
Hewlett Packard Enterprise
Technology Partner
SILVER PARTNER
Momentum Technology Partner of the Year 2019
GRAVIC Shadowbase
HPE SHADOWBASE TECHNICAL ARCHITECTURE OVERVIEW FOR DIGITAL RESILIENCE
(MALWARE AND RANSOMWARE PREVENTION)
Paul J. Holenstein
Executive Vice President
Shadowbase Products Group
Gravic, Inc.
May 2023
E-BITUG
European NonStop Symposium
EDINBURGH 2023

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 SHADOWBASE ARCHITECTURES FOR MALWARE AND RANSOMWARE

Agenda - Protect, avoid, identify, and resolve

Key technology trends and challenges

Malware and Ransomware – general comments

Shadowbase architectures for ransomware recovery

- Ransomware Solution Architecture #1 – Replication Connected via QMGR Files (non air-gapped)
- Ransomware Solution Architecture #2 – Air-gapped, Immutable Data
- Ransomware – additional comments

Malware – new architectures for mission-critical applications

- Shadowbase validation architectures for malware prevention
- Election/balloting application Proof of Concept (POC)

Stuff we won't have time for (sorry!)

- Shadowbase compare technologies
- Shadowbase malware and ransomware data recovery tools

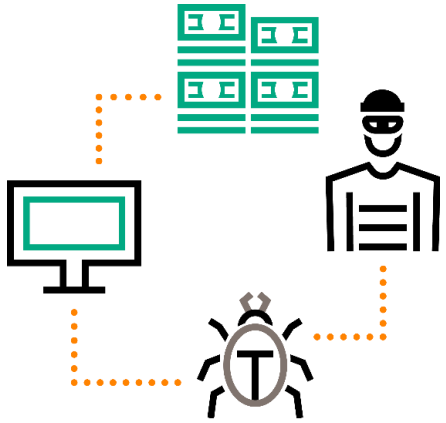
Summary

KEY TECHNOLOGY TRENDS AND CHALLENGES

KEY TECHNOLOGY TRENDS AND CHALLENGES

Look to HPE Shadowbase to help solve them

- **Digital resiliency**
  - Protection, detection, containment, recovery and repair capabilities against information and communication technology (ICT) related incidents
  - **Government regulations are underway**
- **Malware and Ransomware protection**
  - Global business concern
  - New approaches (e.g., “immutable” backups and “air-gapped” systems)
  - **Value of TMF-audited applications and data cannot be overstated**



HPE SHADOWBASE

Malware and Ransomware – general comments

MALWARE AND RANSOMWARE (1)

General comments

1. **Know your Enemy**: *Malware* and *Ransomware* are not (quite) the same thing!
   a) **Malware** is essentially *software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system* (Source: Dictionary.com)
   b) **Ransomware** is essentially *a type of malicious software designed to block access to a computer system until a sum of money is paid* (Source: Dictionary.com)
2. However, we categorize ransomware as a type of malware, noting the protections for each are different but intersecting
3. Gravic is focused on **protecting your data** when it comes to malware and ransomware detection, prevention, and recovery
   a) However, additional techniques will be needed to protect the application environment, network, personnel, etc.
4. Gravic's approach: **prevent the malware or ransomware from working/operating;** and if it occurs, **detect it and terminate it immediately before it can do (more) harm**
   a) And, we have the tools to help you recover corrupted data

MALWARE AND RANSOMWARE (2)

General comments

5. ***Shadowbase data replication*** cannot spread ransomware "programs"
   a) **Shadowbase data replication** does not replicate object code or programs
   b) Hence, data replication will not spread malware or ransomware *object code, programs, libraries, DLL's, modules*, etc
6. ***File Replication*** via backup/restore, PAK/UNPAK, FTP, HPE AutoSYNC, etc. ***can spread malware or ransomware programs***
7. **Data replication is, however, susceptible to a malware or malicious hacker attack** that corrupts or encrypts specific record fields or table columns
   a) These attacks are the focus of the new ***Gravic Labs Shadowbase Validation Architecture (VA)*** for immediate avoidance/detection and resolution (discussed later)
8. We will first look at existing SB architectures to assist with Ransomware recovery

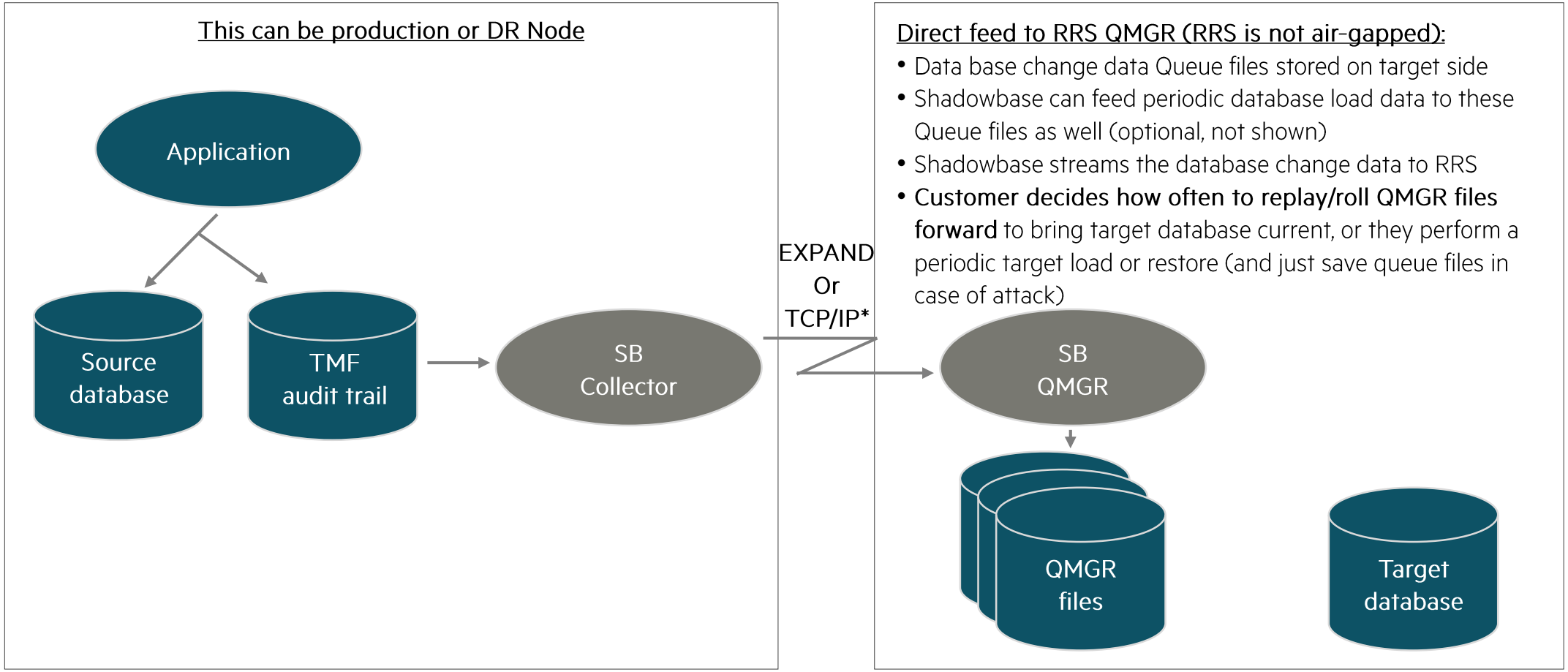
Note: malware that just "monitors" and stealthily culls info is still a challenge and requires additional measures such as *monitoring for unauthorized outbound traffic, fingerprinting all programs, etc*

HPE SHADOWBASE

Ransomware Solution Architecture #1 – replication connected via QMGR files (non air-gapped solution)

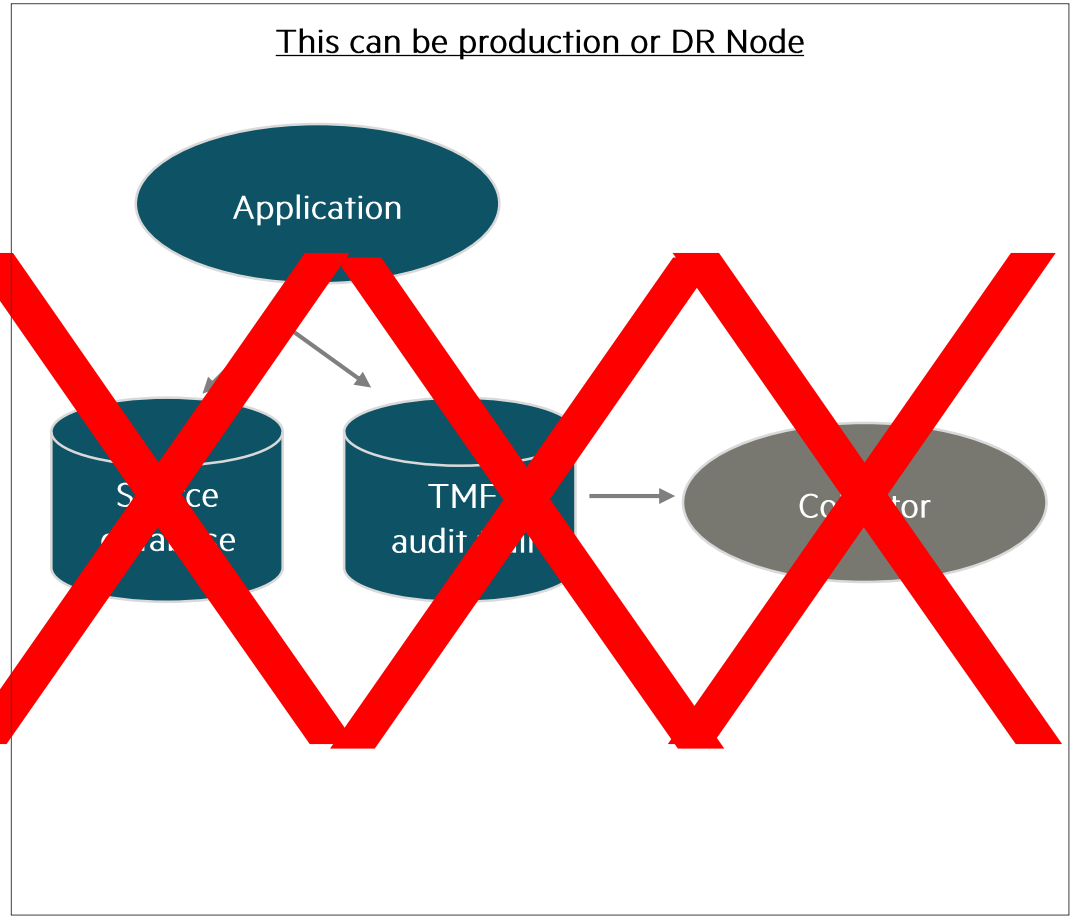
SHADOWBASE REPLICATION TECHNOLOGY (1)

NonStop server to NonStop server – QMGR fed on target Ransomware Remediation System (RRS)



SHADOWBASE REPLICATION TECHNOLOGY (2)

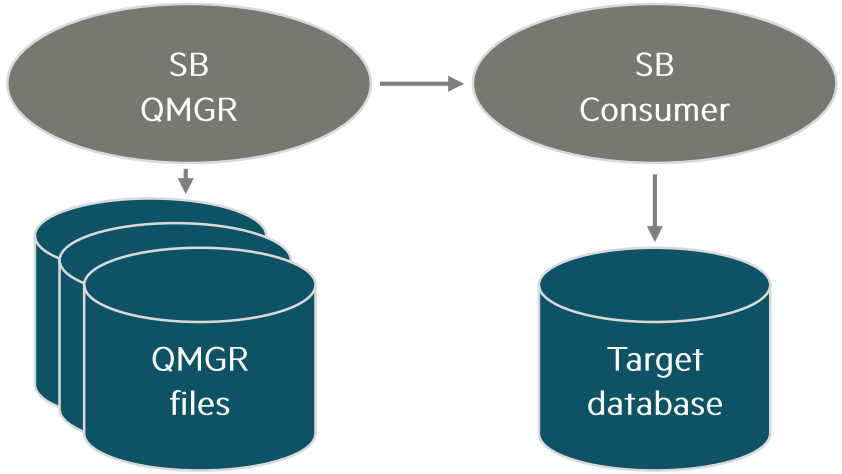
NonStop server to NonStop server – QMGR fed on target Ransomware Remediation System (RRS)



System \PROD or \DR

Direct feed to RRS QMGR (RRS is not air-gapped):

- When attack occurs, start Consumers and optionally load target database
- Then replay queued change data to bring the target database current to a particular point in time
- Continue application processing on RRS, preserving original environment for forensic analysis



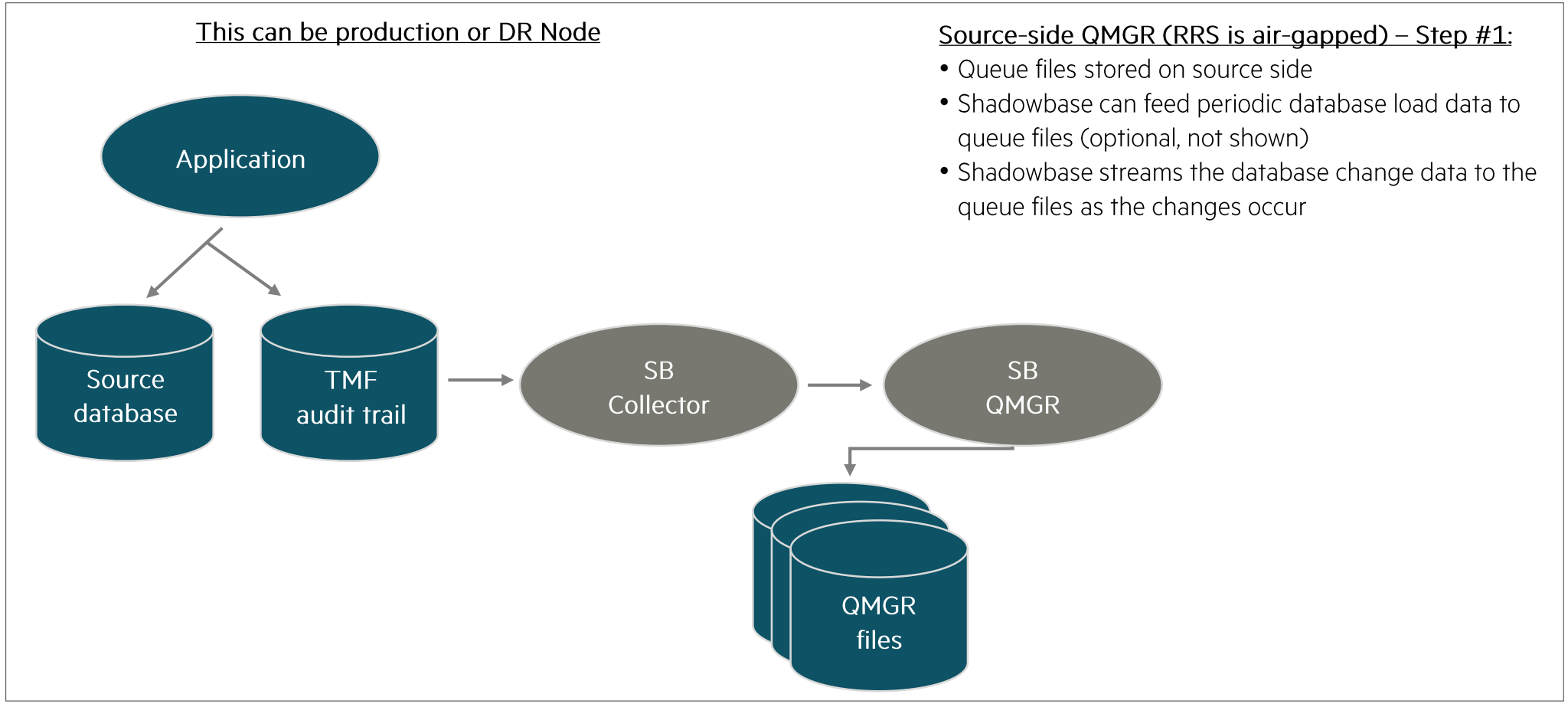
System \RRS

HPE SHADOWBASE

Ransomware Solution Architecture #2 – air-gapped, immutable data

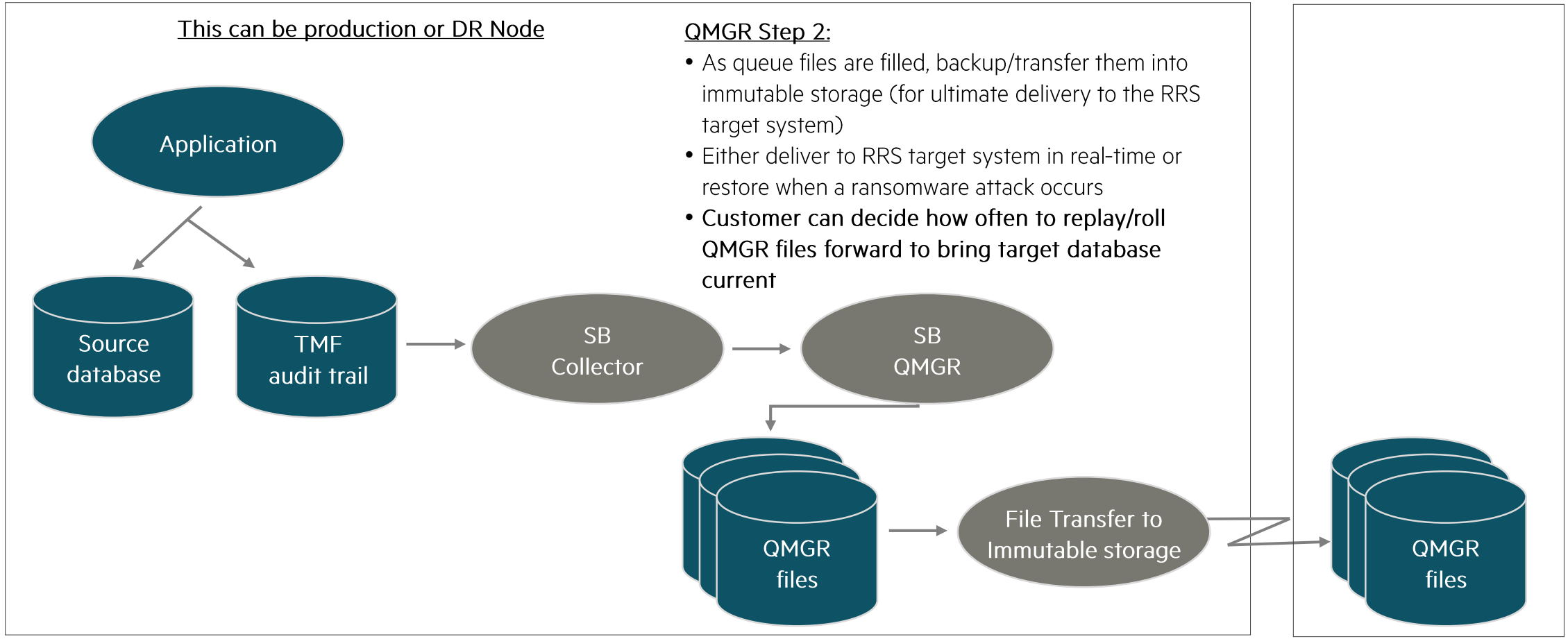
SHADOWBASE REPLICATION TECHNOLOGY (1)

NonStop server to NonStop Server – QMGR on source side (air-gapped target) – Step 1



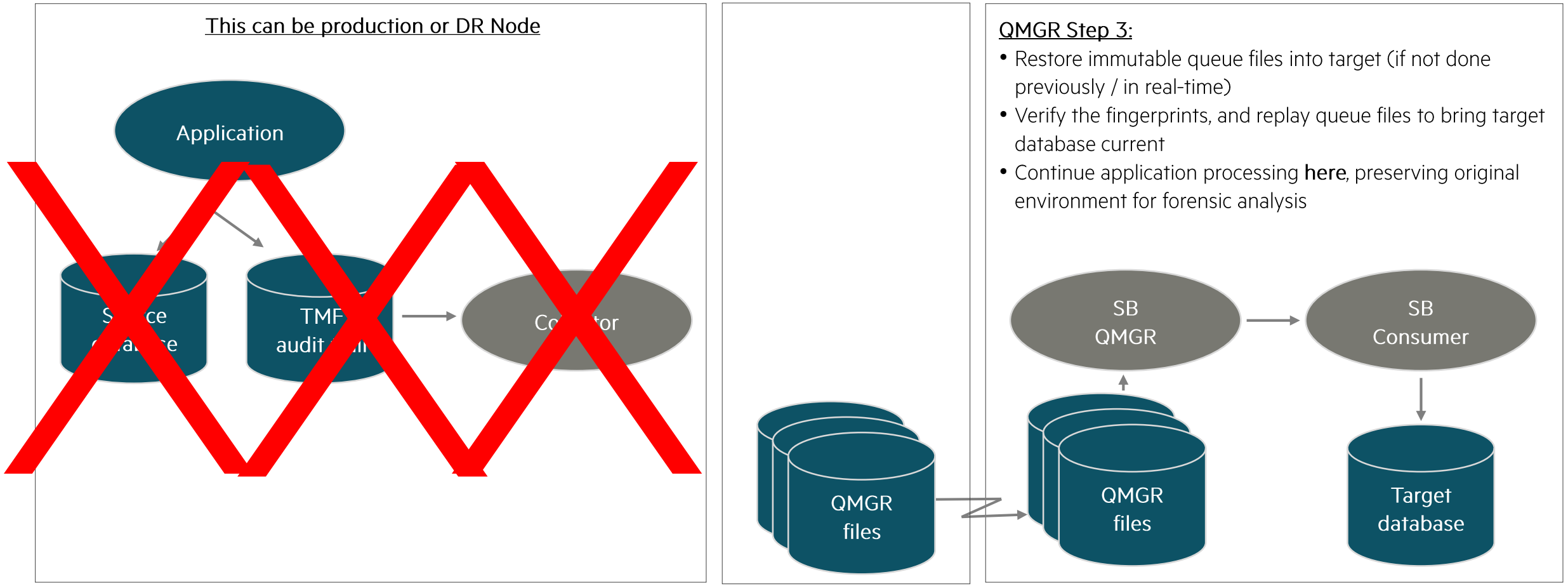
SHADOWBASE REPLICATION TECHNOLOGY (2)

NonStop server to NonStop/SBOS platforms – QMGR on source side (air-gapped target) – Step 2



SHADOWBASE REPLICATION TECHNOLOGY (3)

NonStop server to NonStop/SBOS platforms – QMGR on source side (air-gapped target) – Step 3



HPE SHADOWBASE

Malware and Ransomware – Additional Comments

MALWARE AND RANSOMWARE (1)

Additional comments

1. **The RRS does not replace a proper DR target environment – it is a new isolated environment** (best practice)
   a) Ideally, the RRS is managed by an independent 3rd party (for example, Greenlake)
2. **Where should the Shadowbase QMGR queue files be stored?**
   a) Source side vs target side? Customer choice…
   b) On NonStop disk or on immutable storage? Customer choice…
3. **Where should the Shadowbase QMGR queue files be fed from?**
   a) From the Production source system? Customer choice…
   b) From the DR system? Customer choice…
4. **On the NonStop, TMF-audited data is your first line of defense!**
   a) TMF **guarantees <u>all</u> database changes are logged into an audit trail, and this can be used for recovery!**
   b) Non-audited data does not have these same advantages, capabilities, nor protection

MALWARE AND RANSOMWARE (2)

Additional comments

5. **Shadowbase QMGRs provide some unique capabilities to fight ransomware and malware**
   a) **They can selectively replay** the change data from the queue files into the target database to bring it current, or to roll-it-backward to a particular point in time before the corruption occurred
   b) **Shadowbase can detect man-in-the-middle (MiTM) attacks between its key processes as IPC's are fingerprinted**
   c) **The Shadowbase queue files are fingerprinted/validated** (queue file tampering or corruption will be detected by Shadowbase before replay)
6. **Shadowbase replication can also replicate/queue replicated data on non-NonStop target systems!**
   a) **Our customers build "data vaults" on non-NonStop target systems this way**
   b) This data can be optionally replayed into a target database, or just stored there for safe keeping
   c) We support Linux, Unix, Windows, IBM, and cloud environments as targets…as well as a host of common/popular target databases including Oracle, SQL Server, DB2, SAP Hana, SAP Sybase, MySQL, PostgreSQL, flat-files, and others

HPE NONSTOP SHADOWBASE

Ransomware defense and recovery utility solutions

- Shadowbase Compare & Repair
- Shadowbase Data Recovery Utilities (REDO, UNDO)

Sorry, not enough time to review these now…Visit the Gravic booth or contact us for more info ☺…

Shadowbase Validation Architecture (VA)

New architectures from Gravic Labs to stop malware (and ransomware) in their tracks

***** Future/Rapidly Evolving Technology *****

Let's take a look at the VA deck!

Validation Architectures to Improve Data Integrity

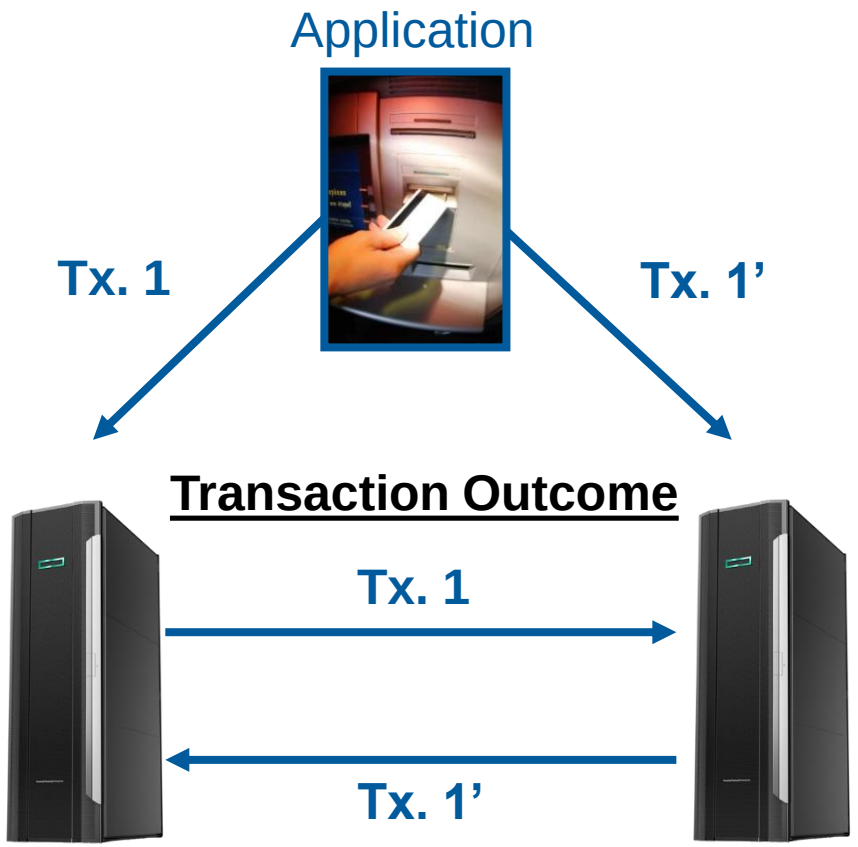
Redundant, independent processing

Key properties

- Applications active on all nodes
- Transactions are duplicated to all nodes
- Redundant processing of each transaction occurs at each node
- Validation of outcomes

Key benefit

- Optimized to maximize ***Reliability & Data Integrity***



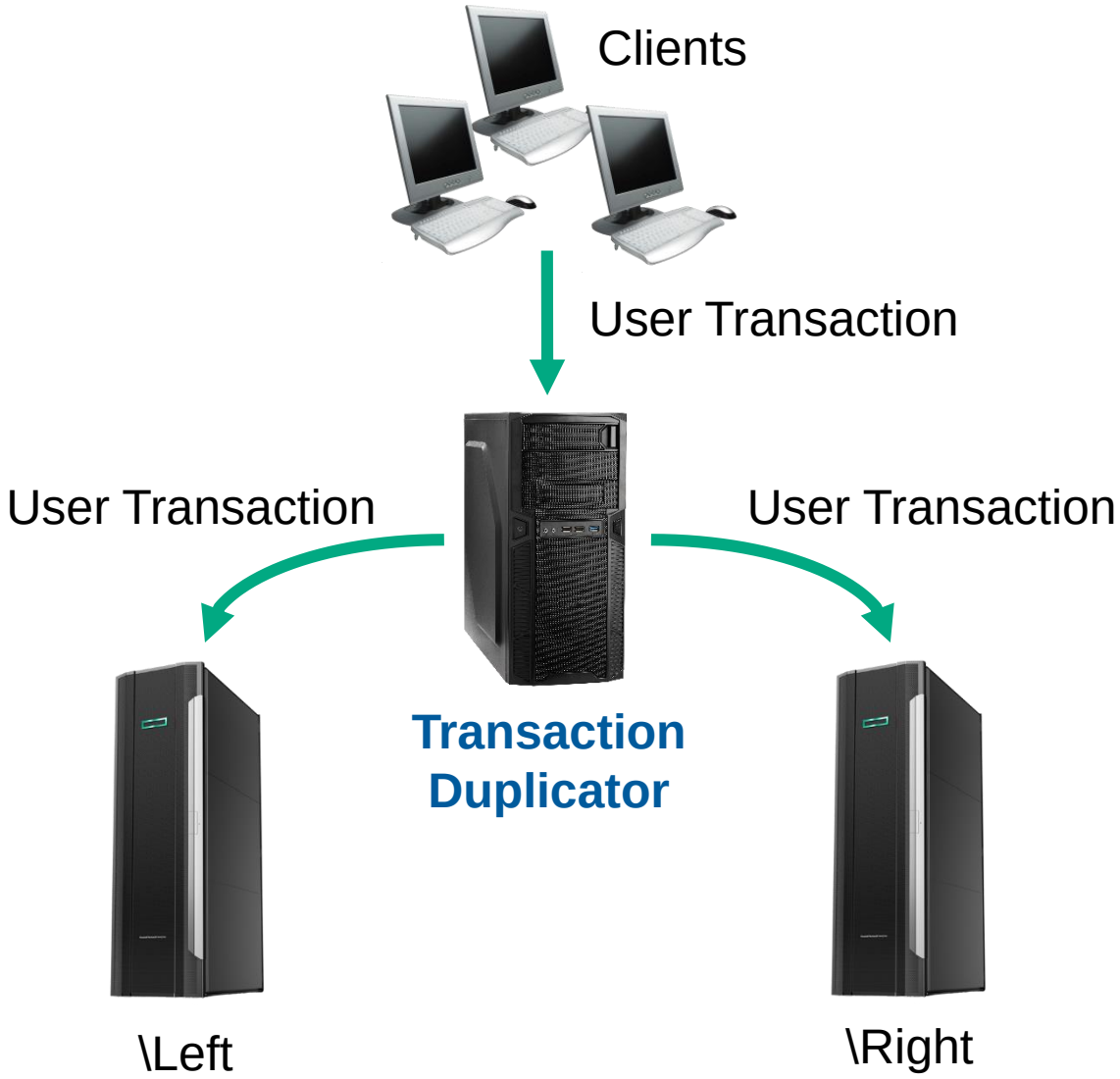
Validation Architectures

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

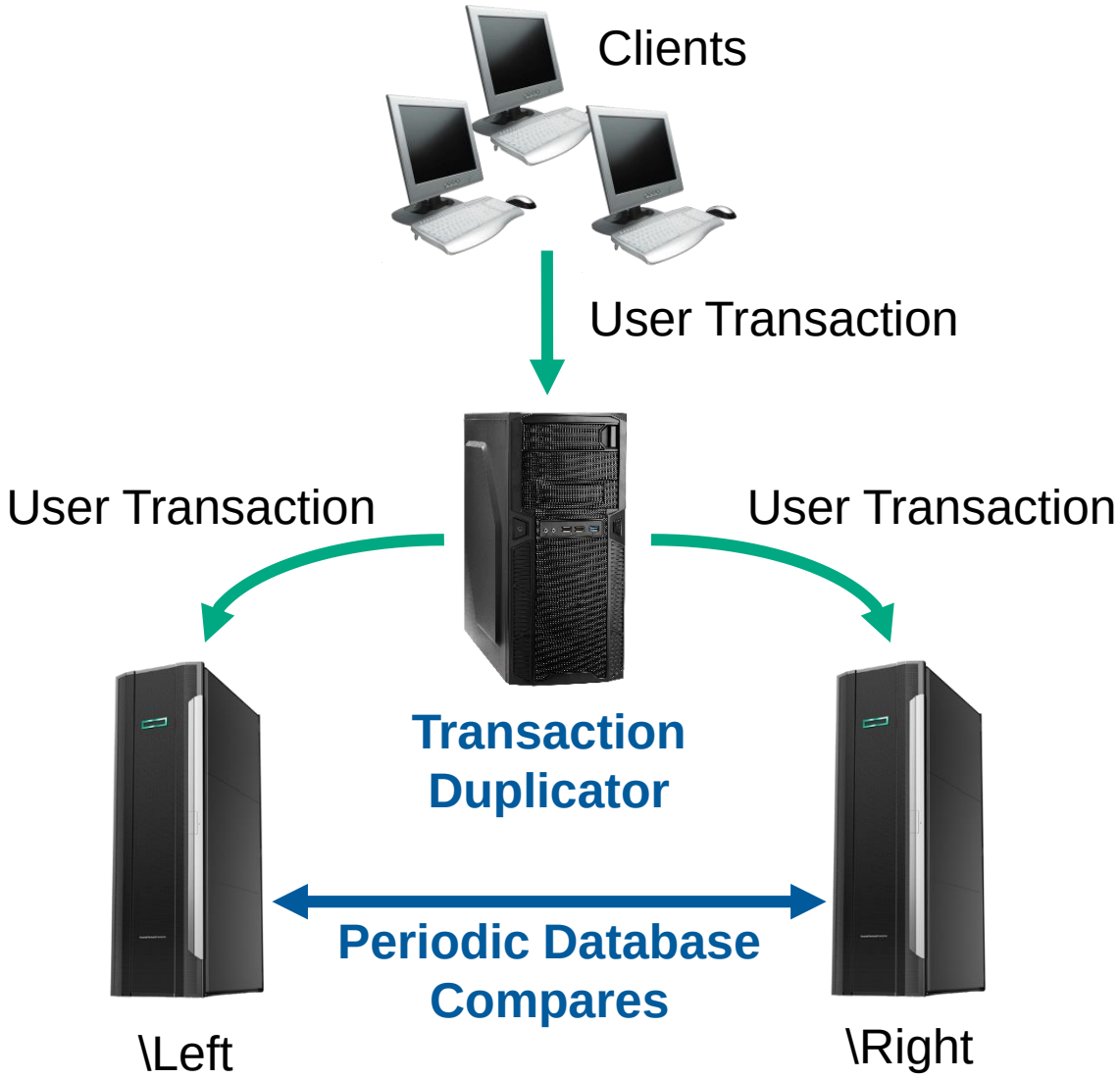
…which can be part of the application



Level 0: Periodic Transaction Validation

Transaction Duplicator to Two Separate Nodes

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



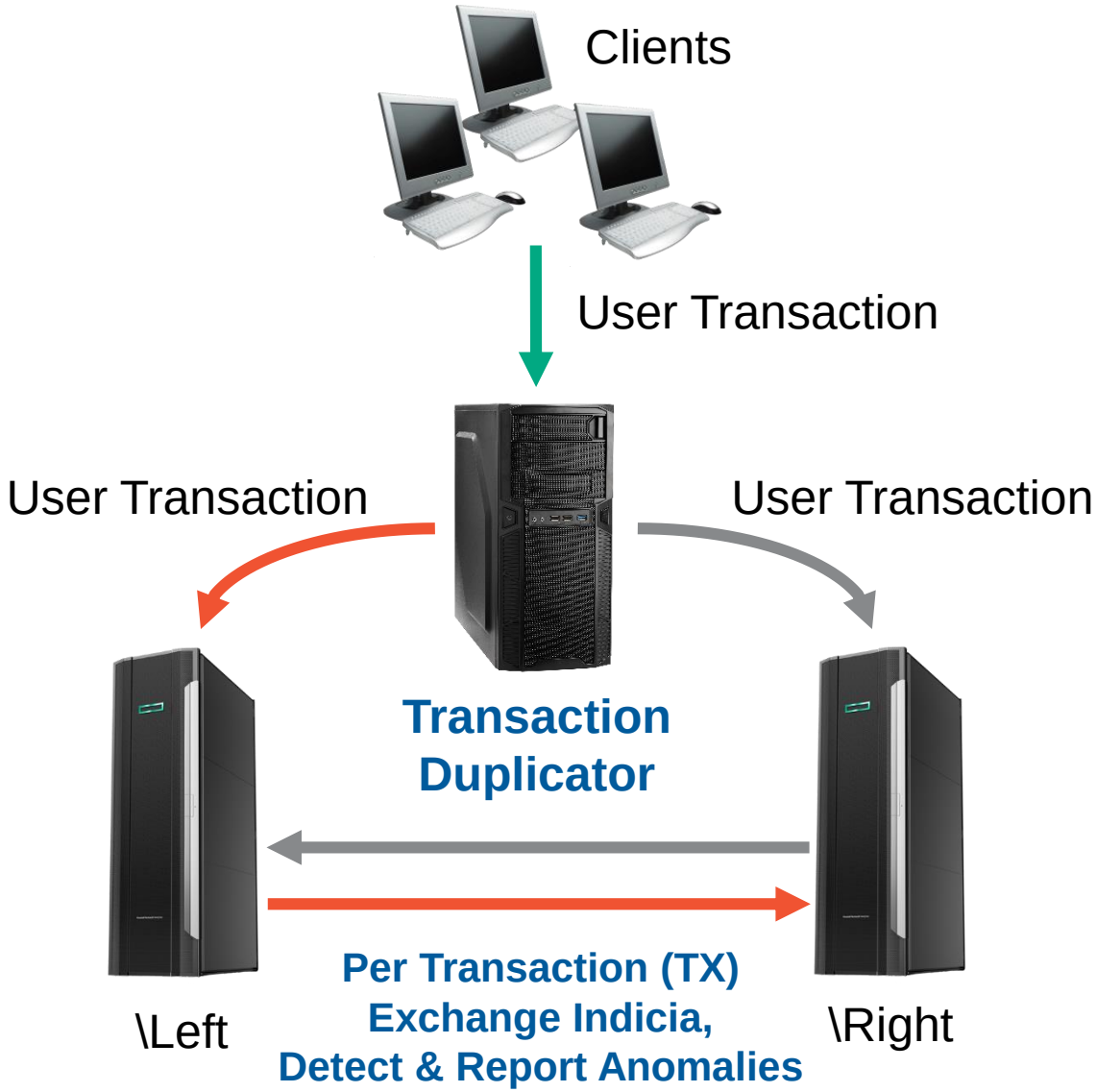
Level 1: Asynchronous Transaction Validation

Transaction duplicator to two separate nodes

Like Level 0, with two additional features

1. Indicia is calculated, 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

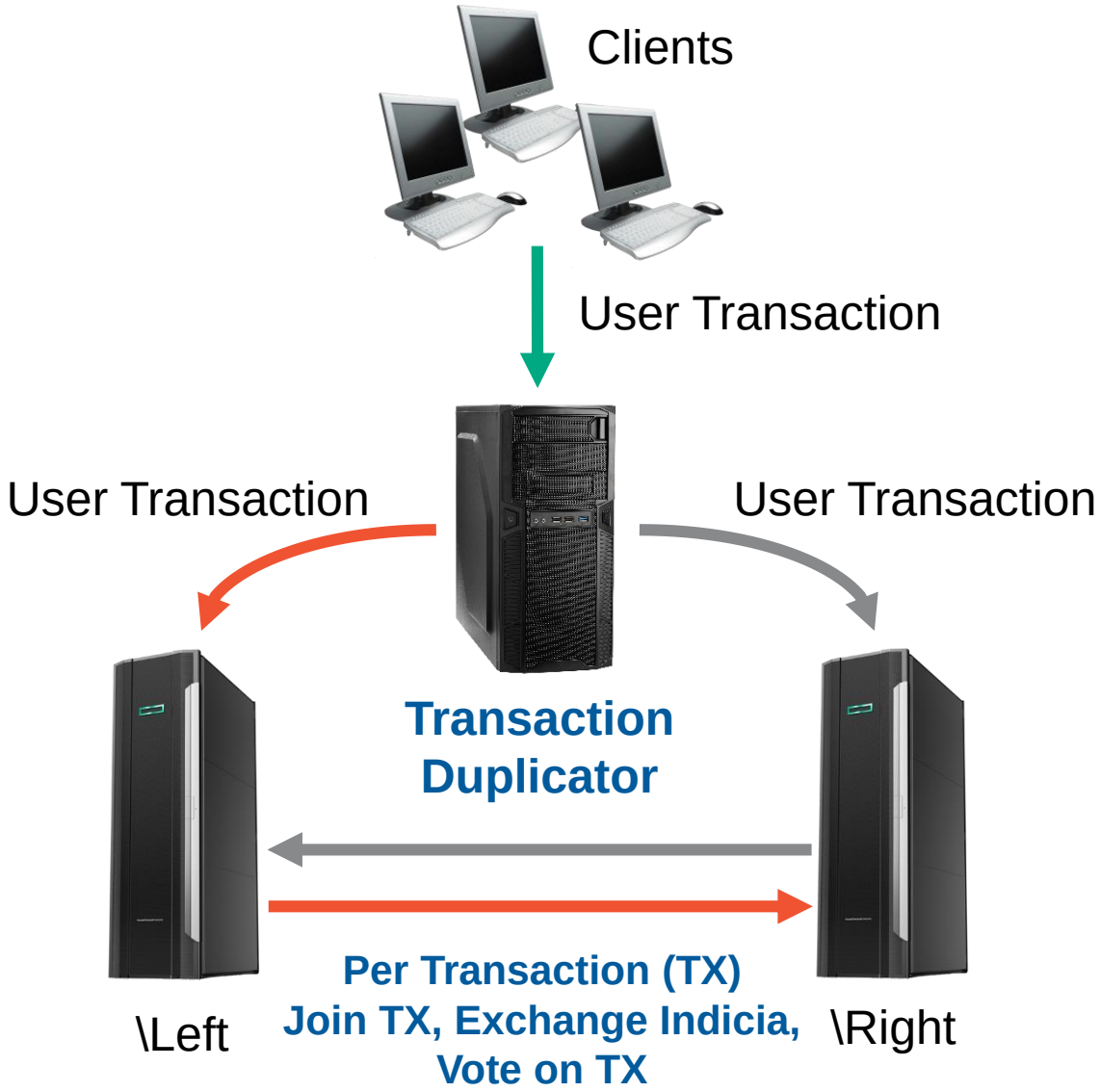
Transaction duplicator to two separate nodes

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



Adding Continuous Availability to Validation Architectures

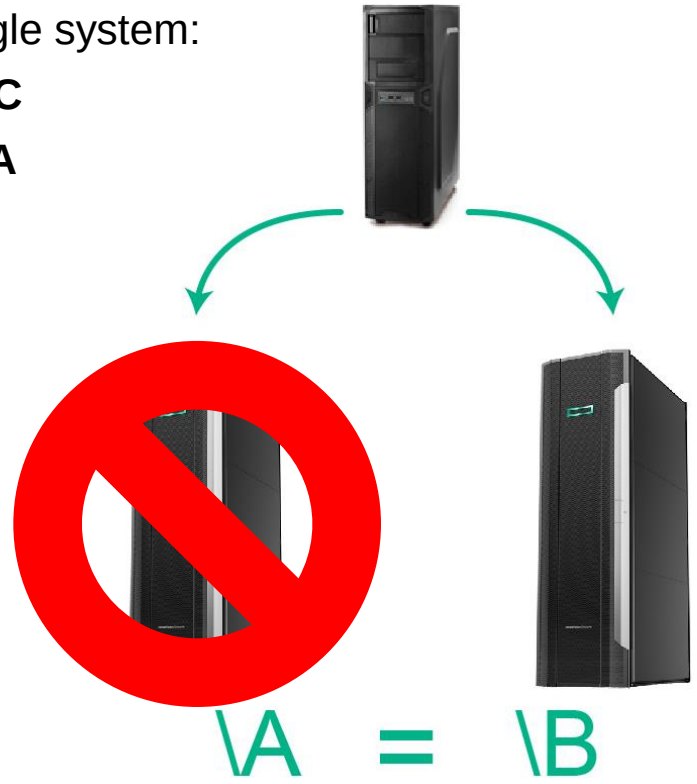
Dual Server (DSR) vs. Triple Server (TSR) Reliability

Validation architecture extension for improved availability and data integrity

DSR

Loss of a single system:

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



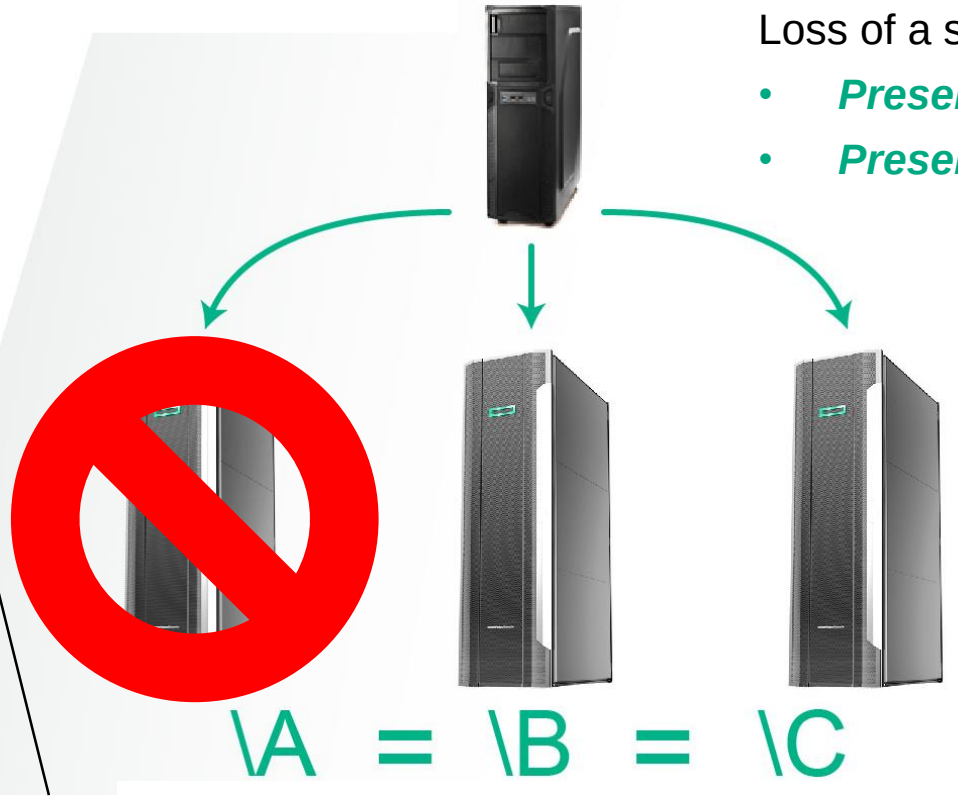
\A = \B

Dual Server Reliability

TSR

Loss of a single system:

- ***Preserves*** **BC**
- ***Preserves*** **VA**



\A = \B = \C

Triple Server Reliability

GRAVIC® Shadowbase

Use Case POC

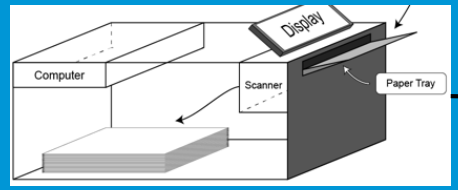
High integrity voting system

Preventing Election Fraud – *Balloting GOLD Standard*

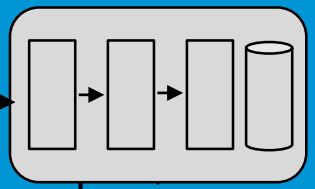
Solution: A voter-facing scanner uses Gravic software to 'score' the ballots

1 Voter fills out paper ballot

2 Marked ballot scanned by voter



3 Process/validate images

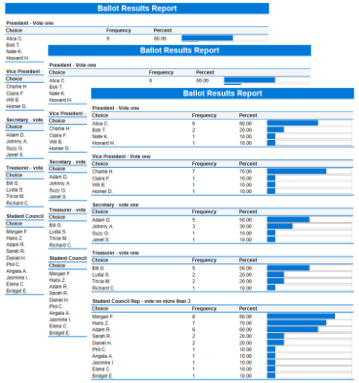


4 Valid?

No
Return for self-adjudication

Yes
Write to disk

5

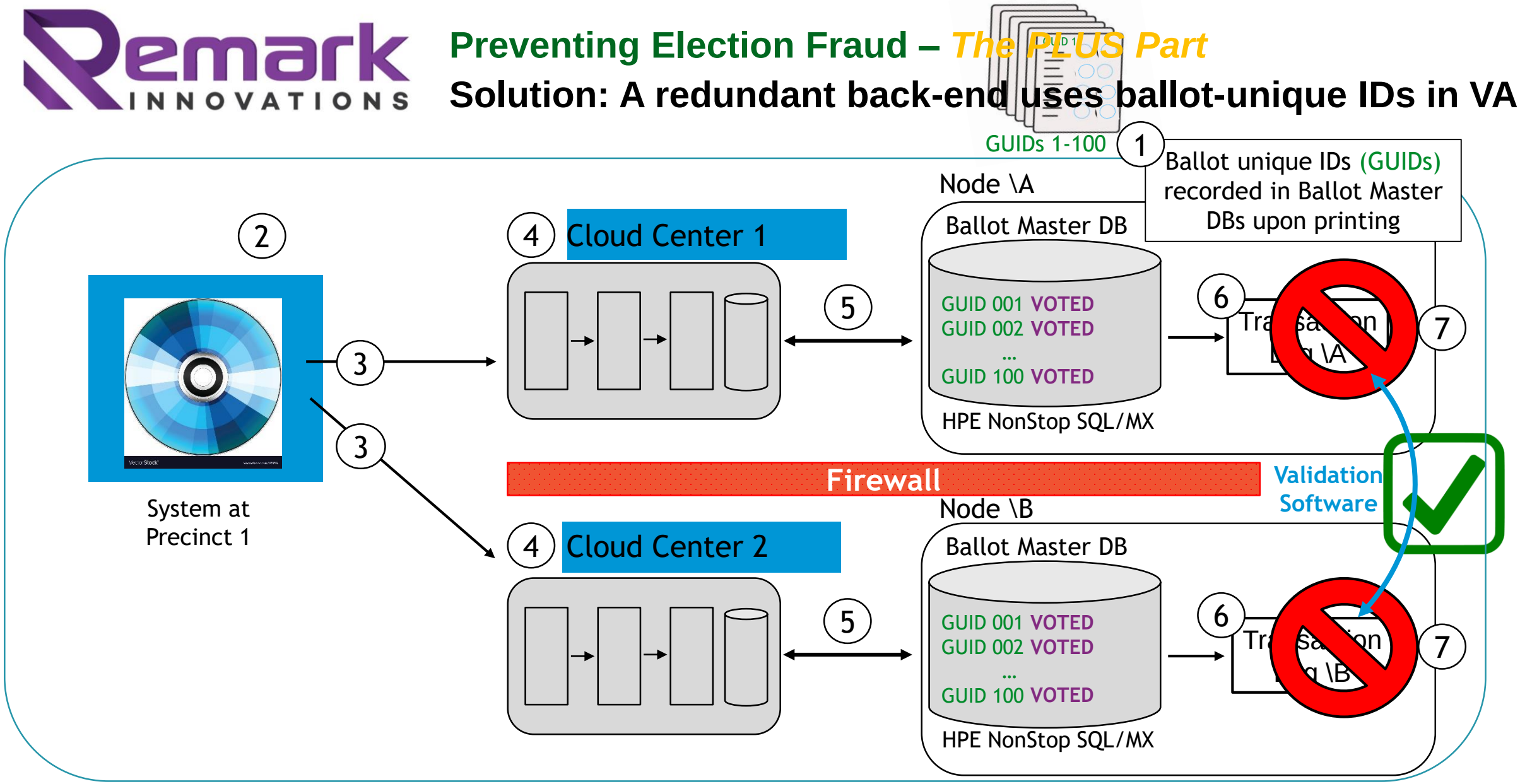


Print reports after polls close

Voter-Facing Scanner and Gravic software at precinct

Preventing Election Fraud – *The PLUS Part*

Solution: A redundant back-end uses ballot-unique IDs in VA

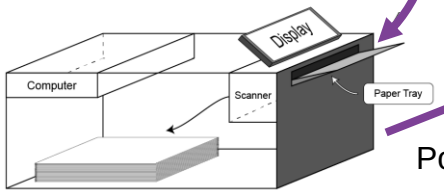


Preventing Election Fraud – *Recent testing…*

Ballot Tabulation Between Private and Public Clouds

Voters fill out paper ballots, millions of them…

Completed Ballots



Voter Facing Scanners

After Polls Close

Precinct Manager Systems

Upload Process

App

HPE vNonStop SQL/MX

\VALIDATION Public Cloud running in GCP, Azure, [AWS]

Firewall

App

HPE vNonStop SQL/MX

\PRODUCTION Private Cloud in Brick & Mortar Datacenter

Shadowbase VAM Transaction Validation

VA POC Video Overview

bit.ly/3LVN9d0: (3m:07s)

GRAVIC®
HPE Shadowbase

E-BITUG
European NonStop Symposium
EDINBURGH 2023

Sessions of Interest

HPE Shadowbase – Digital Resilience, Data Integration, and Data Validation for HPE NonStop Systems
Braemar Suite, Tuesday, 11:40 am – 12:10pm

Base24™ ATM Active-Active Business Continuity with Shadowbase Software (Customer Talk!)
Glamis Suite, Tuesday, 1:50pm – 2:20pm

Advanced Data Resiliency and Data Integrity Architectures for Mission Critical Servers
Braemar Suite, Wednesday, 11:40am – 12:10pm

Use HPE Shadowbase to Rapidly Extend HPE NonStop Databases and workloads to the Cloud
HPE In-Booth Demo

Hewlett Packard Enterprise
Technology Partner
SILVER PARTNER

Momentum Technology
Partner of the Year 2019

GRAVIC®
Shadowbase

Thank you!

SBProductManagement@Gravic.com