

Introducing IBM Safeguarded Copy for IBM FlashSystem and SVC

Speed recovery from cyber attacks

Automatic

creation of regular backup copies

Immutable

point-in-time copies of production data

Isolated

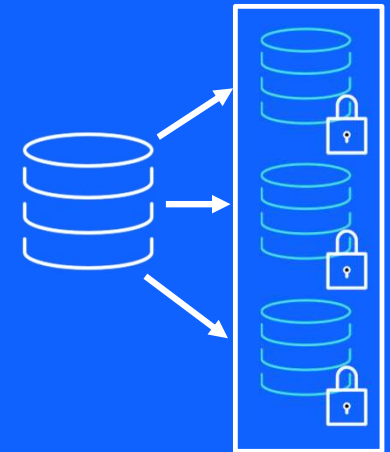
logical air-gap offline by design

Fast

restore from copies on primary storage

Prevents modification

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



Spectrum Virtualize Safeguarded Copy provides Cyber Resiliency against a cyber attack



Protect against cyber attack

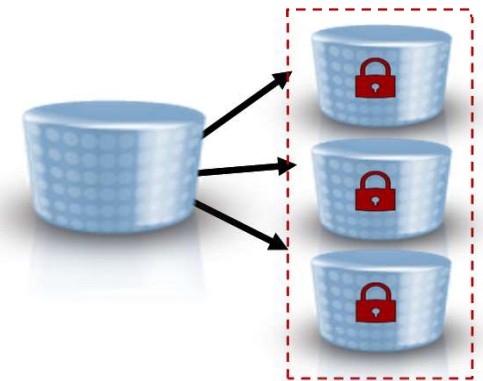
- **Immutability:** Safeguarded Copy for immutable point-in-time copies of production data
- **Isolation:** Air Gap “offline by design”

Up to
15,864

Objects to provide immutable point-in-time copies of data

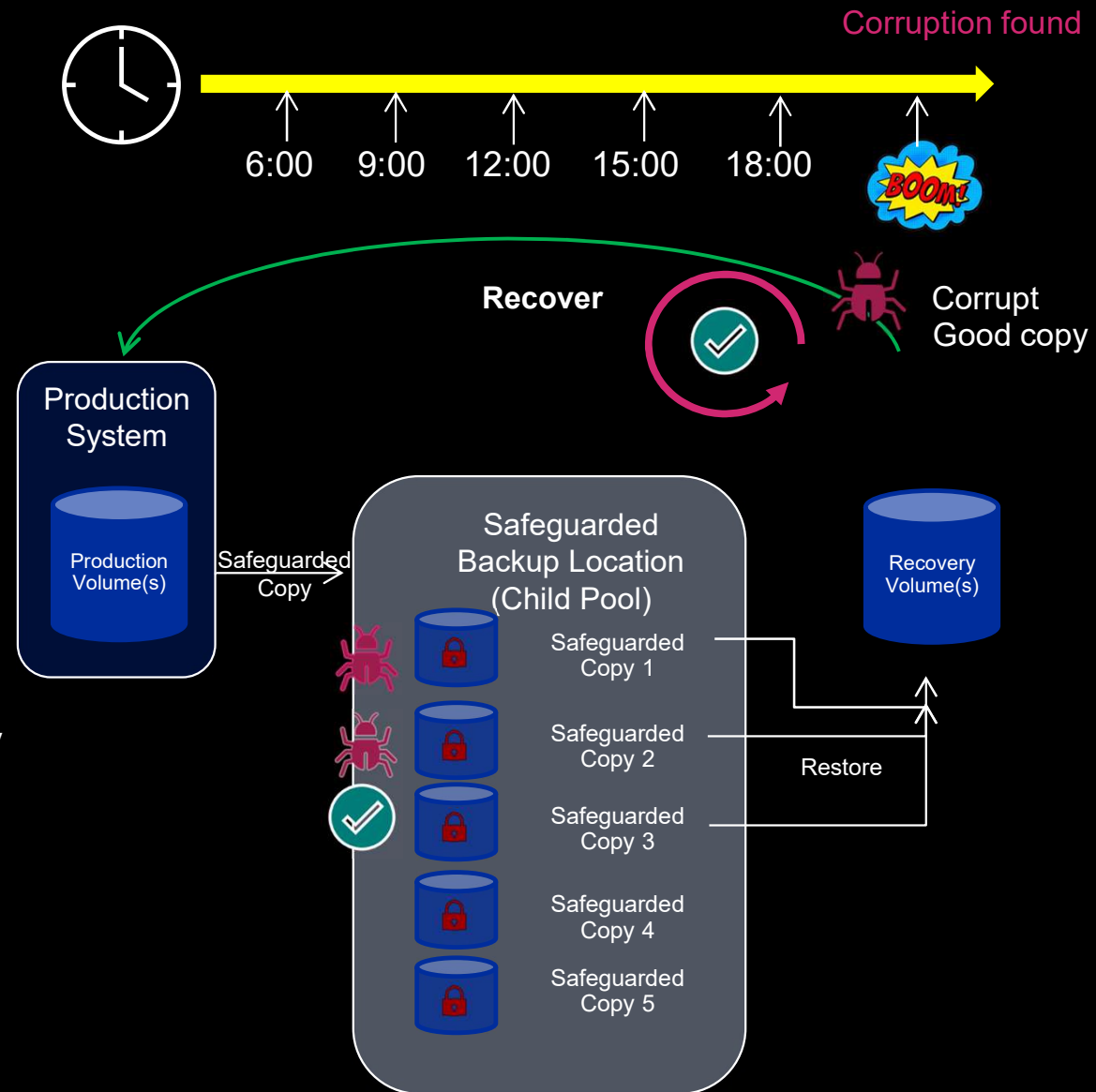
Fast restore
from
Primary
Storage

Prevents modification or deletion of sensitive point-in-time copies due to user error, malicious destruction, or ransomware attack



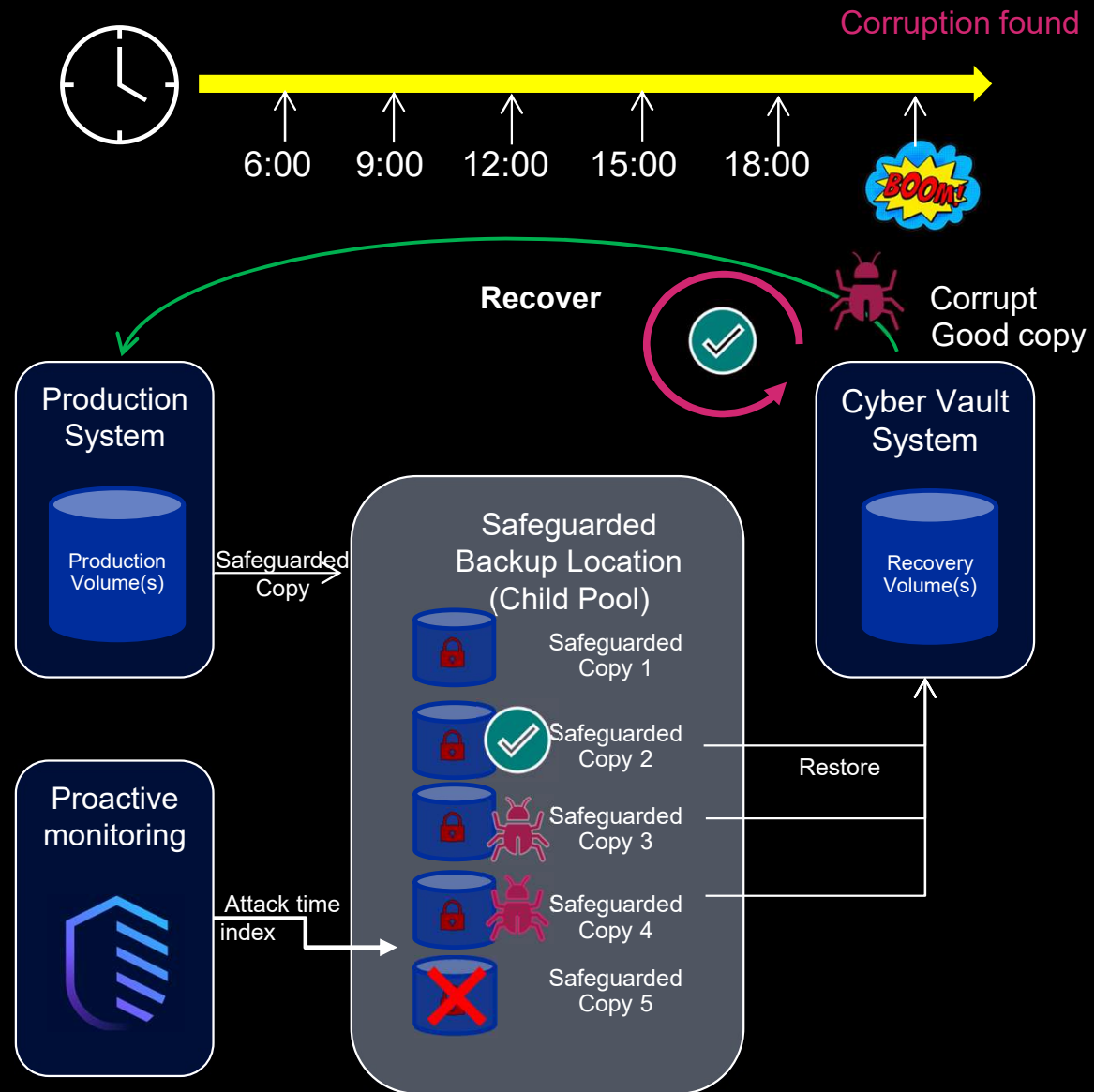
IBM Spectrum Virtualize provides Safeguarded Copy

- 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.
- Recovery volumes are used for:
 - Data validation
 - Forensic analysis
 - Restoration of production data



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



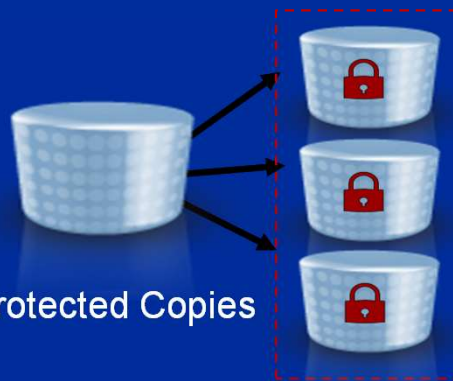
Spectrum Virtualize Safeguarded Copy Data Resilience

IBM FlashSystem Safeguarded Copy feature prevents point in time copies of data from being modified or deleted due to user errors, malicious destruction or ransomware attacks



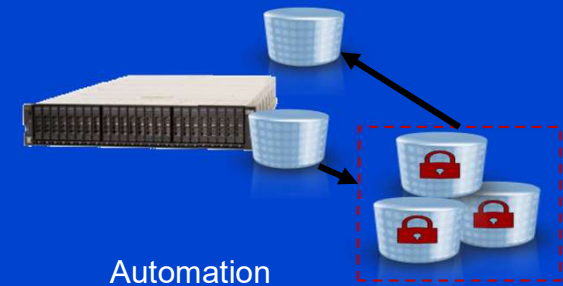
Separation of duties

Provide additional security capabilities to prevent non-privileged users from compromising production data



Protected Copies

Provide capabilities to regularly create immutable point in time copies of the data



Automation

Provide the ability to manage and restore immutable point in time copies

Separation of Duties: Current user role overview



Other:
VASA Provider Service
3SiteAdmin

Separation of Duties

Administrator



Day-to-Day tasks

- Can provision and configure Safeguarded Copies
- Can create Safeguarded Policies and modify them
- Can **not** remove or damage existing Safeguarded backups
- Can **not** remove or compromise a Safeguarded backup location (child pool)

Superuser



Highest Authority, Maintenance

- Can perform maintenance actions unrestricted
- Can remove a Safeguarded Copy and Safeguarded backup location (child pool)
- Account can be disabled for extra security.
Re-enable by Remote Support (IBM) or Tech Port

Security Administrator



- Can manage users and security
- Can remove a Safeguarded Copy and Safeguarded Pool