Hewlett Packard Enterprise

GRAVIC®

1979 45 2024

Improving Society Through Innovation®

HPE SHADOWBASE:

DIGITAL RESILIENCE AND DATA RECOVERY FOR HPE NONSTOP SYSTEMS

Kenneth Scudder
VP, Global Sales and Business Development
Gravic, Inc.

April 2024

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.

HPE Shadowbase Discussion Topics

- **HPE Digital Resilience Framework**
- **Data Recovery for Cybersecurity**
  - New concepts for resiliency
  - New architecture requirements
  - Rapid recovery
  - Bare-metal recovery
- **Data Recovery Demo**
- **Wrap-up**

About Gravic

- **Leaders in HPE NonStop data availability**
  - Strong commitment to HPE NonStop and other servers
  - 80+ technology patents
  - Hundreds of customers use Shadowbase worldwide
- **Mission critical data availability solutions**
  - Data replication, streaming, and validation
  - High and continuous availability for Digital Resilience
- **HPE's strategic, go-forward partner**
  - HPE Shadowbase globally sold and supported by HPE since 2014
  - Close collaboration between Product and Engineering groups

Gravic HQ in Pennsylvania, USA

Hewlett Packard Enterprise

Technology Partner

SILVER PARTNER

Momentum Technology
Partner of the Year 2019

HPE Digital Resilience Framework

Digital Resilience

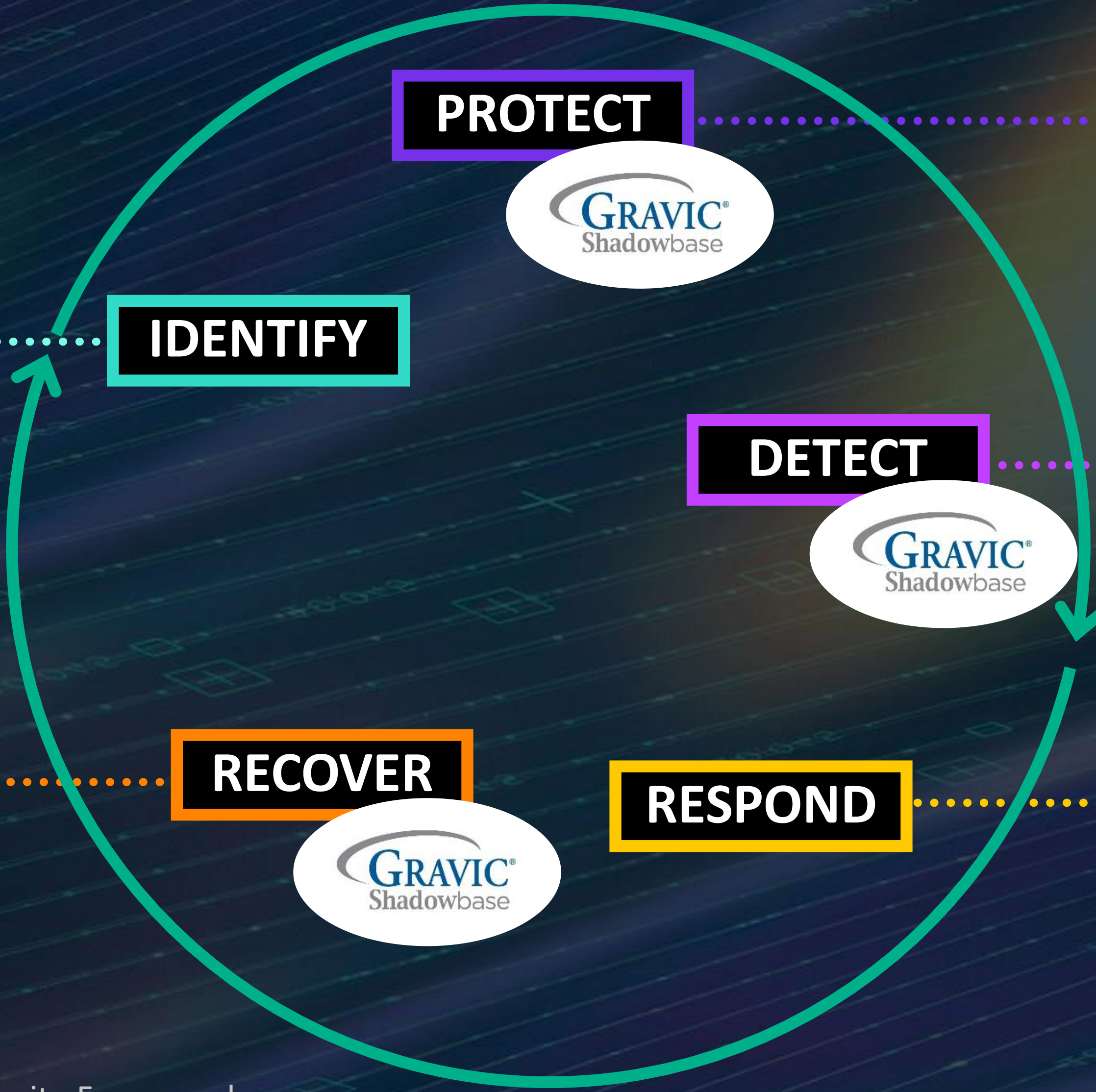
- **What is it?**
  - "Protection, detection, containment, recovery and repair capabilities against information and communication technology (ICT) related incidents" – **EU Digital Operational Resilience Act (DORA)**
  - Additional government regulations are underway

FCA FINANCIAL CONDUCT AUTHORITY

MARCH 09, 2022

Executive Order on Ensuring Responsible Development of Digital Assets

DIGITAL RESILIENCE – THE ENDLESS LOOP



IDENTIFY

PROTECT

GRAVIC Shadowbase

DETECT

GRAVIC Shadowbase

RESPOND

RECOVER

GRAVIC Shadowbase

Shape Of Data
Viable Data Age
Rapid Security Assessment
In-depth Security Assessment
Compliance
Analyze Threat Profiles
Backup Restore Strategy
Tape Catalog Recovery

Multi Factor Authentication
NonStop Hardening Guide
Security Assessment
Encryption/Tokenization/DIM
DevOps – Human Gapped
Access control and auditing
Backup Processes/Procedures/Test

Security Alerting, NonStop Intelligence, SIEM
Reporting
Object Monitoring, File Integrity
Data Validation

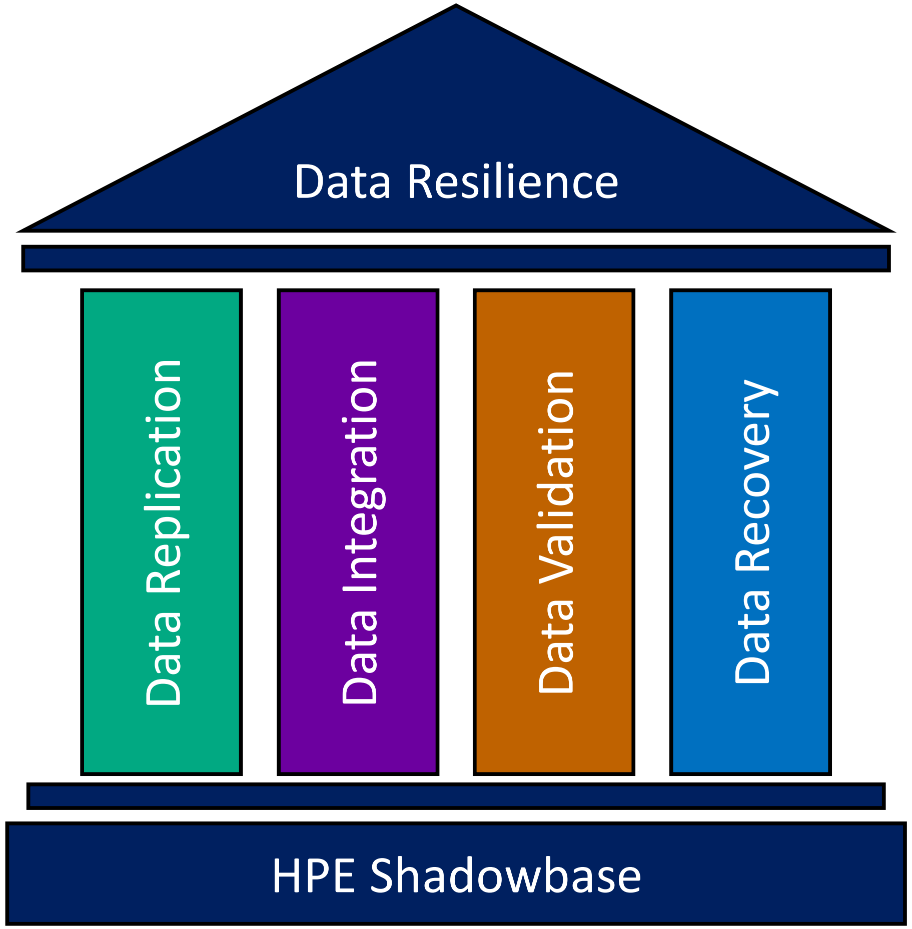
Forensics
Procedures
Automation
Triggers from “Detect”

DR Site/Prove Synch
3rd Site(Not the DR site)
Immutable Backup
Backup Restore Strategy
3-2-1-1 Rule
Bare Metal Recovery
Test

Aligned with NIST Cybersecurity Framework

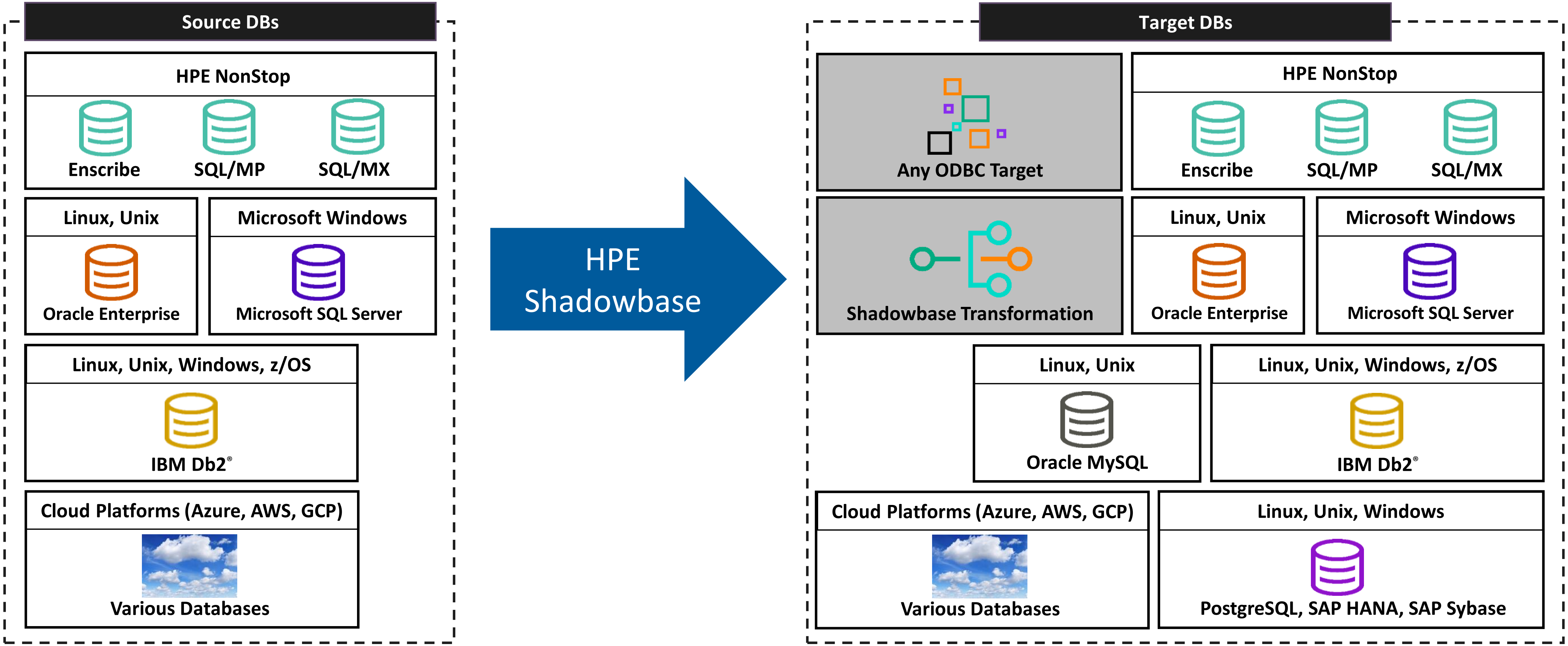
HPE Shadowbase

- **Digital Resilience for mission critical HPE NonStop environments**
- **Key pillars of HPE Shadowbase**
  - Data Replication for Business Continuity
  - Data and Application Integration
  - Data Validation
  - Data Recovery for Cybersecurity



Homogeneous & heterogeneous uni-directional data replication and streaming

All combinations supported



Source DBs

HPE NonStop

Enscribe SQL/MP SQL/MX

Linux, Unix

Oracle Enterprise

Microsoft Windows

Microsoft SQL Server

Linux, Unix, Windows, z/OS

IBM Db2®

Cloud Platforms (Azure, AWS, GCP)

Various Databases

HPE Shadowbase

Target DBs

Any ODBC Target

HPE NonStop

Enscribe SQL/MP SQL/MX

Shadowbase Transformation

Linux, Unix

Oracle Enterprise

Microsoft Windows

Microsoft SQL Server

Linux, Unix

Oracle MySQL

Linux, Unix, Windows, z/OS

IBM Db2®

Cloud Platforms (Azure, AWS, GCP)

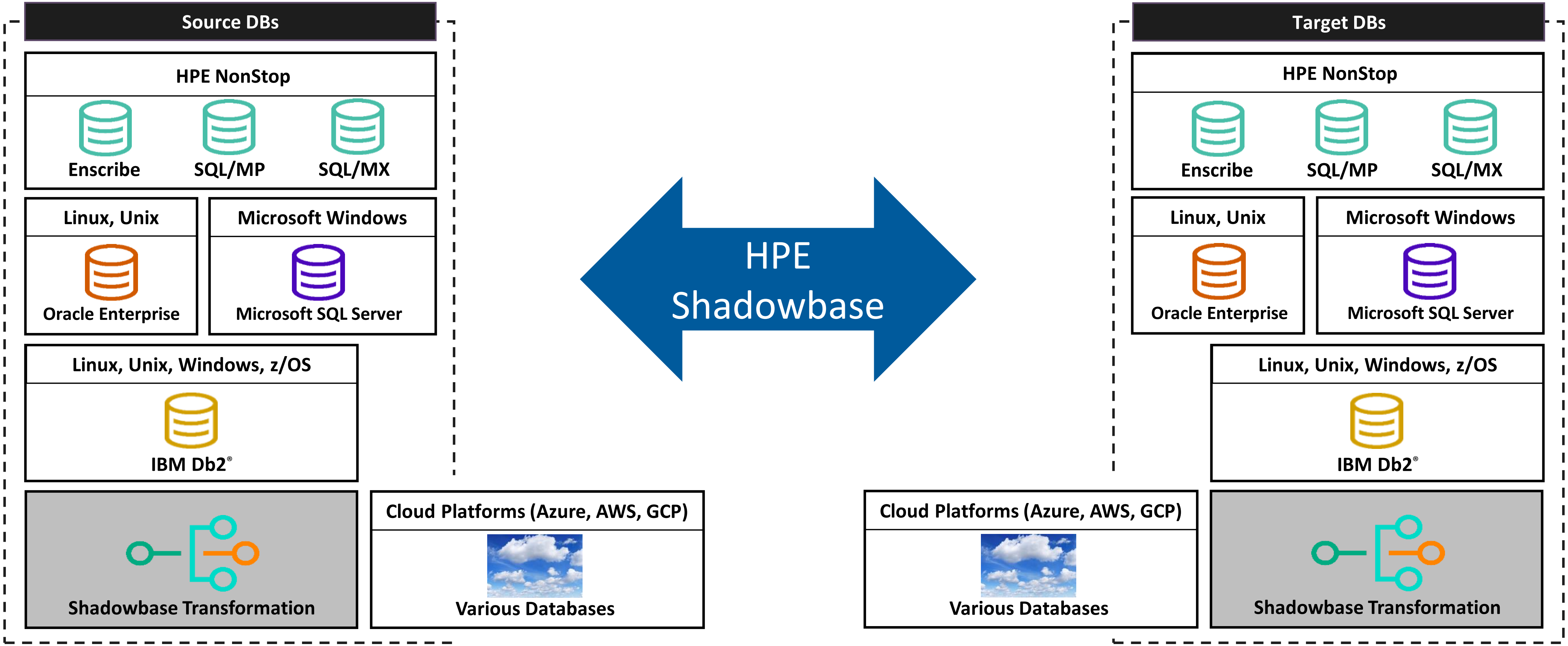
Various Databases

Linux, Unix, Windows

PostgreSQL, SAP HANA, SAP Sybase

Homogeneous & heterogeneous bi-directional data replication and streaming

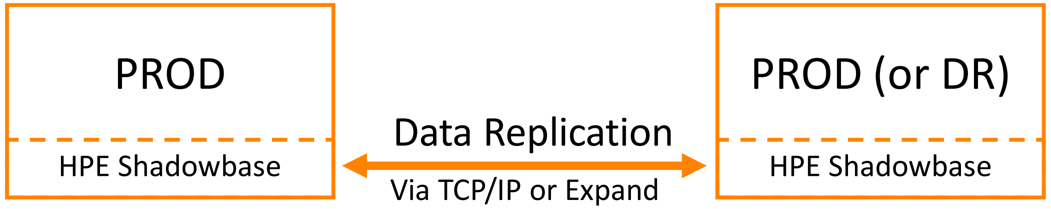
All combinations supported



Data Recovery for Cybersecurity

“Traditional” Data Replication for Business Continuity (BC)

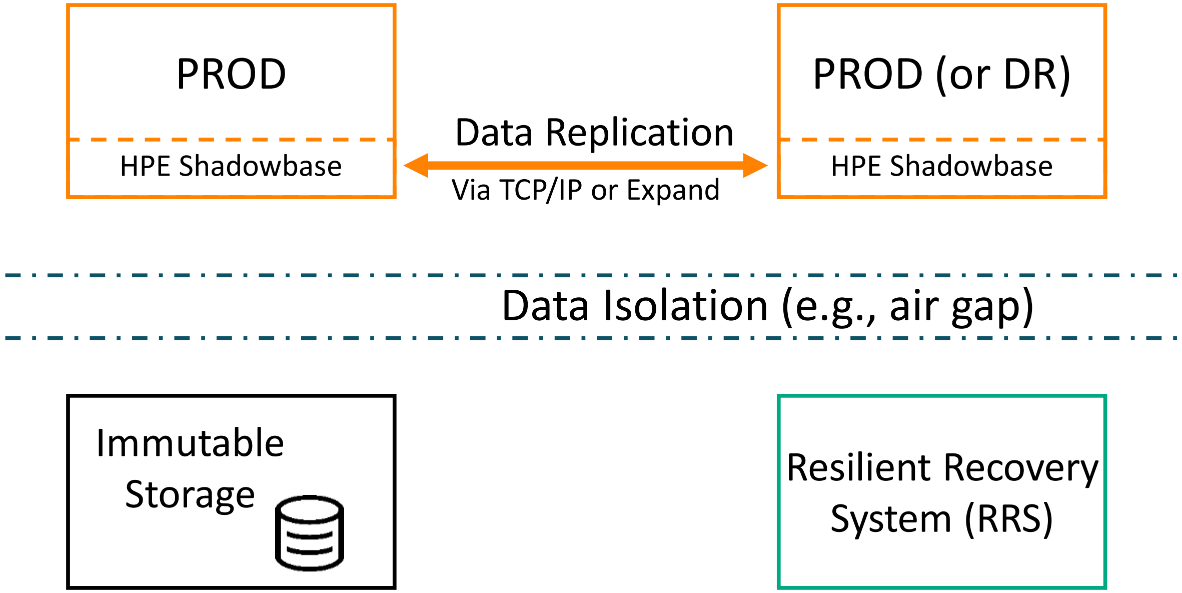
Typically designed to protect against natural disasters or accidents



- **BC for Disaster Recovery**
  - A/P, A/Near-A, and A/A
  - Data replicated in real-time
  - Data transferred via TCP/IP or Expand
  - Geographic “isolation”
  - Online, on-platform data validation
  - Database correction tools
- **Addresses BC concepts**
  - Recovery Point Objective (RPO)
  - Recovery Time Objective (RTO)

Data Recovery for Cybersecurity

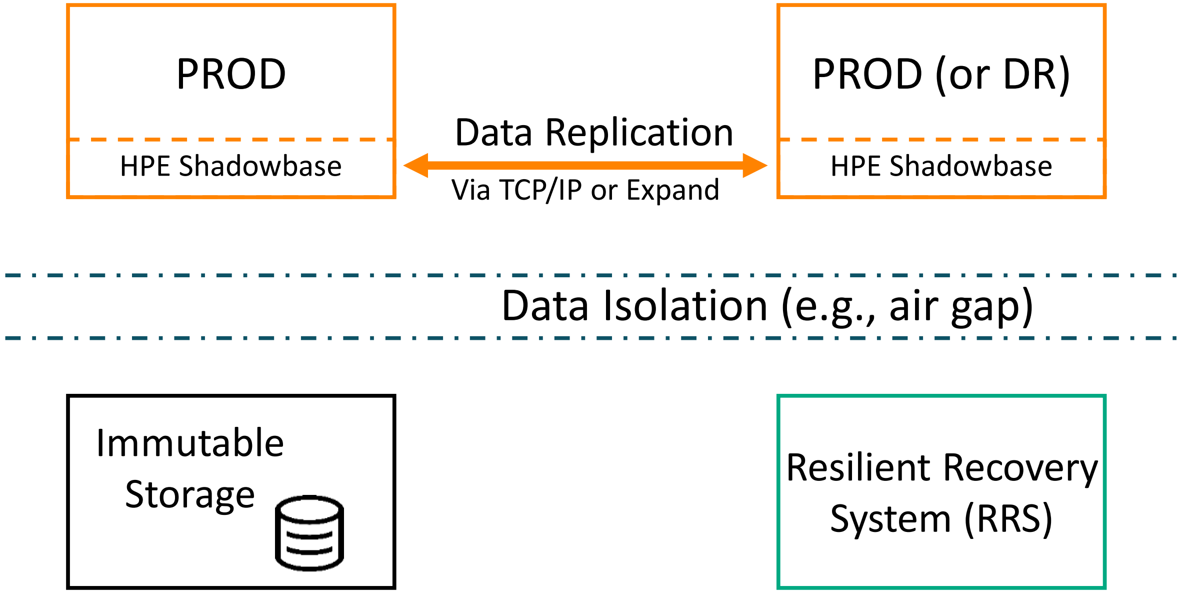
New requirements are evolving for Ransomware recovery



- **New architectural requirements**
  - 3-2-1-1 backup rule
    - Immutable storage
  - Data isolation
    - “Air-gapped” systems
    - Secure, non-persistent connectivity
    - RBAC for recovery data and systems
  - Resilient Recovery System (RRS)
    - 3rd-site
    - “People-gapped”
    - Managed Service Provider (MSP) (e.g., GreenLake)

Data Recovery for Cybersecurity

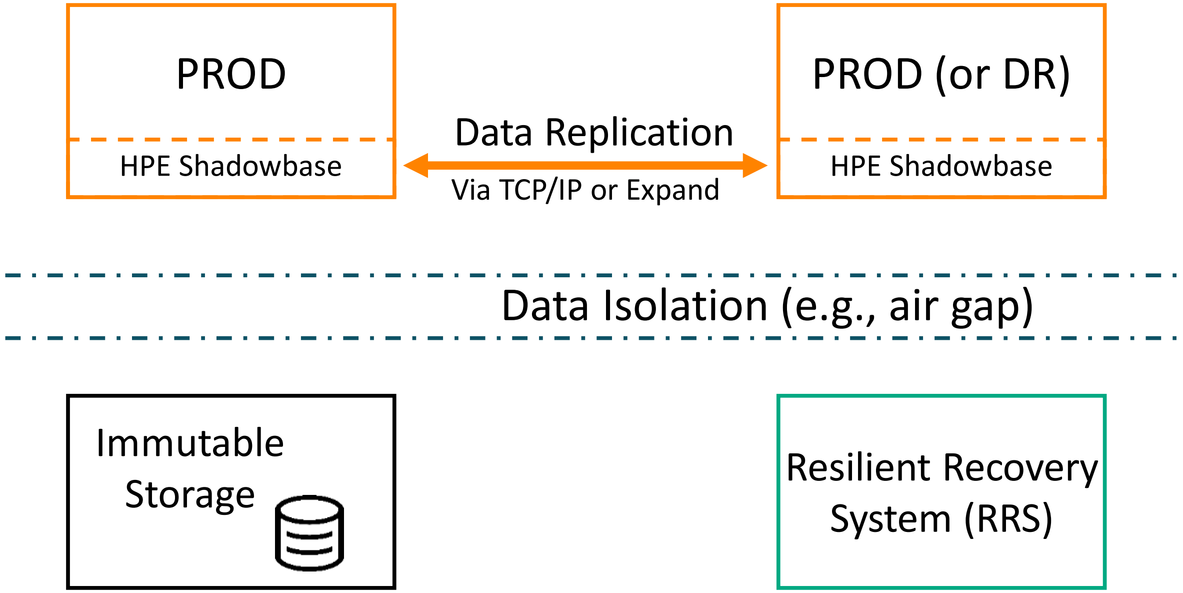
New “Resiliency-related” concepts are needed



- **New “Resiliency” concepts**
  - Resilient Recovery Point Objective (R-RPO)
  - Resilient Recovery Time Objective (R-RTO)
  - Attack-type differentiation
    - Theft of data
    - Modifying data
    - Denial of data access (e.g., encryption)
  - Data “Threat Window”
    - Time required to detect an attack
  - Data “Quarantine”
    - Time period when data is not fully trusted and held back from being applied to RRS

Resilient Recovery Architectures

Two emerging options

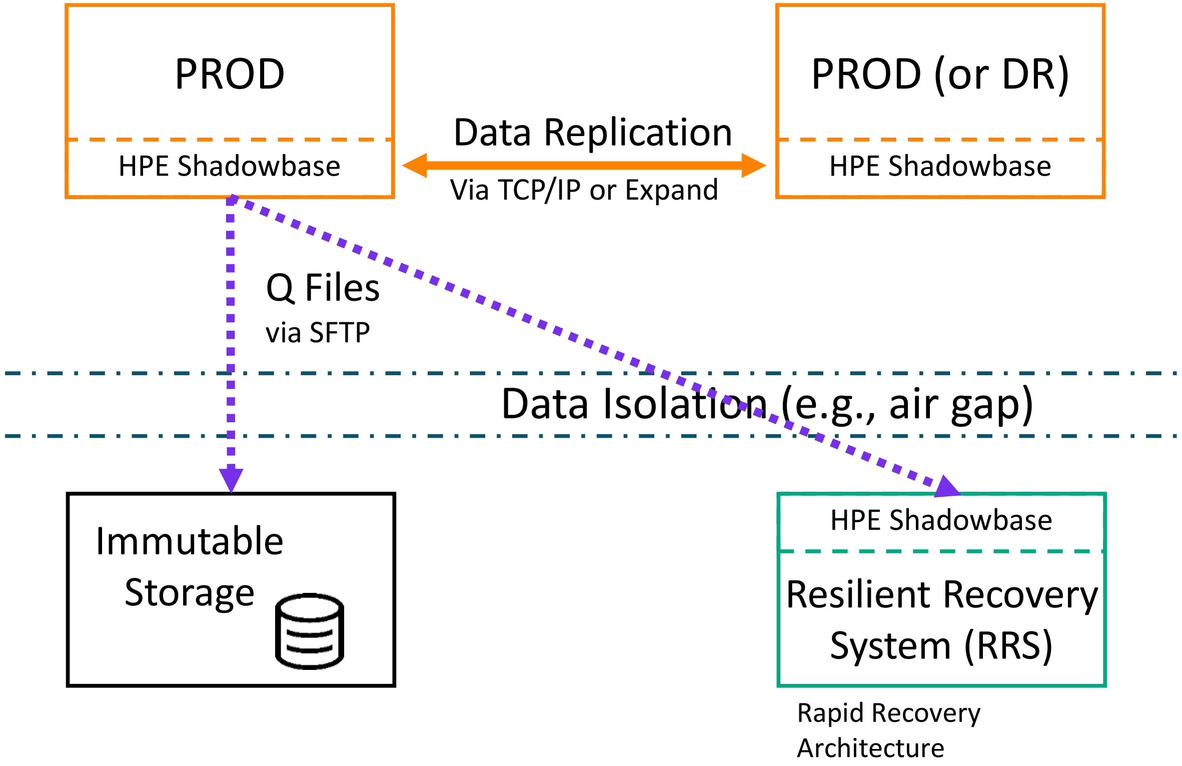


- **RRS architectures**

1. Rapid Recovery Architecture (RRA)
   - Designed to balance isolation with faster recovery than Bare Metal Recovery
   - Data is progressively applied to RRS database (after Quarantine period)
2. Bare Metal Recovery Architecture (BMRA)
   - Designed to completely rebuild entire production environment on "factory fresh" system
   - OS, application, and database must be installed
   - Data must be fully loaded, and rolled forward
   - Longer recovery time

Rapid Recovery Architecture – Option 1a

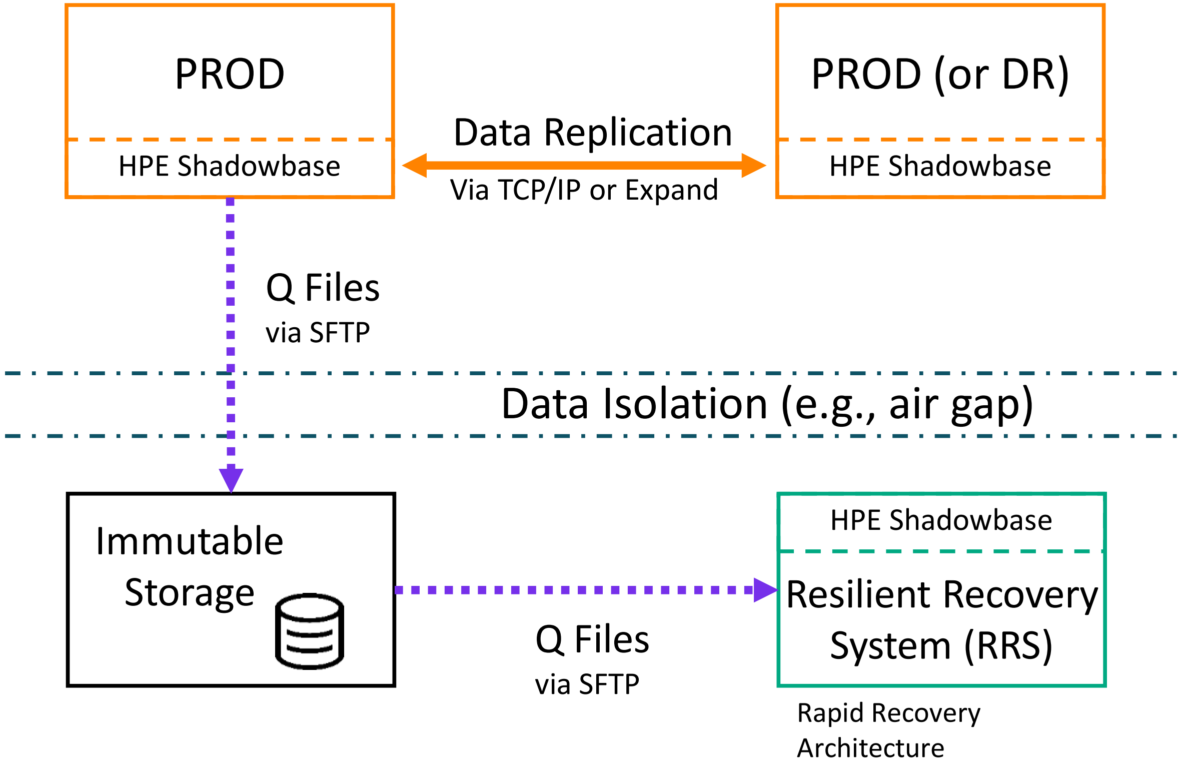
Pull data from PROD or DR for faster recovery



- **Protect**
  - Pre-configure RRS with clean app and initial database
  - Capture and store queued DB change data in "Q Files"
  - Pull Q Files to 3rd-site RRS
  - Send Q Files to Immutable storage
- **Detect**
  - Validate Q Files to detect Man-in-the-Middle (MitM) attacks or other corruption
- **Recover**
  - Hold Q Files in suspension (or "Quarantine") until rolling Threat Window has passed
  - Apply (or roll-back) Q Files to a trusted point on RRS

Rapid Recovery Architecture – Option 1b

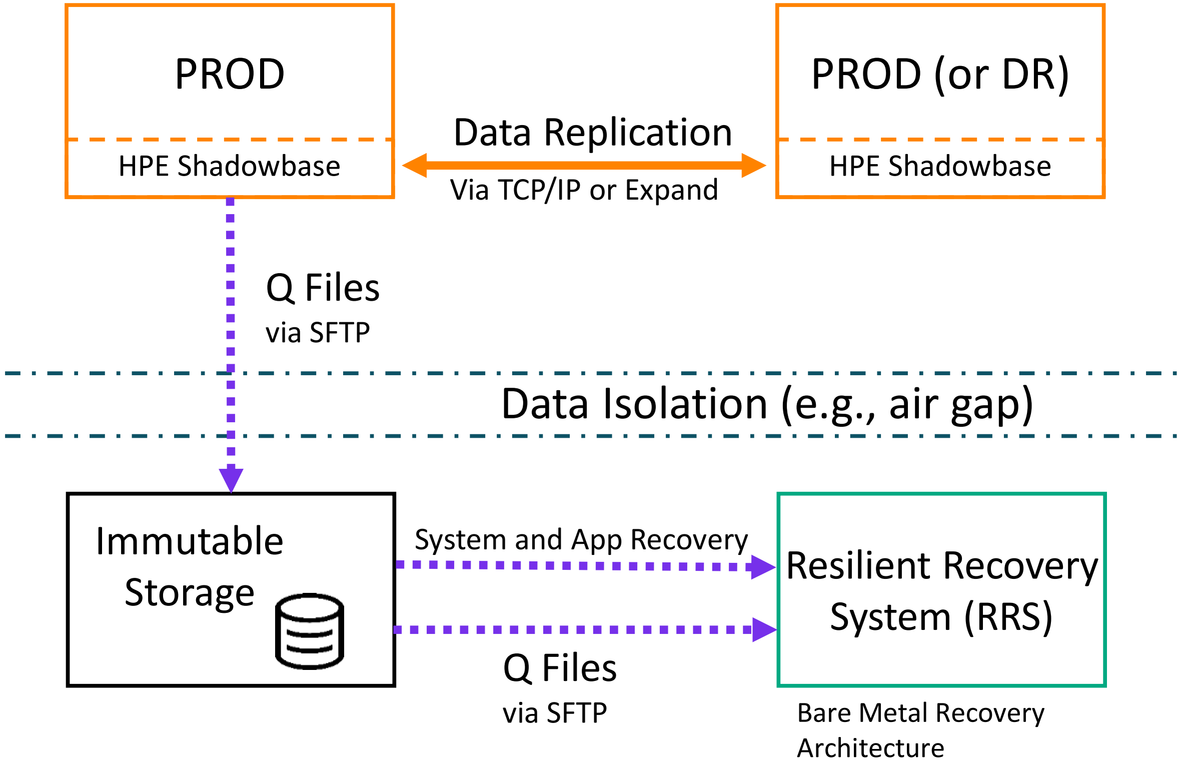
Pull data from Immutable Storage for greater isolation



- **Protect**
  - Pre-configure RRS with clean app and initial database
  - Capture and store queued DB change data in "Q Files"
  - Send Q Files to Immutable Storage to isolate data from cyber threats
- **Detect and Recover**
  - Pull Q files from Immutable Storage to RRS
  - Validate Q Files to detect Man-in-the-Middle (MitM) attacks or other corruption
  - Hold Q Files in suspension (or "Quarantine") until rolling Threat Window has passed
  - Apply (or roll-back) Q Files to a trusted point on RRS

Bare Metal Recovery Architecture – Option 2

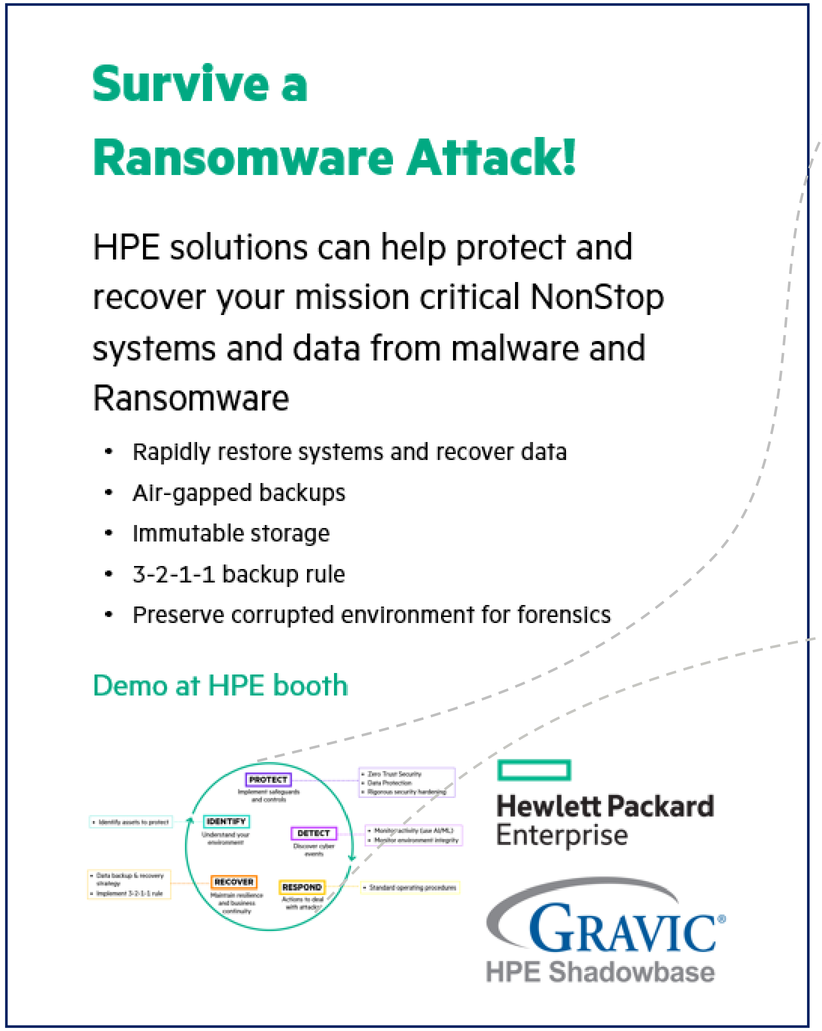
Increases isolation but with longer recovery time



- **Protect**
  - Store system, application, and DB backup on Immutable Storage
  - Capture and store queued DB change data in “Q Files”
  - Send Q Files to Immutable Storage to isolate data
- **Recover**
  - Recover system, app, and backup data from Immutable Storage to RRS
  - Send Q Files to RRS
  - Validate Q Files
  - Apply Q Files to roll the data up to trusted recovery point and recover operations
  - Consider HPE GreenLake Managed Services

Data Recovery Demo

HPE Shadowbase Ransomware Recovery Demo



Survive a Ransomware Attack!

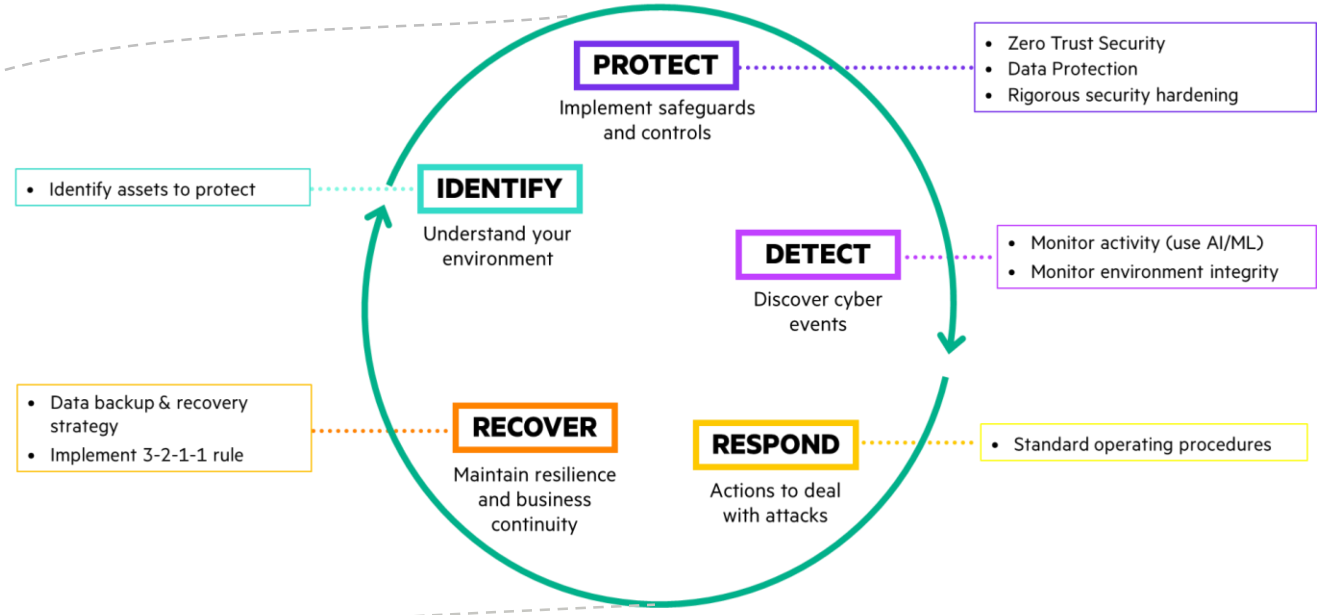
HPE solutions can help protect and recover your mission critical NonStop systems and data from malware and Ransomware

- 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

Hewlett Packard Enterprise

GRAVIC® HPE Shadowbase



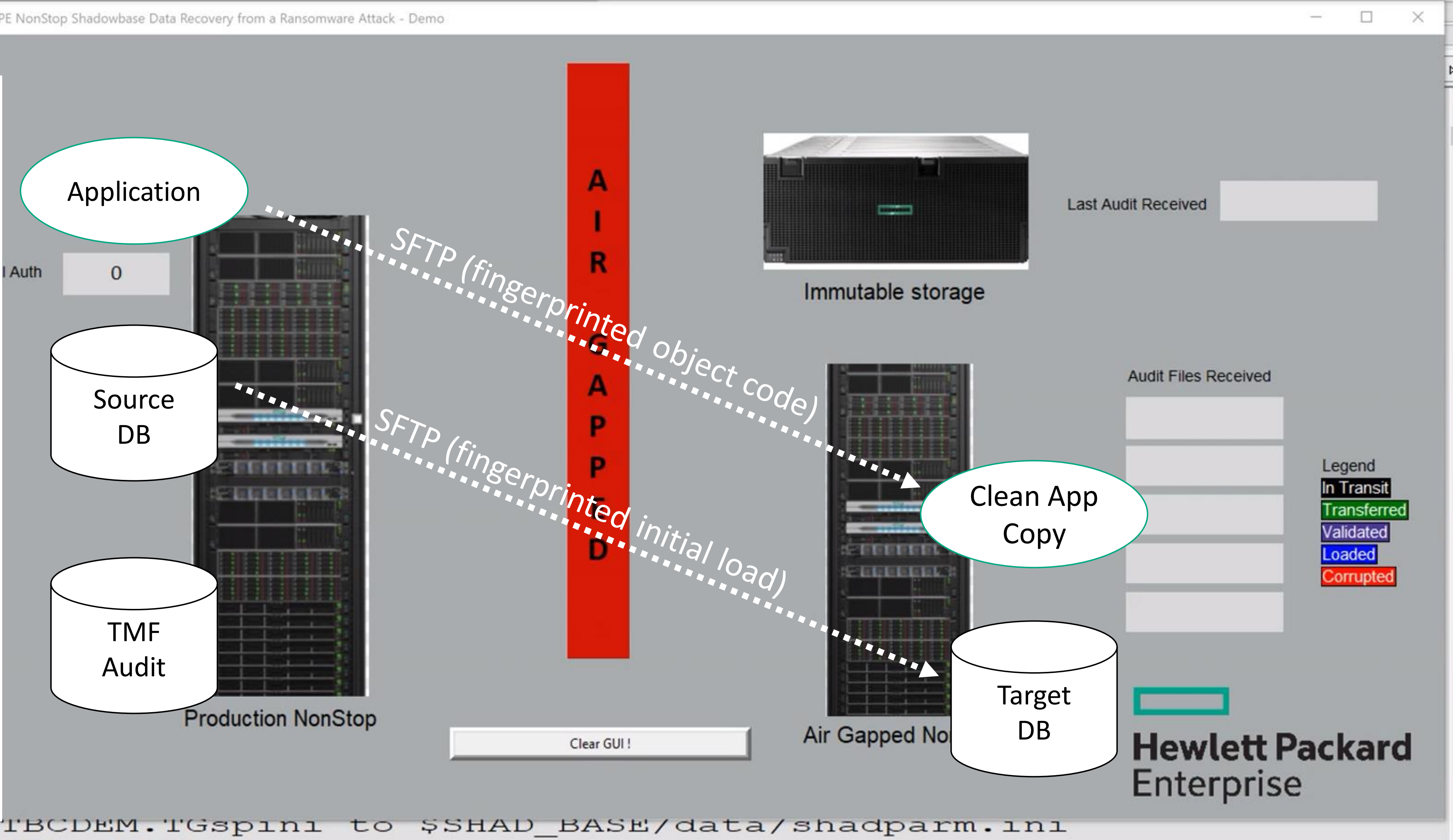
PROTECT
Implement safeguards and controls
• Zero Trust Security
• Data Protection
• Rigorous security hardening
IDENTIFY
Understand your environment
• Identify assets to protect
DETECT
Discover cyber events
• Monitor activity (use AI/ML)
• Monitor environment integrity
RECOVER
Maintain resilience and business continuity
• Data backup & recovery strategy
• Implement 3-2-1-1 rule
RESPOND
Actions to deal with attacks
• Standard operating procedures

- HPE Digital Resilience Framework based on NIST guidelines
- New HPE Shadowbase capabilities to rapidly RECOVER critical data
- Demo at HPE booth during TBC 2023

Create and **send a clean copy of the application and source \PROD DB to the \RRS** (Resilent 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



```
C:\Windows\System32>C:\Windows\System32\cmd.e
```

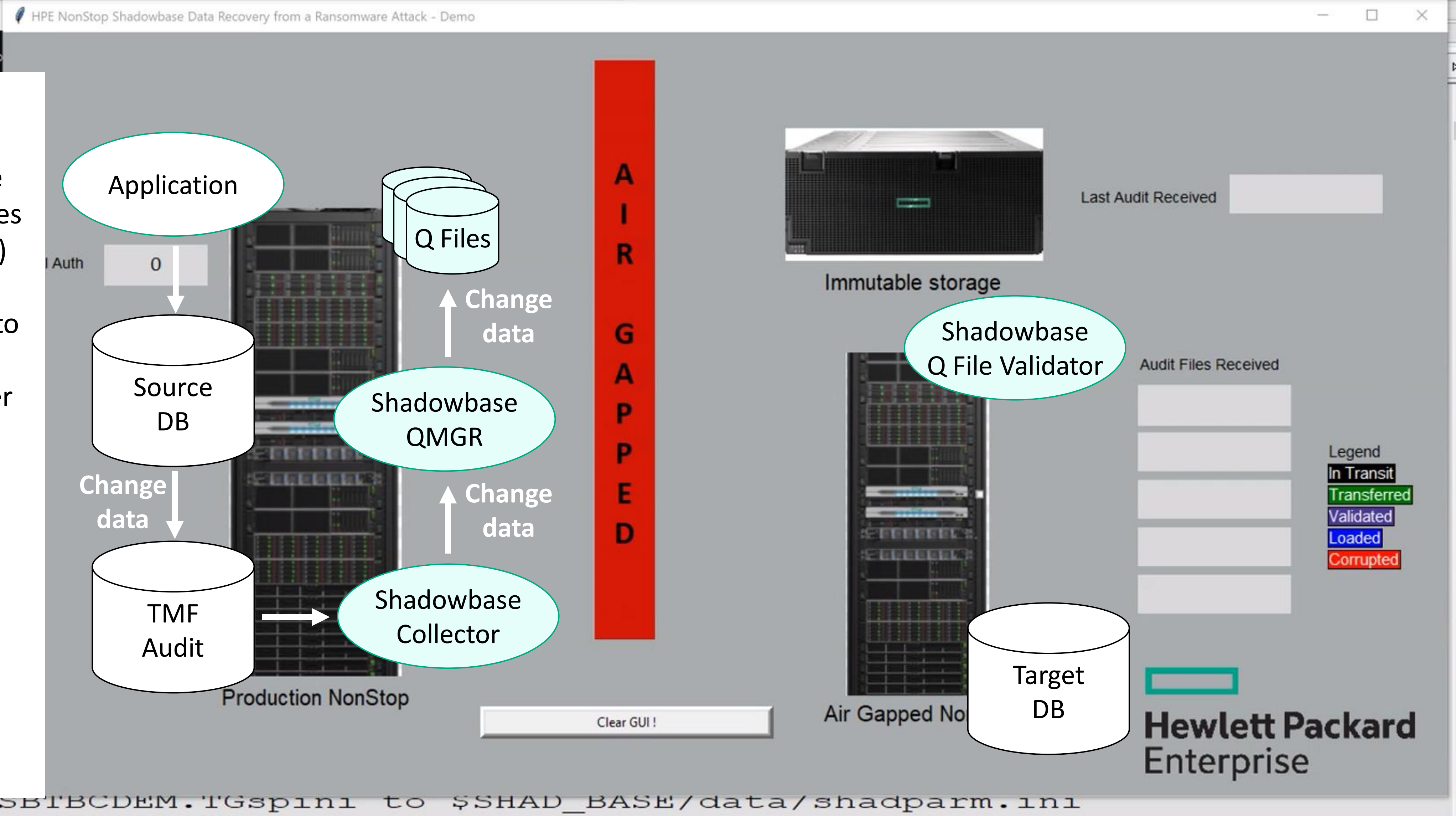
```
Copying $DATA04.SBTBCDEM.TGspini to $SHAD_BASE/data/shadparm.ini
Adding DOC Writer (P) SBDCP
Adding TRS SBTRS
Adding DOC Cleaner (P) SBCLP
Starting DOC SBDCP
Starting TRS SBTRS
Starting DCL SBCLP
```

RansomWareDemoMain

```
C:\Windows\System32\C:\Windows\System32\cmd.e
```

Steps:

1. Configure and start Shadowbase to capture \PROD database changes (audit trail change data)
2. Shadowbase bundles change data capture into “Q Files” on source system awaiting transfer request from target system

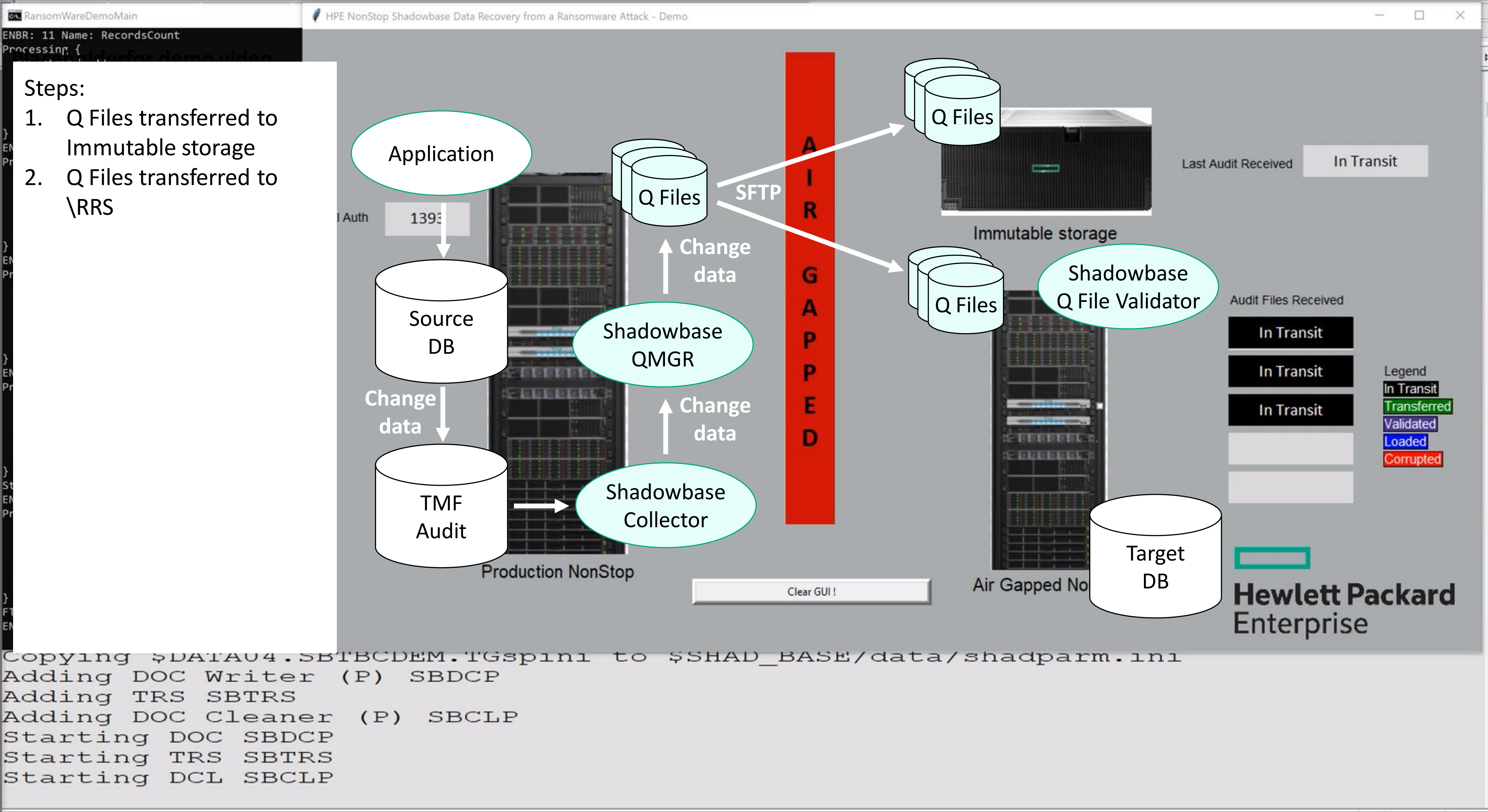


```
Copying $DATA04.SBTBCDEM.TGspini to $SHAD_BASE/data/shadparm.ini
Adding DOC Writer (P) SBDCP
Adding TRS SBTRS
Adding DOC Cleaner (P) SBCLP
Starting DOC SBDCP
Starting TRS SBTRS
Starting DCL SBCLP
```

Placeholderfor demo video

Steps:

1. Q Files transferred to Immutable storage
2. Q Files transferred to \RRS



RansomWareDemoMain

```
ENBR: 11 Name: RecordsCount
Processing {
```

HPE NonStop Shadowbase Data Recovery from a Ransomware Attack - Demo

Last Audit Received: In Transit

Audit Files Received:
In Transit
In Transit
In Transit

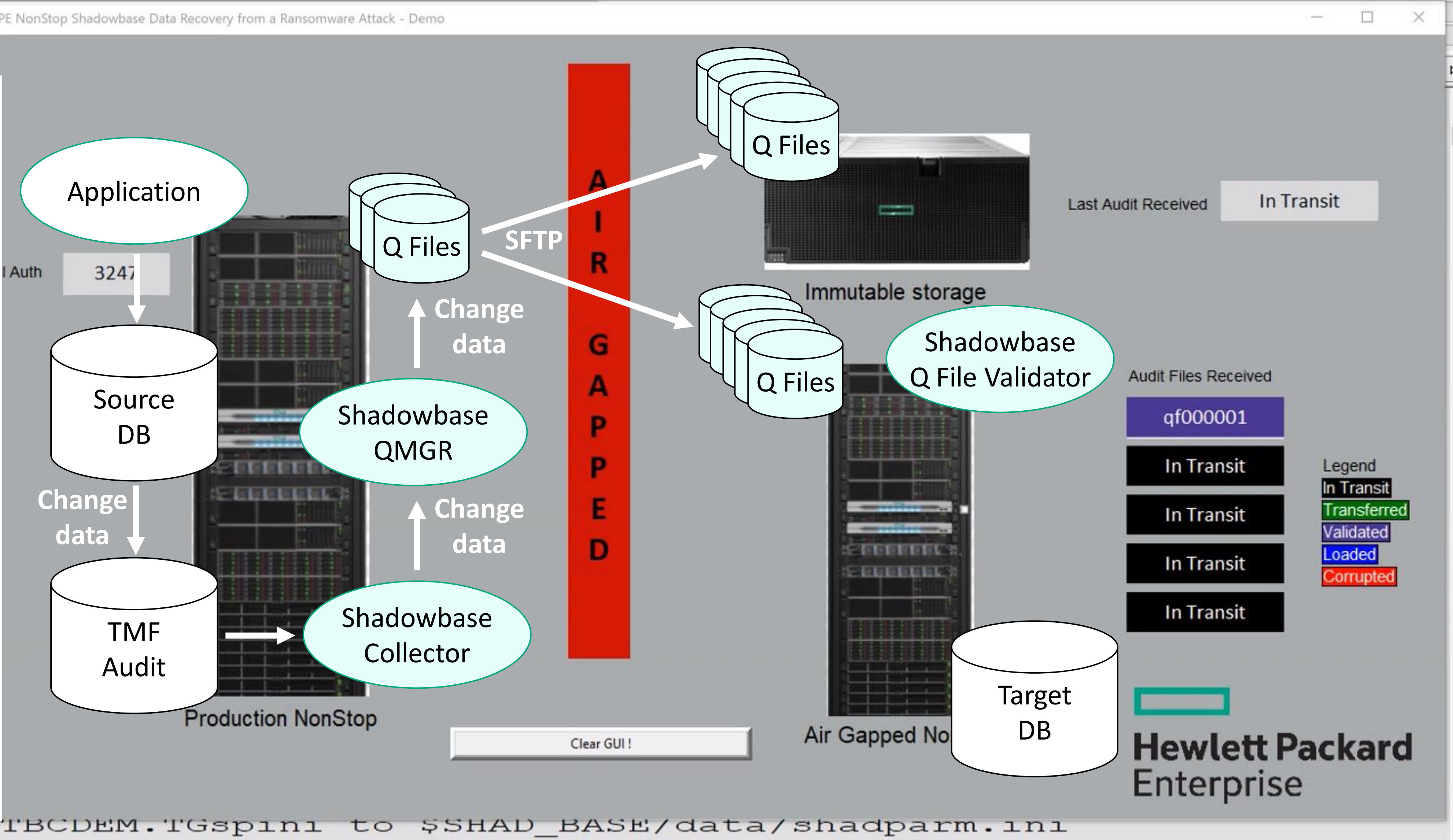
Legend:
In Transit
Transferred
Validated
Loaded
Corrupted

```
Copying $DATA04.SBTBCDEM.TGspini to $SHAD_BASE/data/shadparm.ini
Adding DOC Writer (P) SBDCP
Adding TRS SBTRS
Adding DOC Cleaner (P) SBCLP
Starting DOC SBDCP
Starting TRS SBTRS
Starting DCL SBCLP
```

```
"eventnum": 12,
"event": "EndFTP",
```

Steps:

1. Shadowbase validates Q Files to verify integrity
2. Note: additional Q Files being transferred



Last Audit Received: In Transit

Audit Files Received

- qf000001
- In Transit
- In Transit
- In Transit
- In Transit

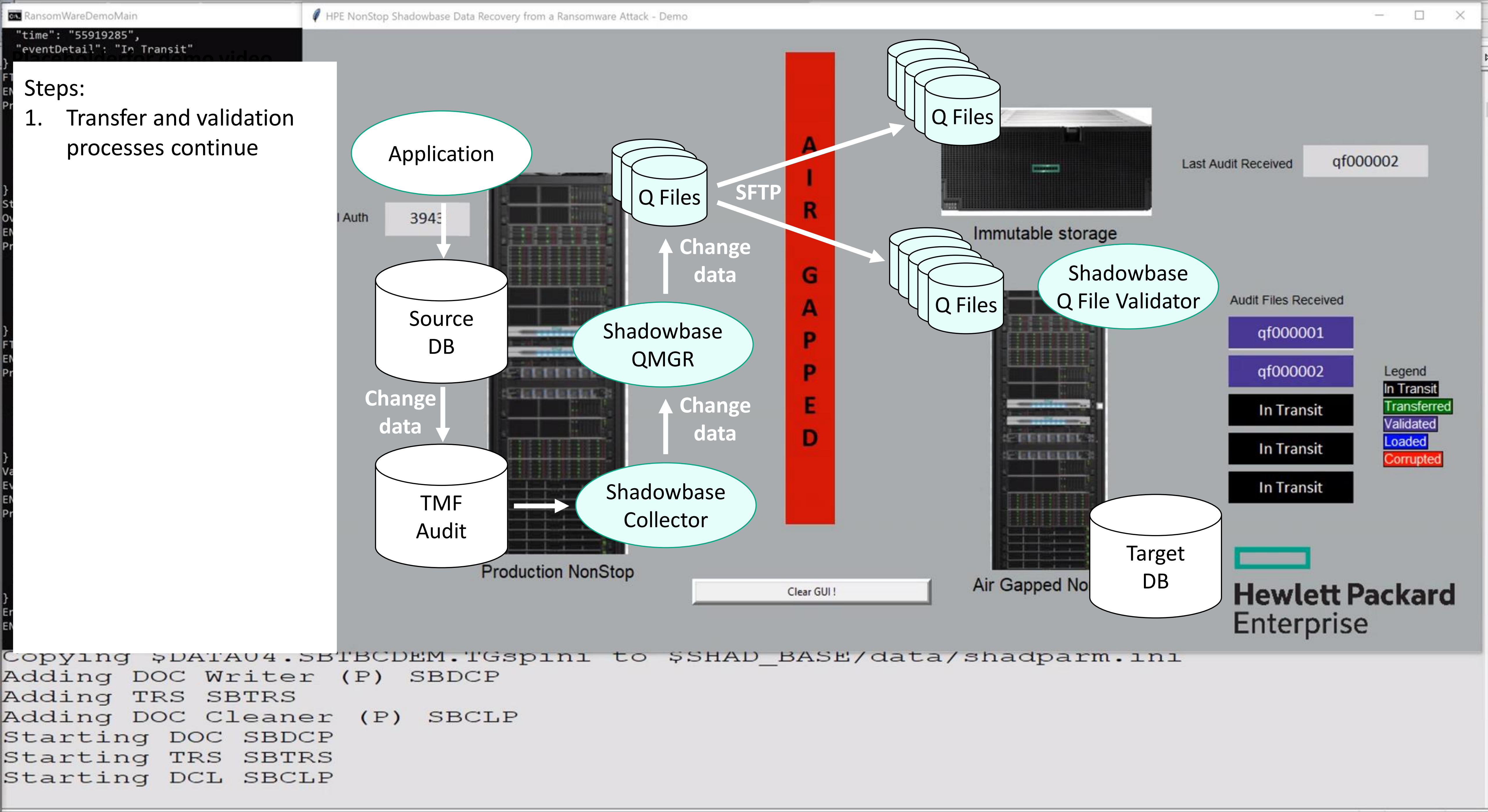
Legend

- In Transit
- Transferred
- Validated
- Loaded
- Corrupted

```
Copying $DATA04.SBTBCDEM.TGspini to $SHAD_BASE/data/shadparm.ini
Adding DOC Writer (P) SBDCP
Adding TRS SBTRS
Adding DOC Cleaner (P) SBCLP
Starting DOC SBDCP
Starting TRS SBTRS
Starting DCL SBCLP
```

Steps:

1. Transfer and validation processes continue



```
"time": "55919285",
"eventDetail": "In Transit"
```

Auth 3943

Last Audit Received qf000002

Audit Files Received

- qf000001
- qf000002
- In Transit
- In Transit
- In Transit

Legend

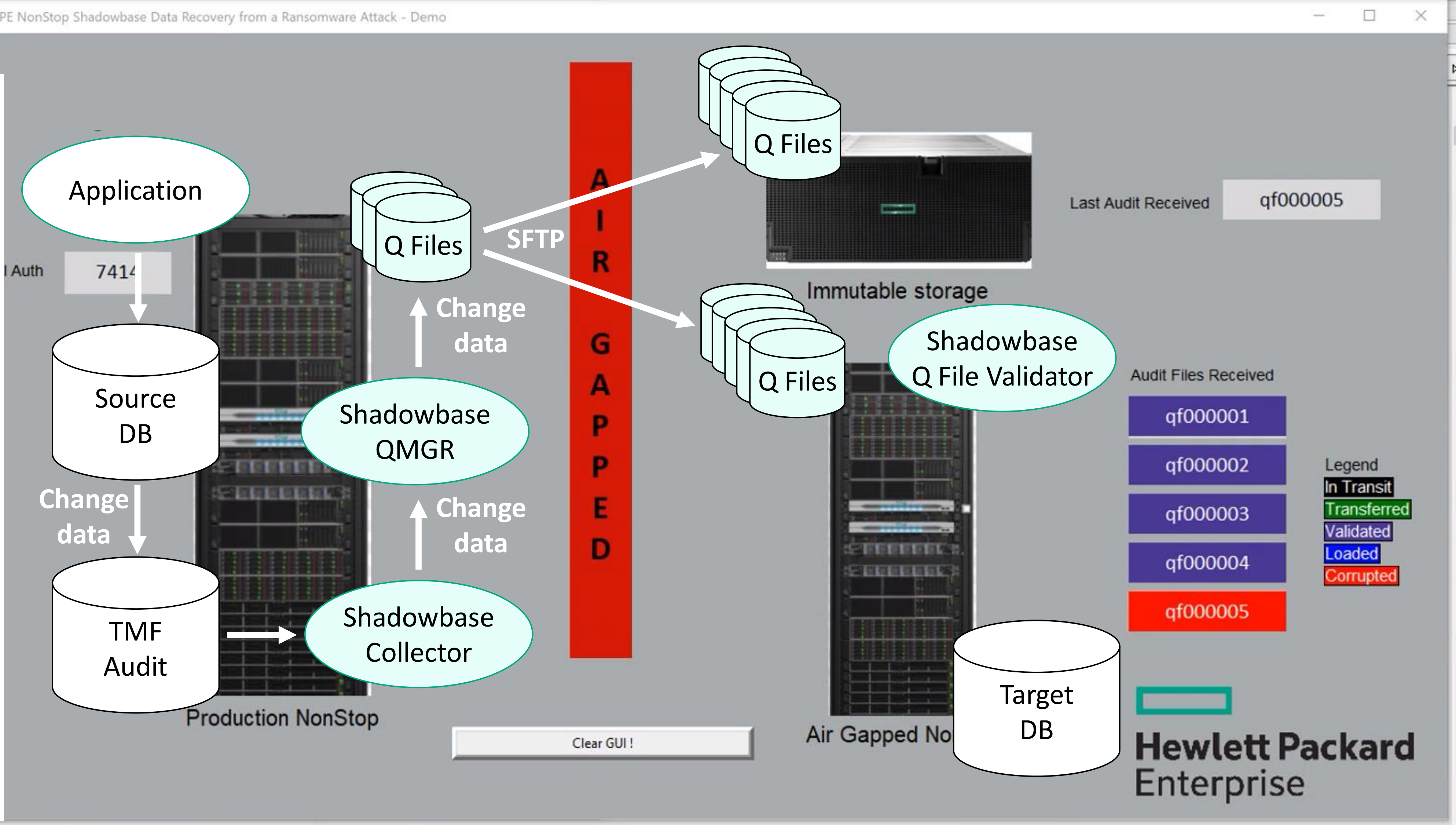
- In Transit
- Transferred
- Validated
- Loaded
- Corrupted

```
Copying $DATA04.SBTBCDEM.TGspini to $SHAD_BASE/data/shadparm.ini
Adding DOC Writer (P) SBDCP
Adding TRS SBTRS
Adding DOC Cleaner (P) SBCLP
Starting DOC SBDCP
Starting TRS SBTRS
Starting DCL SBCLP
```

```
"increment": 3,
"time": "55994501",
```

Steps:

1. Corrupted Q File detected
2. Ransomware attack identified
3. Initiate cybersecurity response



Last Audit Received qf000005

Audit Files Received

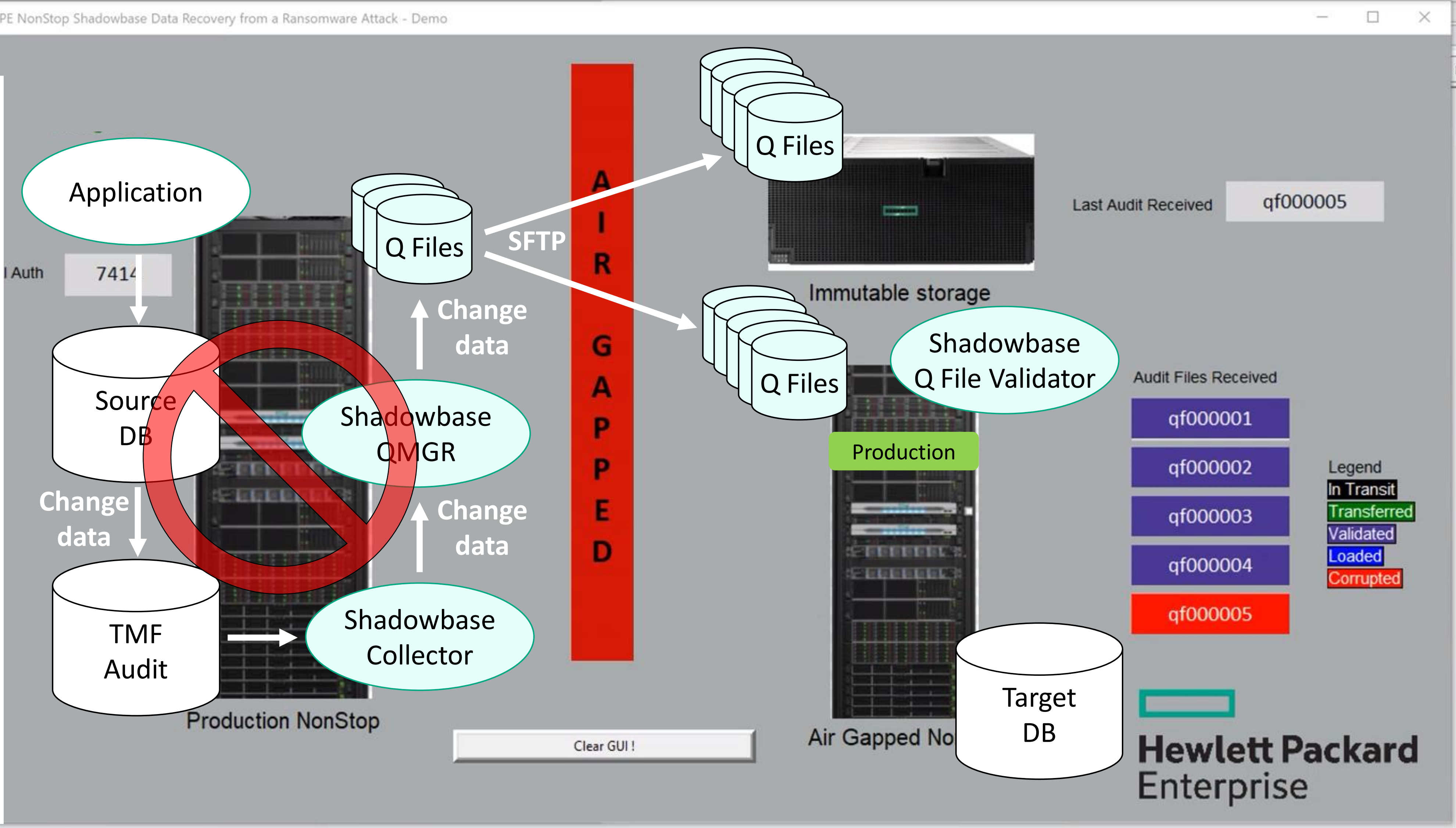
- qf000001
- qf000002
- qf000003
- qf000004
- qf000005

```
Starting DCL SBCLP
Warning, file is not audited
4
QueueSeqno = 7
QueueSeqno = 4
QueueRBA = 136132
QueueRBA = 458752
```

```
 "increment": 3,
 "time": "55994501",
```

Steps:

1. Old production system is quarantined
2. \RRS becomes production system
3. Note last validated Q File: qf000004

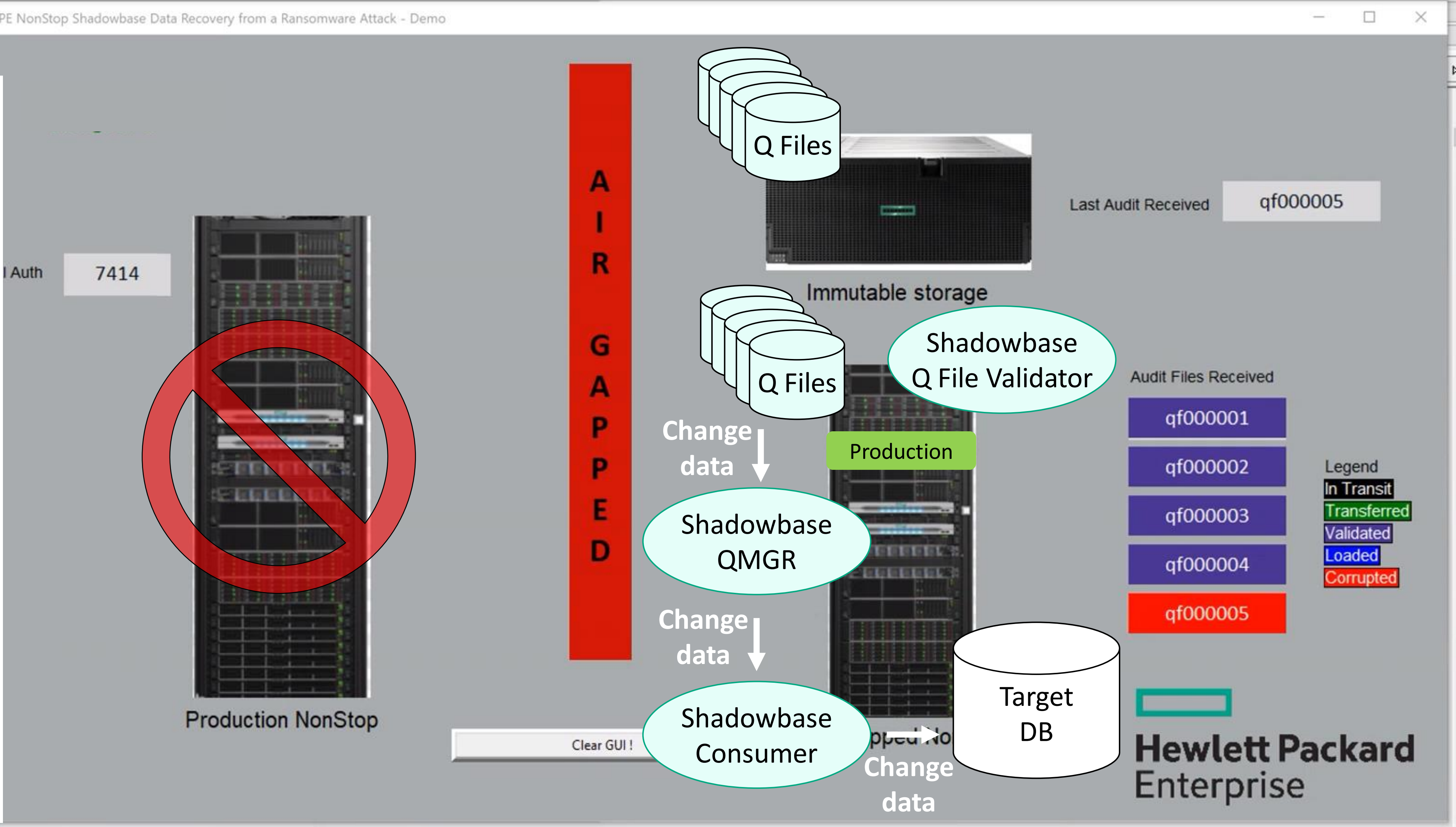


```
Starting DCL SBCLP
Warning, file is not audited
4
QueueSeqno = 7
QueueSeqno = 4
QueueRBA = 136132
QueueRBA = 458752
```

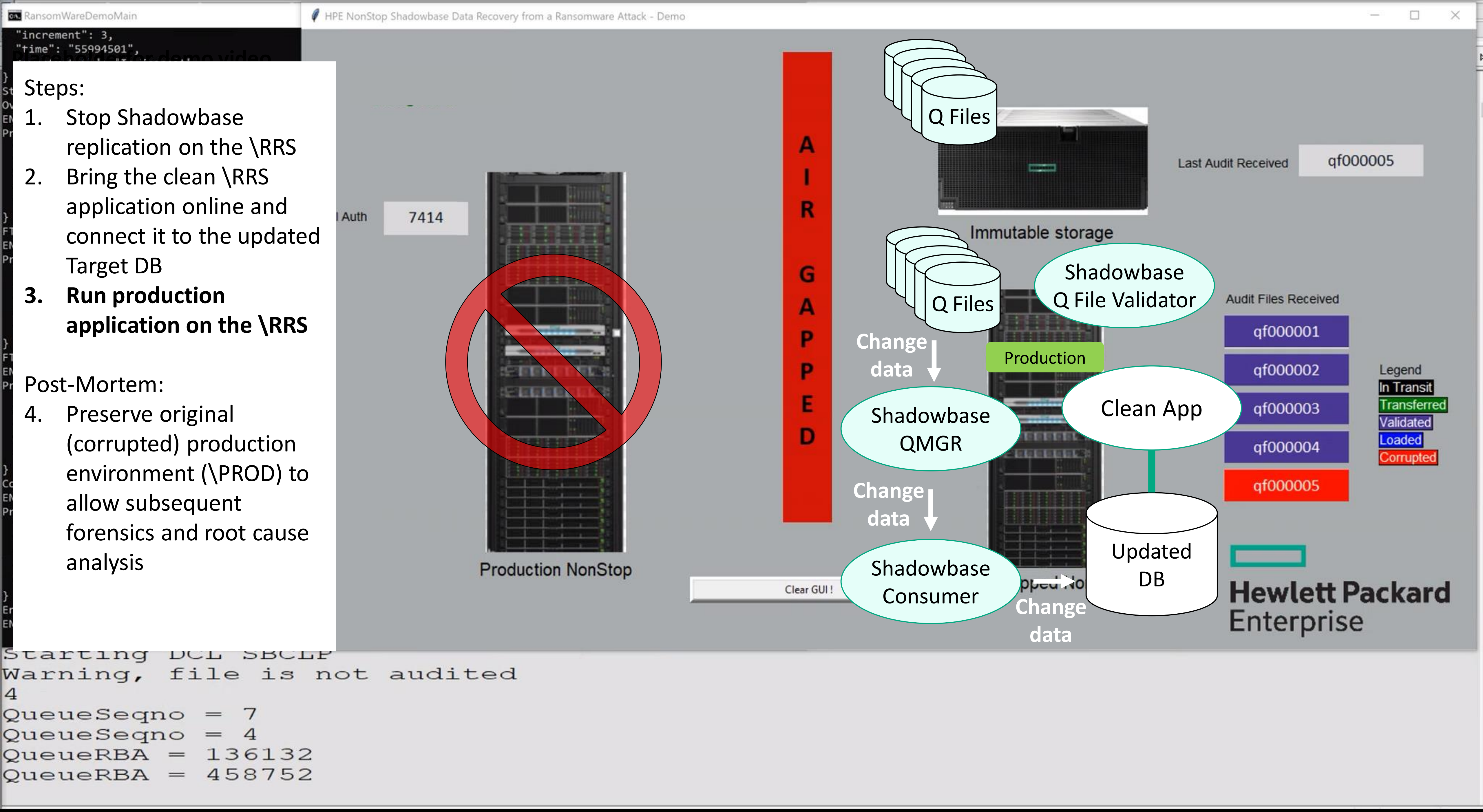
```
"increment": 3,
"time": "55994501",
```

Steps:

1. Start HPE Shadowbase on on \RRS
2. Replay valid Q Files into Target DB to bring it up to a trusted point
3. Note: HPE Shadowbase has UNDO/REDO functionality if trusted point needs adjustment



```
Starting DCL SBCLP
Warning, file is not audited
4
QueueSeqno = 7
QueueSeqno = 4
QueueRBA = 136132
QueueRBA = 458752
```



```
"increment": 3,
"time": "55994501",
```

Steps:

1. Stop Shadowbase replication on the \RRS
2. Bring the clean \RRS application online and connect it to the updated Target DB
3. **Run production application on the \RRS**

Post-Mortem:

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

Auth 7414

Last Audit Received qf000005

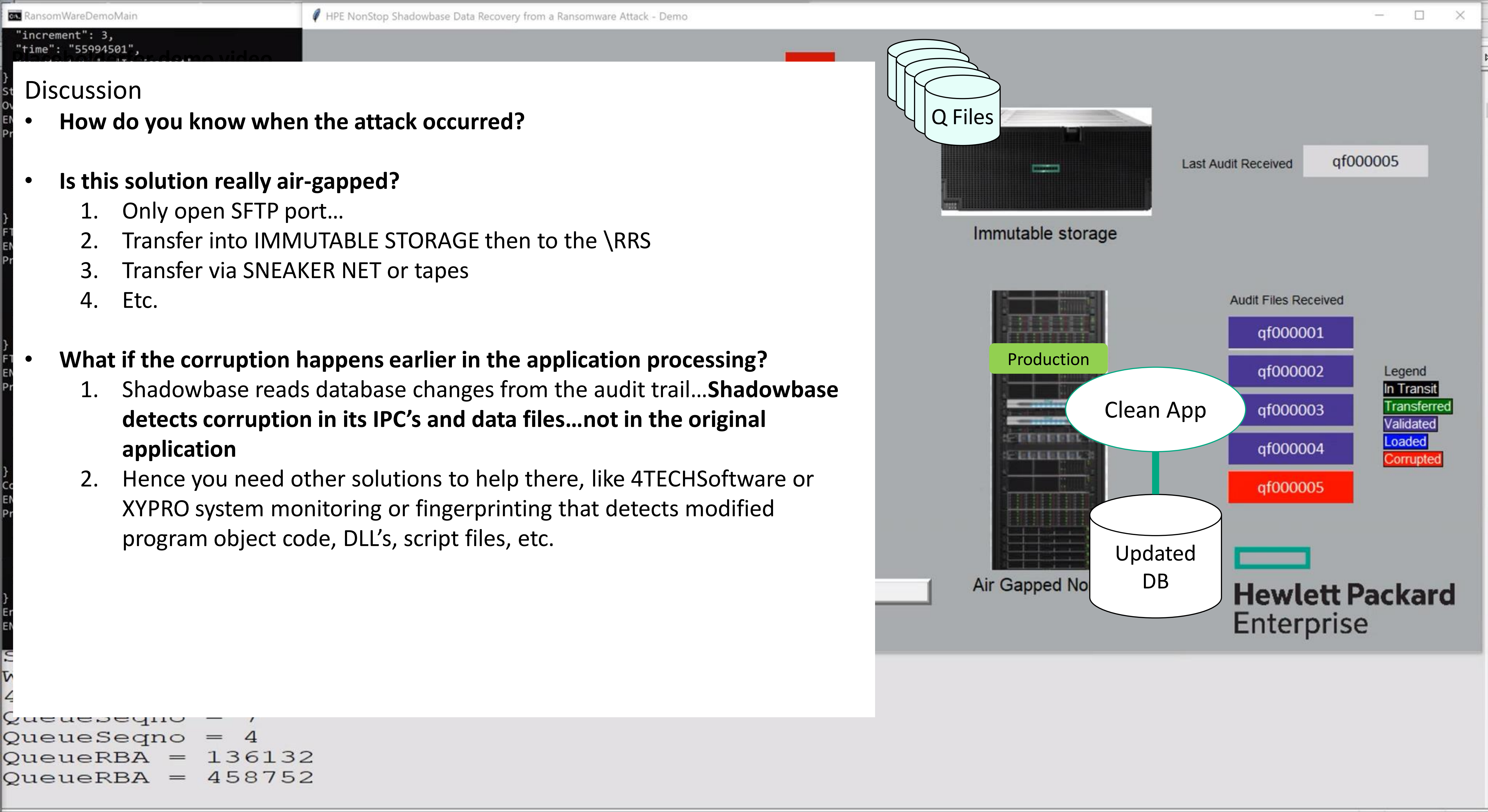
Audit Files Received

- qf000001
- qf000002
- qf000003
- qf000004
- qf000005

Legend

- In Transit
- Transferred
- Validated
- Loaded
- Corrupted

```
Starting DCL SBCLP
Warning, file is not audited
4
QueueSeqno = 7
QueueSeqno = 4
QueueRBA = 136132
QueueRBA = 458752
```



```
"increment": 3,
"time": "55994501",
```

Discussion

- **How do you know when the attack occurred?**

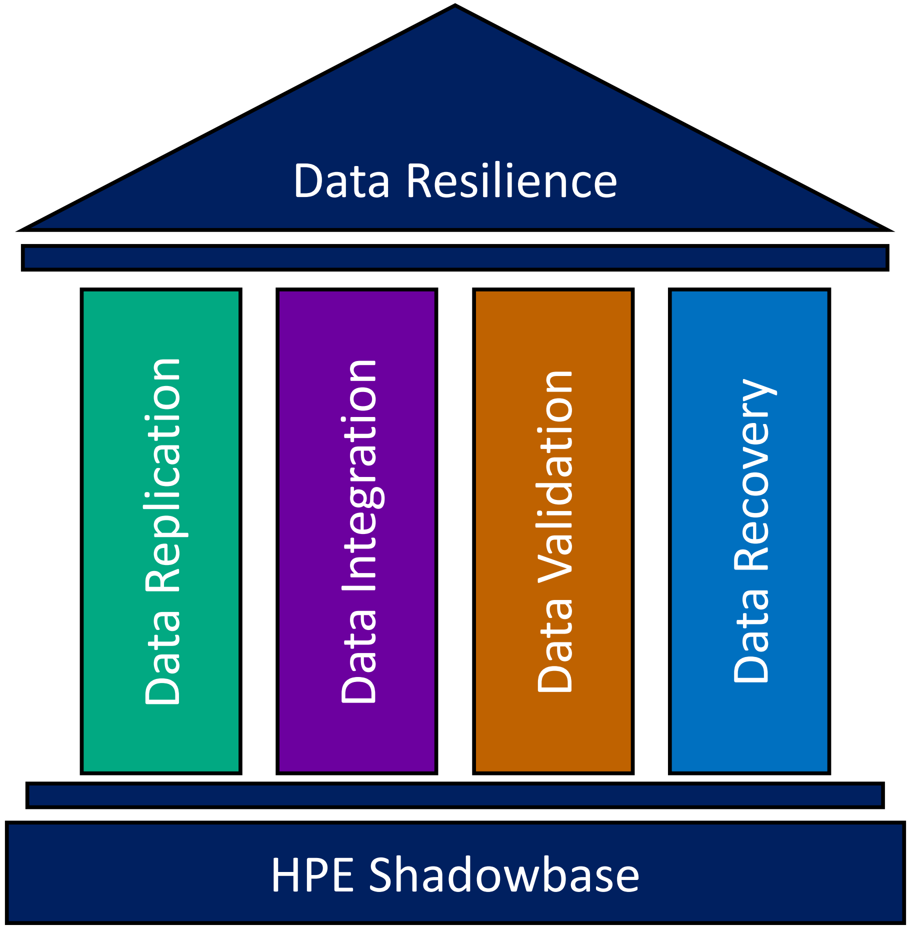
- **Is this solution really air-gapped?**
  1. Only open SFTP port…
  2. Transfer into IMMUTABLE STORAGE then to the \RRS
  3. Transfer via SNEAKER NET or tapes
  4. Etc.

- **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.

```
QueueSeqno = 7
QueueSeqno = 4
QueueRBA = 136132
QueueRBA = 458752
```

Wrap-up

Why customers choose HPE Shadowbase



What we hear from customers

- **HPE Shadowbase provides tremendous value**
  - Licensing and support aligned with NonStop (including GreenLake flexible capacity models)
  - Typically much less expensive
- **HPE Shadowbase has advanced features**
  - Ongoing innovation, including Data Recovery for Cybersecurity
- **HPE Shadowbase has outstanding support**
  - GNSC provides global, 24x7 coverage (with Gravic backup)
- **HPE Shadowbase is committed to NonStop**
  - Robust roadmap for NonStop and Other Servers
  - HPE's strategic, go-forward NonStop data replication solution

Learn more about HPE Shadowbase solutions

Wednesday, April 10th @ 9:15 h (Salon VI)

HPE Shadowbase Solutions:
New Innovation and Recent Customer Projects

Session topics:

- **HPE Shadowbase Solutions**
- **Recent Projects**
  - Data Replication Project (Rick S. from TCM presenting)
  - Data Migration Project (Anke M. from CSX Software presenting)
- **New innovation**
  - Zero Data Loss (ZDL) synchronous replication
  - Data Recovery for Cybersecurity
  - Cloud Integration
  - Roadmap

Thank you

Kenneth Scudder
KScudder@Gravic.com

GRAVIC®

1979 45 2024

Improving Society Through Innovation®