up one-click, non disrupted disaster recovery testing
- Create an immutable data vault (IDV)
- Effectively utilize an isolated recovery environment (IRE)
- Ensure confidence that ransomware recovery will be successful when it counts

**Veritas had a 100% recovery success rate for customers that were hit by a ransomware attack in 2020.**

**Tracking toward a repeat in 2021!**

Automated Recovery Orchestration



# Recap: Achieving Ransomware Immunity

## What customers want to know:

**How can I reduce the chance an attack is successful?**

**If an attack is successful, how can I limit any disruptions?**

**How do I know I am recovering from clean data?**

## Best practices to ensure desired outcomes:



### **UPGRADE NETBACKUP AND EXPAND**

*Don't fight today's ransomware with yesterday's technology.*



### **ADOPT 3-2-1-1**

*Keep at least one (1) copy on immutable and indelible storage.*



### **ACHITECT FOR ZERO TRUST**

*Apply Zero Trust to communications, processes, and user access.*



### **OPTIMIZE FOR RECOVERY AND TEST**

*Limit downtime through automation and orchestration; test often.*



### **UNLOCK TOTAL VISIBILITY**

*Detect anomalies and malware across data and infrastructure.*



VERITAS™

**Thank You**

Copyright © 2021 Veritas Technologies, LLC. All rights reserved.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.



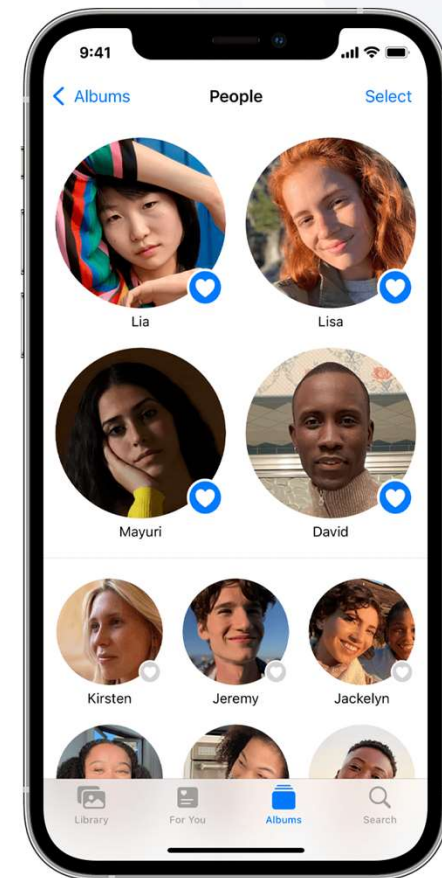
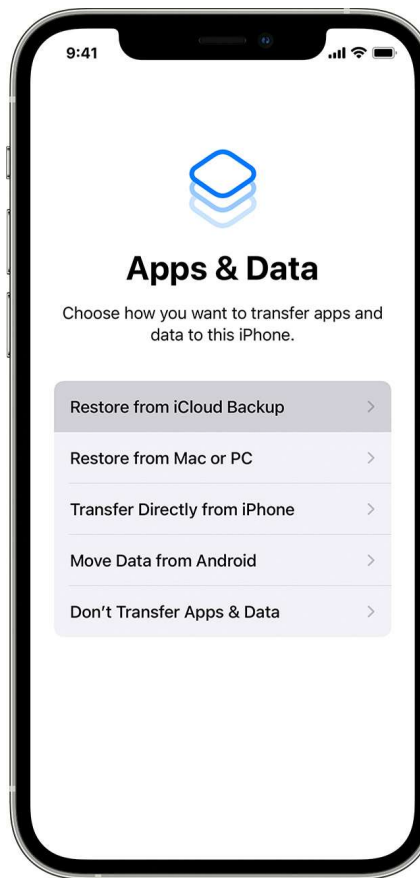


VERITAS™

# **Best Practices for Hardening SaaS Applications like Microsoft 365 Against Ransomware Threats**

Frédéric Assuncao, Specialist Technologies  
Sales, Veritas Technologies

# Another Vision of Veritas Enterprise Data Services Platform



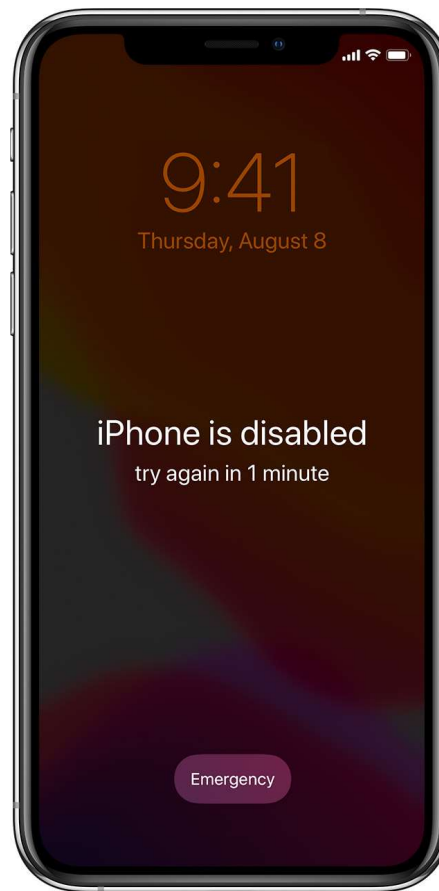
VERITAS™



*[The page contains dense handwritten Japanese text, likely bleed-through from the reverse side. The text is organized into vertical columns and includes various characters, some of which are circled or underlined. Due to the extreme density and orientation, specific words cannot be transcribed accurately.]*



# Human Error





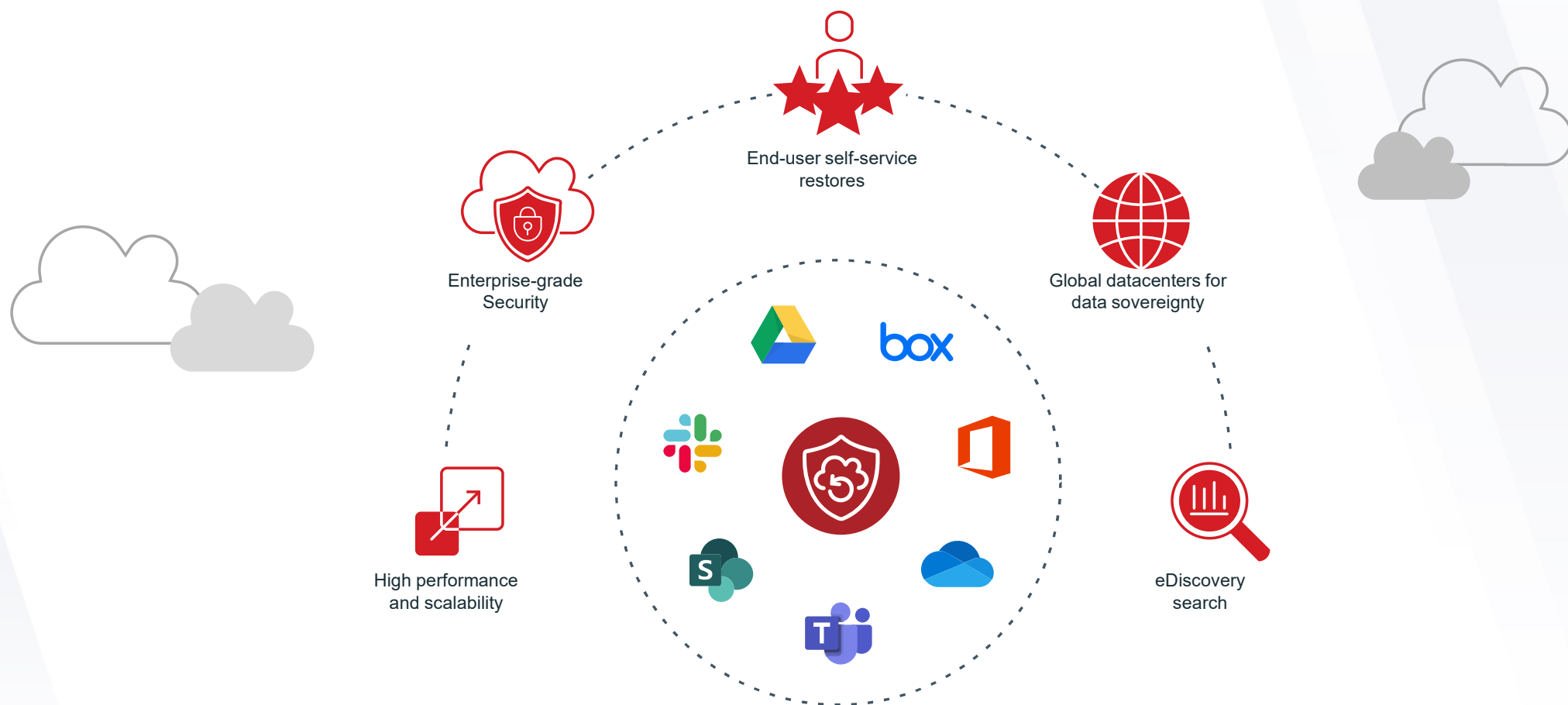
VERITAS™

# Veritas NetBackup SaaS Protection

Backup and recovery for your  
SaaS application data

# NetBackup SaaS Protection

Your single hub of secure cloud data management



# Backup and Recovery

- **Automatic data protection**

- Protection for new users, mailboxes, and folders requires no action on your part.

- **Time and bandwidth savings**

- NetBackup SaaS Protection only copies data that has changed since the last backup.

- **Flexible restore options**

- You can restore data to its original location, or to an alternate location of your choice.

- **Granular restore**

- You can restore a single file, email message, or Teams chat – or a select group of objects. NetBackup SaaS Protection also supports bulk restores.



# Do I really need backup for my SaaS data?

Yes. You really do.

## What is the “Shared Responsibility Model”?

- It's Microsoft's explicit policy – customers are responsible for protection and security of their own data.

## But the cloud makes synchronized copies of my data, doesn't it?

- Replication is not a backup! Deletes and encryption will sync to all copies.

## OK, but there's the Recycle Bin, right?

- Recycle bins have short retention and are challenging to restore from.

## But I have Microsoft E3 or E5 – doesn't that protect my data?

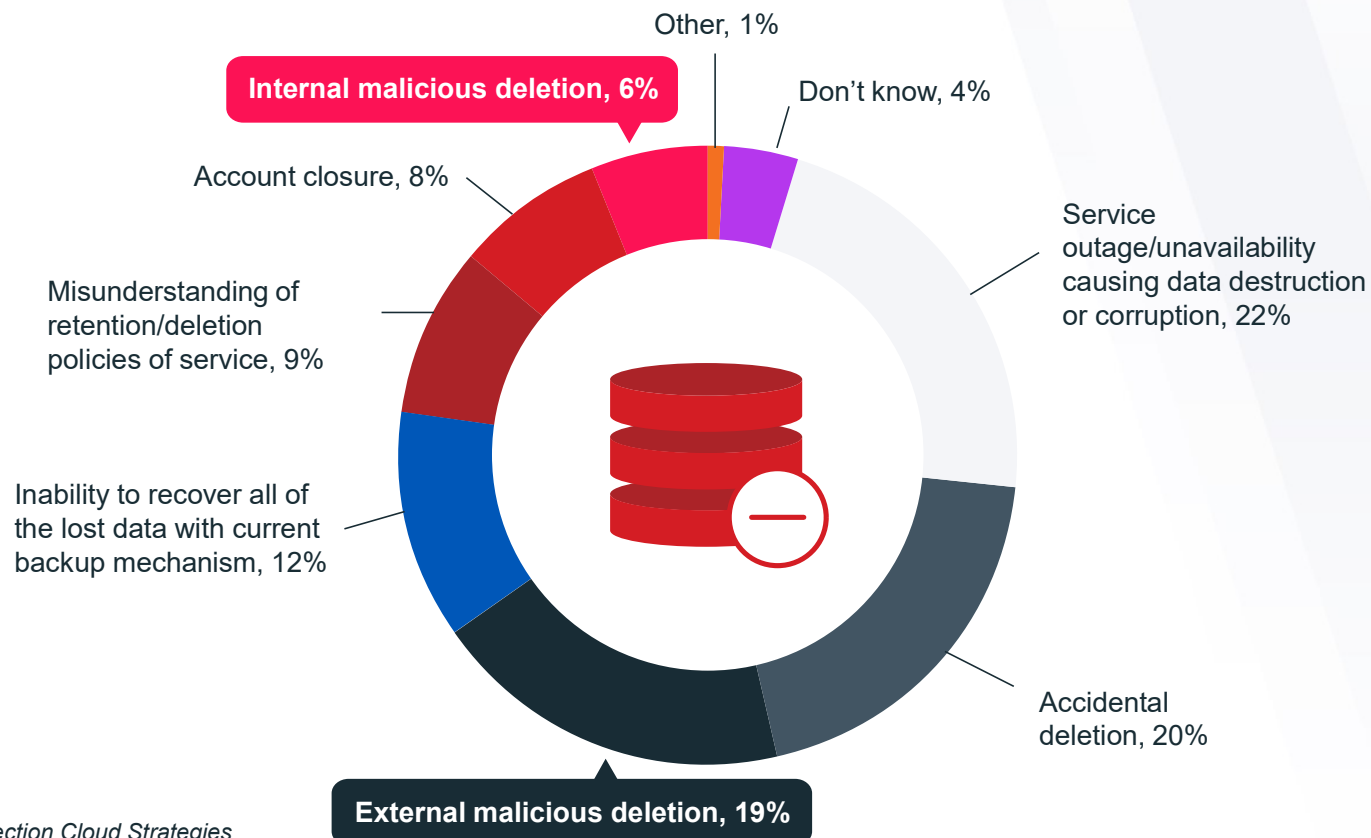
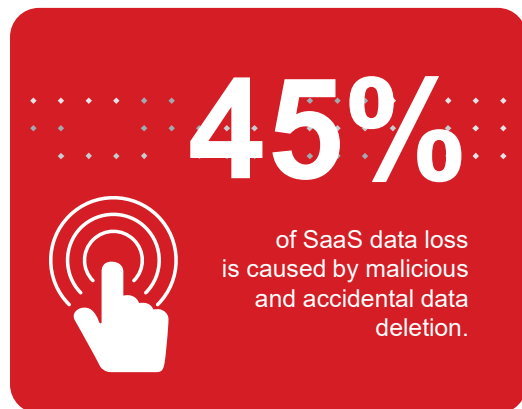
- Both E3 and E5 help with in-line threats and security, but do not provide backup.

***To have total control of your data, you must have a data protection solution for your SaaS Workloads.***



# You need to protect your SaaS applications from threats like ransomware

Native SaaS offerings are NOT enough to provide the protection you need



Source: ESG Research Report, *The Evolution of Data Protection Cloud Strategies*



VERITAS™

# Anatomy of a Ransomware Attack

SaaS data is vulnerable, too

# What is ransomware?

- Ransomware is a specific class of malware or virus
  - It won't just delete data.
  - It encrypts your data in place.
  - The bad actor claims they will give you the key to decrypt your data – at a price, of course.
- More sophisticated ransomware steals a copy of the data
  - The data will be mined, looking for:
    - Employees' personal data. (e.g., credit card, Social Security numbers)
    - Your organization's intellectual property. (e.g., trade secrets, plans for future products)
    - Any evidence of bad behavior. (e.g., unethical business practices, litigation against you)
- The bad actor then tries to blackmail you, threatening to make your data available to the public...



# But surely SaaS is not affected by ransomware, right?

Sadly, no – any data your users can access is vulnerable

- **I thought that anything stored in the cloud is safe from ransomware.**
  - Some people **believe cloud provides protection** from ransomware, but they also thought that their cloud data was being backed up by their provider, but both are **not services offered by the providers.**
- **OK, maybe cloud storage is vulnerable, but isn't SaaS safe?**
  - If only...
  - Security experts have found **multiple examples of malware** “in the wild” **specifically targeting SaaS applications.**
- **But ransomware only affects data on the local machine...**
  - Not quite – **any data the user or their machine can access can be attacked.**
  - **Some applications** like OneDrive **store a local copy of the data.**



# The harsh reality of ransomware

It can happen to anyone

**We're **ALL** just a **single mis-click** away from  
having our organizations fall victim to  
ransomware.**

**Not just a mis-click by an **administrator** – but  
**a mis-click by any one of our users.****



# How ransomware attacks SaaS – through your users

## Bob from Product Marketing

- Bob took the corporate security training, but just so he could “check the box”.
- Bob feels like he’s overloaded and always trying to catch up, jumping from task to task.
- Bob’s moving so fast all the time, it’s easy to see how he might click a malicious link or open an infected attachment without really thinking about it.

## Sue from Product Management

- Sue took the corporate security training very seriously and works to be vigilant.
- Sue is on top of her workload and only moves to the next task when the first is done.
- Sue is very diligent and works to only open attachments from people she trusts, and she checks every link before clicking. She will easily avoid 9 out of 10 phishing attempts.

***It’s easy for ANY user to make a mistake – that’s why you back up your data.***

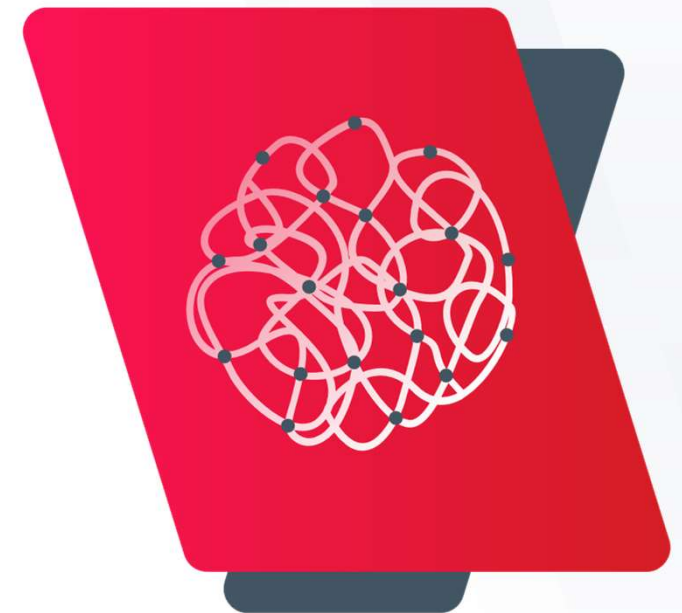
# How ransomware hits your organization's data

- One of your users makes that bad mis-click whether it's a link or attachment.
- This unleashes the ransomware which starts in doing its thing – in this case, that means encrypting all the user's files.
- That's bad enough, but it doesn't stop there – it encrypts every file for which the user has write access.
  - Do you use shared spaces for collaboration, like OneDrive and SharePoint?
  - ALL files that the user can edit get encrypted.
  - It doesn't matter who owns them or what folder they're in.



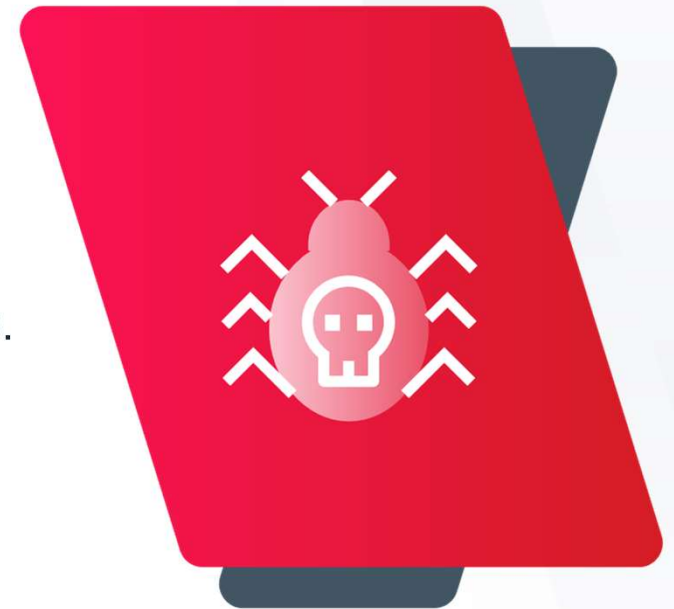
## Why this makes a horrible mess

- This could hit hundreds of files – even with a single user as the “point of entry”.
- The Recycle Bin is useless here.
- Most organizations will have no easy way to identify which specific files were affected.
- Most SaaS backup solutions have an “all or one” approach to restores – forcing you to choose between overwriting unaffected files or recovering them one by one...



## It can be even worse than that...

- Ransomware creators are aware that frequent backups are the best way their victims can “bounce back” quickly from an attack.
- More and more ransomware now includes code to have the ransomware attack and encrypt your backup data, too.
- If both your Production environments and your backups get infected, you’re pretty much done for.



## How NetBackup SaaS Protection can help

- Keeps a completely segregated copy of your data.
- Stores backup data on immutable storage – your backups are not vulnerable to ransomware attacks.
- NetBackup SaaS Protection has enough performance to run multiple backup jobs each day – and in continuous data protection mode on site collections.
  - Greater backup frequency minimizes data loss.
- The high performance makes for speedy restores.
  - Fast restores minimize the time lost.



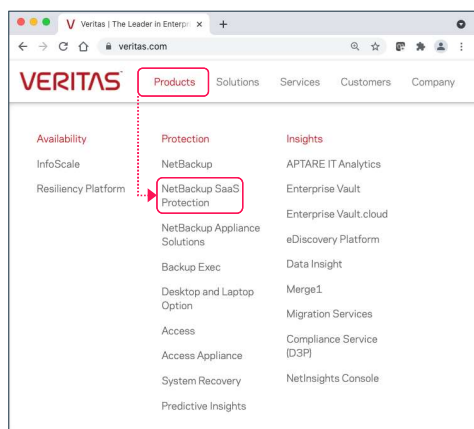
# Why Choose NetBackup SaaS Protection?

- Protects data from loss and ransomware, putting you in control of your data.
- Designed from the ground up to protect multiple enterprise SaaS application workloads.
- Best-in-class SaaS backup performance, scalability, and security provisions.
- Dedicated tenancy and data sovereignty via multi-geo support.
- Veritas NetBackup suite of solutions is the leader in the enterprise data protection market.

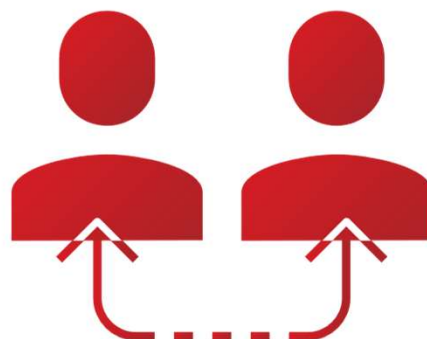




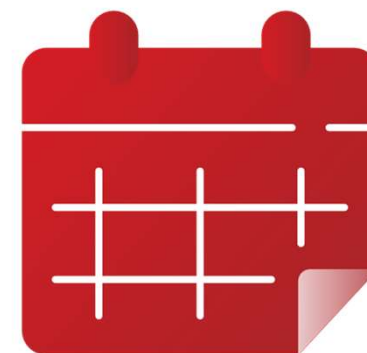
# Want to know more?



Find more info on NetBackup SaaS Protection on [veritas.com](https://www.veritas.com).



Set up a call or meeting with your Veritas account manager.



Schedule a demo for your organization's specific data protection requirements.

Always have a “Plan B”



VERITAS™





VERITAS™

Thank You

Copyright © 2021 Veritas Technologies, LLC. All rights reserved.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.