IBM SECURITY DAYS EVENT

NDB

DIGITALL

IBM Platinum Partner

telelink BUSINESS SERVICES

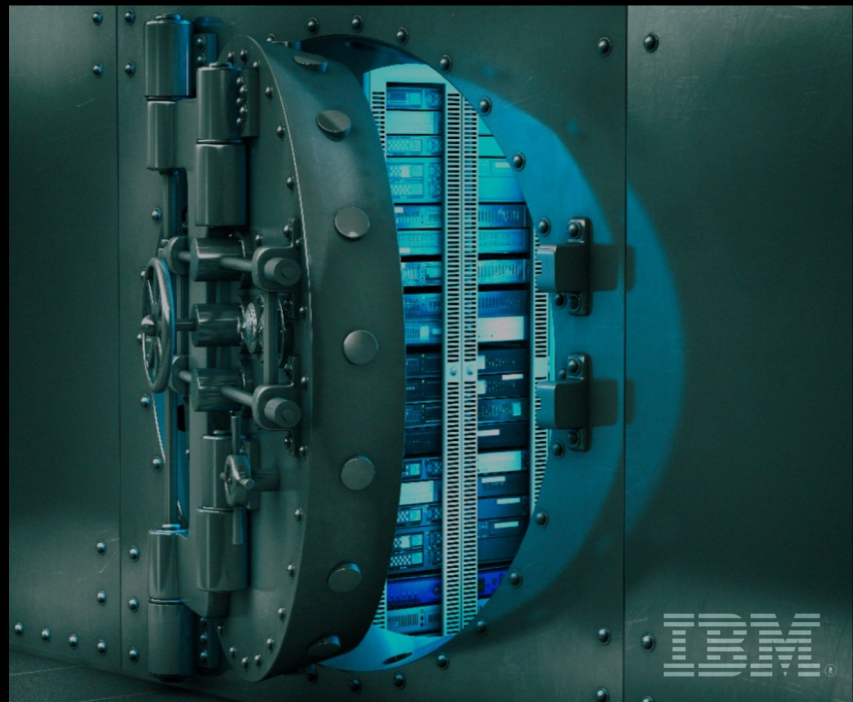
IBM Platinum Partner

CNSYS

IBM Gold Partner



Cyber Resilience with Storage Virtualize, FlashSystem and SAN Volume Controller



Krasimir Rashev

Systems Brand Sales Partner Leader, IBM
Technology Sales, Bulgaria
krasimir.rashev@bg.ibm.com
+359 888 608 645

IBM FlashSystem and SVC Family 2023

FlashSystem 5200



FlashSystem 5015 and 5035



FlashSystem 7300



FlashSystem 9500 and 9500R



SVC SV3

Hybrid Cloud



Storage Virtualize for Public Cloud





IBM **Spectrum Virtualize** *Storage function, scalability, interoperability, cloud integration and automation*



IBM **Storage Insights** Anomaly detection, fabric monitoring, full stack visibility, predictive support

Storage Virtualize Across The Family

IBM Spectrum Virtualize

Storage Insights (AI Predictive Analytics and Proactive Monitoring)



VMware & Container Integration

Multi-tenancy

3-Site Data Copies

Metro/Global Mirror (Remote copy)

Local and cloud snapshots

Volume Mobility for non-disruptive Data Migration across FlashSystem and SVC

Easy Tier (Automated hot/cold extent movement)

Data Migration (from >500 supported arrays)

Distributed RAID 1, 5 & 6 | DRAID 1 and 6

DRP (Software only) | Data Reduction Pools (Hardware assisted compression)

Clustering (Multiple I/O groups)

HyperSwap (Active / active access)

Encryption (Local and server based keys)

NVMe-oF Host Connections

External Storage Virtualization (>500 Supported Arrays)

Safeguarded Copy – delivering immutable copies

FCMs (NVMe with compression & encryption) & NVMe/SCM drives

Storage Class Memory (ultra low latency drives)

Storage Virtualize Across The Family

IBM Spectrum Virtualize

Storage Insights (AI Predictive Analytics and Proactive Monitoring)



VMware & Container Integration

Multi-tenancy

3-Site Data Copies

Metro/Global Mirror (Remote copy)

Local and cloud snapshots

Volume Mobility for non-disruptive Data Migration across FlashSystem and SVC

Easy Tier (Automated hot/cold extent movement)

Data Migration (from >500 supported arrays)

Distributed RAID 1, 5 & 6 | DRAID 1 and 6

DRP (Software only) | Data Reduction Pools (Hardware assisted compression)

Clustering (Multiple I/O groups)

HyperSwap (Active / active access)

Encryption (Local and server based keys)

NVMe-oF Host Connections

External Storage Virtualization (>500 Supported Arrays)

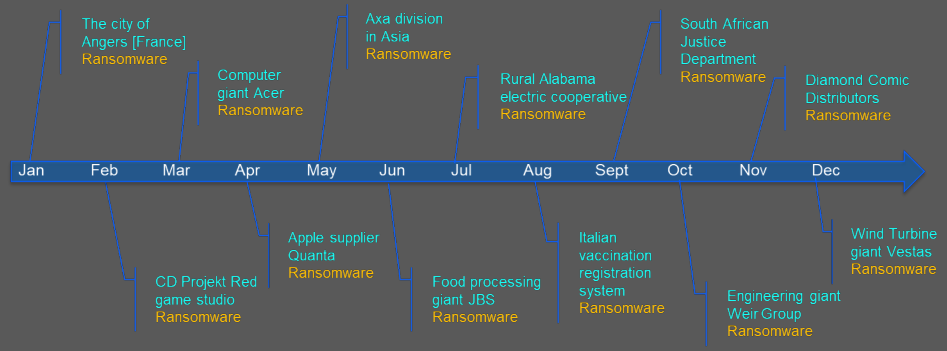
Safeguarded Copy – delivering immutable copies

FCMs (NVMe with compression & encryption) & NVMe/SCM drives

Storage Class Memory (ultra low latency drives)

Why Cyber Resiliency is so important

2021 headlines in review



23 days

Average recovery after a ransomware attack

83%

of Ransomware Victims Pay Their Attackers

5

Unexpected ransomware costs CFOs must account for:

1. Higher Borrowing Costs
2. Higher Insurance Premiums
3. Customer Notification Cost
4. Brand Damage
5. Potential Lawsuits

$5.2m

Average cost of Ransomware

IBM primary storage solutions for immutable copy

Immutable copies

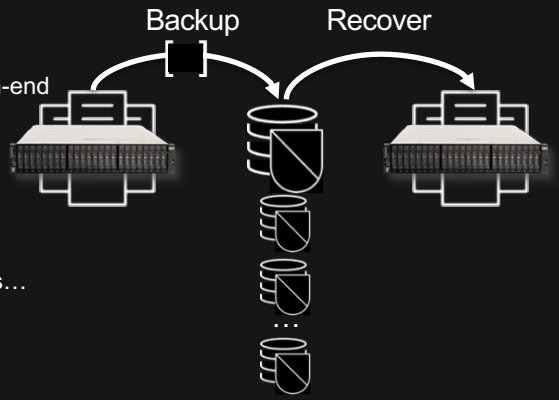
When you need a copy that bad actors can't reach

Built with
IBM Spectrum Virtualize

Cross-vendor support

Enterprise storage from entry to high-end
IBM FlashSystem

Heterogeneous storage with
SAN Volume Controller
Pure HPE IBM
Dell/EMC NetApp 500+ others…



Safeguarded Copy

Immutable point-in-time copies of production data

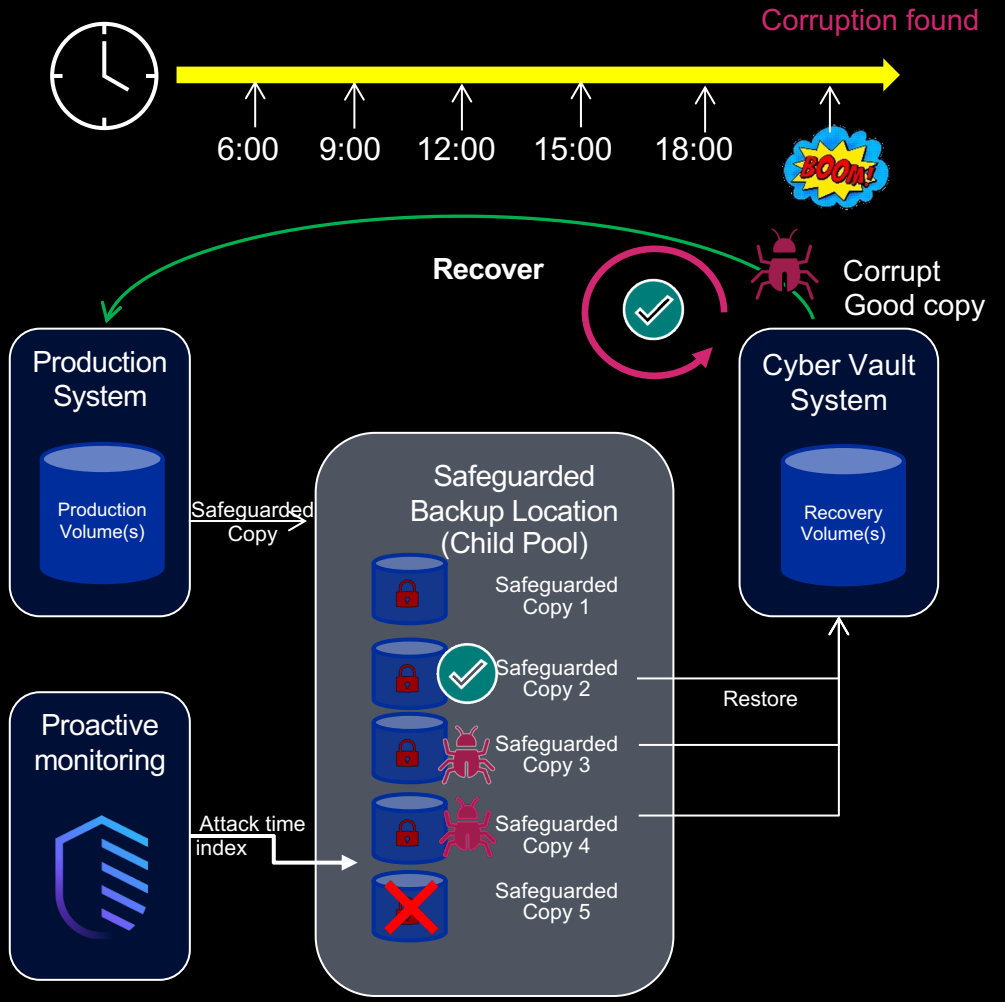
Isolated logical air-gap offline by design

Separate privileges for admins of production data and Safeguarded Copies

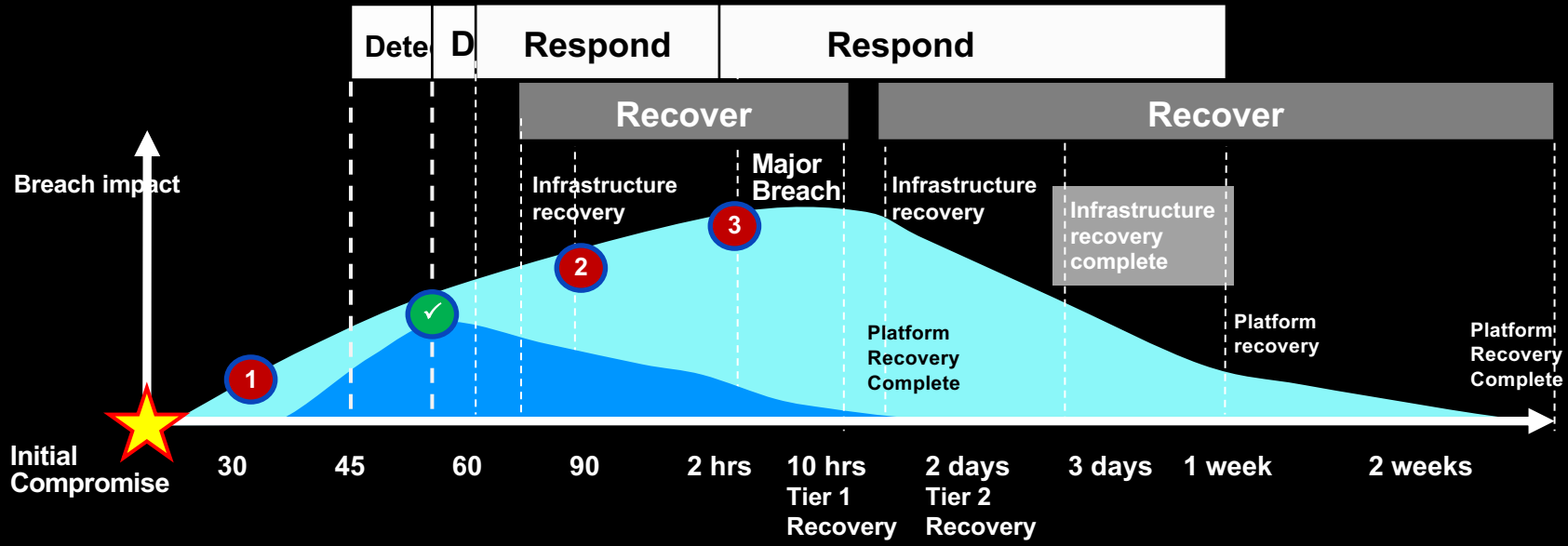
Consistent automation with other copy services

IBM Spectrum Virtualize provides Safeguarded Copy

- **Logical Corruption Protection** to prevent sensitive point in time copies of data from being modified or deleted due to errors, destruction or ransomware
- Up to 15864 objects to provide immutable Safeguarded copies of production data stored in Safeguarded backup capacity known as a Child Pool
  - Not directly accessible to any server or application
- Data is accessible *only* after a Safeguarded copy is **recovered to a separate recovery volume**.
- **Proactive monitoring** for signs of attack
  - Identify Safeguarded Volume to recover based on time index of identified attack
- Recovery volumes are used for:
  - Data validation
  - Forensic analysis
  - Restoration of production data



Cyber attack detection and recovery



1. Corruption of data occurs - but not yet detected
2. Without the IBM Cyber Vault environment corruption is detected much later and has a greater chance to spread
3. It takes even longer to identify all impacted data once the corruption has spread within the enterprise

IBM Cyber Vault Effect

Due to the Cyber Vault environment and the use of Safeguarded Copy technology, data is continuously checked and corruption is found and corrected EARLIER and FASTER

IBM Cyber Vault – Solution Elements

Immutable Copies of Data

IBM DS8000
IBM FlashSystem
IBM Safeguarded Copy

Proactive Monitoring

IBM Storage Insights

IBM QRadar
or
Non-IBM SIEM

Cyber Vault

Methodology and Automation

Rapid Recovery

Safeguarded Copy's are the enabler
Recovery from copy on primary storage array
Automation with:

- Copy Services Manager
- Copy Data Management
- Ansible
- Scripts

Data Copy Test and Validation

Application Independent

IBM Storage Sentinel
Predatar
CyberSense
Others

Application Tools

MongoDB – Validate
SQL – Checkdb, Checktable
Db2 - Inspect, Db2dart
Oracle – DBVerify, Db_checksum




Thank
you