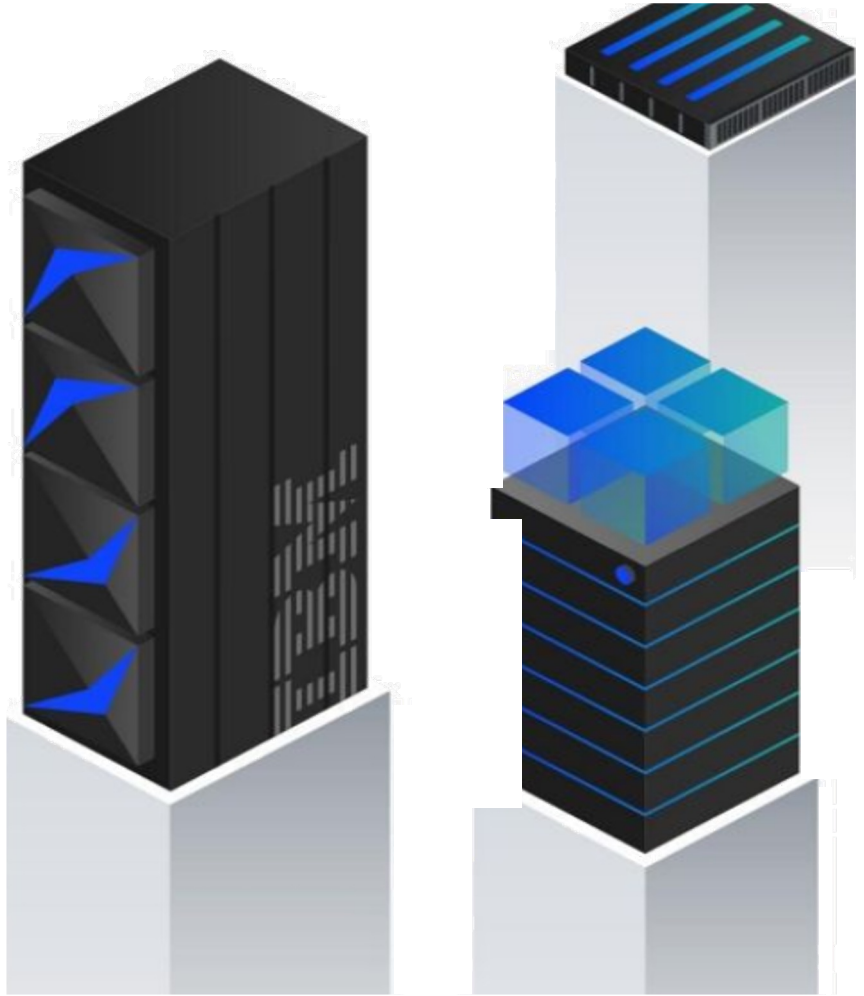
# Zaščitite podatke z IBM Storage rešitvami (tudi v MS Azure)



**David Kosmač**

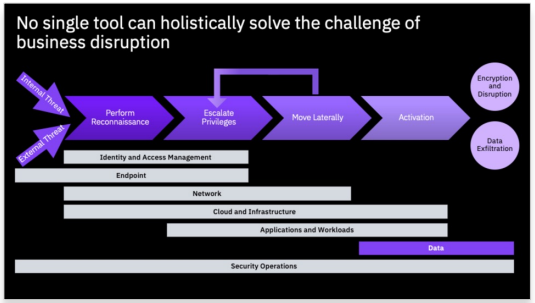
Acting Infrastructure Technical Sales Leader,
Eastern Europe Territories
david.kosmac@ibm.com

IBM

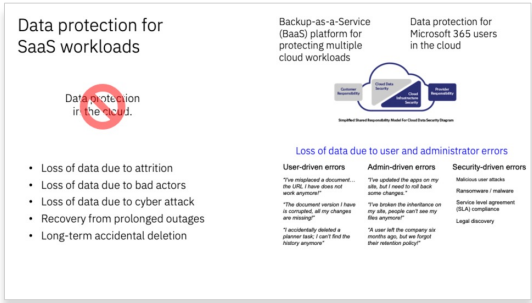
# Agenda

1 Introduction


2 Data Resilience on primary storage: **On-prem & IaaS**




3 Data Resilience for **SaaS data**



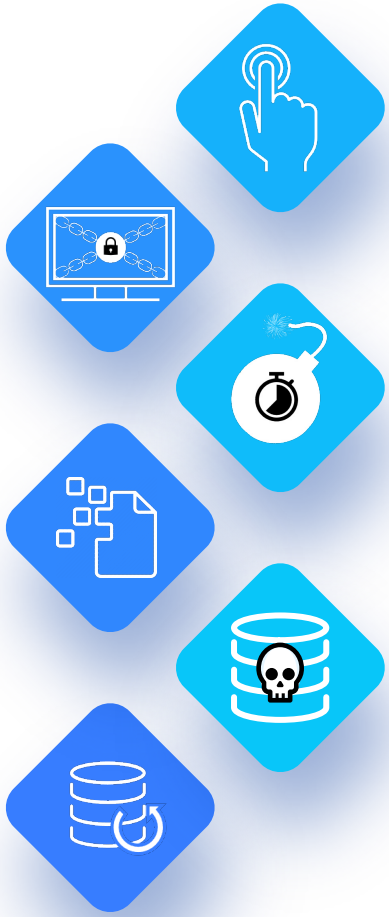
# Data Resilience

## Why Act Now?

**17%**
of Cyber Attacks are Ransomware

**26%**
Clients who paid the ransom still could not recover the data

**23**
days, average recovery after a ransomware attack



**2X**
Cyber Attacks YTY

**21%**
dormant threats, up from 5% YTY

**45%**
45% of production data affected

# Ransomware-as-a-Service (2020) → Military Grade Malware (2022+)

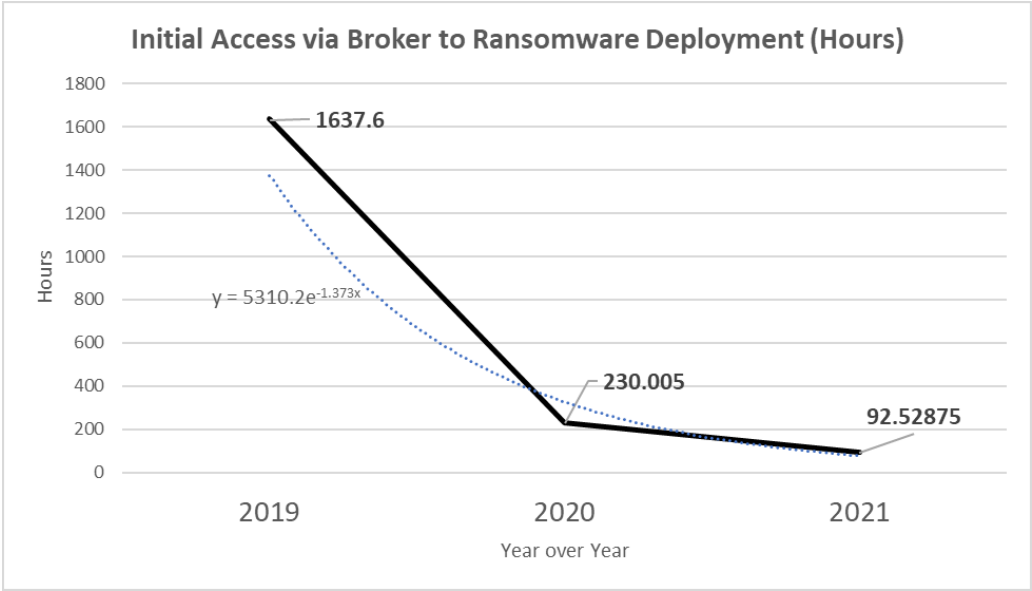
| Malware | MBR | GPT | Files | Associated Ransomware | Target OS | Languages |
|---|---|---|---|---|---|---|
| WhisperGate | Y | N | Y | Y | Windows | C++ (Stage 1)<br>.NET (Stage 2, 3) |
| HermeticWiper | N** | N** | Y | Y | Windows | C, Assembly |
| IsaacWiper | Y | N** | N | N | Windows | C, C++, Assembly |
| DesertBlade | ? | ? | Y | N | Windows | Golang |
| ACIDRAIN* | N/A | N/A | Y | N | Linux (MIPS) | C |
| CaddyWiper | Y | N | Y | N | Windows | C |
| DoubleZero | N** | N** | Y | N | Windows | .NET |
| AwfulShred | Y | Y | Y | N | Linux | Bash |
| SoloShred | Y | Y | Y | N | Solaris | Bash |

*Table 1: High-level overview of each wiper's functionality (Source: Recorded Future)*
** ACIDRAIN targets satellite modems, not desktop operating systems, so some fields may not be relevant.*
*** Although the MBR/GPT may be recoverable (or not affected at all), the wiper destroys the filesystem or critical files that prevent the system from successfully booting.*

Overview of the 9 Distinct Data Wipers Used in the Ukraine War (recordedfuture.com)

# How long does an attack actually take?

- **2019: 2+ months** — The TrickBot (initial access) to Ryuk (deployment) attack path resulted in a 90% increase in ransomware attacks investigated by X-Force Incident Response (IR) in 2019.
- **2020: 9.5 days** — Increased initial access broker economy and RaaS industry built upon a repeatable ransomware attack lifecycle established in 2019.
- **2021: *3.85 days*** — Large scale malspam campaigns such as with BazarLoader and IcedID and increased speed to transition access to ransomware affiliates like Conti.




Linux threats on the rise

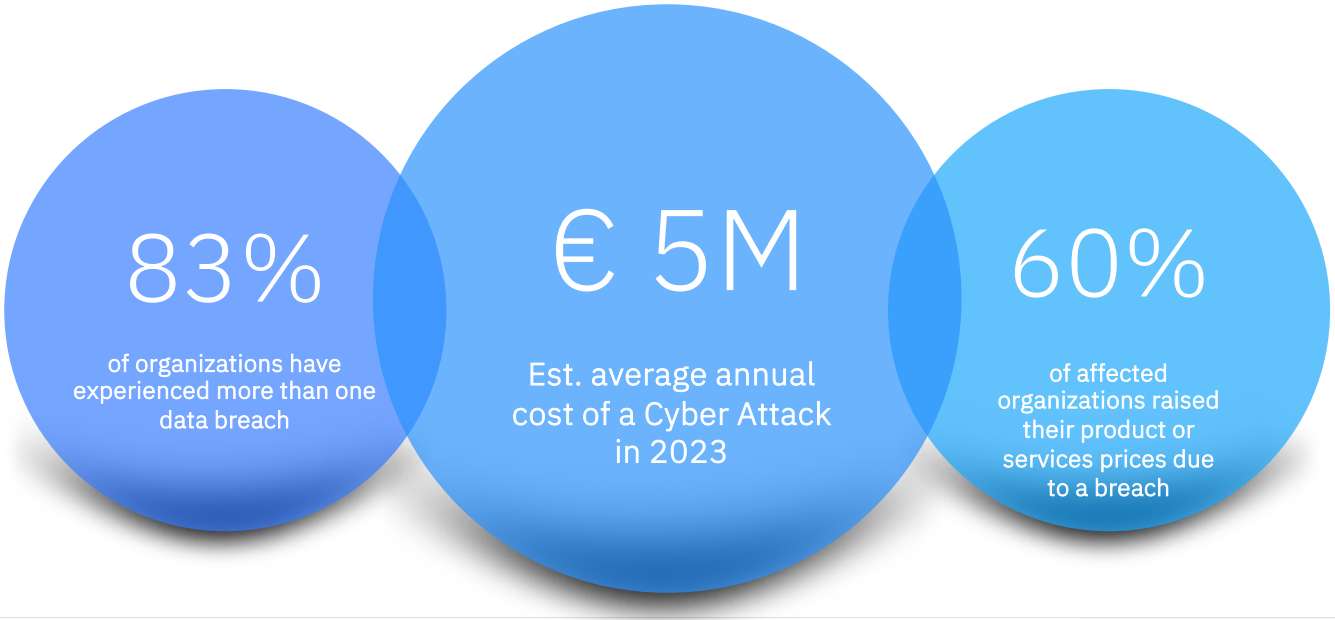
146%

year-over-year increase in Linux ransomware innovation across cloud environments

Sources: 2022 IBM X-Force Threat Intelligence Report; 2021 IBM Security Cost of a Data Breach Report

https://securityintelligence.com/posts/analysis-of-ransomware/

# Business Impacts of Cyber Attacks



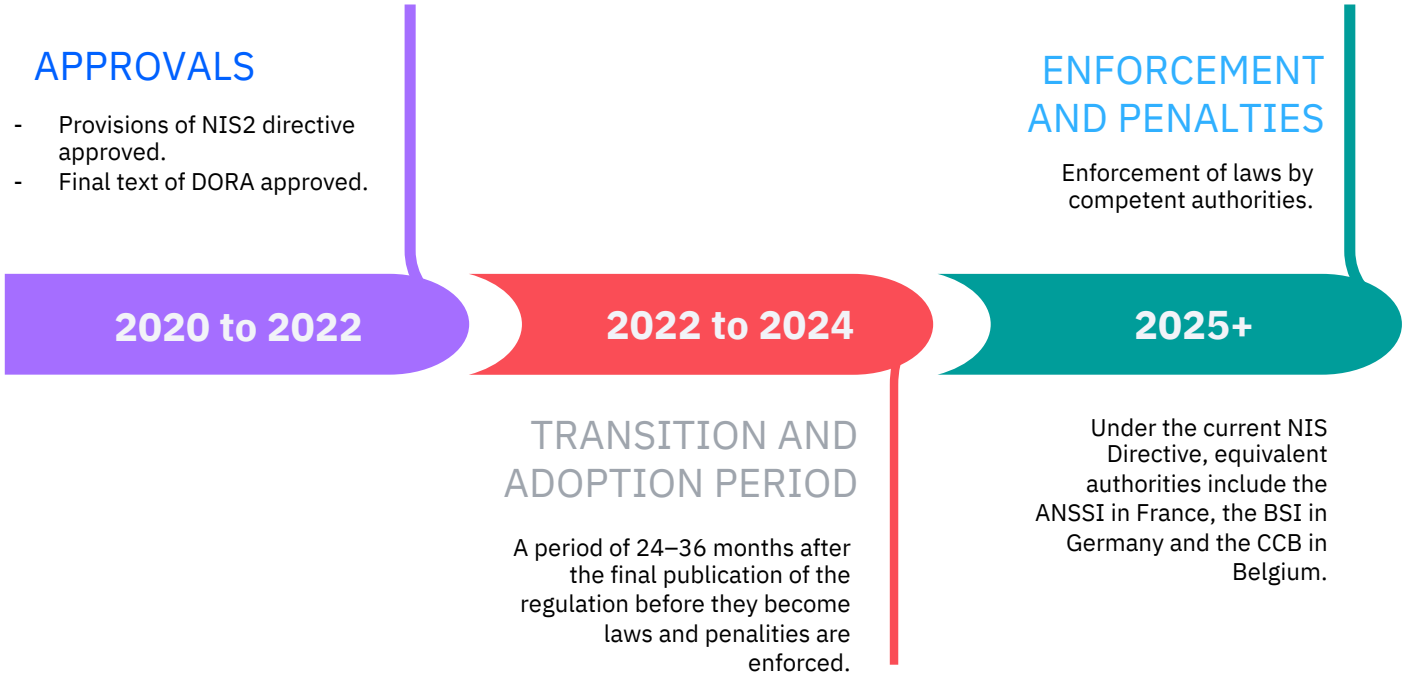

## € 10M

for noncompliance of Operational Resilience regulations

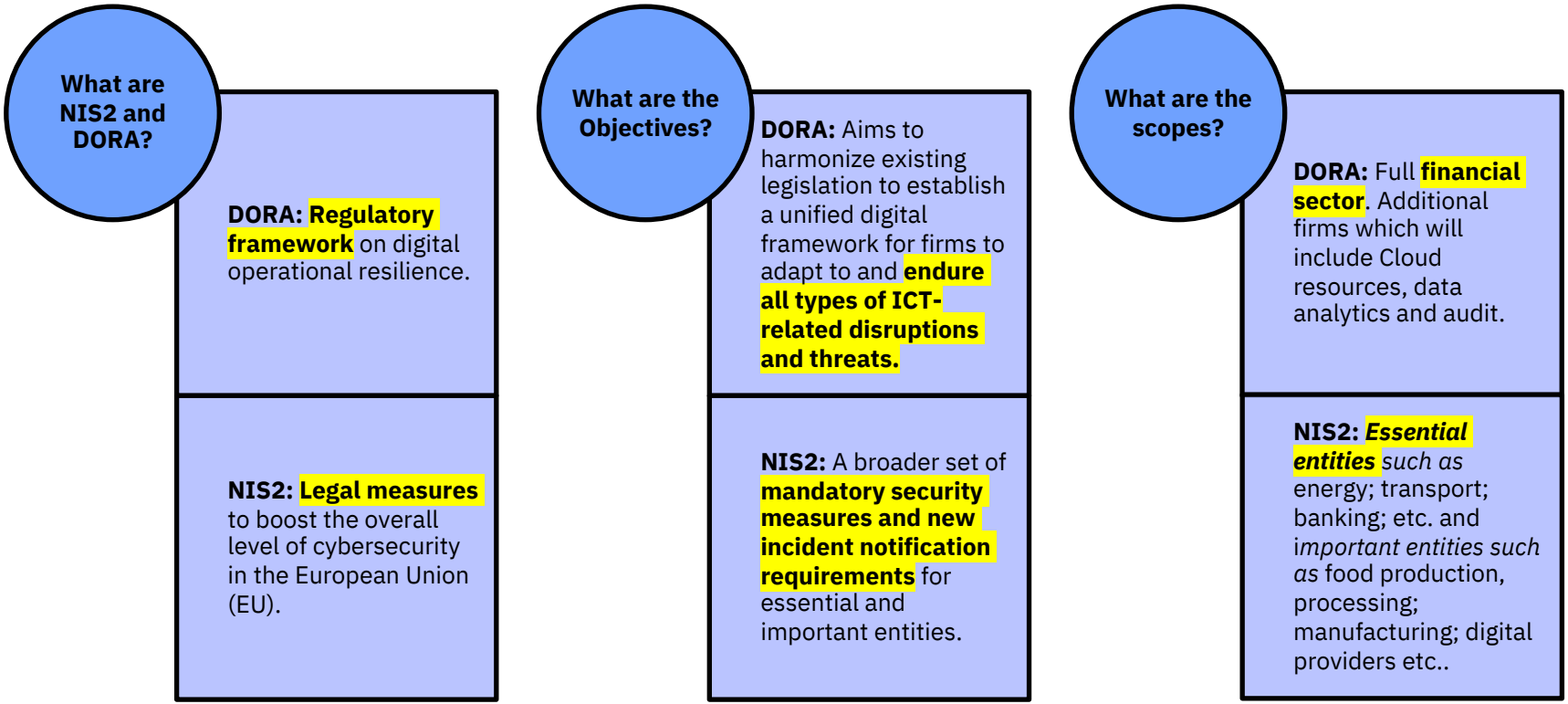
# EU regulations: DORA & NIS2

**NIS2 PROPOSED PENALTIES:**
At least 10.000.000 EUR or up to 2% of the total worldwide annual turnover whichever is higher. CEOs or legal representatives can be suspended.

**DORA PROPOSED PENALTIES:**
Can impose criminal penalties. Third parties may be fined 1% of the average daily worldwide turnover.



# DORA & NIS2

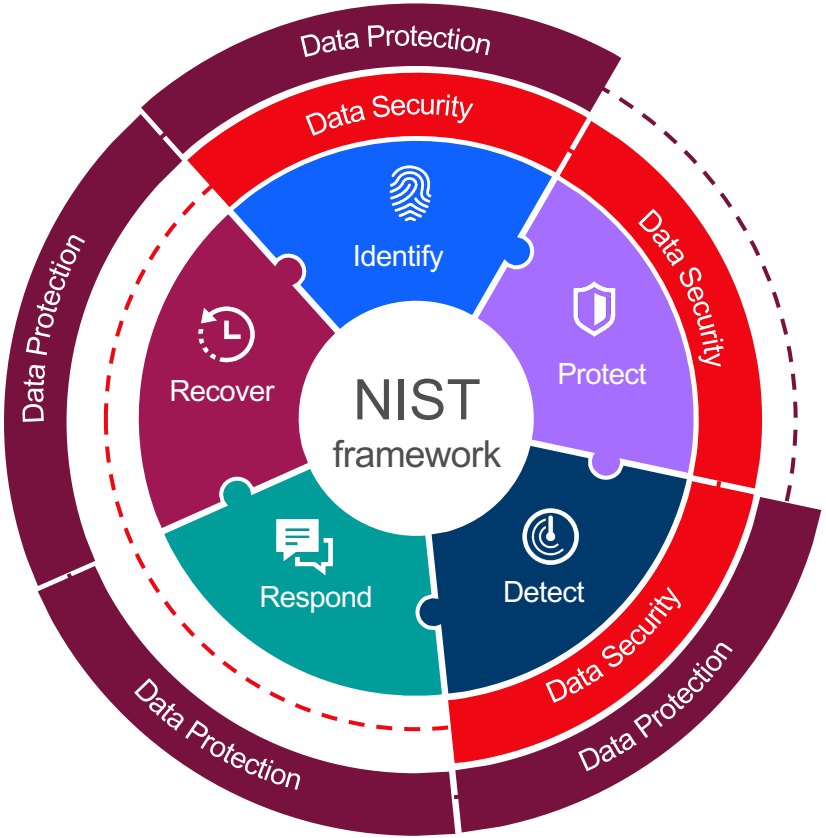

What are NIS2 and DORA?
DORA: Regulatory framework on digital operational resilience.
NIS2: Legal measures to boost the overall level of cybersecurity in the European Union (EU).
What are the Objectives?
DORA: Aims to harmonize existing legislation to establish a unified digital framework for firms to adapt to and endure all types of ICT-related disruptions and threats.
NIS2: A broader set of mandatory security measures and new incident notification requirements for essential and important entities.
What are the scopes?
DORA: Full financial sector. Additional firms which will include Cloud resources, data analytics and audit.
NIS2: Essential entities such as energy; transport; banking; etc. and important entities such as food production, processing; manufacturing; digital providers etc..

# Organizations Need Integrated Data Protection and Security

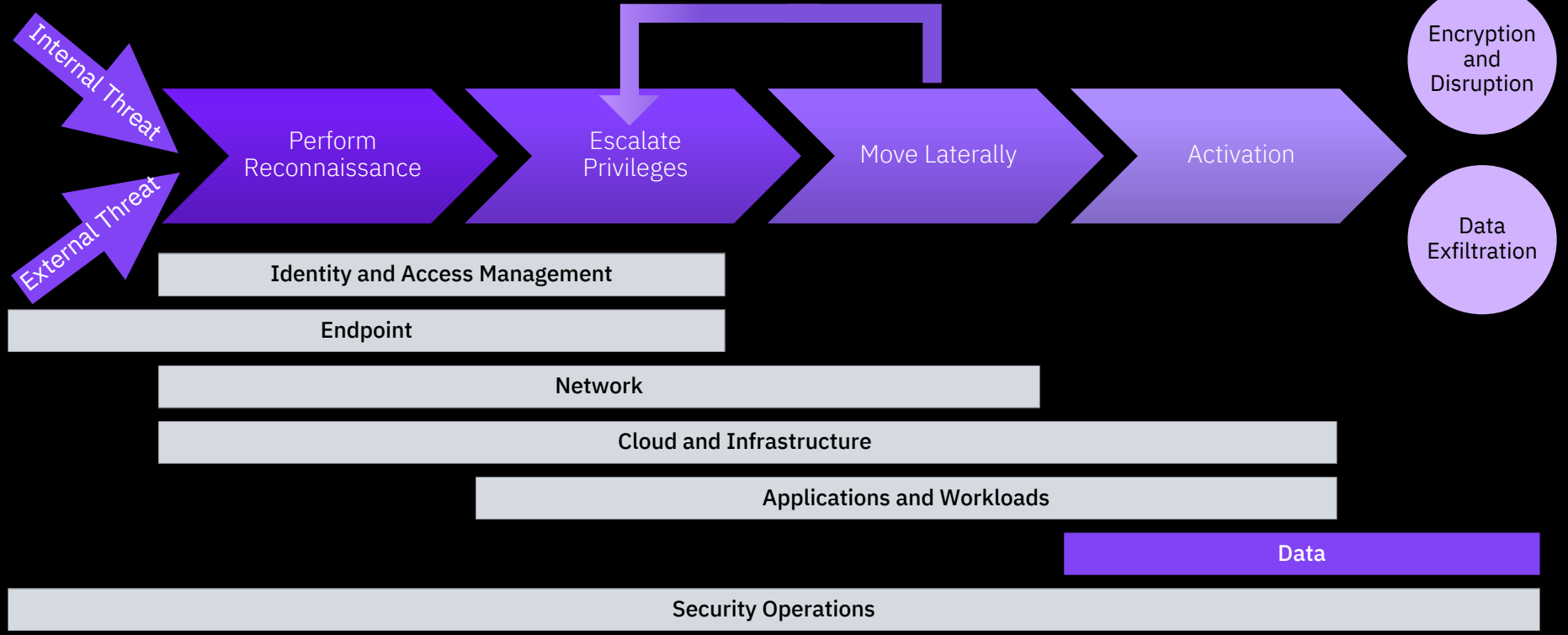
Data Protection is primarily reactionary and does not help avoid attack

Data Security helps detect and prevent attacks, but nothing to recover

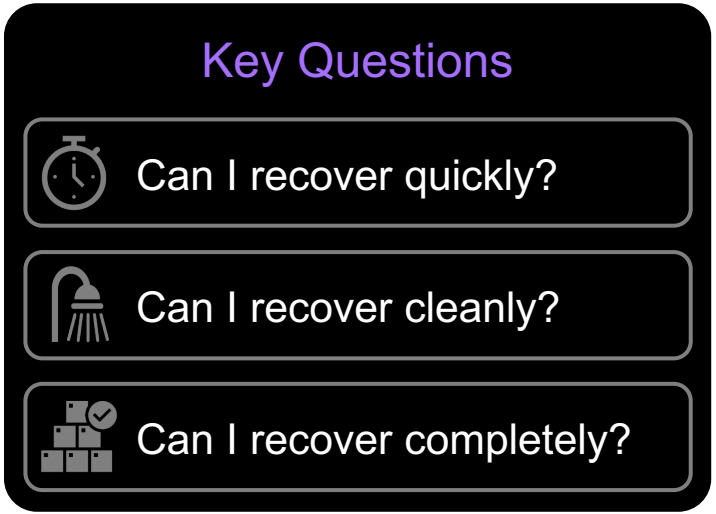
Together, data protection and security fulfill the NIST framework = Data Resilience



# No single tool can holistically solve the challenge of business disruption



# Key Data Resilience Questions



# Is YOUR Business Resilient?


Predict attacks
Cyber attack prevention
Respond to Cyber Attacks

Minimize/eliminate downtime
Protect from infrastructure failures
Avoid data loss from disasters

**Immutable data copies**
**Malware scanning**
**Business Recovery Automation**

Understand your BLIND SPOTS

# Capability Steps to Data Resilience

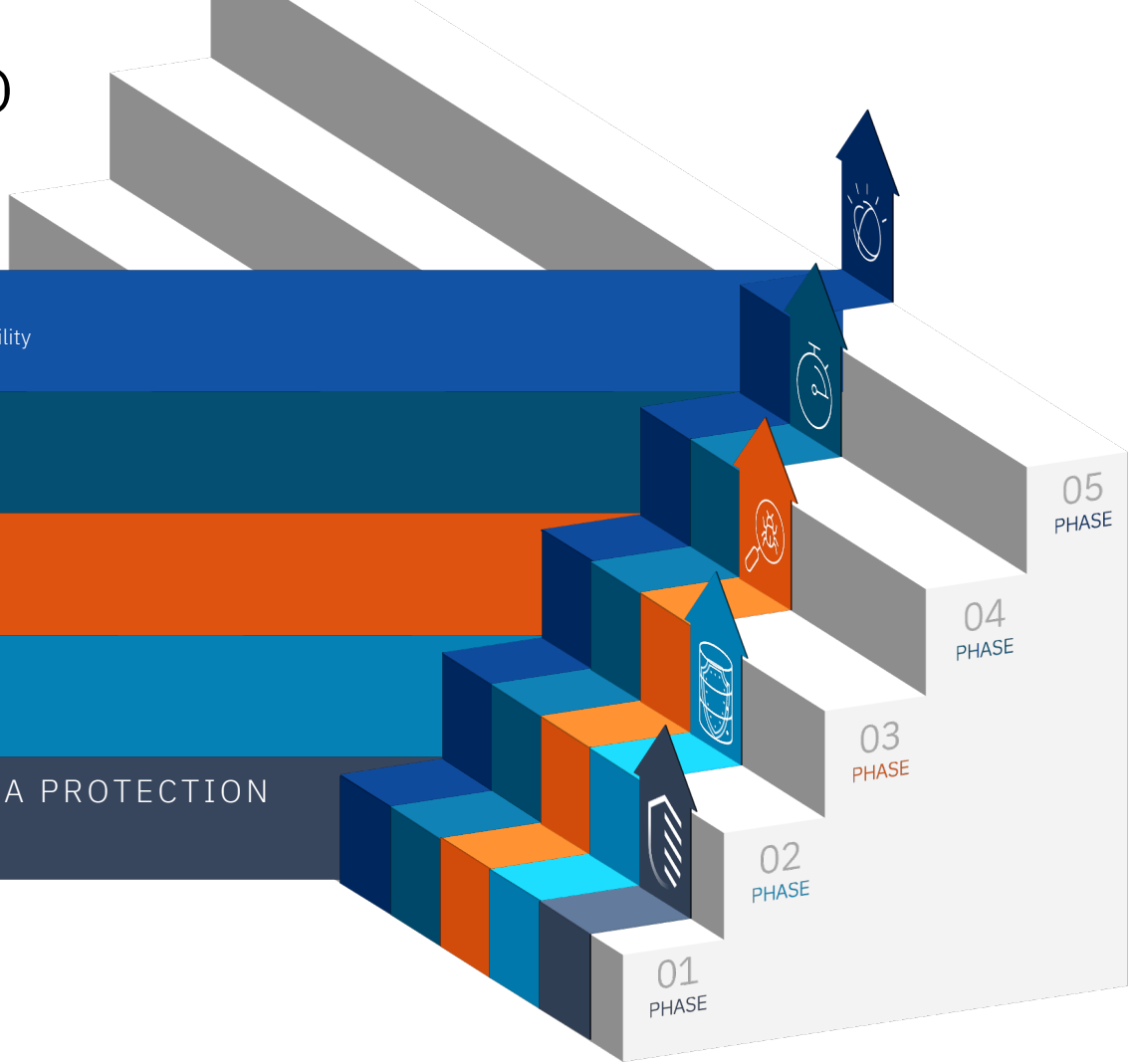
## AUTOMATION
Simplified operations plus ability to test and prove recoverability
Integration between Cyber Security & Cyber Resiliency

## RECOVERY
Rapid business recovery in minutes to hours
Avoid paying ransomware

## DISCOVERY
Understand when defences have been compromised
Malware scanner and data pattern insights

## SECURE IMMUTABILITY
Recoverable data points
Incorruptible, data can not be deleted

## FOUNDATIONAL SECURITY & DATA PROTECTION
Predict, prevent, and respond SIEM Consultation, SOAR, XDR
Protect from infrastructure failures and Natural disasters

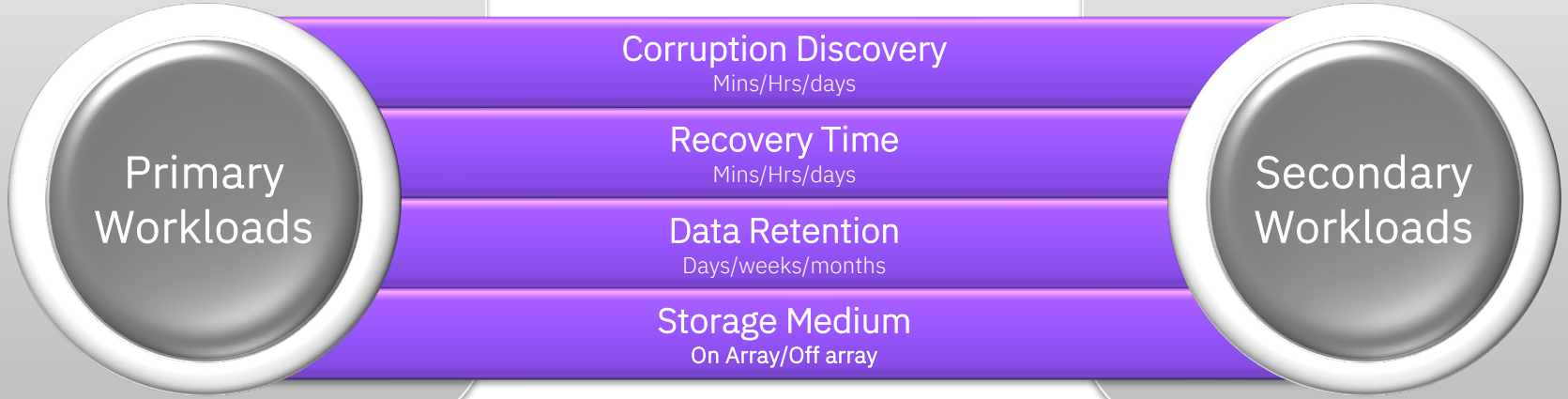


# Minimum Viable Company

Workloads that are costing the business money every second/minute/hour they are non-operational

# Full Company Recovery

All workloads including non-critical workloads for back-office etc.



Unique

# IBM Storage supports amazing data resiliency

## Safeguarded Copy

- Immutable, on-array, data snapshots
- Can’t be modified
- Can’t be deleted
- Invisible to bad actors

## Cyber Vault

- Early detection of cyber threats
- Easy ways of assessing data viability
- Rapid recovery of compromised data
- Process automation

SV4PC
Storage Virtualize for Public Cloud


IBM SAN Volume Controller


IBM FlashSystem 5200


IBM FlashSystem 7300


IBM Scale System ESS3500


IBM FlashSystem 9500

IBM Storage DS8900F

*now also on NEW FS5045

# Inline data corruption detection

## How do we detect ransomware on IBM Storage?

| | |
|---|---|
| **Threat Signatures** | **Sample Hash Comparisons** |
| **Data Behaviour Signals** | **Block Level Anomaly Monitoring** |
| **Network Signals** | **Network level Anomaly Monitoring** |

Workload I/O Streams

100101101010
101001110101

Calculate **Shannan Entropy** on sampling of write cache destine

Alterting via Storage Insights

Cyber Threat statistics used to detect signs of ransomware encryption

Est. 2003

# SVC20

## 20 years of Storage Virtualization

# IBM Safeguarded Copy for Microsoft Azure

*Also on: DS8XXX, FlashSystem, SAN Volume Controller, and Spectrum Virtualize*

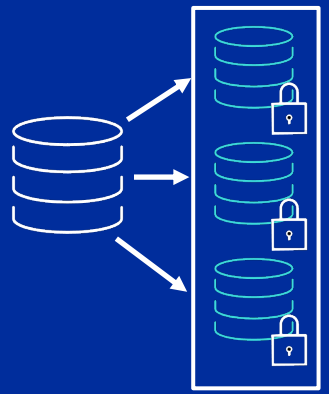
**Automatic**
creation of copies on a scheduled basis

**Immutable**
point-in-time copies of production data

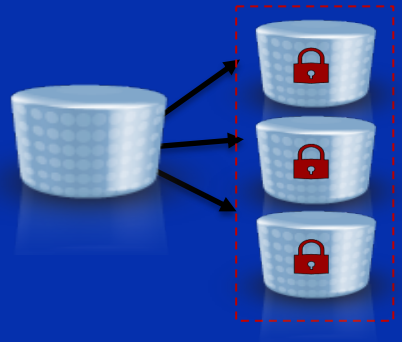
**Isolated**
logical air-gap offline by design

**Fast**
restore from copies on primary storage

**Prevents modification**
or deletion of copies due to user error, malicious destruction, or ransomware attack



# Protected Copies of Data: Safeguarded Copy (SGC)



Can **not** be mapped to a host

**Immutable**:
Can **not** be written or read by an application

Automatically created and deleted based on a predefined **schedule**

Protected Copies of production volumes

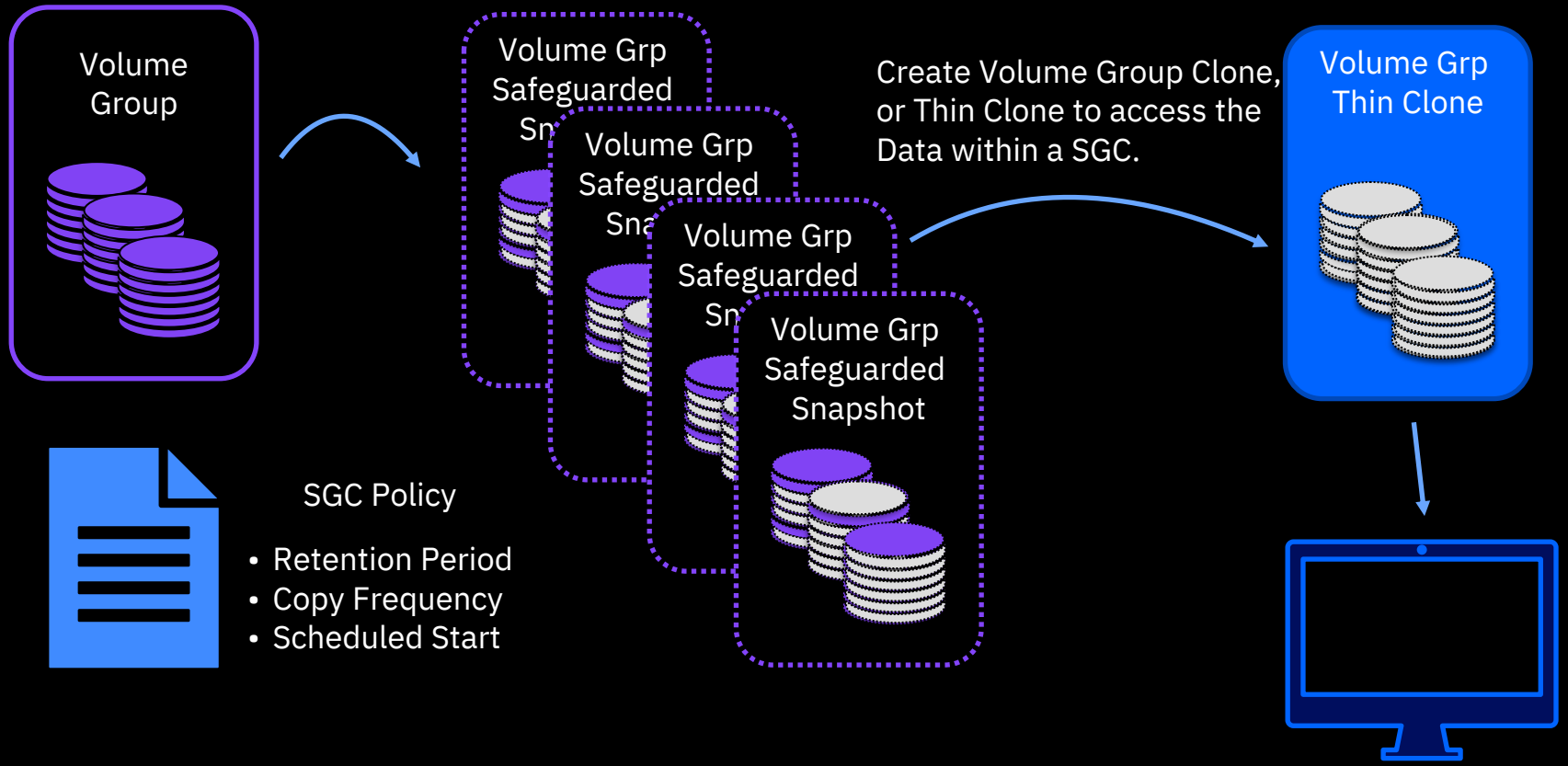
Thinly-provisioned, space efficient and point-in-time

Built on existing FlashCopy snapshot technology

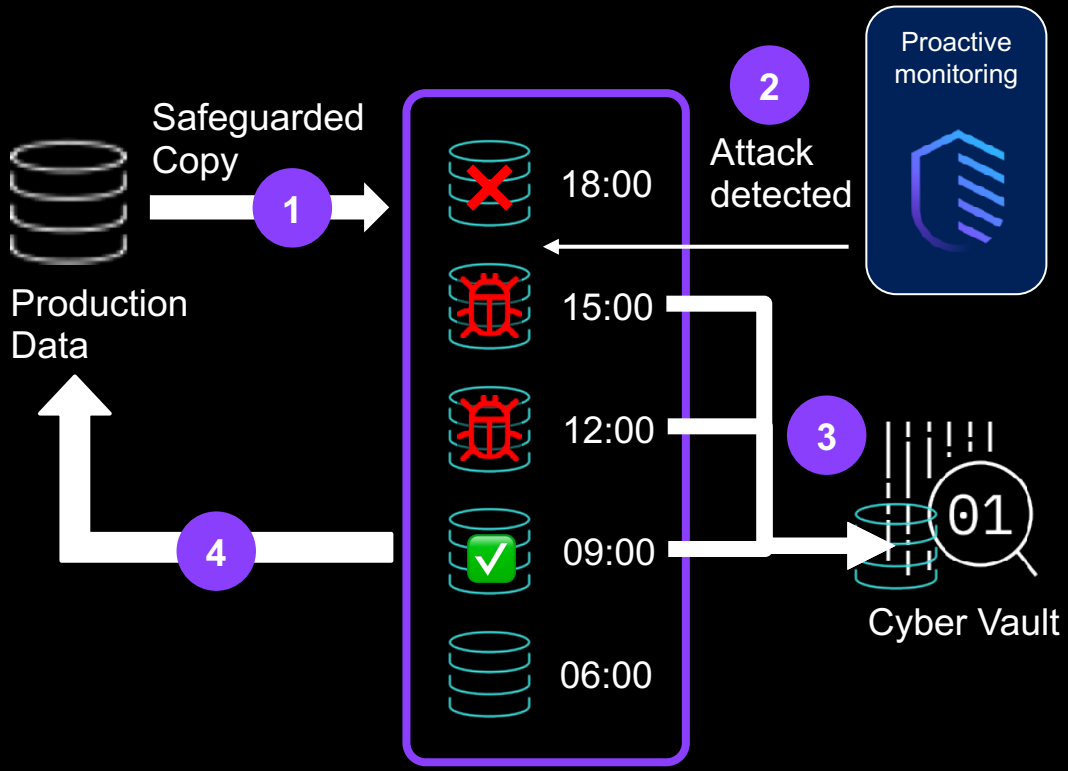
Stored in a **Safeguarded copy location**:

- Uses either Child Pool technology or copy resides in same pool as the source volume
- Logical separation from other volumes
- Capacity control
- Access restrictions (separation of duties)

# How does SGC work?



# Using Safeguarded Copy
## Example - building and using a Cyber Vault

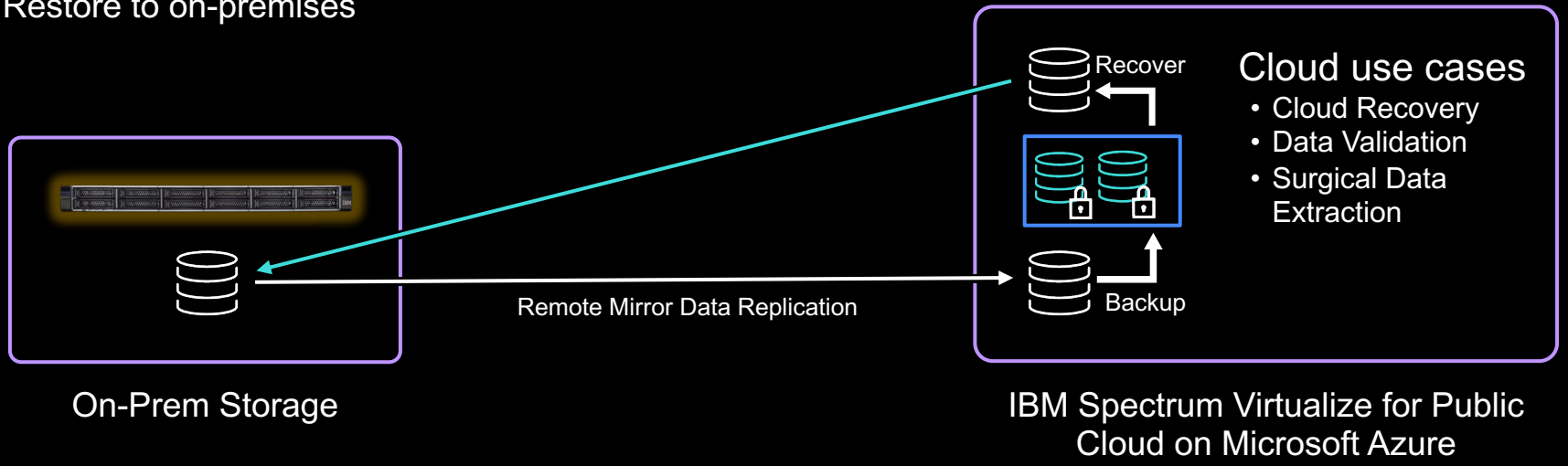



1. Safeguarded immutable copies created throughout the day
2. Attack detected by monitoring software
3. Restore volumes to Cyber Vault and run tools to validate if data corrupted
4. Clean copy quickly identified and restored to production

# New Safeguarded Copy deployment models with Azure

Safeguarded Copy on Azure can protect cloud-hosted data and data from on-premises storage

- Replicate operational data to Microsoft Azure
- Create protected Safeguarded Copy backups providing greater separation from potential on-prem threats
- Do recoveries in the cloud
- Restore to on-premises



# Simple deployment on Microsoft Azure

*Available from the Azure Marketplace*

1 **Purchase IBM Spectrum Virtualize for Public Cloud**

Order through your IBM Business Partner

*Easy ordering in conjunction with IBM FlashSystem*

2 **Deploy IBM Spectrum Virtualize for Public Cloud from Azure Marketplace**

Find IBM Spectrum Virtualize for Public Cloud on Azure Marketplace.
Select VM type

*Cluster is deployed automatically, along with a quorum VM and a minimum set of Azure managed disks*

# IBM Spectrum Virtualize for Public Cloud

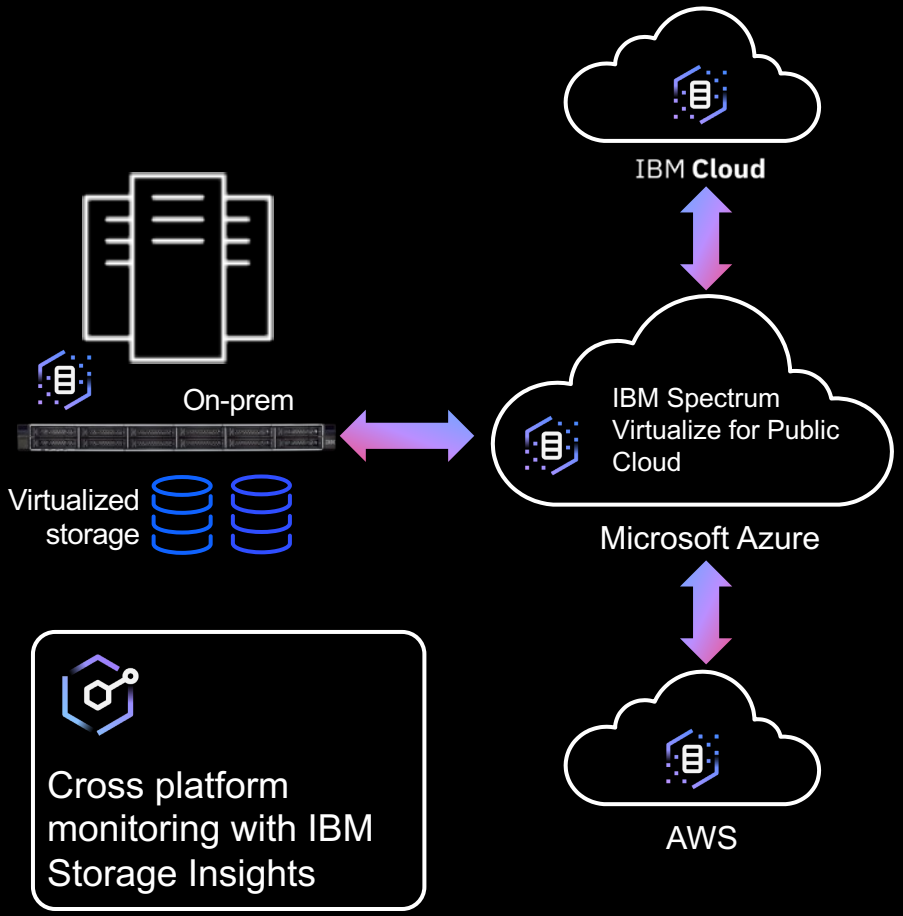
Consistent function across on-prem and public cloud platforms

Consistent APIs, Ansible support, management, user interface

Integrated with cloud platform deployment

Ideal for common cloud use cases

- DR (on-prem to cloud or cloud to cloud)
- Cloud DevOps
- Data migration (between on prem and cloud or cloud to cloud)



# Included Features

IBM Spectrum Virtualize for Public Cloud is an all-inclusive license that gives you access to key Volume Management, DR and Point in Copy Features that work on all supported Public Clouds

## Volume Management

- Thin Provisioning w/Zero Detect
- Volume Mirroring (Thick to Thin, Compressed)
- IBM EasyTier
- Data Reduction Pools with Compression and Deduplication
- VMware vVol certified
- **Clustering for capacity and performance**

## DR and HA

- IBM MetroMirror Sync Replication (300km)
- IBM GlobalMirror Async Replication (80ms roundtrip)
- IBM GlobalMirror w/Change Volumes Async Replication (5min - 24 hr)
- Native IP Replication w/Network Artificial Intelligence and Compression

## Point in Time Copy

- IBM FlashCopy of volumes for backup, continuity and application test
- 256 copies of source
- 255 consistency groups
- Incremental copies
- Cascaded copies
- Thin Provisioned, Compressed, Copies in different pools
- Simple 'Reverse' Operation
- IBM SafeGuarded Copy for immutable snapshots

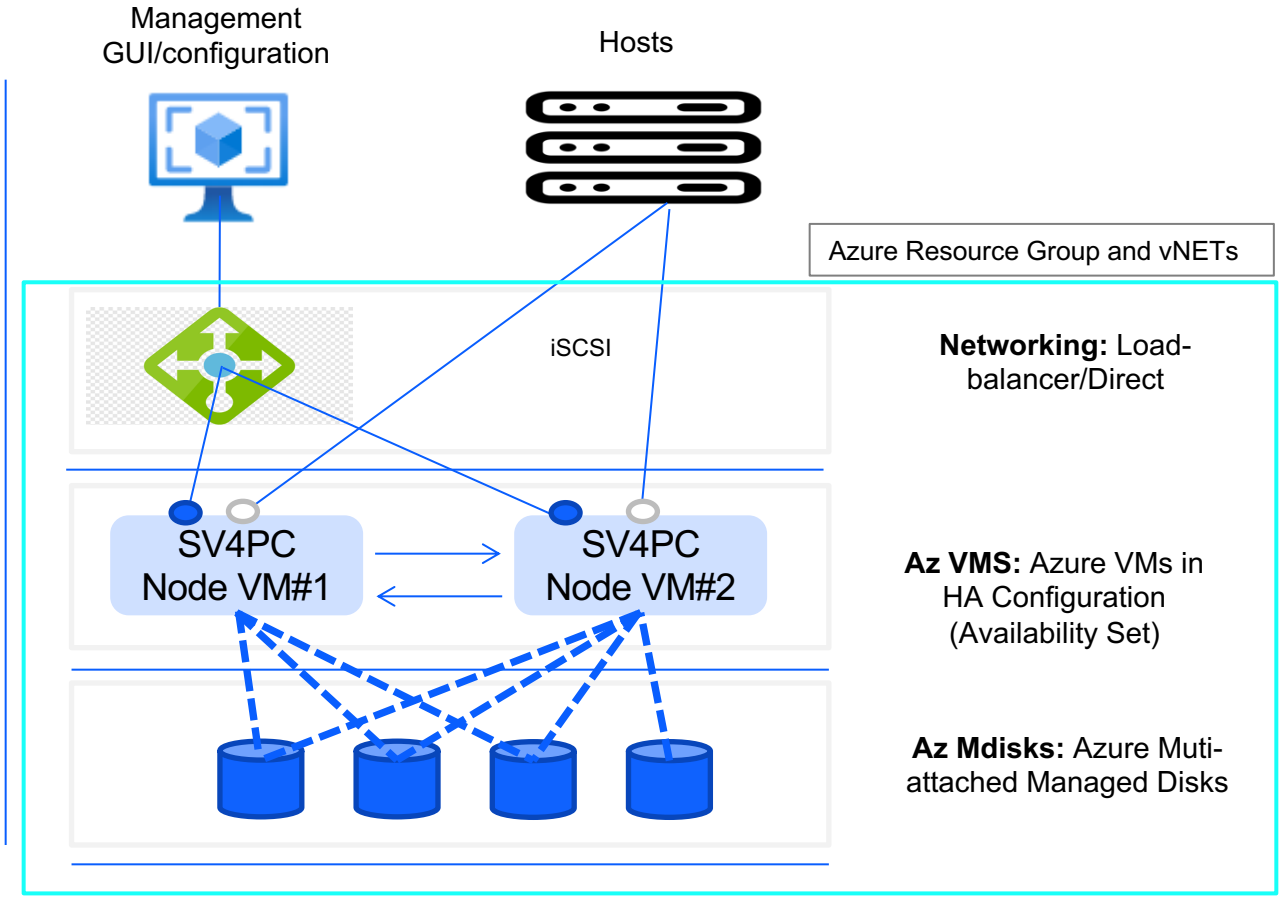
## Deployment

- Azure Marketplace (Azure Apps)
- 20 EBS Volumes, 31 Azure Managed Disks
- 3 Types of Azure VMs supported
- Premium and Standard SSD Azure Managed Disks
- WW Support
- **AWS and Azure Gov Cloud**

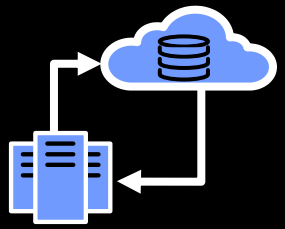
# IBM Spectrum Virtualize for Public Cloud on Azure: Architecture

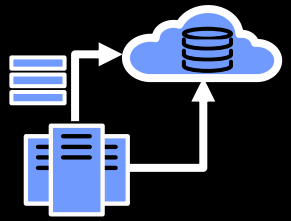
## Design Highlights :

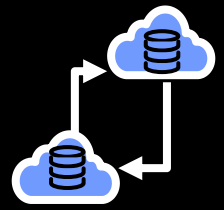
- Storage controllers are modelled as Azure VMs in a High Availability (HA) Configuration
- Customer has a choice of VMs based workload requirements
- High Availability:
  - In order to support IP Failover of the cluster, the Microsoft Azure IP Load Balancer service is used between
  - Shared Azure Managed disks for Fast backend Failover



# Use Cases: Spectrum Virtualize for Public Cloud



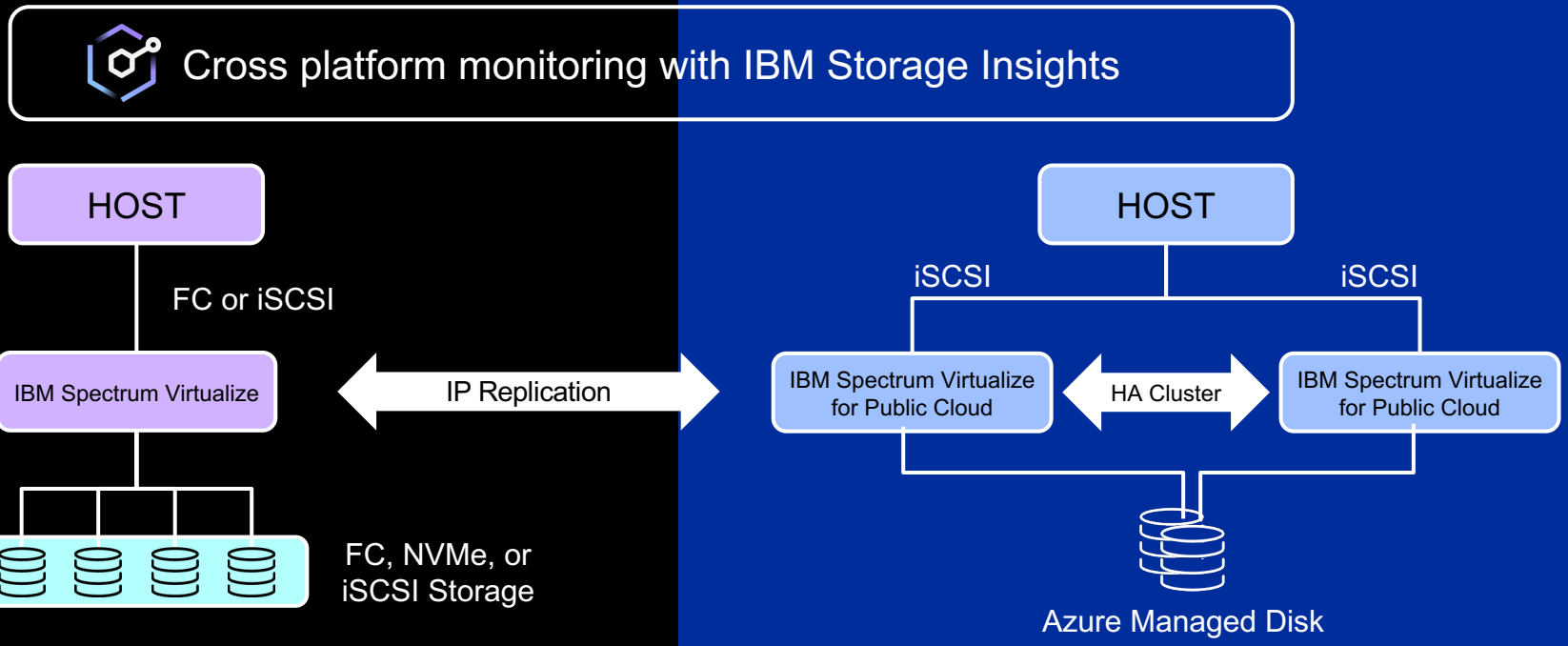


| Optimize Public Cloud Block Storage | Extend On Premises to Hybrid MultiCloud | Business Continuity on Public Cloud | Protection of Data in Public Cloud |
|---|---|---|---|
| • Lower Cost, Improve Performance of native Public Cloud IaaS<br>• Thin-Provisioned Volumes, Space Efficient Snapshots, AI based Auto Tiering, Data Reduction Pools with Compression and Dedupe<br>• Increase Scalability of Public Cloud Storage for Enterprise Apps | • Add cloud capabilities to existing Storage on Prem<br>• Temporary or permanent data migration to/from Public Clouds, and between Public Cloud providers.<br>• Move data to cloud resources, such as containers, VMs.<br>• Consistent Management | • Create a DR site in the public cloud<br>• Synchronize local storage data with sync or async storage replication<br>• Protect on prem data for virtualized, containerized, or bare metal applications<br>• Integrate an ‘air gap’ solution to protect against cyber threats | • For workloads moved to cloud<br>• Use Sync or Async Mirror to protect cloud data center deployments<br>• Supported within and between disparate Cloud Provider data centers |

# IBM Spectrum Virtualize for Public Cloud on Microsoft Azure

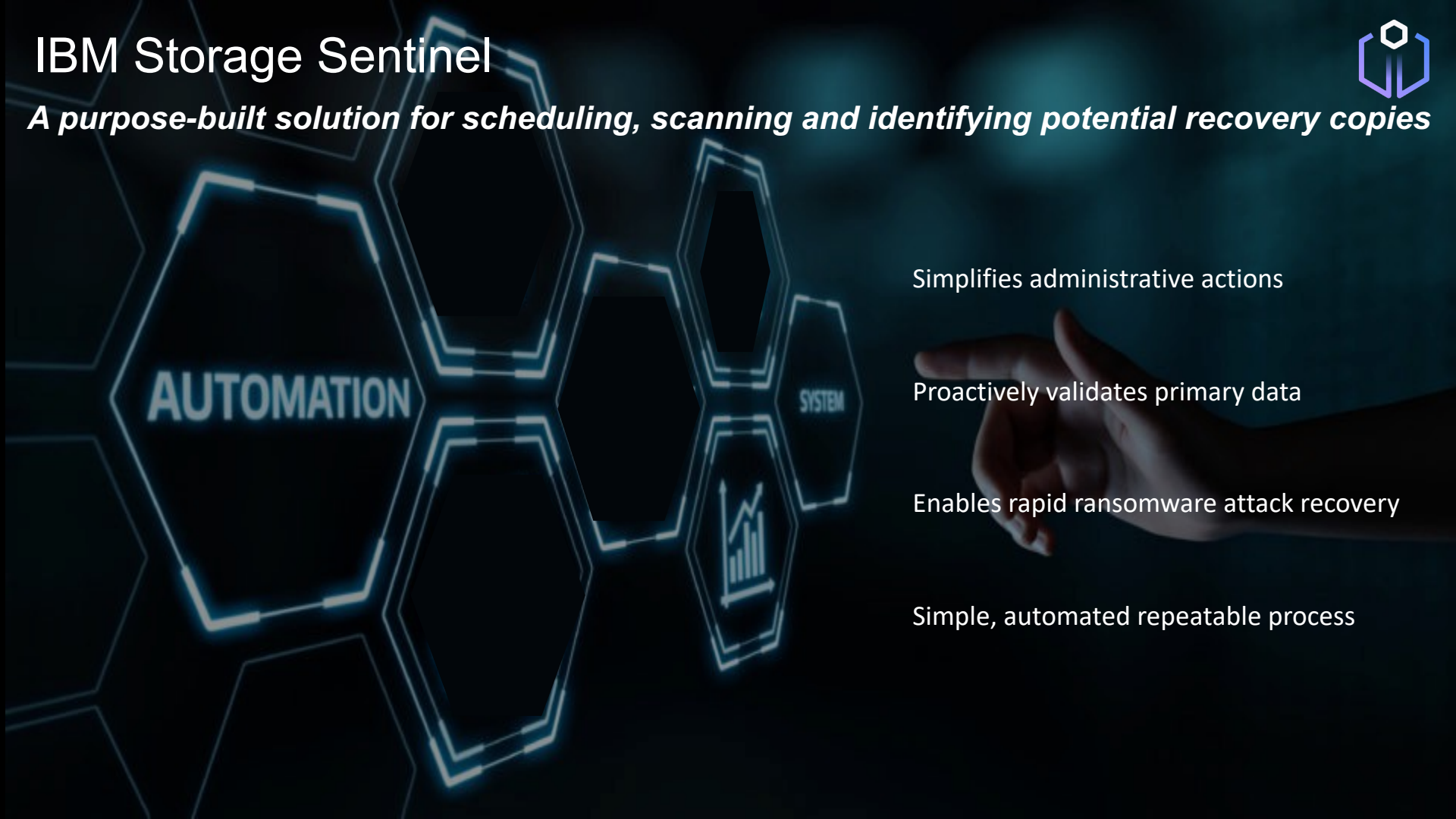
On Premises

On Azure, IBM Spectrum Virtualize for Public Cloud is built on Azure Virtual Machine instances and Managed Disk (Standard or Premium) storage up to 922TB



# IBM Storage Sentinel

***A purpose-built solution for scheduling, scanning and identifying potential recovery copies***



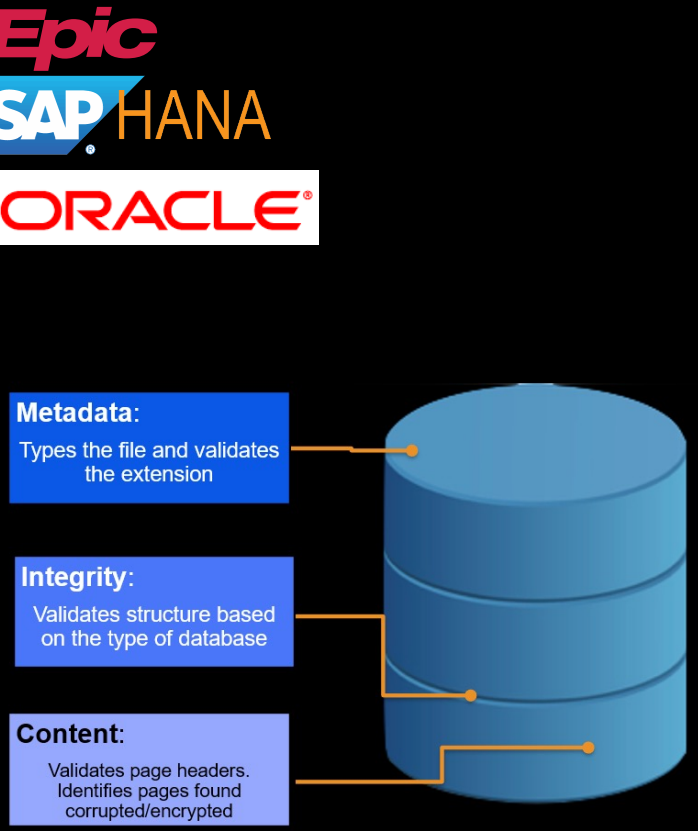

Simplifies administrative actions

Proactively validates primary data

Enables rapid ransomware attack recovery

Simple, automated repeatable process

# Storage Sentinel Analytics for

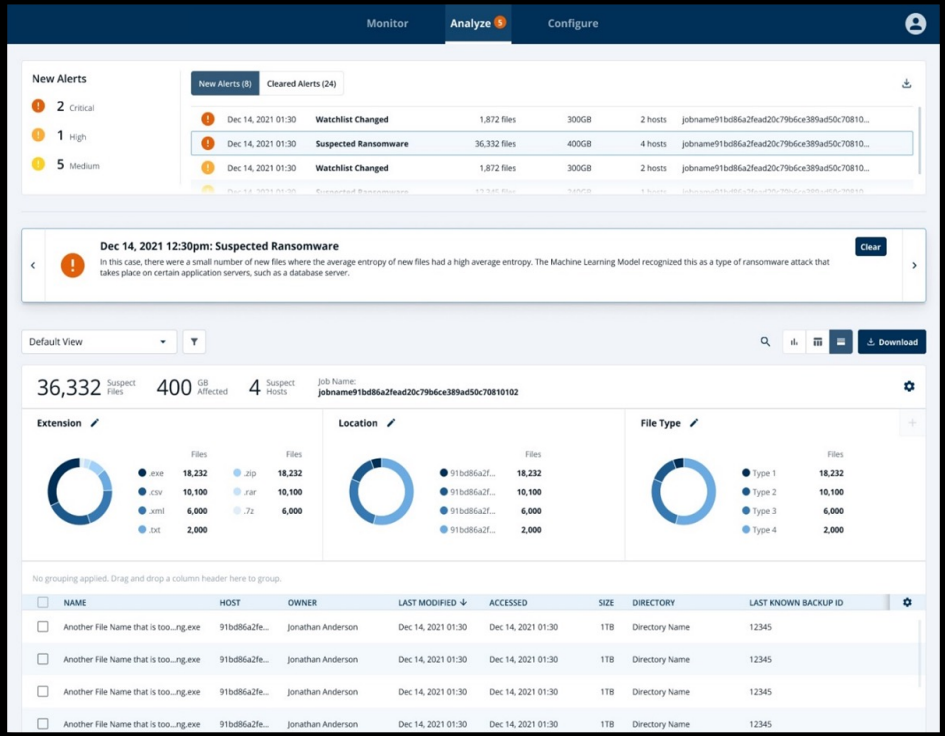



## IBM Storage Sentinel;

- Sentinel 1.1 – 22Q2
  - Scan EPIC Cache and IRIS databases running on Linux
- Sentinel 1.1.1 - 22Q3
  - Scan SAP HANA databases (SUSE)
- Sentinel 1.1.2 - 22Q4
  - Scan SAP HANA databases on RHEL 8
- Sentinel 1.1.3 – 23Q1
  - Scan EPIC databases running on AIX
- *Sentinel 1.1.4 – 23Q2*
  - Scan Oracle DB on Linux (RHEL + SUSE) or AIX
  - Oracle Versions 12c, 18c, 19c (Standalone)
  - AIX7.2 (7.3 in testing)

# IBM Storage Sentinel Analytics

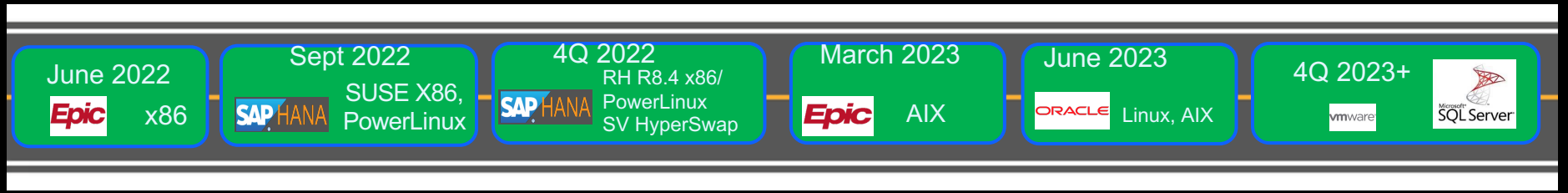
- Full content analytics provide comprehensive insight into data
- Compares snapshots over time to detect unusual patterns due to a cyber attack
- 200+ analytics that are indicative of corruption due to a ransomware attack
- The only cyber analytics solution that inspects file metadata and content
- Machine learning models that have been trained on thousands of variants
- 99.5% confident in detecting corruption



# IBM Storage Sentinel

Automated Cyber Resilience and Recovery

| | |
|---|---|
| Protect | SLA-based<br>Isolated & Immutable Snapshots |
| Verify | Automated Anomaly Scanning Engine |
| Recover | Safe Recover Point Identification |
| | Rapid Data Recovery |




[IBM Storage Copy Data Management Ransomware Detection on EPIC Cache and Iris workloads – Demo]

# Data protection for SaaS workloads


- Loss of data due to attrition
- Loss of data due to bad actors
- Loss of data due to cyber attack
- Recovery from prolonged outages
- Long-term accidental deletion

Backup-as-a-Service (BaaS) platform for protecting multiple cloud workloads

Data protection for Microsoft 365 users in the cloud


Simplified Shared Responsibility Model For Cloud Data Security Diagram

## Loss of data due to user and administrator errors

### User-driven errors

*"I've misplaced a document… the URL I have does not work anymore!"*

*"The document version I have is corrupted, all my changes are missing!"*

*"I accidentally deleted a planner task; I can't find the history anymore"*

### Admin-driven errors

*"I've updated the apps on my site, but I need to roll back some changes."*

*"I've broken the inheritance on my site, people can't see my files anymore!"*

*"A user left the company six months ago, but we forgot their retention policy!"*

### Security-driven errors

Malicious user attacks

Ransomware / malware

Service level agreement (SLA) compliance

Legal discovery

# Data protection in a world of high risk

## Whose responsibility is it to protect SaaS workload data?

Microsoft Services Agreement: "We [Microsoft] recommend that you regularly backup your content and data…using third-party apps and services."

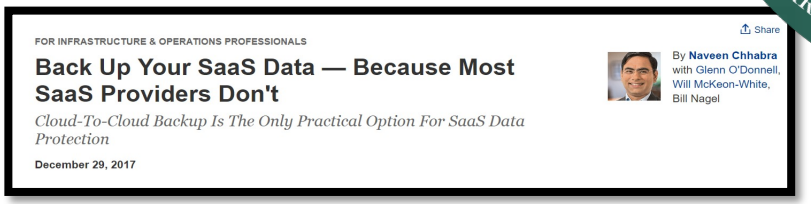
The risk: 3 out of 4 organizations *do not* use a data protection solution to protect their Software-as-a-Service data.


FEATURE

**Businesses still lax about SaaS backup**

TechTarget | Data Backup

The solution: A cloud-to-cloud solution for backup


FORRESTER®

FOR INFRASTRUCTURE & OPERATIONS PROFESSIONALS

**Back Up Your SaaS Data — Because Most SaaS Providers Don't**

*Cloud-To-Cloud Backup Is The Only Practical Option For SaaS Data Protection*

December 29, 2017

Share

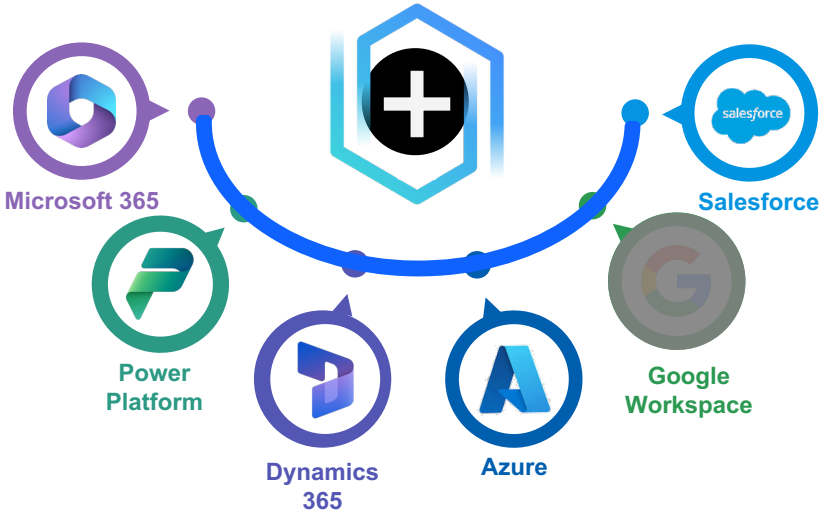
By **Naveen Chhabra** with Glenn O'Donnell, Will McKeon-White, Bill Nagel

# Storage Protect for Cloud – Microsoft 365

## Comprehensive multi-workload data protection platform

- Comprehensive platform protection
- Granular restores
- Backup 4x per day
- Restore from previous versions

- Backup storage on client's terms
- Multi-geo support
- Robust reporting
- Correct user and admin errors



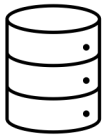
# Storage Protect for Cloud storage options

IBM Storage Protect
Server S3

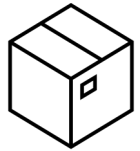
IBM Cloud
Object Storage

Azure BLOB

AWS S3
And compatible



(S)FTP



DropBox

BYOS
Bring Your Own Storage

# SP4C M365 versus Microsoft native

## Built-in recovery capability comparison

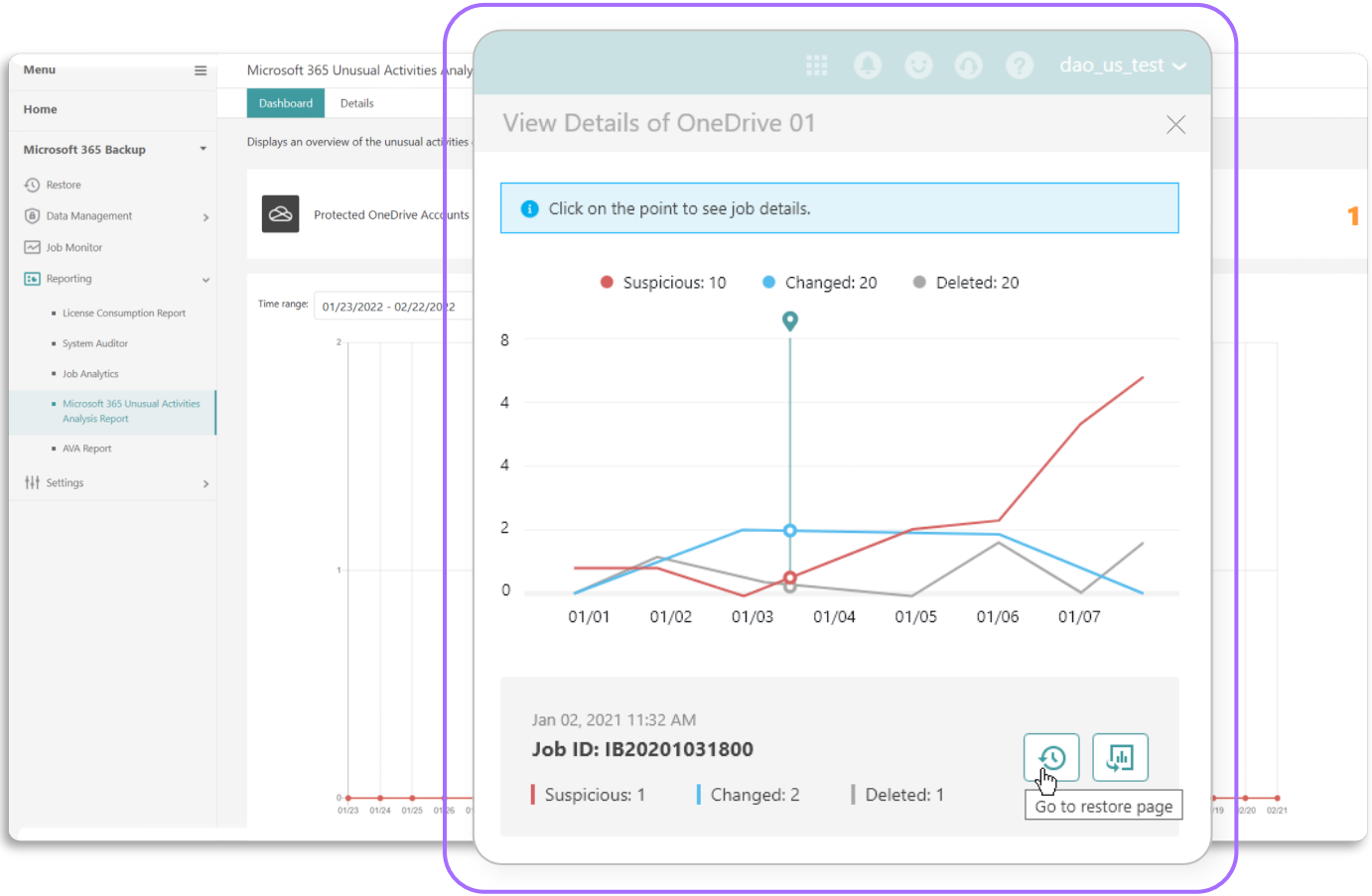
| Problem statement | M365 built-in recovery | IBM SP4C M365 |
|---|---|---|
| A user misplaced a document and can no longer find it. A shared OneNote document was corrupted by parallel edits. | N/A (Not Applicable) | Yes, through self-service or help-desk restore |
| An administrator updated SharePoint Site settings and has broken the inheritance on the Site. Users have no longer access to their documents now. | N/A | Yes, through restore |
| A Mailbox or OneDrive of a user that left the company was hard deleted from M365. | N/A | Yes, restore from retained data either point-in-time or standard |
| A Mailbox item was deleted from inbox and from the recycle bin. | Second level recycle bin keeps mailbox items for a maximum of 30 days. | Yes, through restore, depending on retention settings |
| Malware/Ransomware detection requires restore beyond built-in data recovery and granularity. | N/A | Yes, point-in-time restore, or standard restore |
| Malicious attacks from inside or outside the company. | N/A | Yes, through restore |
| Long-term accidental deletion or legal discovery coverage with selective rollback. | N/A | Yes, through restore |

# SP4C M365 versus Microsoft native

## Built-in recovery capability comparison

| Problem statement | M365 built-in recovery | IBM SP4C M365 |
|---|---|---|
| A Calendar item was deleted from the recycle bin. | Second level recycle bin keeps calendar items for a maximum of 120 days | Yes, through self-service or help-desk restore |
| An administrator deleted a SharePoint site. | Deleted SharePoint Sites are kept for reactivation for 93 days. For additional 14 days administrators can open an M365 ticket and ask for recovery | Yes, through restore, depending on retention settings |
| A user used the native “file restore” feature in Teams or OneDrive and did roll back to a too old version. | No solution. Roll forward not possible | Yes, through self-service for OneDrive or help-desk restore |
| A Team owner did roll back the documents of the complete team by accident. | No solution. Roll forward not possible | Yes, through restore |
| Loss of data due to departing employees and deactivated accounts beyond retention. | N/A (not applicable) | Yes, through restore |
| Recovery from prolonged outages; SLA compliance | N/A | Yes, through restore |

# Ransomware Detection with SP4C Microsoft 365




**Proactively detect ransomware events**

Early event detection

Quick investigation

Faster restore with SP4C

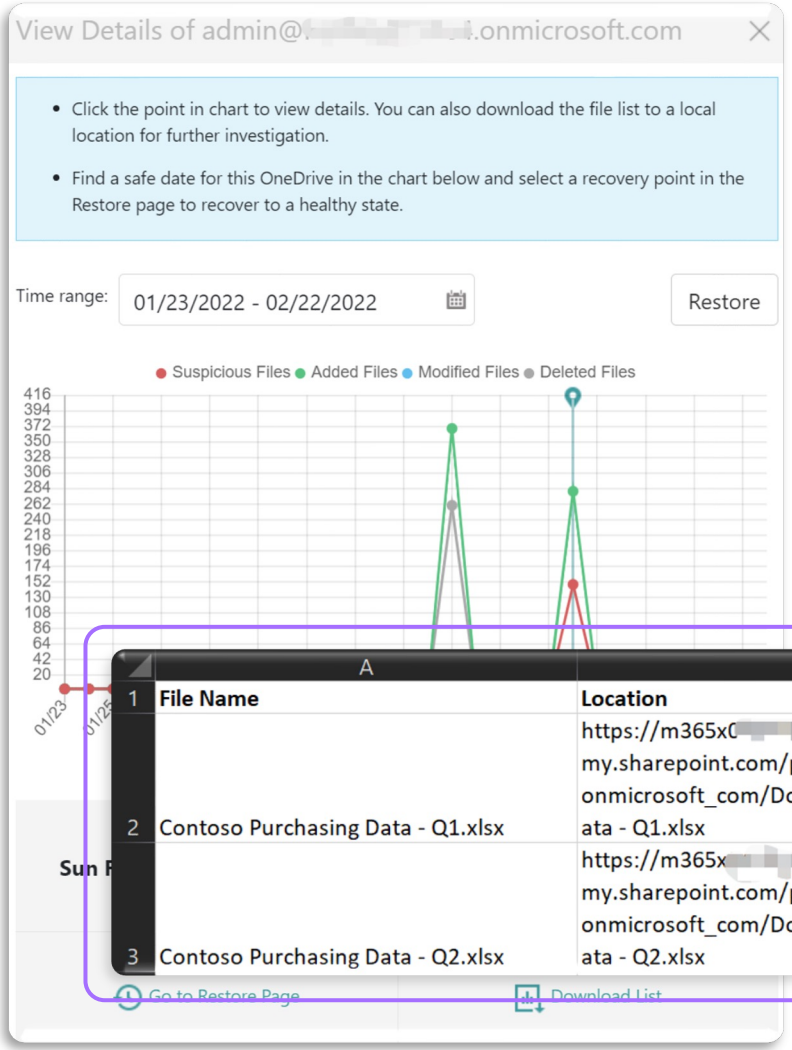
# Quick Investigation

Detailed zoom-in on key activities

Suspicious Files (suspected encryption)

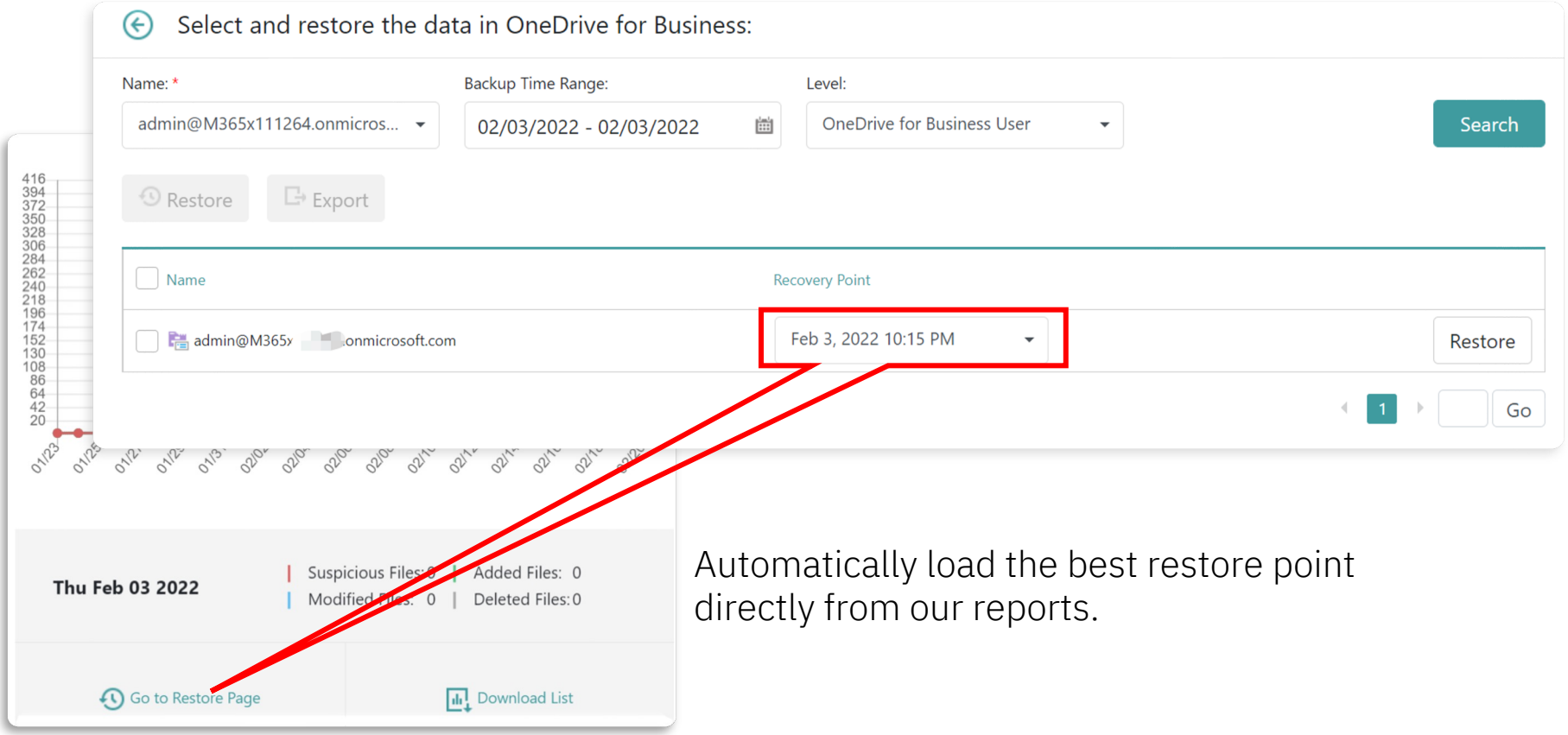
Events Detection (add / delete / modify)

Evidence-based reports for investigation




| | A | B | C | D |
|---|---|---|---|---|
| 1 | File Name | Location | File Status | Unusual Activity Detected Time |
| 2 | Contoso Purchasing Data - Q1.xlsx | https://m365x[redacted]-my.sharepoint.com/personal/admin_m365[redacted]_onmicrosoft_com/Documents/Contoso Purchasing Data - Q1.xlsx | Suspicious, Modified | 08/10/2021 9:00 AM (UTC) |
| 3 | Contoso Purchasing Data - Q2.xlsx | https://m365x[redacted]-my.sharepoint.com/personal/admin_m365x[redacted]_onmicrosoft_com/Documents/Contoso Purchasing Data - Q2.xlsx | Added | 08/10/2021 9:00 AM (UTC) |

# Getting your data to safety – Quick Restore




Automatically load the best restore point directly from our reports.

# Proactive Detection for Ransomware Attacks

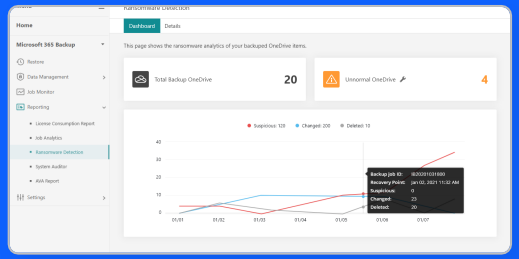
## Problem
### Data Protection

Individual user accidentally downloaded an attachment which caused one of their personal files to get encrypted. A One-Drive sync brought it to the cloud.

## Solution

- Alert for suspicious activity
- Quickly identify source file
- Avoid ransom costs and downtime
- Minimize risk and fire drills
- Minimize IT burden

## How can we help?



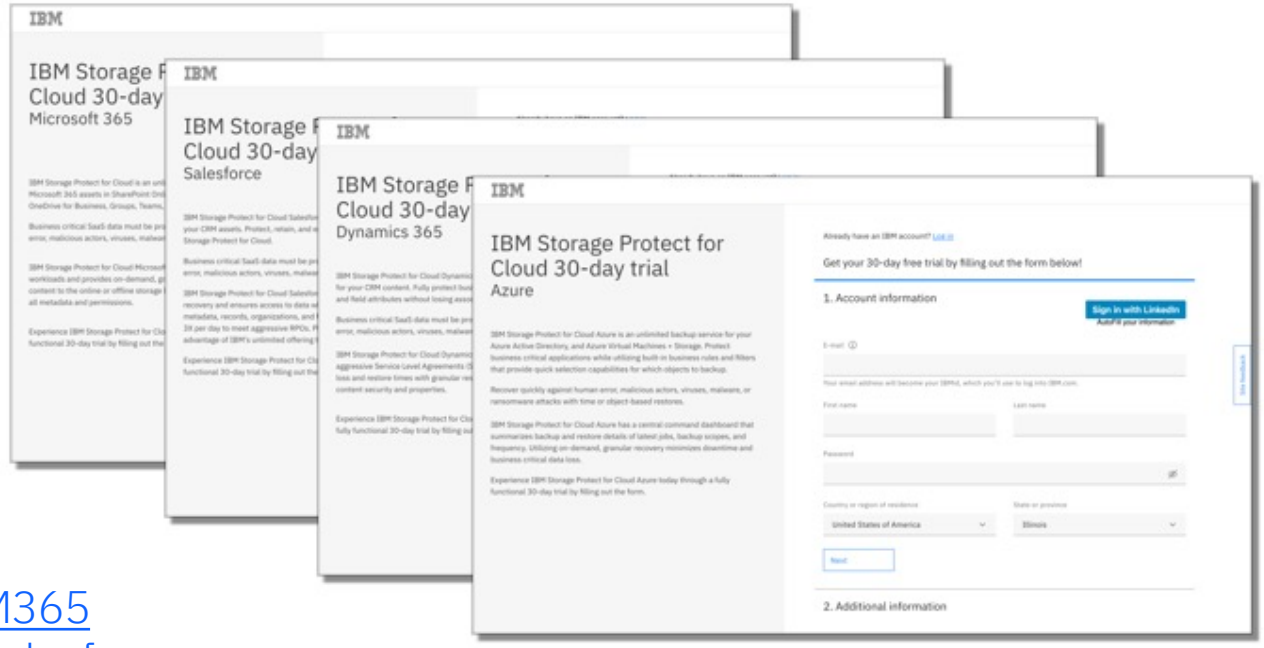

Early event detection

Real-time insights and guidance

Granular level restore

# Storage Protect for Cloud Microsoft 365 free trial

- 30-day trial setup in 10 minutes




Sign up here:

https://ibm.biz/TrySP4CM365
https://ibm.biz/TrySP4CSalesforce
https://ibm.biz/TrySP4CD365
https://ibm.biz/TrySP4CAzure

Prenos prezentacije:

# Hvala za pozornost!

**David Kosmač**

Acting Infrastructure Technical Sales Leader,
Eastern Europe Territories
david.kosmac@ibm.com