Digital Resilience strategies on HPE NonStop

Prashanth Kamath U

April 09, 2024

Hewlett Packard
Enterprise

Forward-looking statements

This is a rolling (up to three year) roadmap and is subject to change without notice.

- This document 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 document concerning these matters only reflect Hewlett Packard Enterprise's predictions and / or expectations as of the date of this document and actual results and future plans of Hewlett Packard Enterprise 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.

HPE confidential information

This is a rolling (up to three year) roadmap and is subject to change without notice.

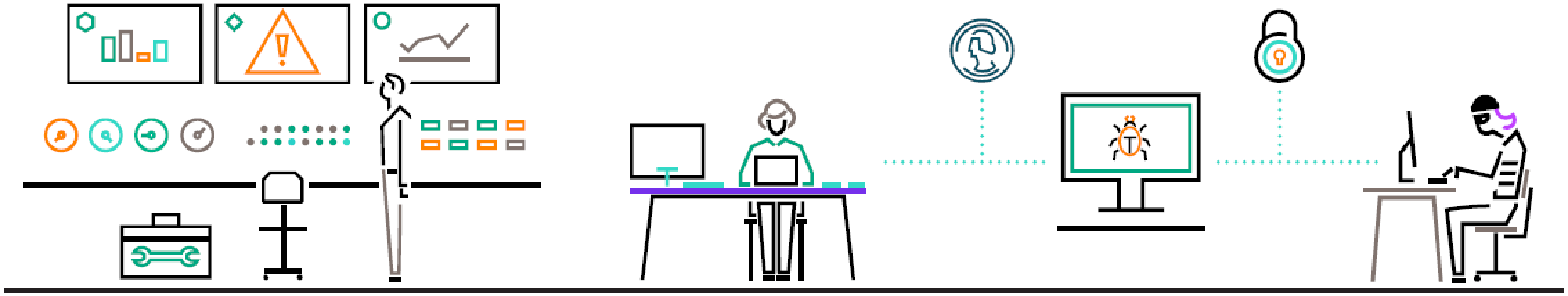
- This Roadmap contains Hewlett Packard Enterprise Confidential Information.
- If you have a valid Confidential Disclosure Agreement with Hewlett Packard Enterprise , disclosure of the Roadmap is subject to that CDA. If not, it is subject to the following terms: for a period of 3 years after the date of disclosure, you may use the Roadmap, which is subject to change at HPE's discretion without notice, solely for the purpose of evaluating product and service offerings from Hewlett Packard Enterprise and use a reasonable standard of care to prevent disclosures. You will not disclose the contents of the Roadmap to any third party unless it becomes publically known, rightfully received by you from a third party without duty of confidentiality, or disclosed with Hewlett Packard Enterprise's prior written approval.

Agenda

- Cybersecurity trends – 2024
- Ransomware threat – why is it important?
- Protect against ransomware – Cybersecurity strategies
- Protect against ransomware – Recovery strategies
- Conclusion

Ransomware attack trends - 2024

- New technologies such as AI have lowered technology bar for Cybercriminals
- Supply chain attacks gaining momentum due to the extension of blast radius
- Newer business models – Ransomware as a Service
- Capabilities most commonly used for initial access[1]
  - Exploitation of Remote Services
  - Brute Force
  - Phishing
  - Valid Accounts
  - Stage Capabilities: SEO Poisoning



[1] Mitigating Cyber Risks with Mitre Att&cks: https://start.paloaltonetworks.com/2023-unit42-mitre-attack-recommendations

Ransomware—Some statistics

24%

of all cyber attacks were ransomware[1]

24

days—Average downtime due to ransomware attack[3]

$4.5M

Average cost of ransomware attack[2]

1/3

Amount of those who paid ransom that were unable to recover all data[2]

[1] “Verizon Data Breach Investigation Report 2023: www.verizon.com/business/resources/T4c5/reports/2023-data-breach-investigations-report-dbir.pdf

[2] “Cost of a data breach 2022,” IBM, 2022.

[3] [3] Statistica: https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack-global/

Regulatory actions/recommendations

- fbi.gov
  - Keep operating systems, software, and applications current and ***up to date***.
  - Make sure ***anti-virus and anti-malware*** solutions are set to automatically update and run regular scans.
  - ***Back up data*** regularly and double-check that those backups were completed.
  - ***Secure your backups. Make sure they are not connected to the computers and networks they are backing up.***
  - ***Create a continuity plan in case your business or organization is the victim of a ransomware attack***.

- fca.org.uk
  - National Crime Agency (NCA) strongly advises you not to pay
  - Regularly review the controls
  - Provide your staff with continuous cyber resilience training
  - Identify and resolve your vulnerabilities quickly
  - Regularly check that your cyber incident response plans
  - **Maintain adequate secure backups of data and system configuration**
  - **Make sure you know which systems and data is required to recover your business**

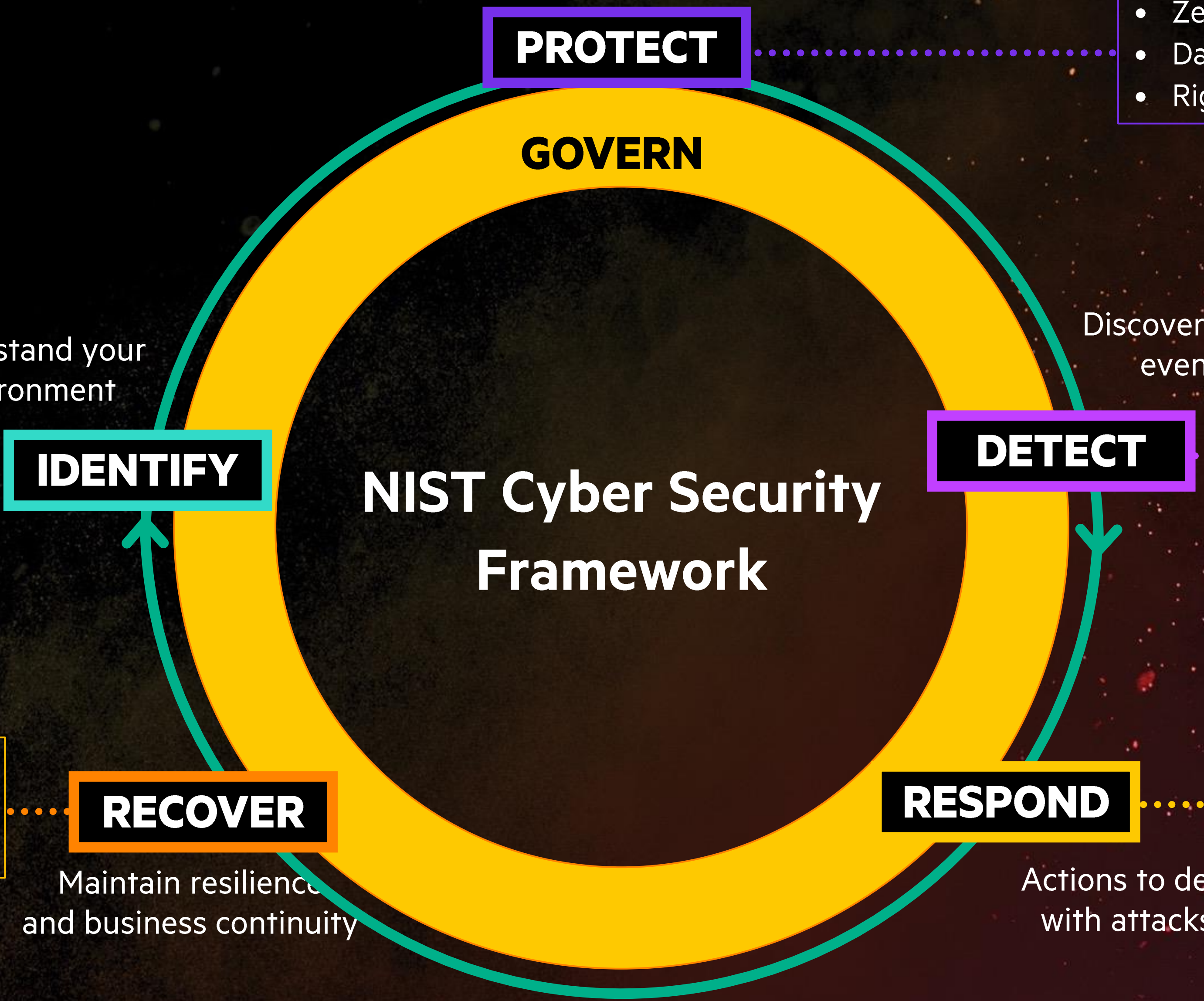
- **eur-lex.europa.eu**
- ***Digital Operational Resilience Act (DORA)***
- ***Coverage***
  - ICT Risk management
  - ICT-related incident management, classification and reporting
  - ***Digital operational resilience testing***
  - ***Managing of ICT third-party risk***
  - Information-sharing arrangements

Digital Operational Resilience Act (DORA)

Important notes

- *Is a Regulation, not a Directive, so it is binding in its entirety and directly applicable in all EU Member States*
- Shall apply from ***17 January 2025***
- ***Key requirements***
  - Establishment of an **independent control function** for managing and overseeing ICT risks
  - Resources and capabilities to ***monitor user activity, the occurrence of ICT anomalies and ICT-related incidents***, in particular cyber-attacks
  - Financial entities ***shall set up backup systems that can be activated*** in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods.
  - When ***restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system***
  - Tests are undertaken by independent parties to ensure that the systems perform as expected under simulated conditions of a cyber attack
  - Scope of services and data protection practices to be followed by ICT service providers

NIST Cyber Security Framework



Implement safeguards and controls

- Zero Trust Security
- Data Protection
- Rigorous security hardening

Understand your environment

- Identify assets to protect

Discover cyber events

- Monitor activity (use AI/ML)
- Monitor environment integrity

- Data backup & recovery strategy
- Implement 3-2-1-1 rule

Maintain resilience and business continuity

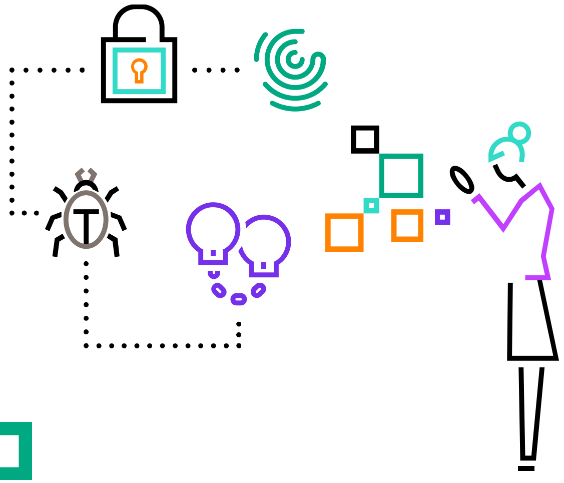
- Standard operating procedures

Actions to deal with attacks

Protection and Recovery – two pillars of digital resilience

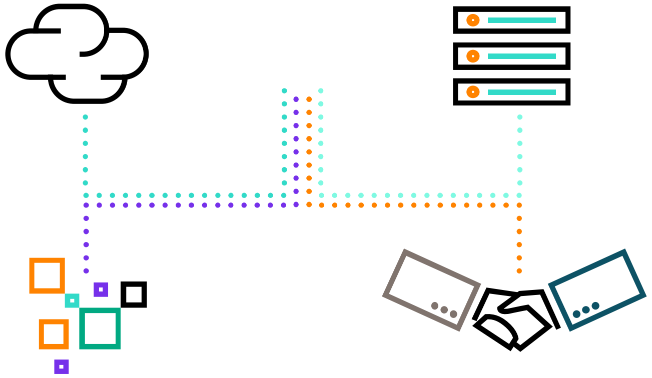
Protect and Monitor

- Implement a robust IAM solution
- Rigorous control to resources
- Protect data at rest and in motion
- Monitor
  - Tamper attempts
  - In consonance with other Enterprise IT systems
  - Use AI/ML



Recover workload and data

- Be “back on your feet” after an attack
- Maintain an isolated infrastructure
  - Keep it up to date w.r.t. image and data
  - To be used exclusively for recovery
- Maintain a recovery playbook and exercise it regularly

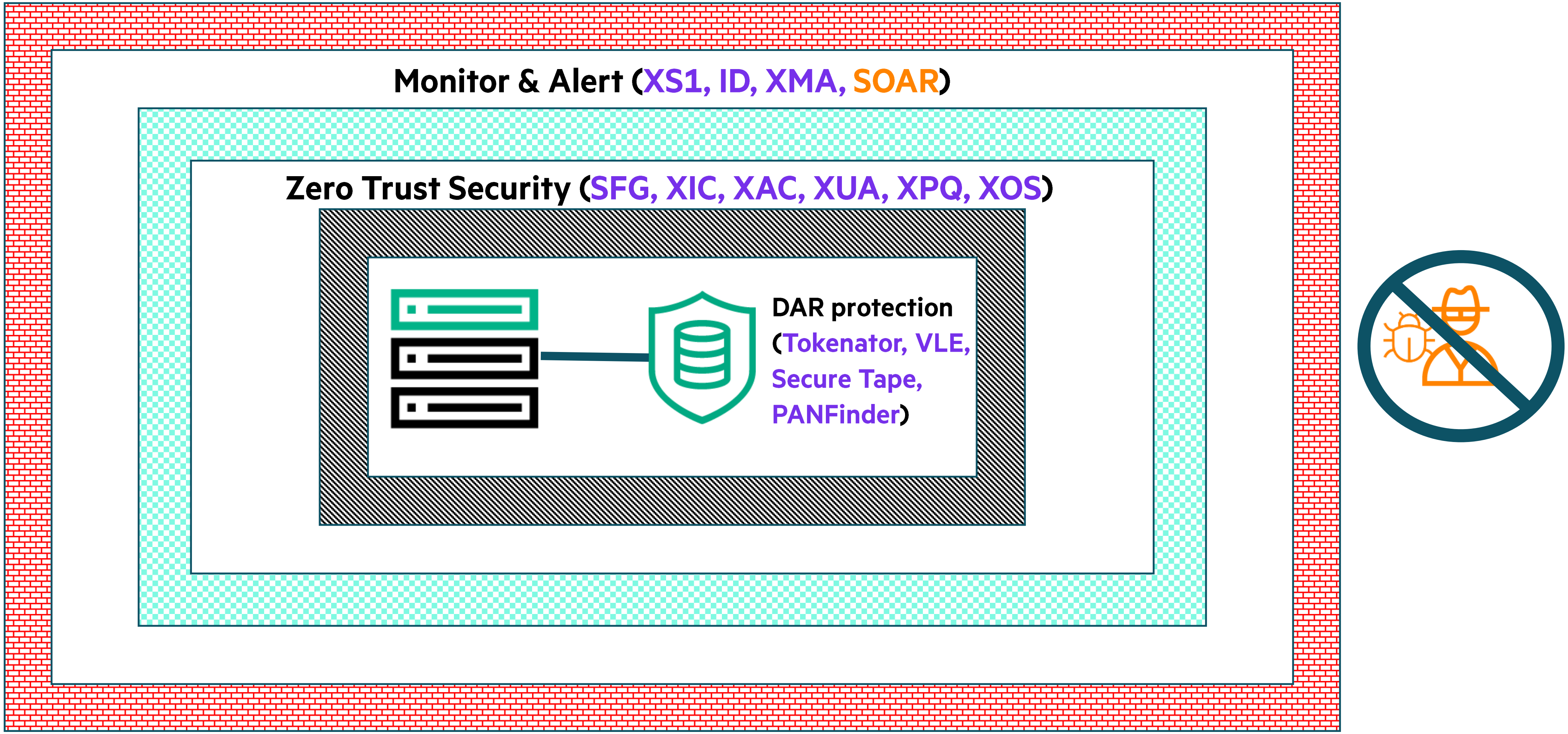


Digital resilience strategies for HPE NonStop

Protect & Detect

Multi-tier protection of NonStop environment

HPE NonStop products
Industry standard products



Perimeter defense (Firewall, IPS)

Monitor & Alert (XS1, ID, XMA, SOAR)

Zero Trust Security (SFG, XIC, XAC, XUA, XPQ, XOS)

DAR protection
(Tokenator, VLE,
Secure Tape,
PANFinder)

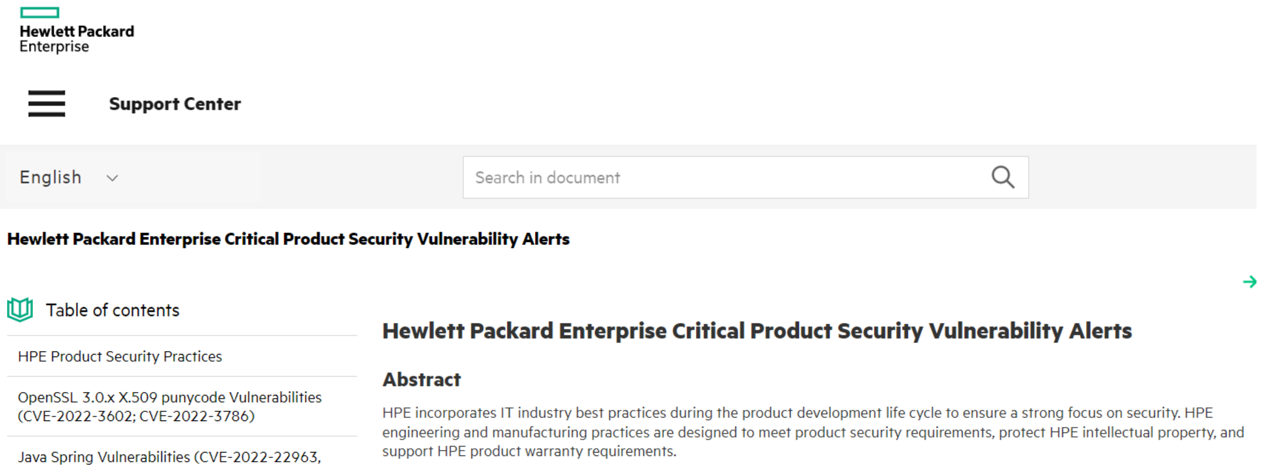
HPE NonStop Security Hardening Guide

- A comprehensive guide on how to secure
  - HPE NonStop system
  - HPE NonStop software
- A live document
- Used as a reference by security monitoring products such as XS1
- Highly recommended read for NonStop users and administrators
- Refer security hardening recommendations of ISV products

HPE Vulnerability bulletins

Subscribe & Act

- HPE has a consolidated external web page for security vulnerability information:
  - https://www.hpe.com/us/en/services/security-vulnerability.html
- The site includes:
  - HPE-wide customer advisories for the vulnerabilities of highest general concern
  - Archive of past security bulletins
  - A link to report a security vulnerability
- Hotstuffs continue to be available from the NonStop eServices portal (Scout)
- Subscribe to both these services to receive immediate alerts on product security issues



Hewlett Packard Enterprise Critical Product Security Vulnerability Alerts

Table of contents

HPE Product Security Practices

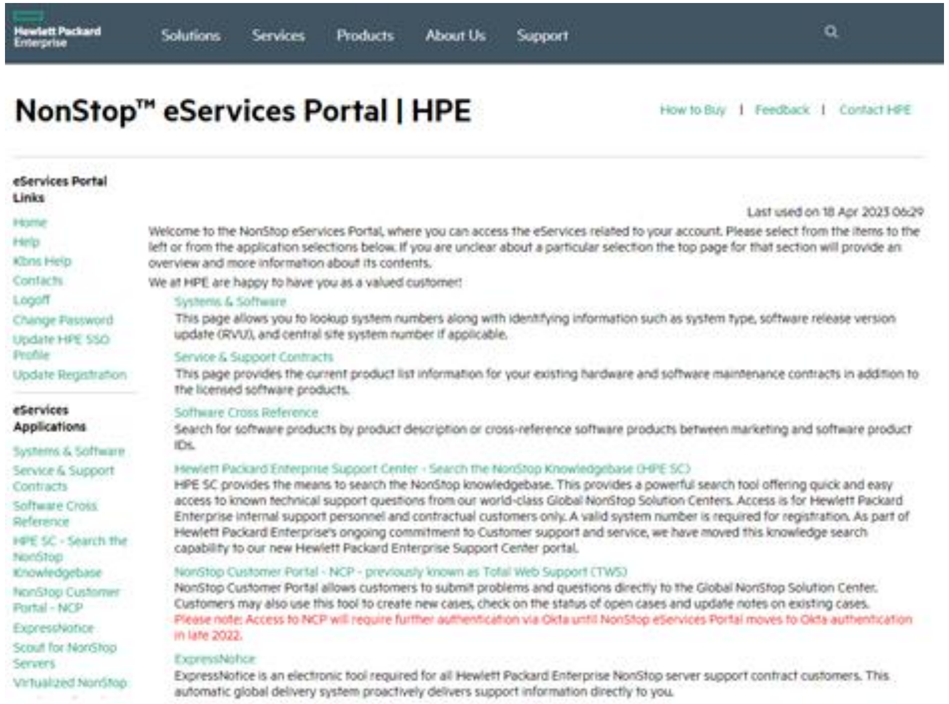
OpenSSL 3.0.x X.509 punycode Vulnerabilities (CVE-2022-3602; CVE-2022-3786)

Java Spring Vulnerabilities (CVE-2022-22963,

Hewlett Packard Enterprise Critical Product Security Vulnerability Alerts

Abstract

HPE incorporates IT industry best practices during the product development life cycle to ensure a strong focus on security. HPE engineering and manufacturing practices are designed to meet product security requirements, protect HPE intellectual property, and support HPE product warranty requirements.



NonStop™ eServices Portal | HPE

Last used on 18 Apr 2023 06:29

Welcome to the NonStop eServices Portal, where you can access the eServices related to your account. Please select from the items to the left or from the application selections below. If you are unclear about a particular selection the top page for that section will provide an overview and more information about its contents.

We at HPE are happy to have you as a valued customer!

Systems & Software

This page allows you to lookup system numbers along with identifying information such as system type, software release version update (RVU), and central site system number if applicable.

Service & Support Contracts

This page provides the current product list information for your existing hardware and software maintenance contracts in addition to the licensed software products.

Software Cross Reference

Search for software products by product description or cross-reference software products between marketing and software product IDs.

Hewlett Packard Enterprise Support Center - Search the NonStop Knowledgebase (HPE SC)

HPE SC provides the means to search the NonStop knowledgebase. This provides a powerful search tool offering quick and easy access to known technical support questions from our world-class Global NonStop Solution Centers. Access is for Hewlett Packard Enterprise internal support personnel and contractual customers only. A valid system number is required for registration. As part of Hewlett Packard Enterprise's ongoing commitment to Customer support and service, we have moved this knowledge search capability to our new Hewlett Packard Enterprise Support Center portal.

NonStop Customer Portal - NCP - previously known as Total Web Support (TWS)

NonStop Customer Portal allows customers to submit problems and questions directly to the Global NonStop Solution Center. Customers may also use this tool to create new cases, check on the status of open cases and update notes on existing cases.
Please note: Access to NCP will require further authentication via Okta until NonStop eServices Portal moves to Okta authentication in late 2022.

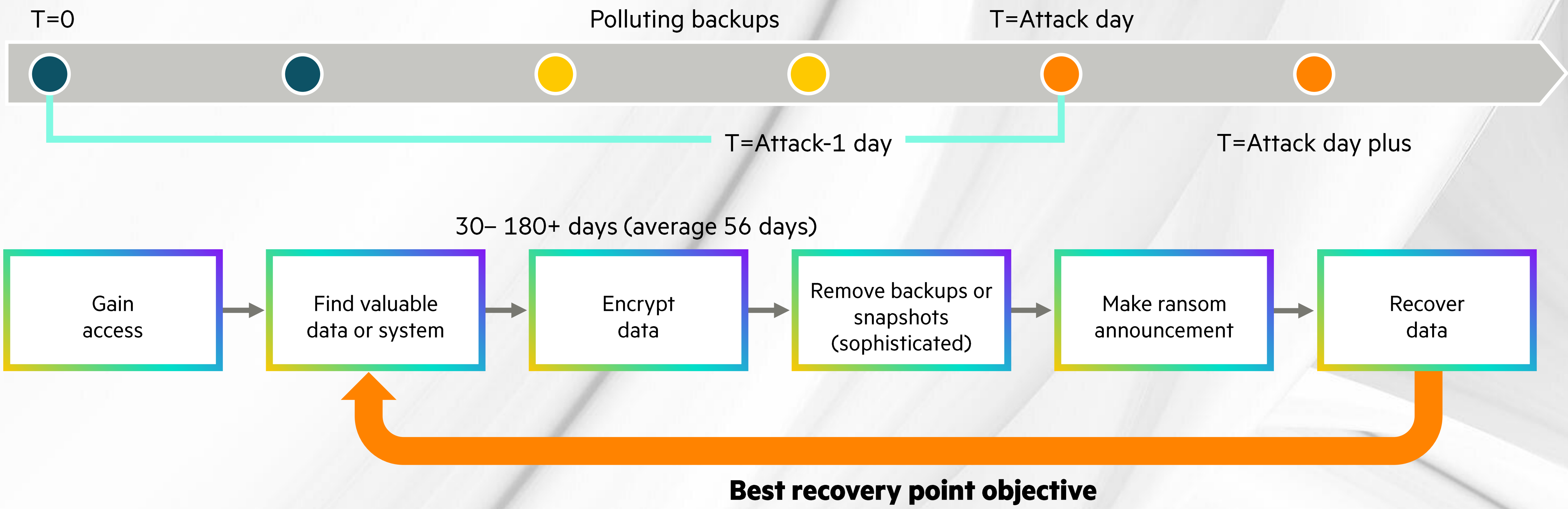
ExpressNotice

ExpressNotice is an electronic tool required for all Hewlett Packard Enterprise NonStop server support contract customers. This automatic global delivery system proactively delivers support information directly to you.

Digital resilience strategies for HPE NonStop

Respond & Recover

Ransomware attack


T=0
Polluting backups
T=Attack day
T=Attack-1 day
T=Attack day plus
30– 180+ days (average 56 days)
Gain access
Find valuable data or system
Encrypt data
Remove backups or snapshots (sophisticated)
Make ransom announcement
Recover data
Best recovery point objective

Terminologies

Immutable

- Data that can only be written, not modified or deleted.

Resilient site

- Be isolated from the existing Production and DR site to facilitate a “clean” recovery environment in the event of a Cyberattack

Air gapped systems

- An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control).

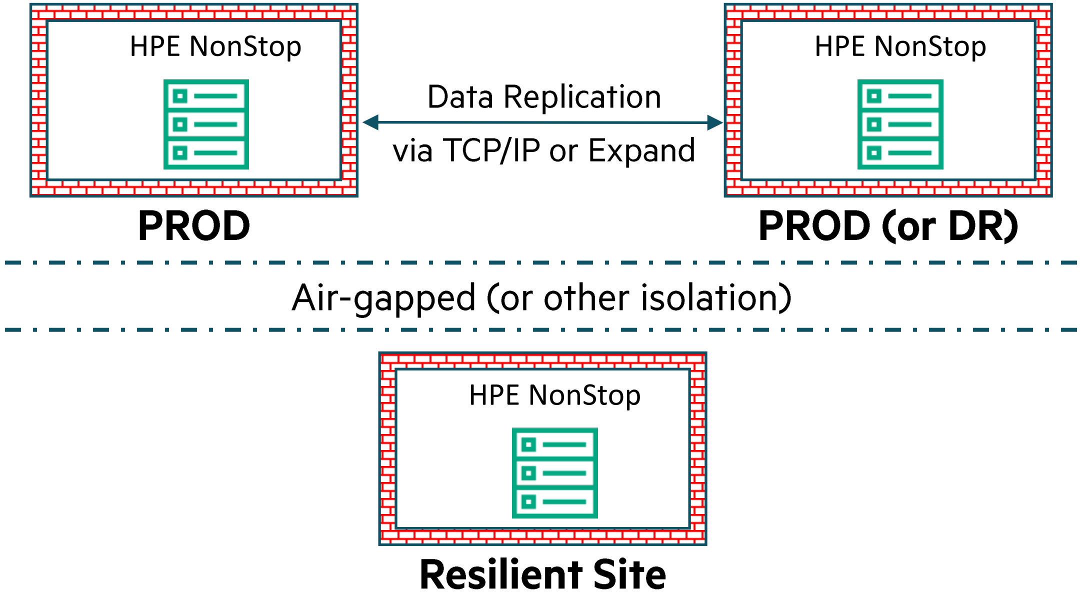
Note: A strict interpretation as above will pose severe challenge to RPO and RTO. A configuration with controlled and intermittent connection can be an alternative

3-2-1-1 rule

- Maintain three copies of data, on two separate media for backup storage, one offsite backup storage location (online) PLUS an offsite backup storage location (offline/air gapped).

Digital Resilience – Need for a resilient site

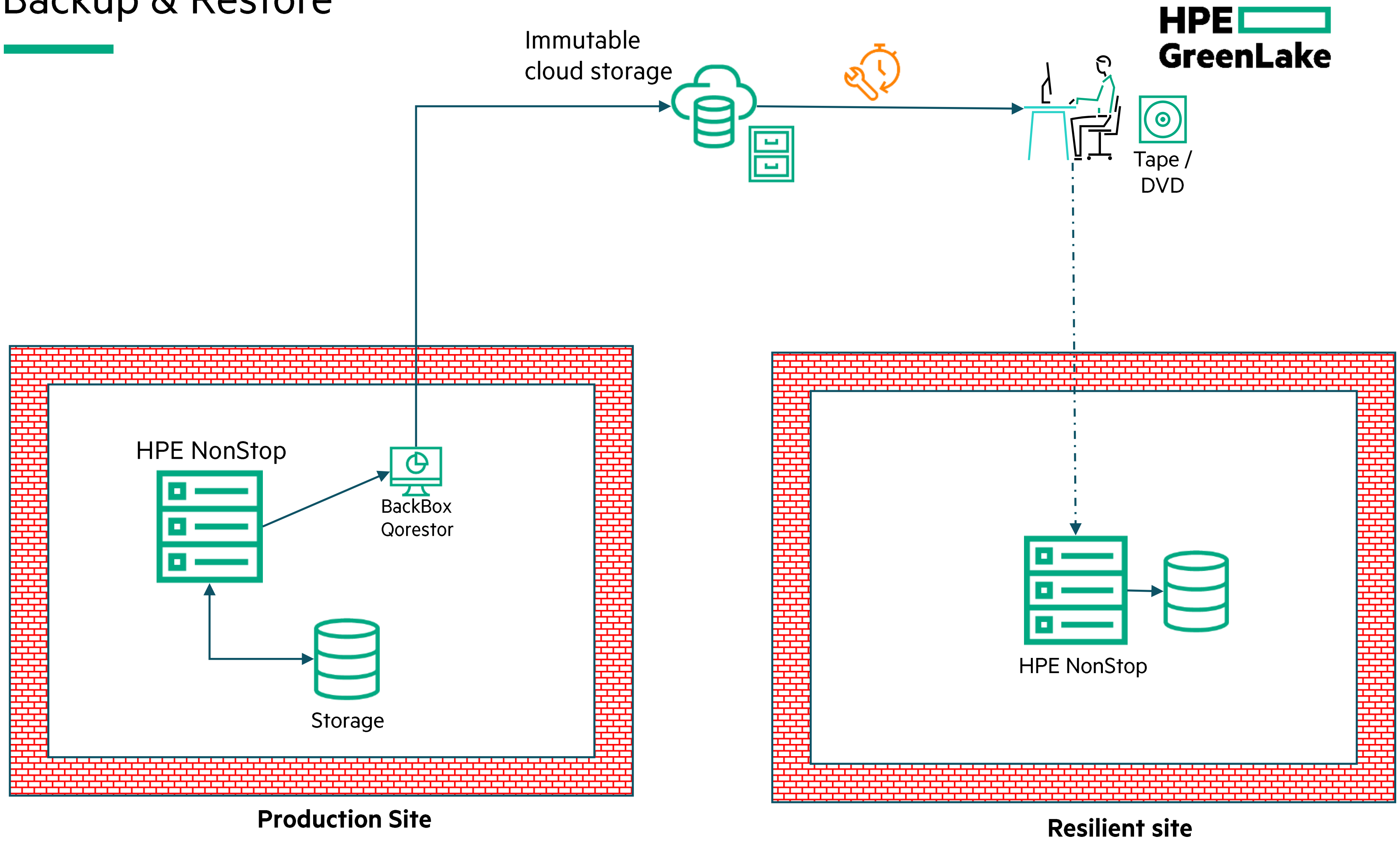
Digital Resilience architecture components



- **Why resilient site**
  - The primary objective of the attacker is to neutralize the ability to recover using shadow copies of data
  - The attacker moves laterally within the enterprise and deletes/encrypts all possible copies of data
- **What is a resilient site?**
  - Has resources to take over the workload in the case of an attack (Infected site is available for forensics)
  - Hosted at an “air gapped” site
  - Managed by a different set of personnel
  - Has clean copies of SW images
  - Has clean copies of data at different points of time

Ransomware Recovery: Option 1

Backup & Restore



Strengths

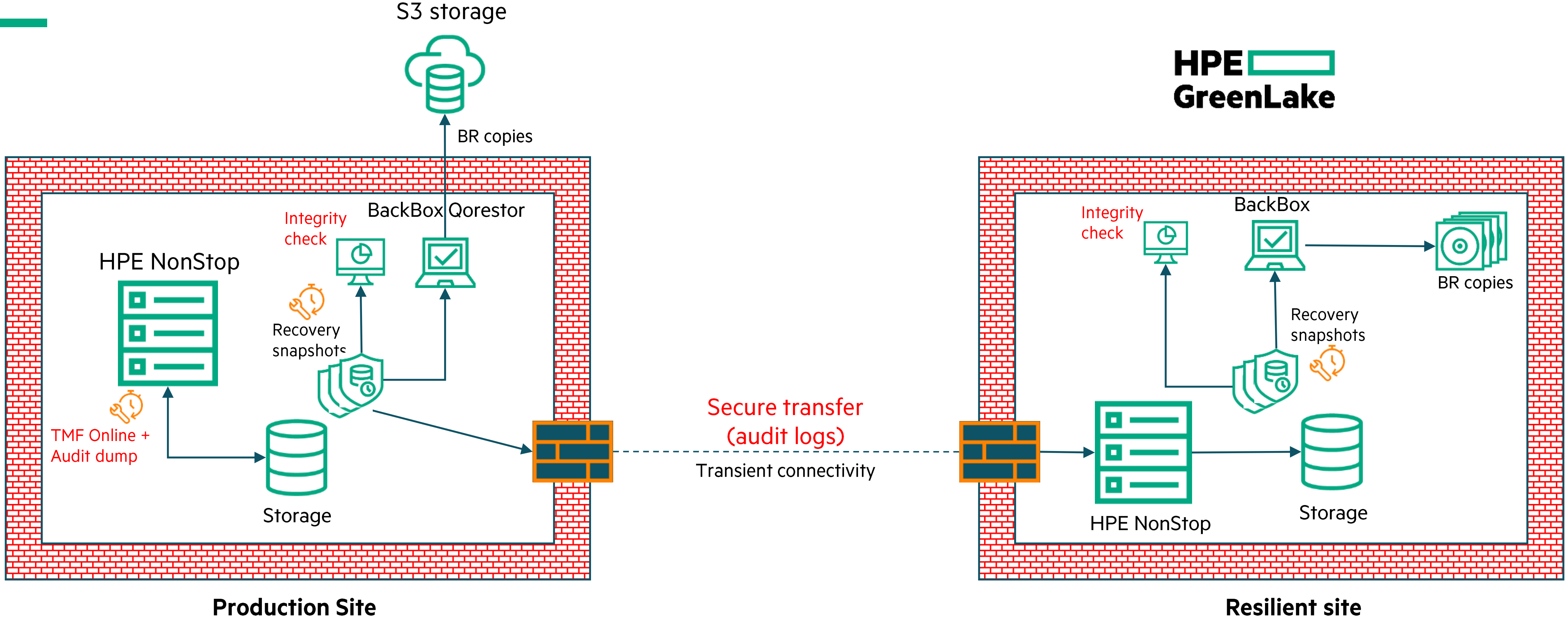
- Easy to implement
- Has no specific product dependency
- Little or no new solutions required

Challenges

- Long recovery period
- Limited frequency (BR is not online)
- A successful attack may go undetected (deep backups is the only option)
- Long RTO and RPO

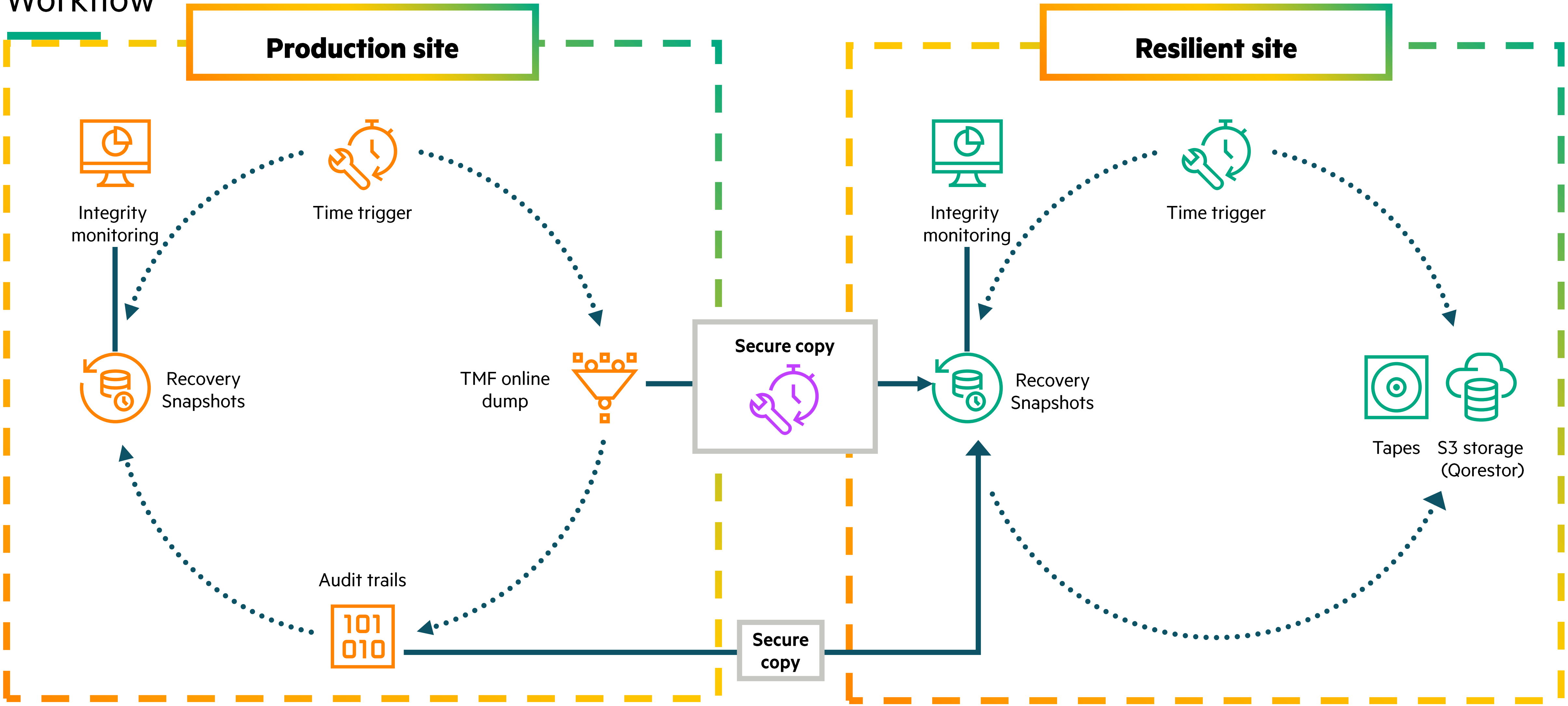
Ransomware recovery– Option 2

HPE TMF



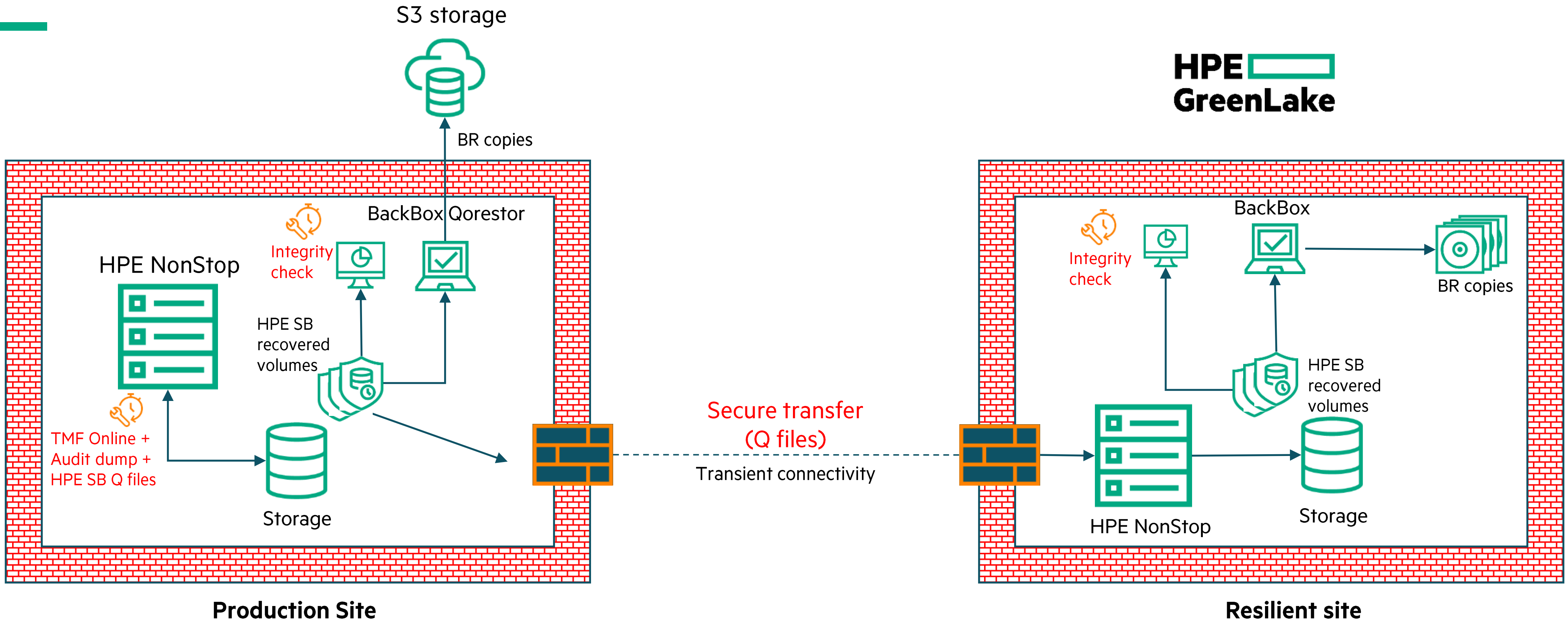
Ransomware Recovery: Option 2

Workflow



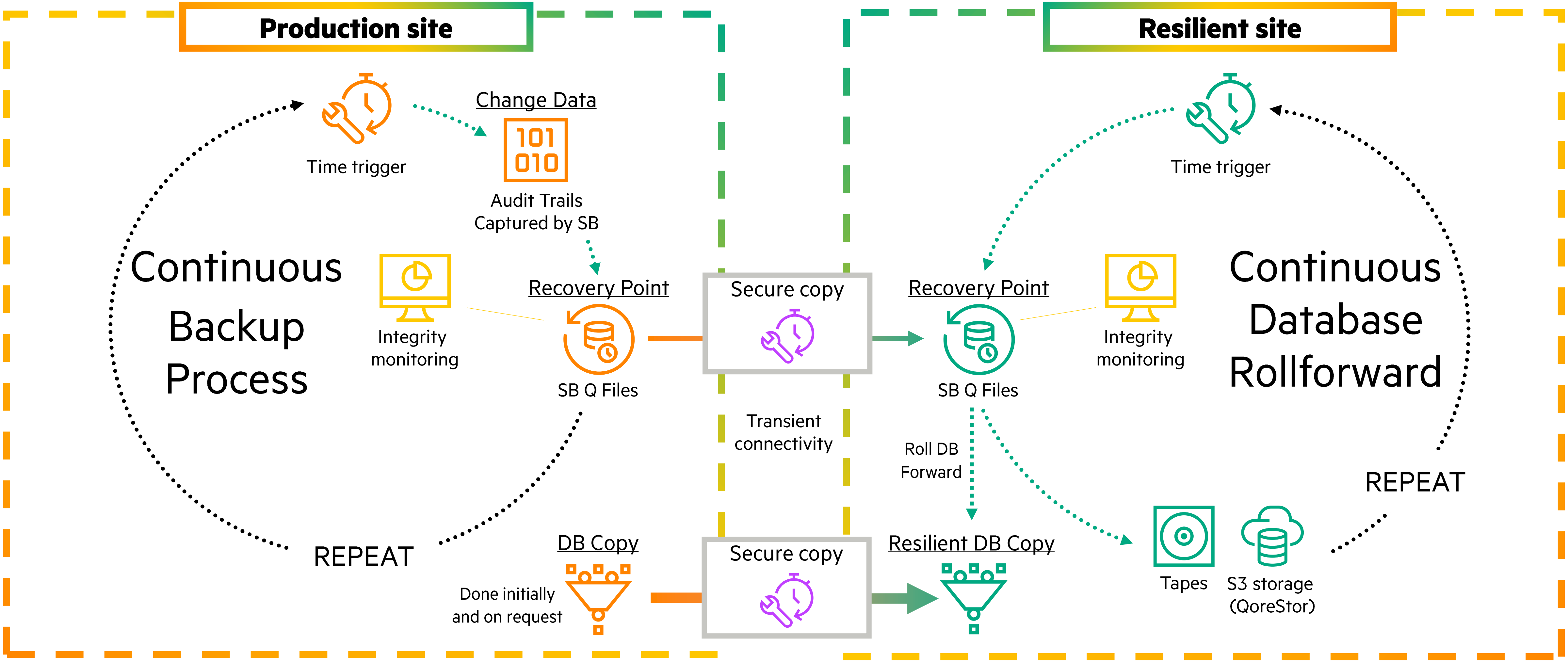
Ransomware recovery– Option 3

HPE Shadowbase Q files



Digital Resilience Data Recovery: Option 3

Shadowbase Q File Recovery



Services

Avail advice and services of experts

Rapid Security assessment

- 120+ different security vectors evaluated in 6 key categories
- Single executable, nothing to install, easy to run
- No sensitive data
- Findings report and recommendations provided
- Free Service!!

Hardening & compliance

- PAN Data Discovery
- Security Implementation and Configuration
- PCI DSS Compliance Assistance

Resilient site managed service

- Hosting services
- Ransomware recovery playbook
- Patching & upkeep
- Data recovery cadence
- Period tests for readiness

Thank you!