




**Hewlett Packard
Enterprise**

TBC23 – VT5 Ransomware Protection and Data Recovery



Paul J. Holenstein
Executive Vice President
Gravic, Inc.

September 2023

Follow us on
LinkedIn



Disclaimer

This presentation contains forward-looking statements regarding future operations, product development, product capabilities and availability dates. This information is subject to substantial uncertainties and is subject to change at any time without prior notification. Statements contained in this presentation concerning these matters only reflect Gravic, Inc.'s predictions and/or expectations as of the date of this presentation and actual results and future plans of Gravic, Inc. may differ significantly as a result of, among other things, changes in product strategy resulting from technological, internal corporate, market and other changes. This is not a commitment to deliver any material, code or functionality and should not be relied upon in making purchasing decisions.

Specifications are subject to change without notice and delivery dates/timeframes are not guaranteed...purchasing decisions should not be made based on this material without verifying the desired features are available on the platforms and environments desired.

NOTICE: This product does not guarantee that you will not lose any data; all user warranties are provided solely in accordance with the terms of the product License Agreement. Each user's experiences will vary depending on its system configuration, hardware and other software compatibility, operator capability, data integrity, user procedures, backups and verification, network integrity, third party products and services, modifications and updates to this product and others, as well as other factors. Please consult with your supplier and review our License Agreement for more information.

All trademarks mentioned in this presentation are the property of their respective owners.

HPE Connect TBC slides are used with express permission from HPE product group.

Agenda

- **Digital resilience** against Malware & Ransomware
 - Current state
- **Detection and recovery methods**
 - #1: Online recovery in real-time
 - #2: Air-gapped recovery from immutable storage
- **HPE Demo drill-down** – Current state of **Malware/Ransomware detection & recovery**
 - How it works...
 - Evolving capabilities...trying to keep up with the bad guys...
- Looking ahead to **Malware/Ransomware detection & prevention**
 - New **Validation Architectures**...trying to **outpace** the bad guys...
- Summary



Digital resilience against Malware & Ransomware

Global impact

Digital resilience against Malware & Ransomware

Malwarebytes LABS Personal Business Pricing Partners Resources

THREAT INTELLIGENCE

Global ransomware attacks at an all-time high, shows latest 2023 State of Ransomware report

Posted: August 3, 2023 by Threat Intelligence Team

Ransomware attacks have shown no signs of slowing down in 2023.

A new report from the Malwarebytes Threat Intelligence team shows **1,900 total ransomware attacks** within just four countries—the US, Germany, France, and the UK—in one year.

The findings, compiled together in the 2023 State of Ransomware Report, show alarming trends in the global ransomware surge from July 2022 to June 2023. For example, the report shows that the **US shouldered a hefty 43 percent of all global attacks** and that ransomware attacks in France nearly doubled in the last five months.

To say ransomware gangs have been unkind to the US in the past year is an understatement.

Malwarebytes found that a total of 48 separate ransomware groups attacked the US in the observed period. To boot, there was a 75 percent increase in the average number of monthly attacks in the US between the first and second half of the last 12 months.

Country	Number of Attacks
US	1462
UK	196
Canada	159
Germany	124
Italy	120
France	118

- “
- **1,900 total ransomware attacks** within just four countries—the US, Germany, France, and the UK—in one year
 - The **US shouldered a hefty 43 percent of all global attacks**
 - Malwarebytes found that a total of 48 separate ransomware groups attacked the US in the observed period
 - If more groups start adopting CLOP's zero-day exploitation techniques, **the ransomware landscape could tilt from service-oriented attacks to a more aggressive, vulnerability-focused model**—a move that could skyrocket the number of victims.
- ”

Source: [Malwarebytes.com/Blog/Threat-Intelligence/2023/08/Global-Ransomware-Attacks-At-An-All-Time-High-Shows-Latest-2023-State-of-Ransomware-Report](https://malwarebytes.com/Blog/Threat-Intelligence/2023/08/Global-Ransomware-Attacks-At-An-All-Time-High-Shows-Latest-2023-State-of-Ransomware-Report)

Global impact

Digital resilience against Malware & Ransomware

- **Digital resilience against Malware & Ransomware**

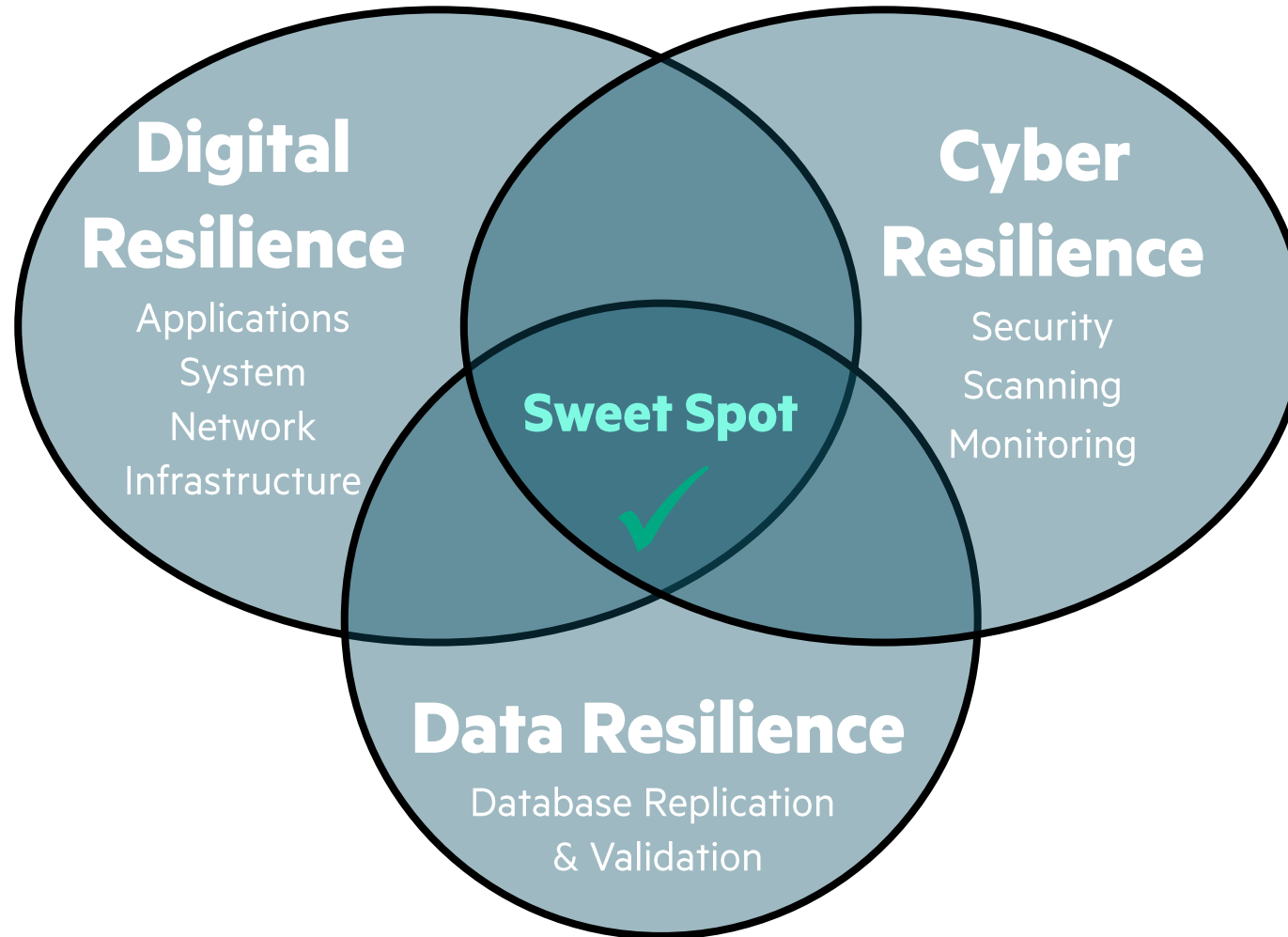
- Global business concern
- Ransomware works slowly, usually only stealing data 3-4 months after a breach
- According to Veeam
 - 93% of attacks targeted backup repositories
 - 4% of Ransomware victims paid the ransom and could not recover their data
 - 77% of payments were covered by insurance
 - On average, only 66% of affected data was recoverable

- **Digital resilience – let us help you get here**

- Government regulations underway to push companies along...
- Protection, detection, containment, recovery and repair capabilities against information and communication technology (ICT) related incidents
- Newly developed approaches (e.g., “immutable” backups and “air-gapped” systems) to thwart these attacks



Business resilience against Malware & Ransomware requires a multi-faceted approach



Malware & Ransomware

Background

1. Know your enemy

- a. **Malware** – software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system*
 - Plus user/operator errors, malfeasance, or any change that unilaterally affects the outcome of the transaction in a ‘negative’ way
- b. **Ransomware** – malicious software designed to block access to a computer system until a sum of money is paid*

2. Resilience against each is (a bit) different

- a. Each has separate attack vectors
- b. **Key point:** multiple solutions are required and must be coordinated

3. Detection & recovery is not the same thing as prevention

- a. Today, state of the art is post event **detection and recovery**
- b. Ultimately, the goal is immediate **identification and prevention**

*Source: Dictionary.com



Malware & Ransomware

Background

4. **HPE Shadowbase** currently provides **data resilience** for detection & recovery
 - a. **Fingerprinting of IPC messages and data files** to detect tampering
 - b. **Data recovery** in real-time to minimize downtime
 - c. **Support for air-gapped architectures** to aid in isolation & recovery efforts
5. However, **HPE Shadowbase is only one piece of the solution** – for example, malware that stealthily steals data requires additional counter-measures
 - a. **Monitoring for unauthorized inbound & outbound traffic**
 - b. **Application & O/S fingerprinting** & verifying signatures to detect tampering
 - c. **And more to come...**
6. The **Gravic Validation Architecture (VA)** is a new technology being developed to immediately *detect & prevent* data corruption



Digital resilience for Ransomware defense using HPE Shadowbase

On HPE NonStop

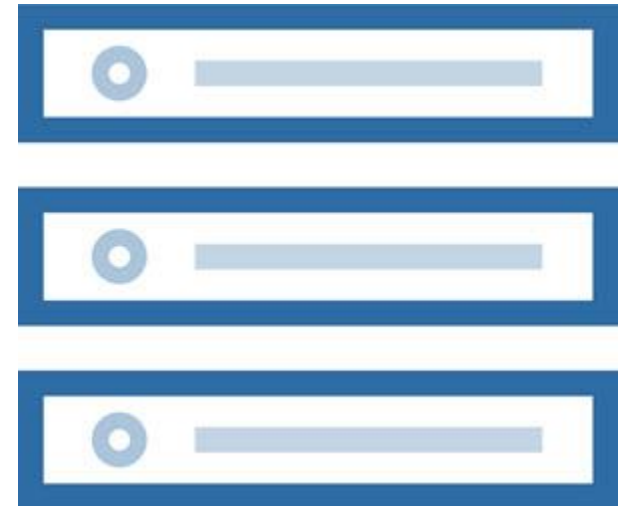
- *TMF is your first line of defense!*
- Non-audited data / data replication *does not* have the same advantages, capabilities, nor protection
 - In a non-audited environment, if malware invaded & performed data tampering – how would you know? No changes are logged...☹️

Using TMF

- Guarantees **all** database changes are **always** logged
- Enables the **Audit Trail** to be used for recovery

HPE Shadowbase provides unique capabilities

- **Integrates with TMF** to extract database change data
- **Detects data in motion & man-in-the-middle (MiTM) attacks** between key processes since messages are fingerprinted
- **Fingerprints Shadowbase Queue Files** to detect data file tampering
- Gravic has provided digital resilience solutions for 40+ years



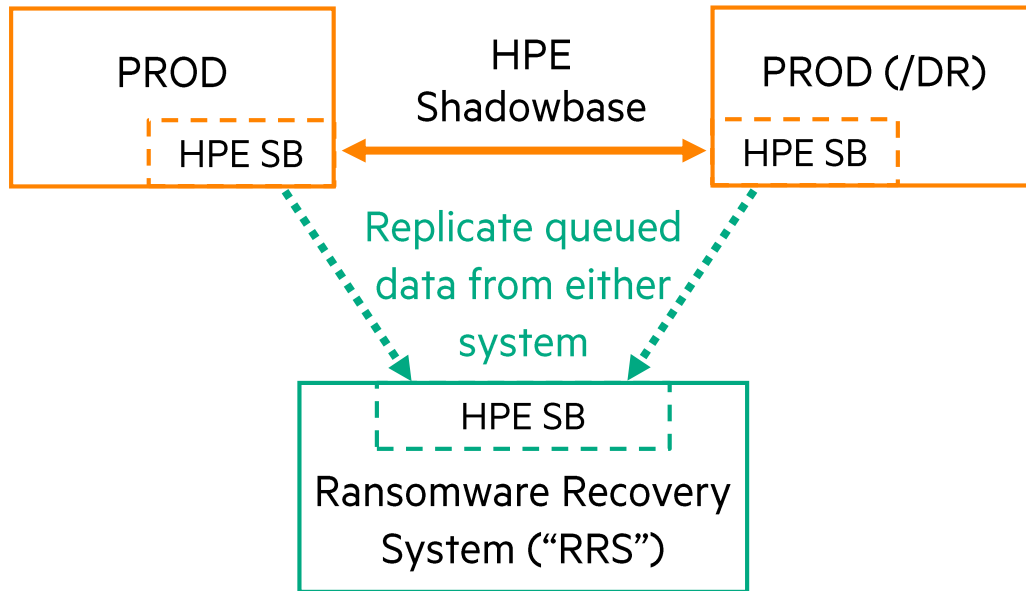
Detection & recovery methods

Available today

HPE Shadowbase Digital Resilience

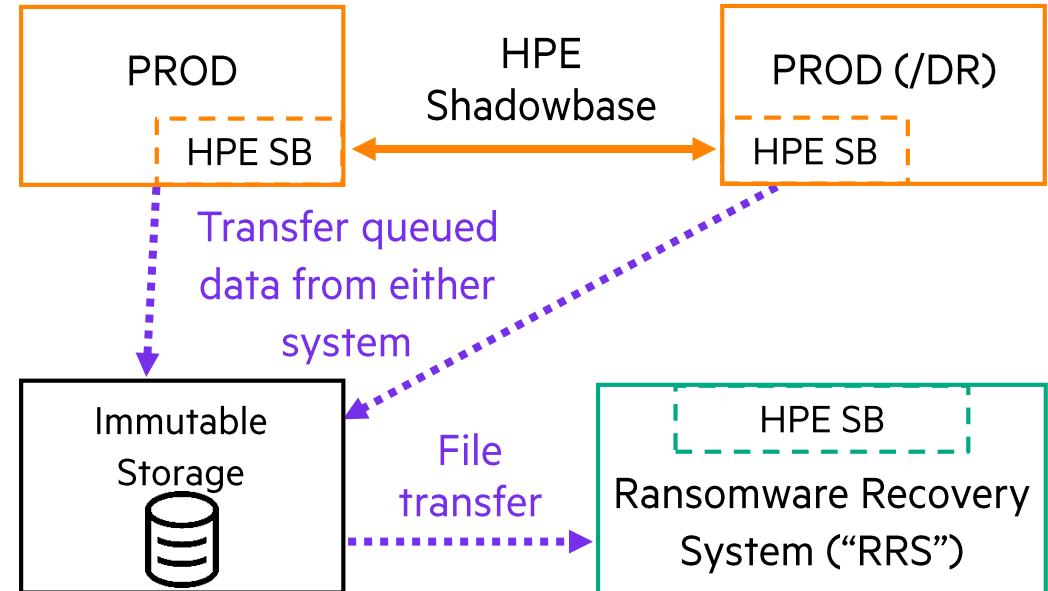
Ransomware & Malware Defense

Solution 1: Real-time recovery system



- TCP/IP or Expand feed from either system to RRS
- Capture and store (queue) DB change data **directly on RRS**
- But is this really S-A-F-E?

Solution 2: Air-gapped, immutable storage



- Air and people gapped RRS
- Capture and store (queue) DB change data **on immutable storage**

How to survive a Ransomware attack!

HPE Shadowbase Ransomware demo



Survive a Ransomware Attack!

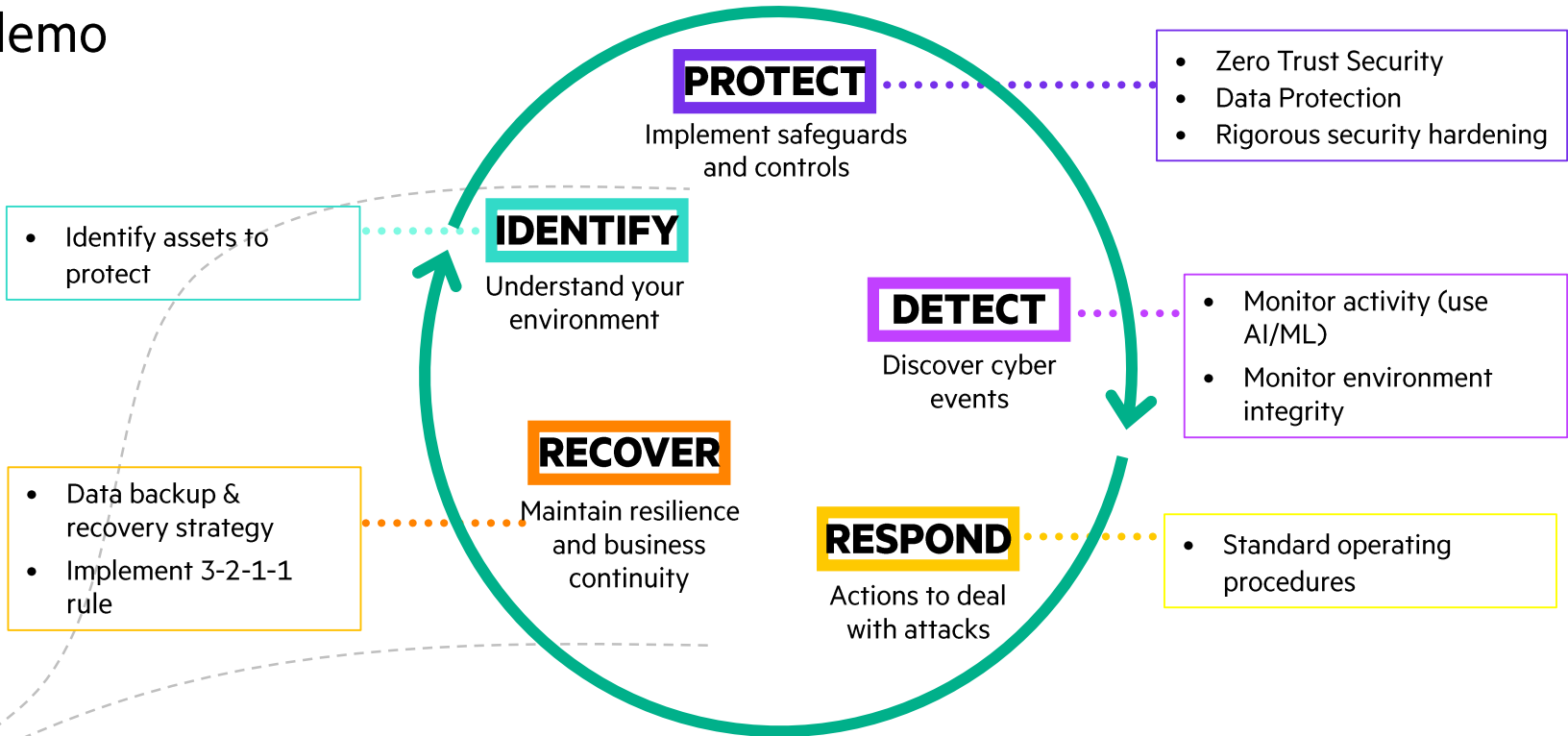
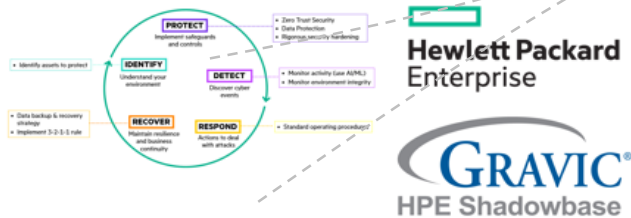
HPE Shadowbase Ransomware demo

Survive a Ransomware Attack!

HPE solutions can help protect and recover your mission critical NonStop systems and data from malware and Ransomware

- Rapidly restore systems and recover data
- Air-gapped backups
- Immutable storage
- 3-2-1-1 backup rule
- Preserve corrupted environment for forensics

Demo at HPE booth

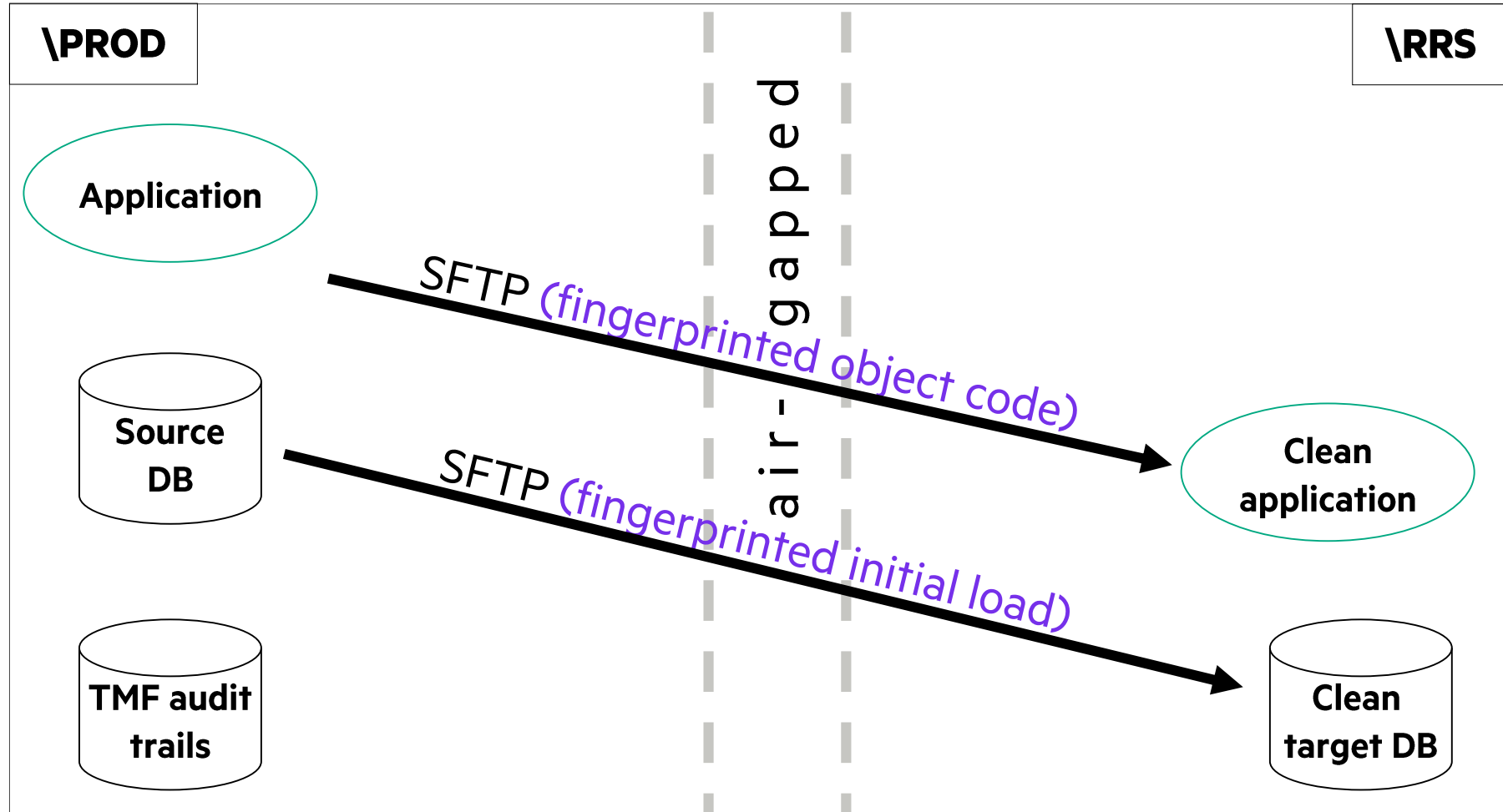


HPE Digital Resiliency Framework based on NIST guidelines

- New HPE Shadowbase capabilities work to rapidly **RECOVER** critical data
- Current focus is on **detection** and **recovery**, with future capabilities directed at **identification** and **prevention** (and hence **avoidance**)

Create a known-good Ransomware Recovery System (\RRS)

Use an air-gapped system & immutable storage



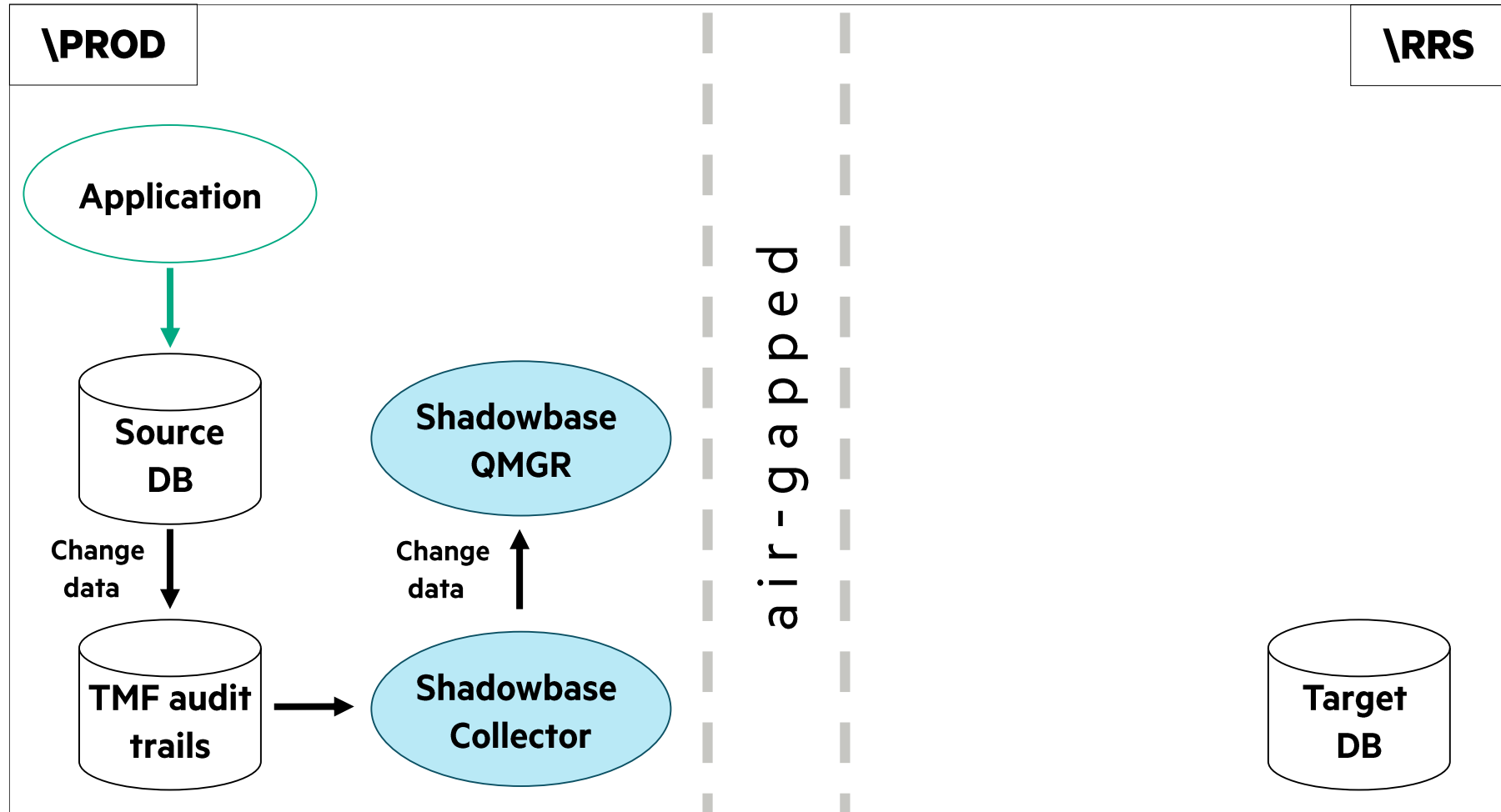
Create and **send a copy of the application and source \PROD DB to the \RRS** (Ransomware Recovery System) target to create a “clean” \RRS environment (‘known-good’ initial state)

Note:

1. Both must be ‘known good’ (uncorrupted)
2. Use SFTP, VTS, or other acceptable method that preserves the “air-gapped” concept
3. Use a fingerprinting technique to verify the files being transferred

Configure & start HPE Shadowbase on \PROD

Capture \PROD change data to synchronize \RRS

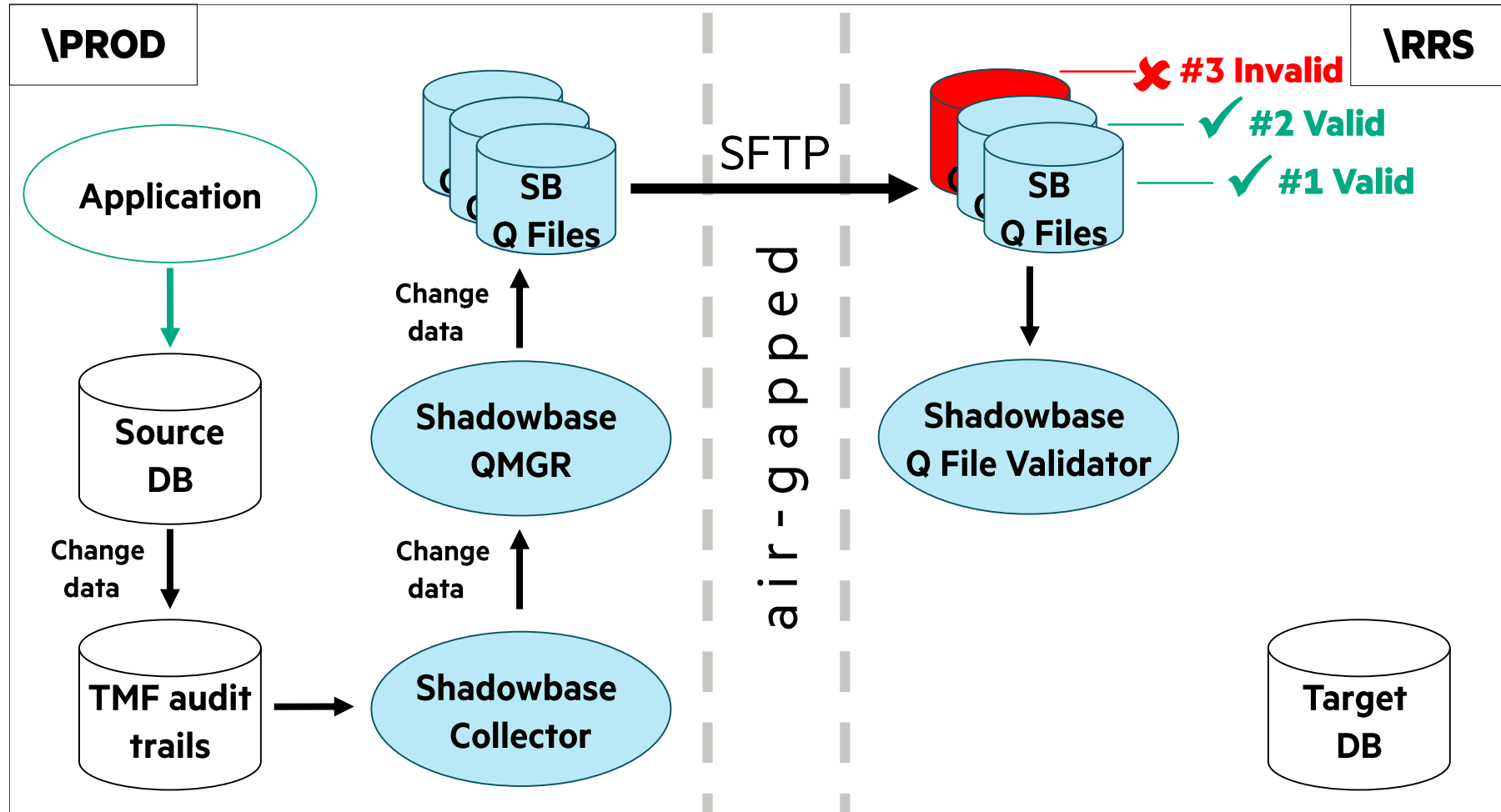


Steps:

- 1. Configure and start HPE SB** to capture \PROD database changes (audit trail change data)

FTP HPE Shadowbase Q files to the \RRS system

Send SB QMGR Q Files from \PROD to \RRS via SFTP as they fill

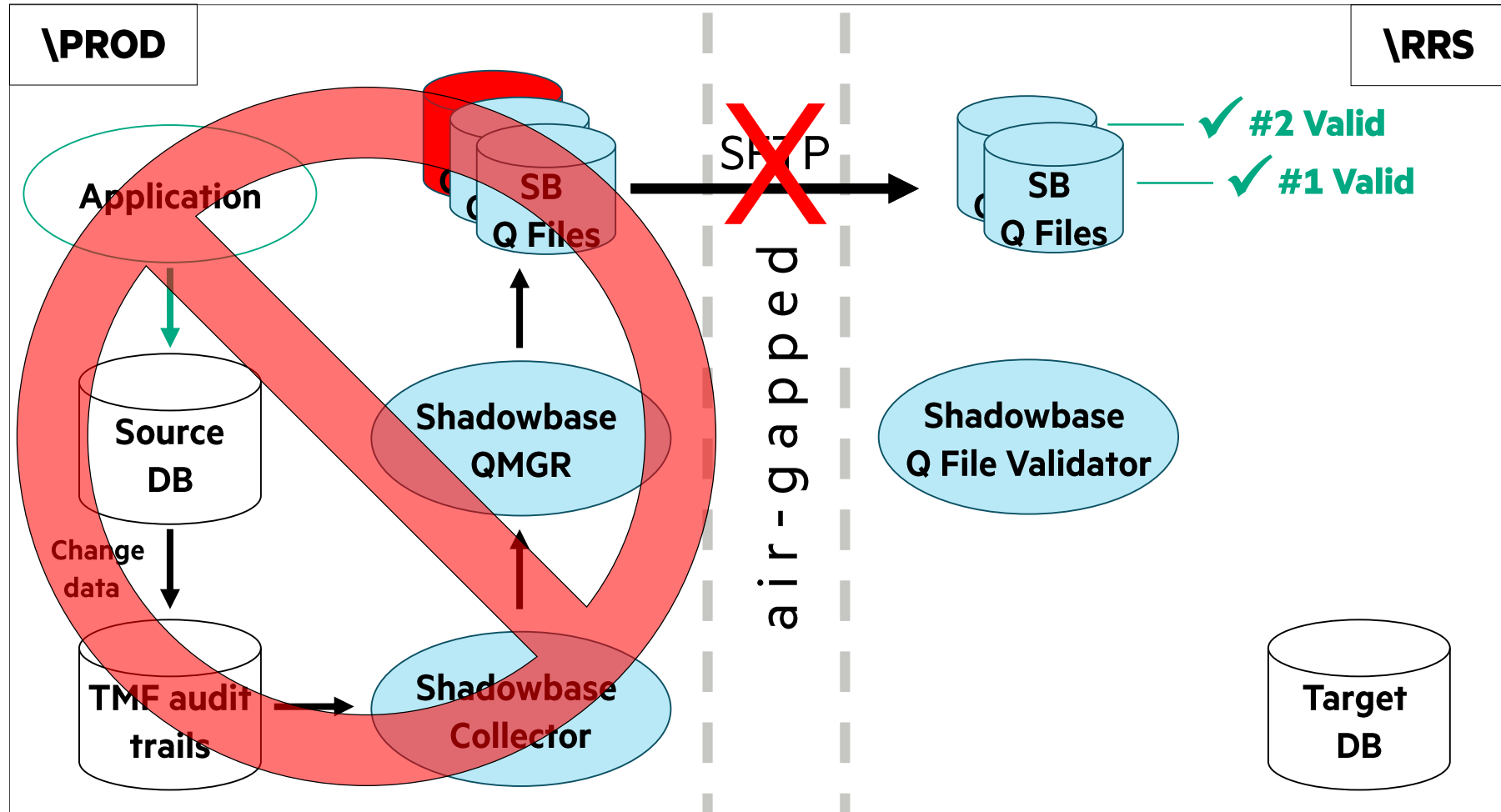


Steps:

1. Configure and start HPE SB to capture \PROD database changes (audit trail change data)
2. As the \PROD QMGR Q Files fill, immediately **transfer them to the \RRS system via secure FTP**
 - a. **Run the SB Q File Validator** to verify each file's fingerprint:
 - i. SB Q File 1 is valid
 - ii. SB Q File 2 is valid
 - iii. SB Q File 3 is invalid (remove)

When a Ransomware attack occurs...

Air-gapped system & immutable storage



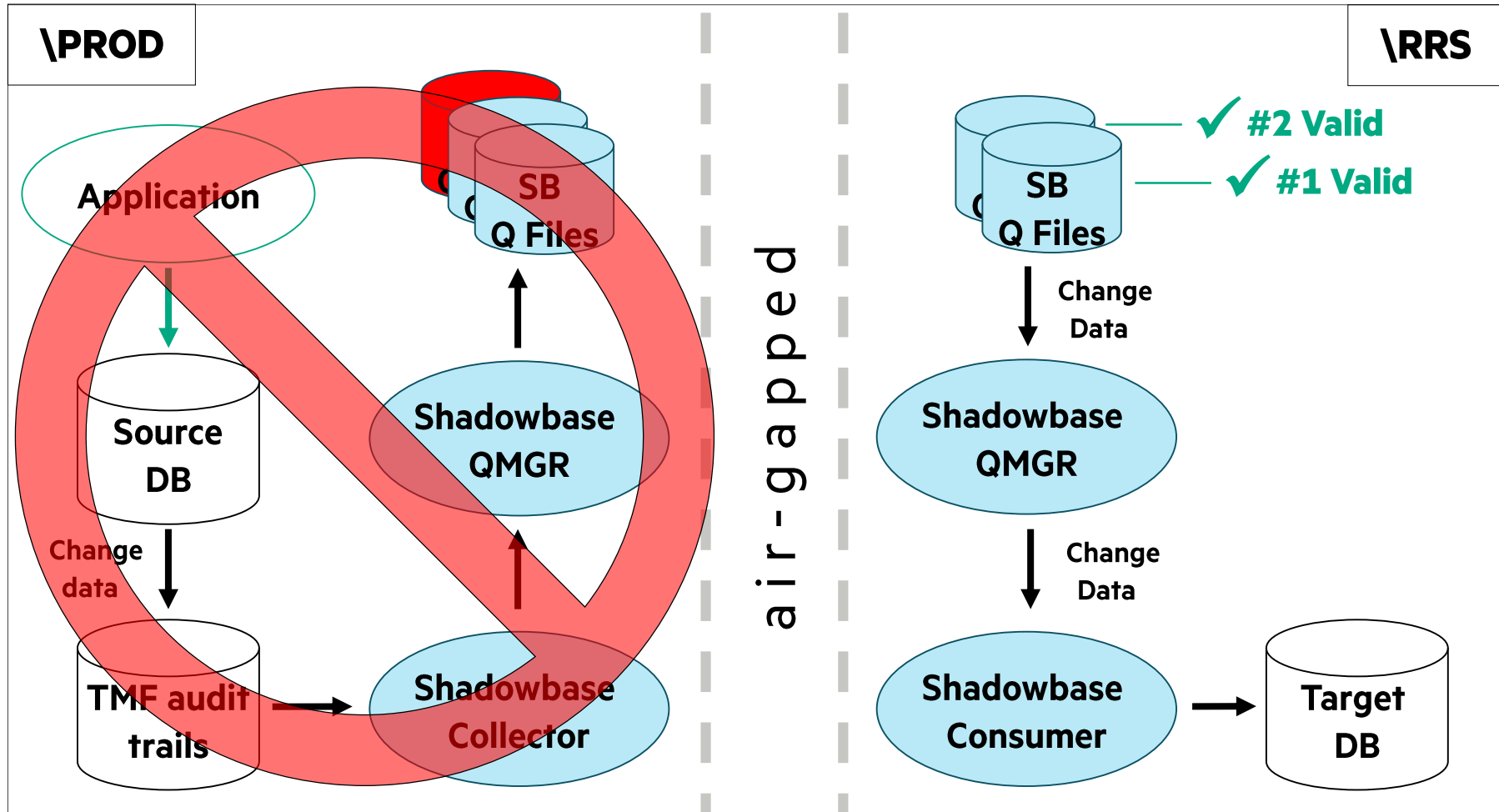
Discussion point: how do you know when the attack occurred?

Steps:

1. Configure and start HPE SB to capture \PROD database changes (audit trail change data)
2. As the \PROD QMGR Q Files fill, immediately **transfer them to the \RRS system via secure FTP**
 - a. **Run the SB Q File Validator** to verify each file's fingerprint:
 - a. SB Q File 1 is valid
 - b. SB Q File 2 is valid
 - c. SB Q File 3 is invalid (remove)

Start HPE Shadowbase

Air-gapped system & immutable storage



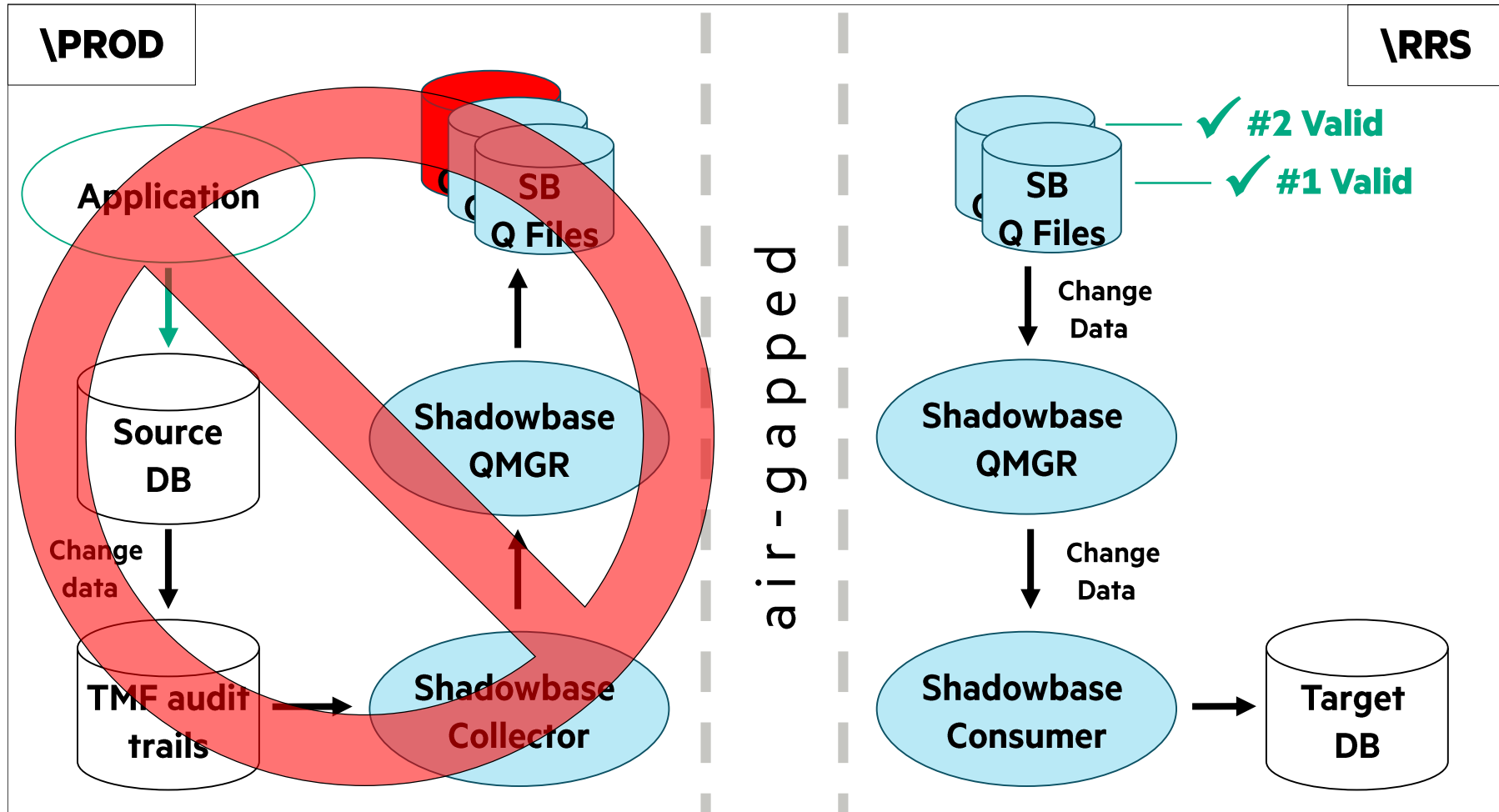
Steps:

3. Start SB and replay the valid Q Files:

- Replay SB Q File 1
- Replay SB Q File 2

Stop HPE Shadowbase

Air-gapped system & immutable storage

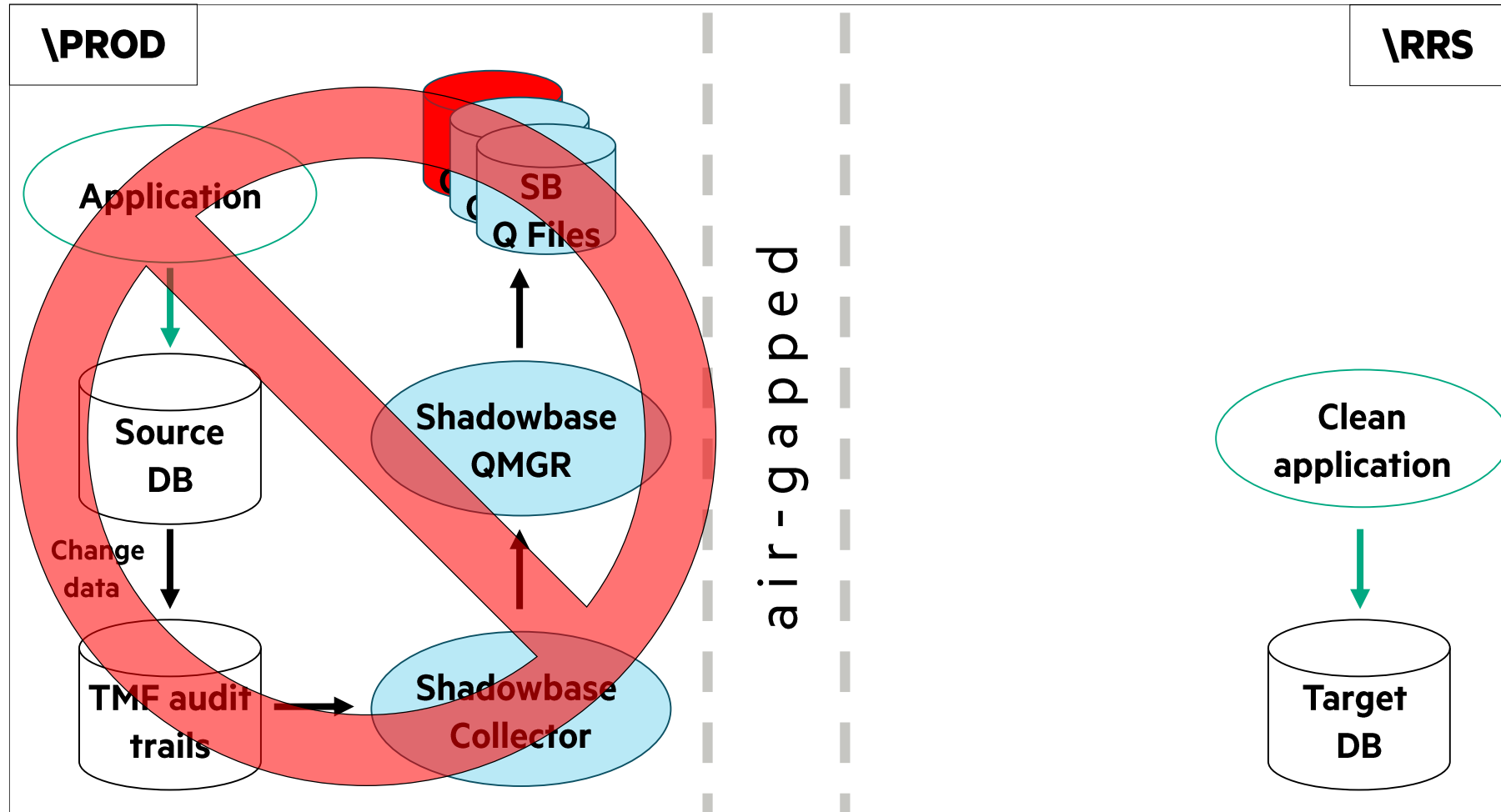


Steps:

3. After verifying the fingerprints, start SB and replay the valid Q Files:
 - a. Replay SB Q File 1
 - b. Replay SB Q File 2
4. **Stop Shadowbase** replication on the \RRS

Bring the clean \RRS application online

Air-gapped system & immutable storage

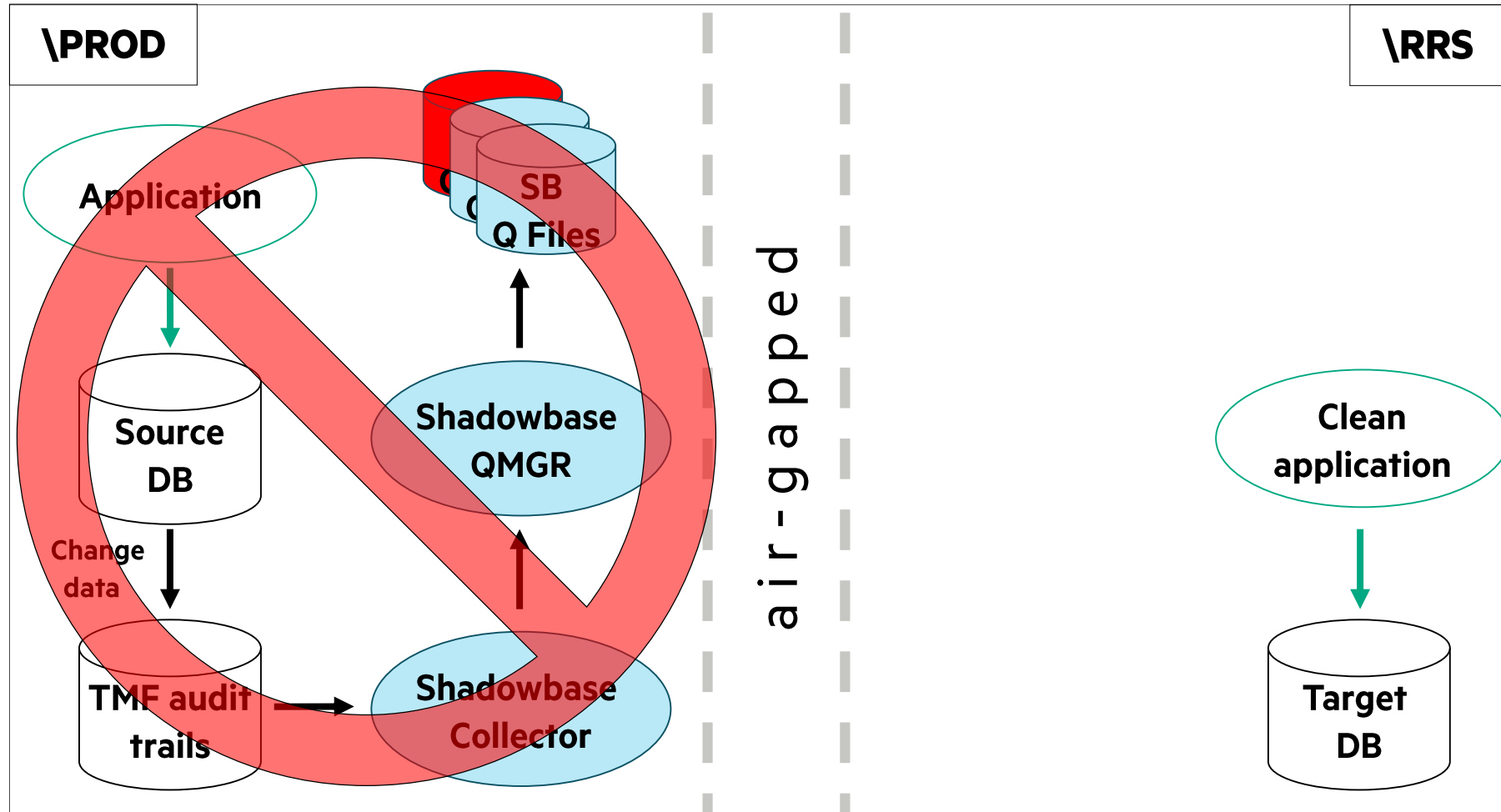


Steps:

3. After verifying the fingerprints, start SB and replay the valid Q Files:
 - a. Replay SB Q File 1
 - b. Replay SB Q File 2
4. Stop Shadowbase replication on the \RRS
5. **Bring the clean \RRS application online** and connect it to the synchronized Target DB

Run production application on the \RRS

Air-gapped system & immutable storage

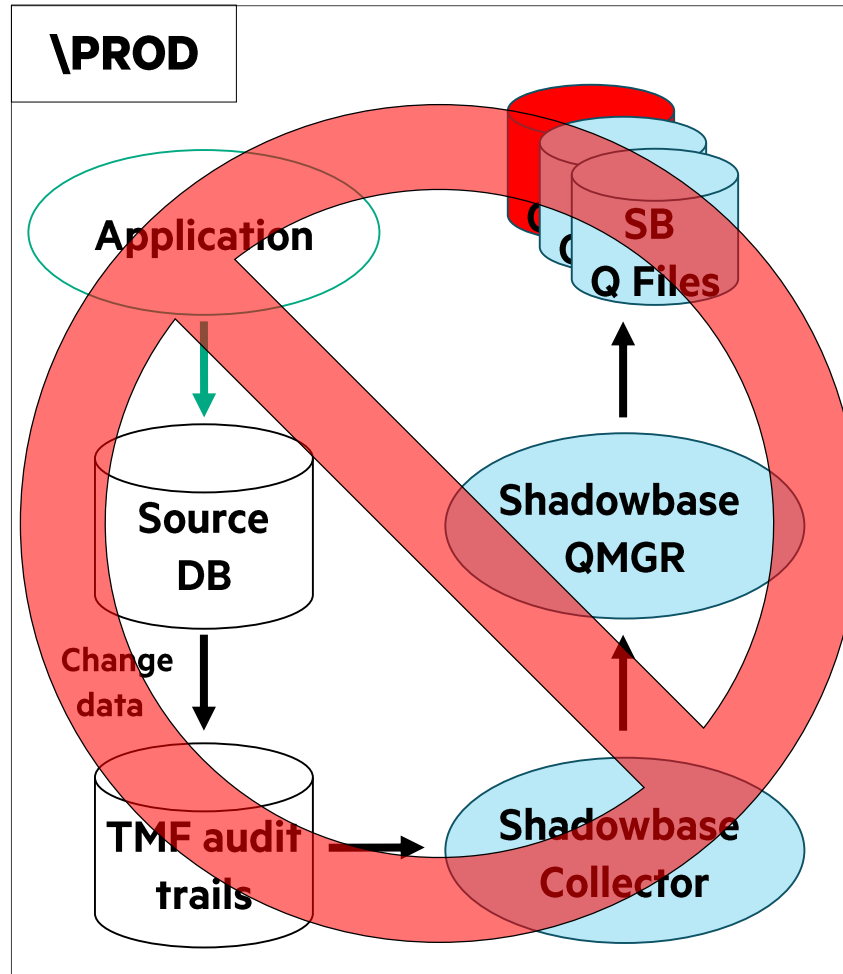


Steps:

3. After verifying the fingerprints, start SB and replay the valid Q Files:
 - a. Replay SB Q File 1
 - b. Replay SB Q File 2
4. Stop Shadowbase replication on the \RRS
5. Bring the clean \RRS application online and connect it to the synchronized Target DB
6. **Run production application on the \RRS**

Preserve original (corrupted) environment for forensics

Air-gapped system & immutable storage



Post-Mortem^2:

- **Is this solution really air-gapped?**

1. Only open SFTP port...
2. Transfer into IMMUTABLE STORAGE then to the \RRS
3. Transfer via SNEAKER NET or tapes
4. Etc.

- **What if the corruption happens earlier in the application processing?**

1. Shadowbase reads database changes from the audit trail...**Shadowbase detects corruption in its IPC's and data files...not in the original application**
2. Hence you need other solutions to help there, like 4TECHSoftware or XYPRO system monitoring or fingerprinting that detects modified program object code, DLL's, script files, etc.

Post-Mortem:

7. Preserve original (corrupted) production environment (\PROD) to allow subsequent forensics and root cause analysis

So how do we improve on this???

Looking ahead to *malware prevention*

- The following video describes a new malware **identification & prevention** architecture
- Note how the example cell phone funds transfer application leverages multiple processing centers to validate the request & detect potential corruption in one of them

Validation Architectures (VA's)

Maximize data integrity & reliability to immediately detect & prevent Malware & Ransomware



***** Future/Rapidly Evolving Technology *****
Not yet available for sale

Validation Architectures

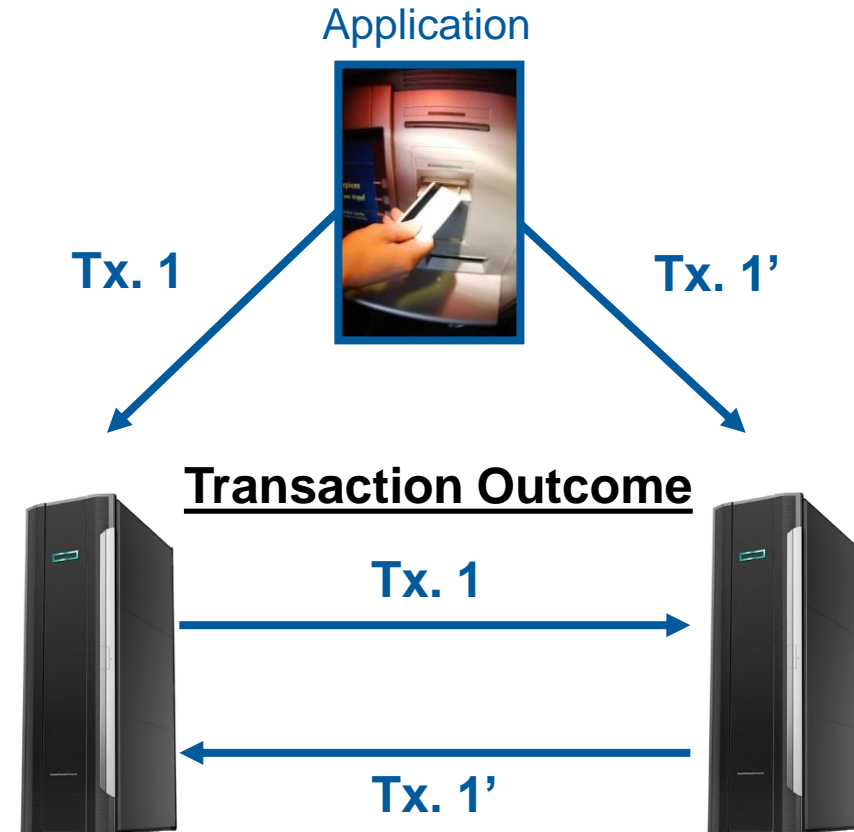
Redundant, Independent Processing

Key properties

- Applications active on all nodes
- Transactions are duplicated to all nodes
- Redundant processing of transactions at each node
- Comparison of transaction outcomes to determine if corruption has occurred

Key benefits

- Optimized to maximize Reliability & Data Integrity
- Provides a basis architecture for improving availability



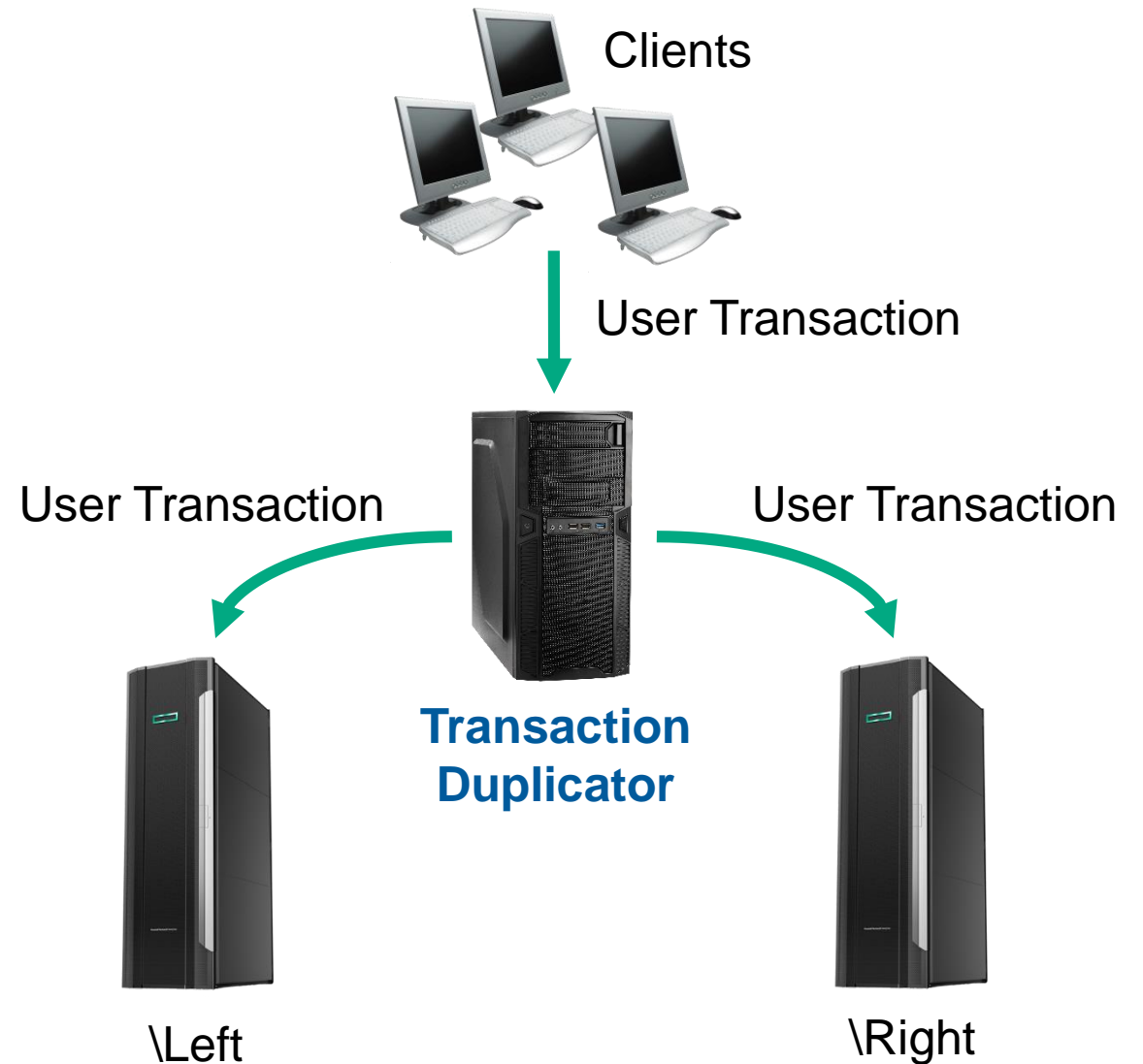
Validation Architectures

Three Key Levels: **0**, **1**, and **2**

- **Level 0** – Periodic Transaction Validation
- **Level 1** – Asynchronous Transaction Validation
- **Level 2** – Synchronous Transaction Validation

All leverage a Transaction Duplicator

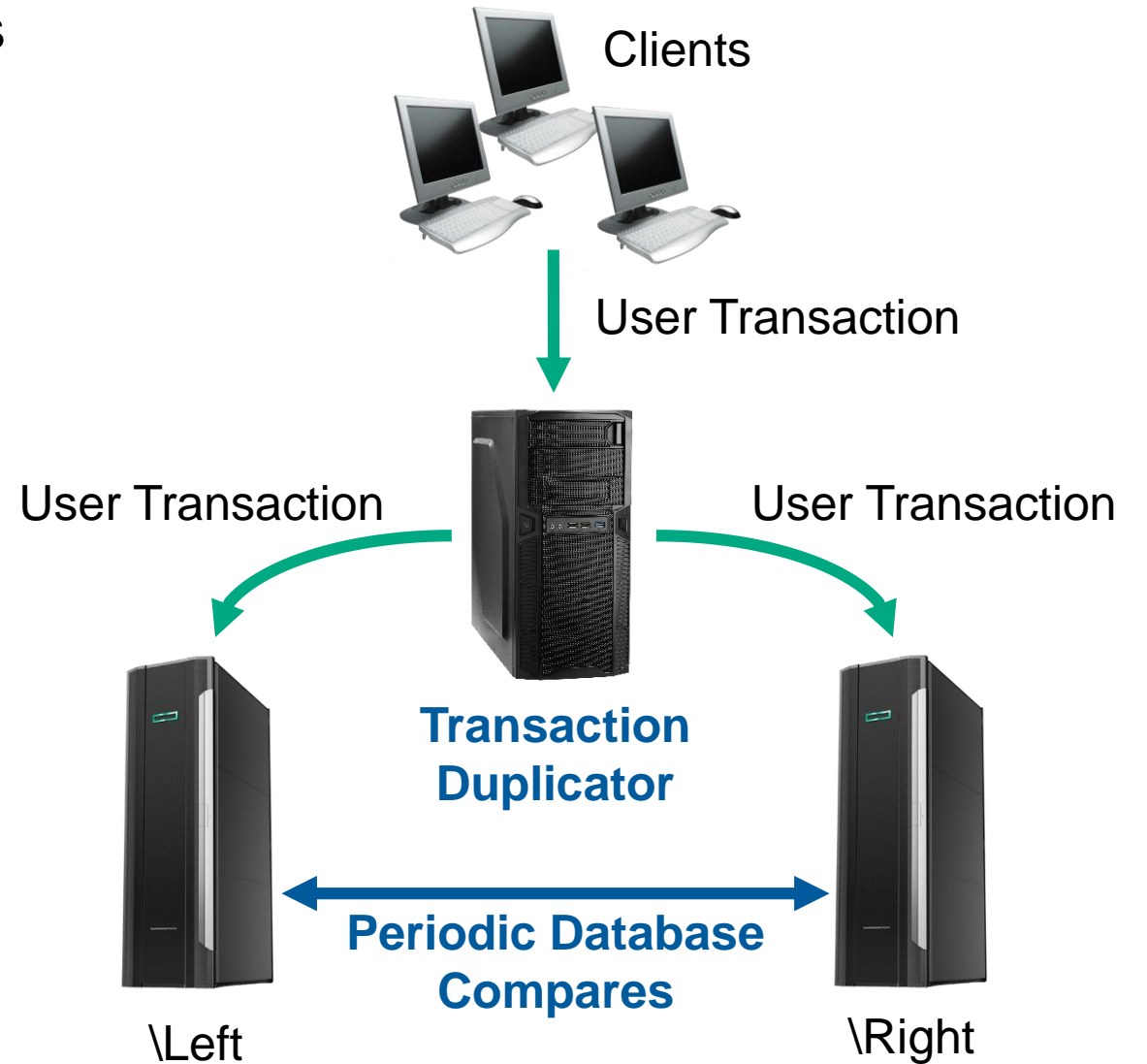
- This can be embedded into the client-side application or presented as a separate network function



Level 0: Periodic Transaction Validation

Transaction Duplicator to Two Separate Nodes

- Perform periodic database compares
- Use **Shadowbase Compare** to ensure data integrity



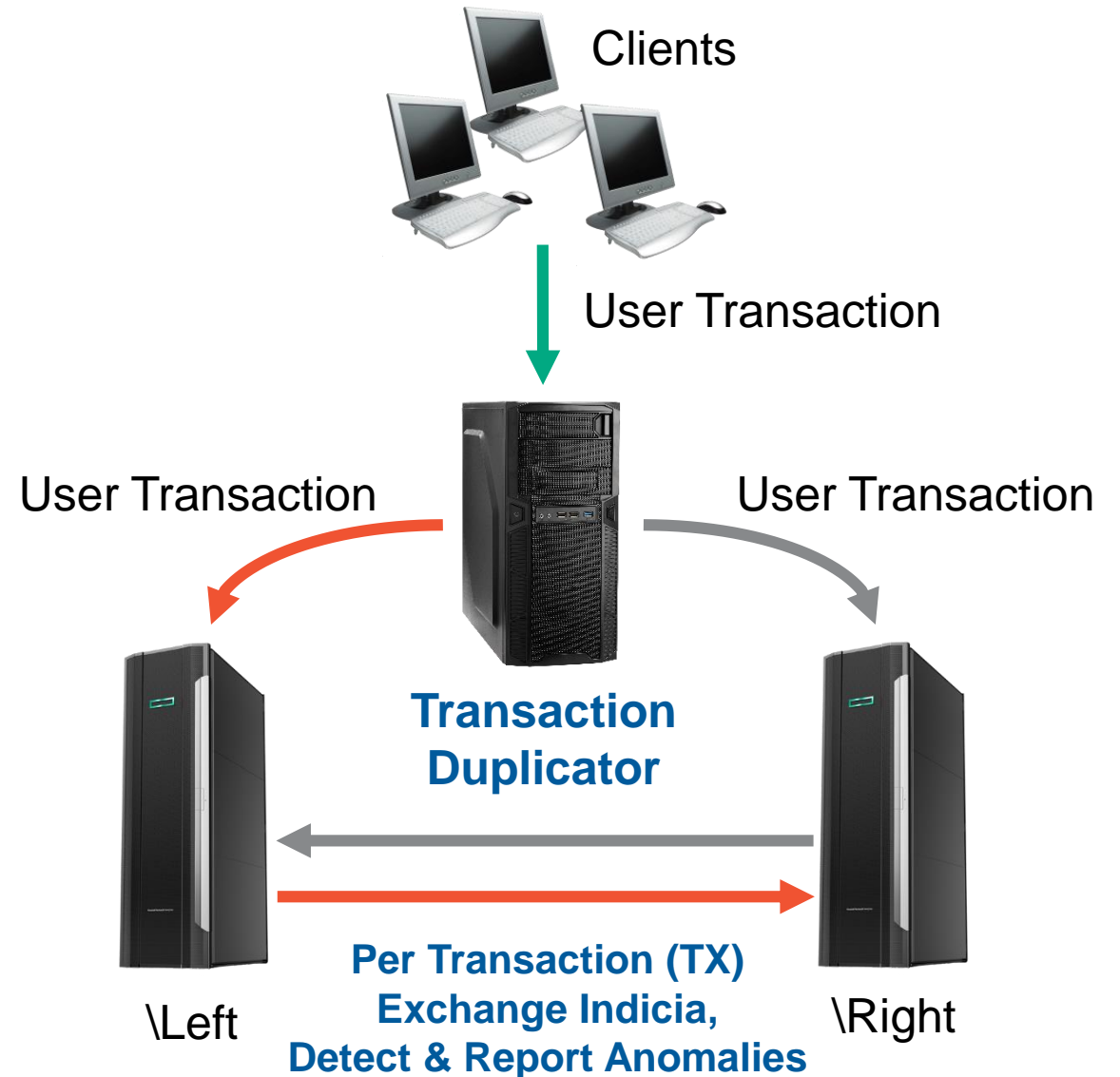
Level 1: Asynchronous Transaction Validation

Transaction duplicator to two separate nodes

Like level 0, with two additional features

1. Indicia is calculated and exchanged and compared for each transaction
2. Therefore, mismatches are detected faster and can trigger events to resolve the mismatch

Provides near real-time, but after the fact, data integrity problem detection



Level 2: Synchronous Transaction Validation

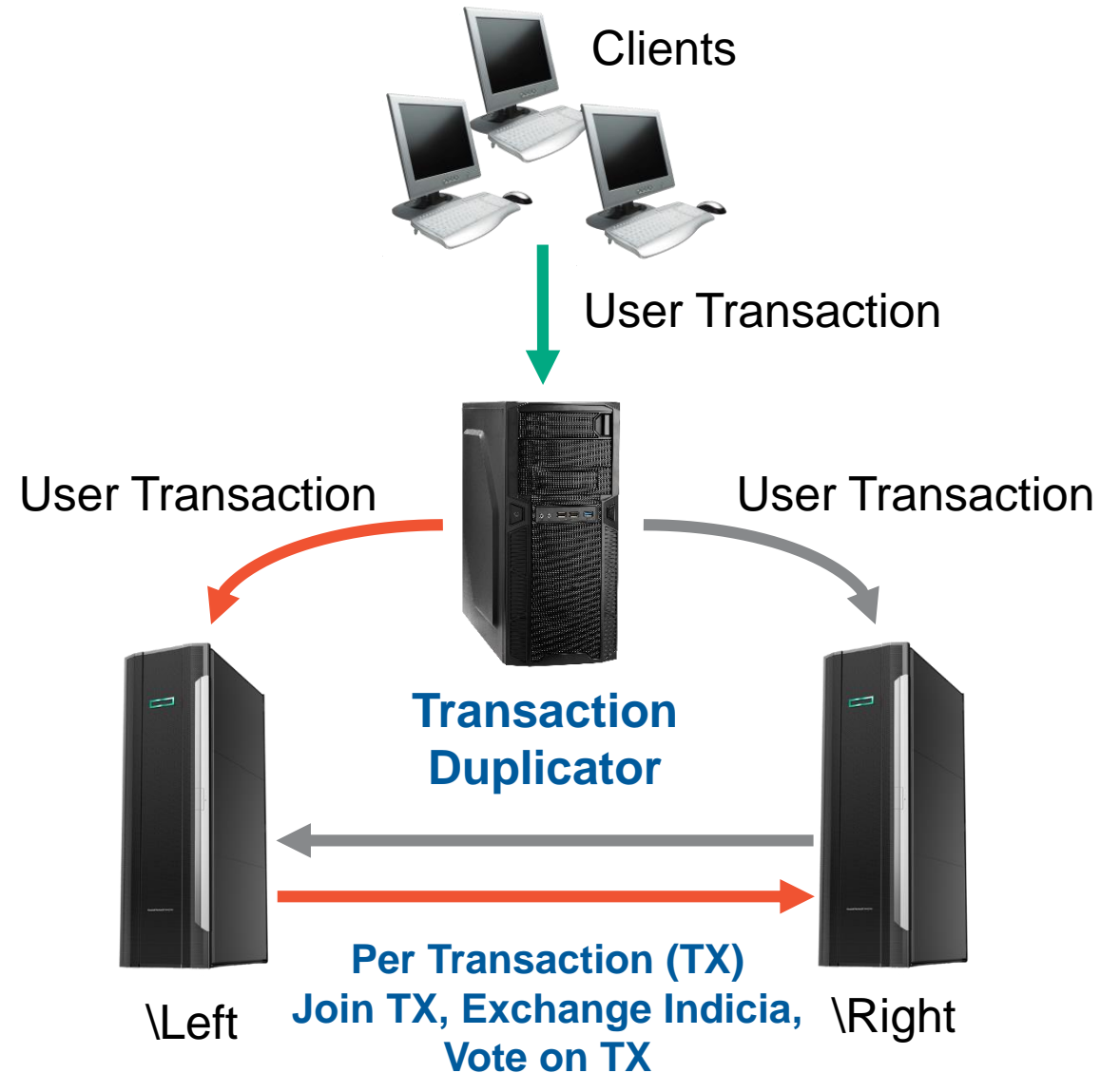
Transaction duplicator to two separate nodes

Like level 1

1. Indicia is calculated and exchanged
2. Mismatches are detected and can trigger events
3. Provides real-time data integrity problem detection

Plus, when exchanging indicia (#1 above), each node votes on the outcome of the TMF transaction *before* the transaction is allowed to commit

Prevents data integrity problems in real-time



Bringing Continuous Availability to the VA



Dual Server (DSR) vs. Triple Server (TSR) Reliability

Validation architecture (VA) extension for improved business continuity (BC) availability

- *Has BC*
- *Has VA*



Dual Server Reliability

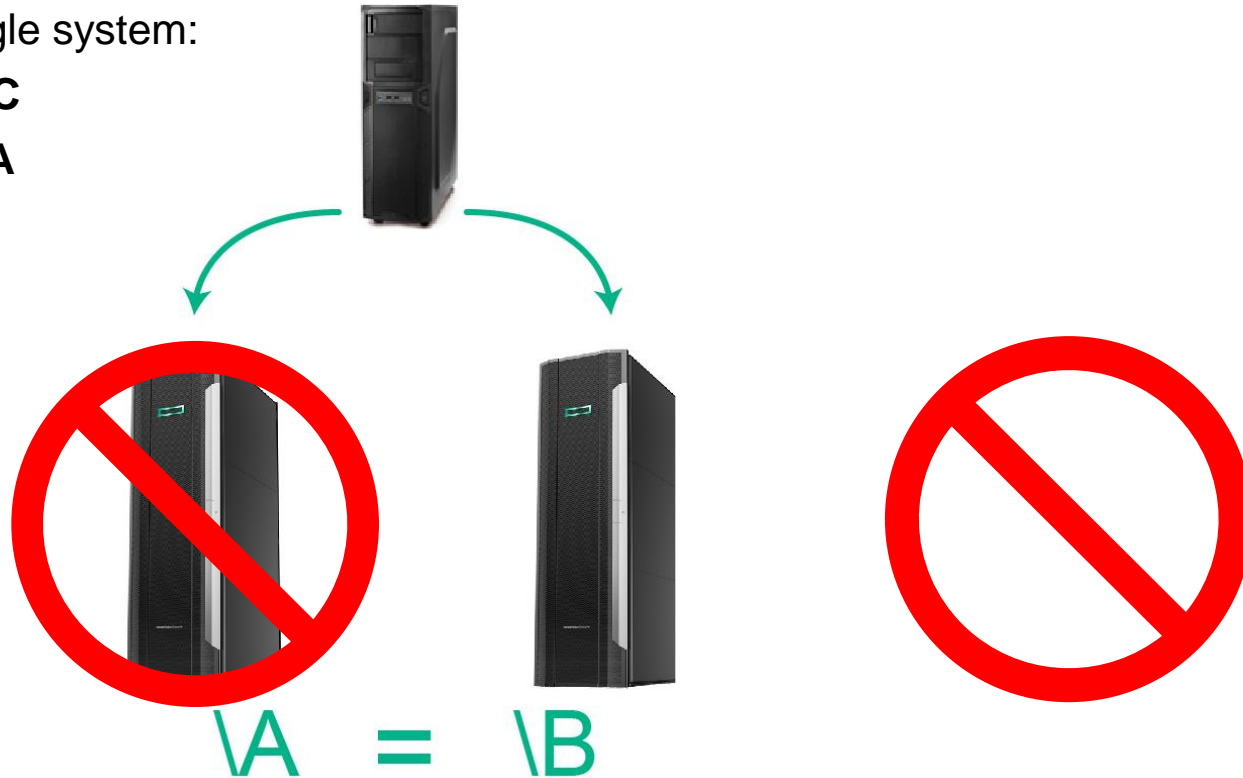
Dual Server (DSR) vs. Triple Server (TSR) Reliability

Validation architecture (VA) extension for improved business continuity (BC) availability

DSR

Loss of a single system:

- **Loses BC**
- **Loses VA**



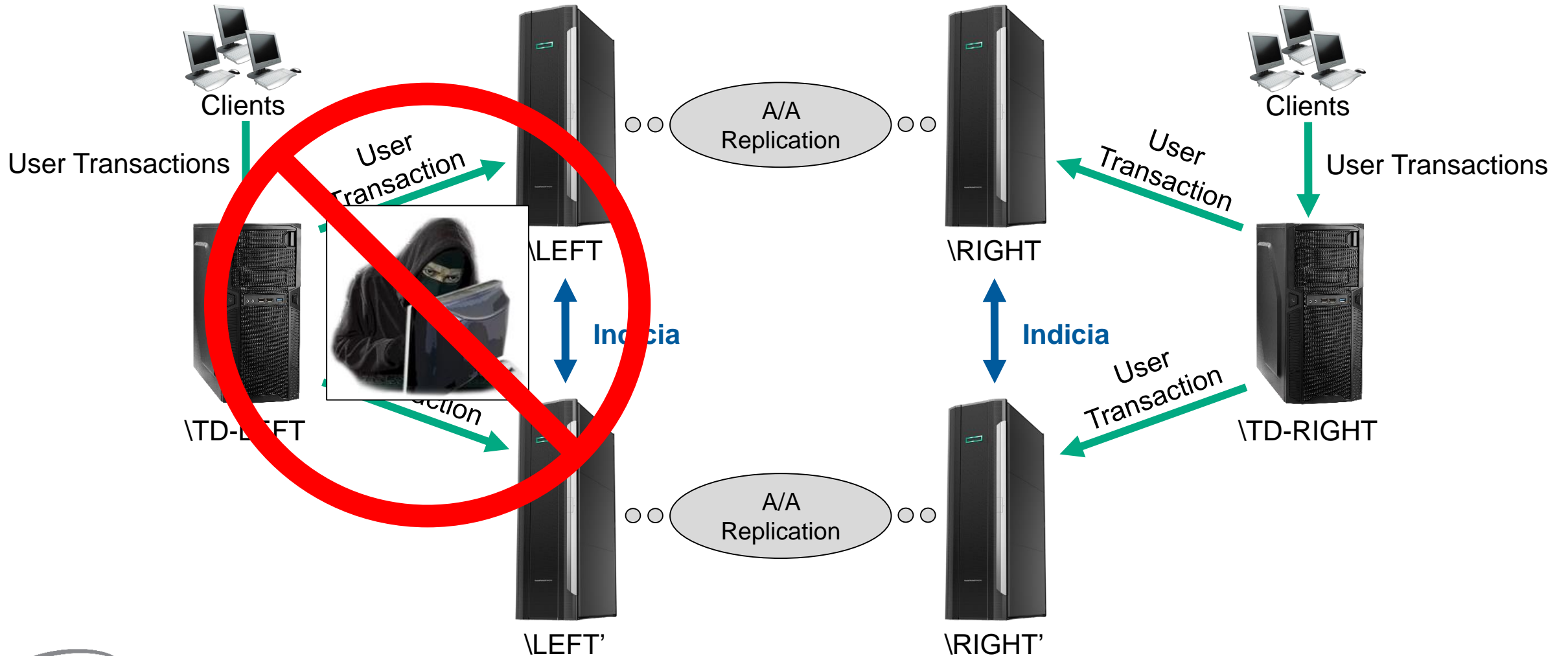
Dual Server Reliability

Best of Both Worlds



Best of Both Worlds

Loss of a VA & failover to surviving VA



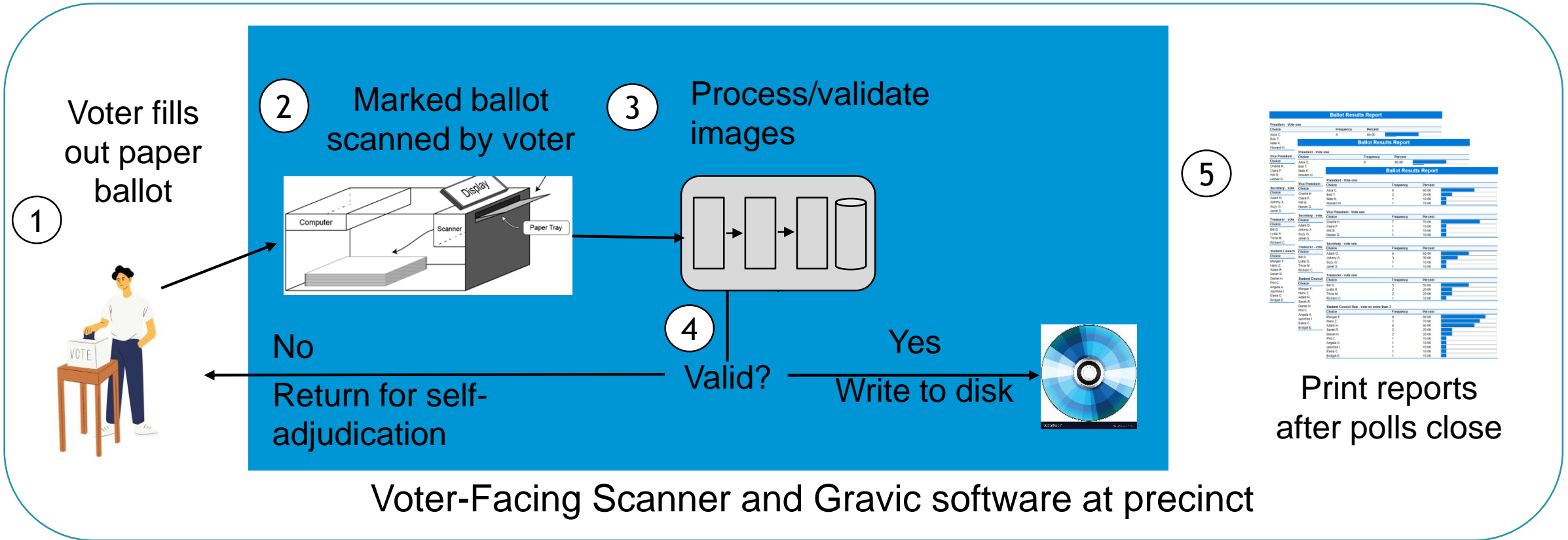
VA POC Overview

High integrity voting system



Preventing Election Fraud – *Balloting GOLD Standard*

Solution: A voter-facing scanner uses Gravic software to ‘score’ the ballots

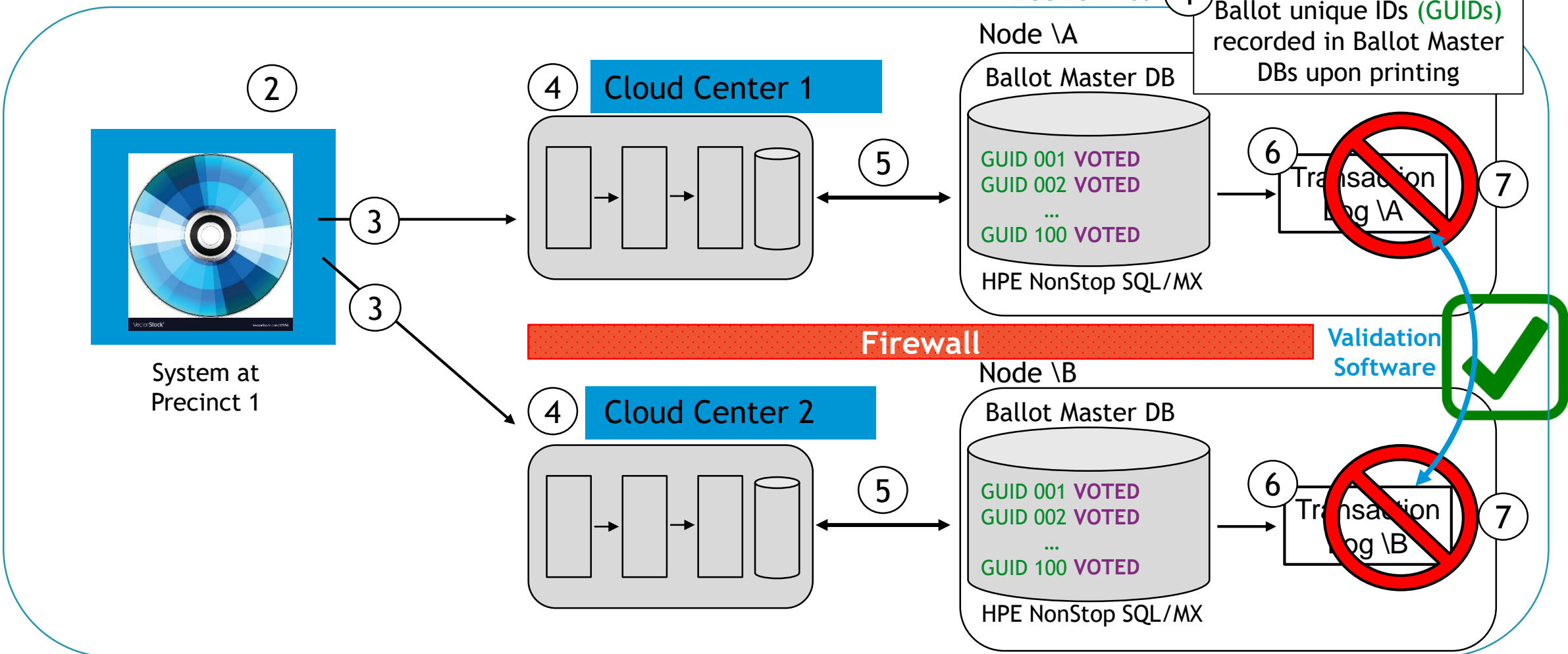


Ballot Results Report			
President - Vote one	Frequency	Percent	
Alan C	9	90.00	
Bob T	0	0.00	
John D	0	0.00	

Ballot Results Report			
Vote Two/Three	Frequency	Percent	
Alan C	9	90.00	
Bob T	0	0.00	
John D	0	0.00	

Ballot Results Report			
President - Vote one	Frequency	Percent	
Alan C	9	90.00	
Bob T	0	0.00	
John D	0	0.00	

Voter-Facing Scanner and Gravic software at precinct



Summary



Summary: Malware & Ransomware attacks are on the rise

- Digital resilience **requires a multi-faceted approach**
- Protect your data in the event of a disaster
 - Real-time recovery systems
 - Air-gapped, immutable storage
- Future **Validation Architectures** will maximize data integrity & reliability to immediately detect & prevent Malware & Ransomware
- HPE Shadowbase is HPE's strategic *go-forward* data replication & streaming solution:
 - It is globally sold and supported by HPE (and HPE's regional resellers)
 - Global professional services are available
- **Use HPE Shadowbase for digital resilience, data protection, & recovery**



Momentum Technology
Partner of the Year 2019

HPE Sessions of Interest

VT4

- HPE Shadowbase: Maximize NonStop Digital Resilience with Data Replication, Integration, and Validation
 - Tuesday, 1-2:00 PM, Denver 4

CFP1 – *Customer Talk!*

- Major UK Bank Migrates its BASE24™ Application to Active/Active for Continuous Availability
 - Wednesday, 10:30-11:30 AM, Denver 1-2

TB67

- New HPE NonStop Business Continuity & Data Integration Features and Roadmap
 - Wednesday, 2:45-3:45 PM, Denver 1-2

VT5

- Ransomware Protection and Data Recovery
 - Wednesday, 4-5:00 PM, Denver 1-2



TBC23 – VT5: Ransomware Protection and Data Recovery

Copyright © 2023 Hewlett Packard Enterprise & Gravic, Inc. use only. Future delivery dates and functionality may change without notice.

Follow us on



Thank you

Product-related questions: ask your HPE Sales team

Technical-related questions: SBProductManagement@Gravic.com

Marketing-related questions: PRHolenstein@Gravic.com

