HPE NonStop Security and Ransomware Protection

Prashanth Kamath U

May 17, 2023

Hewlett Packard Enterprise

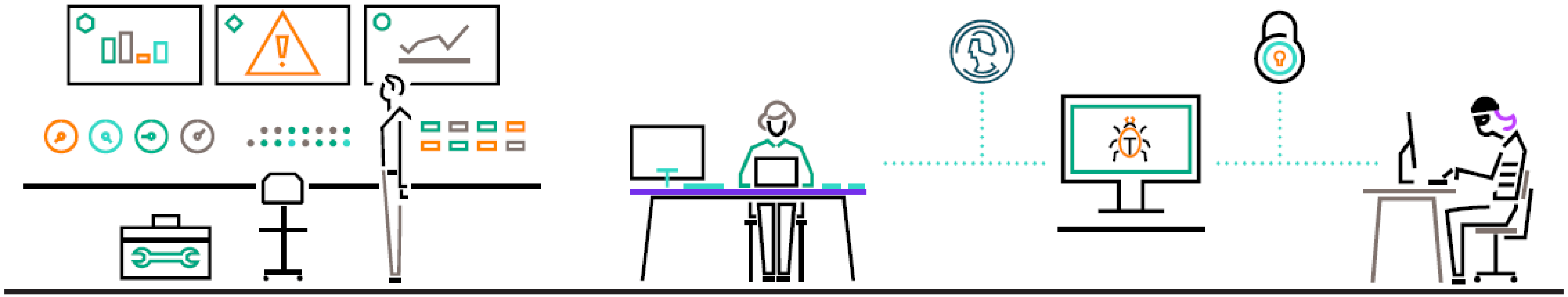
E-BITUG
European NonStop Symposium
EDINBURGH 2023

Agenda

- Cybersecurity trends – 2023
- Ransomware – a challenging Cybersecurity threat
  - Regulatory actions
  - Compliance options on HPE NonStop
- Security updates & Futures
- Conclusion

Cybersecurity trends - 2023

- Phishing remains an epidemic
- Ransomware attacks are getting simpler than ever
- Hostile nation states are on the rise
- Insider attacks are increasing
- Vulnerabilities hit a record high
- Supply fabric complicates security



Ransomware—Some statistics

76%

of organizations targeted by a ransomware attack[1]

22

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] "New cyberattack tactics rise up as ransomware payouts increase," CSO Online, February 2023.
[2] "Cost of a data breach 2022," IBM, 2022.
[3] "Cyber Crime & Security," Statista.

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.*

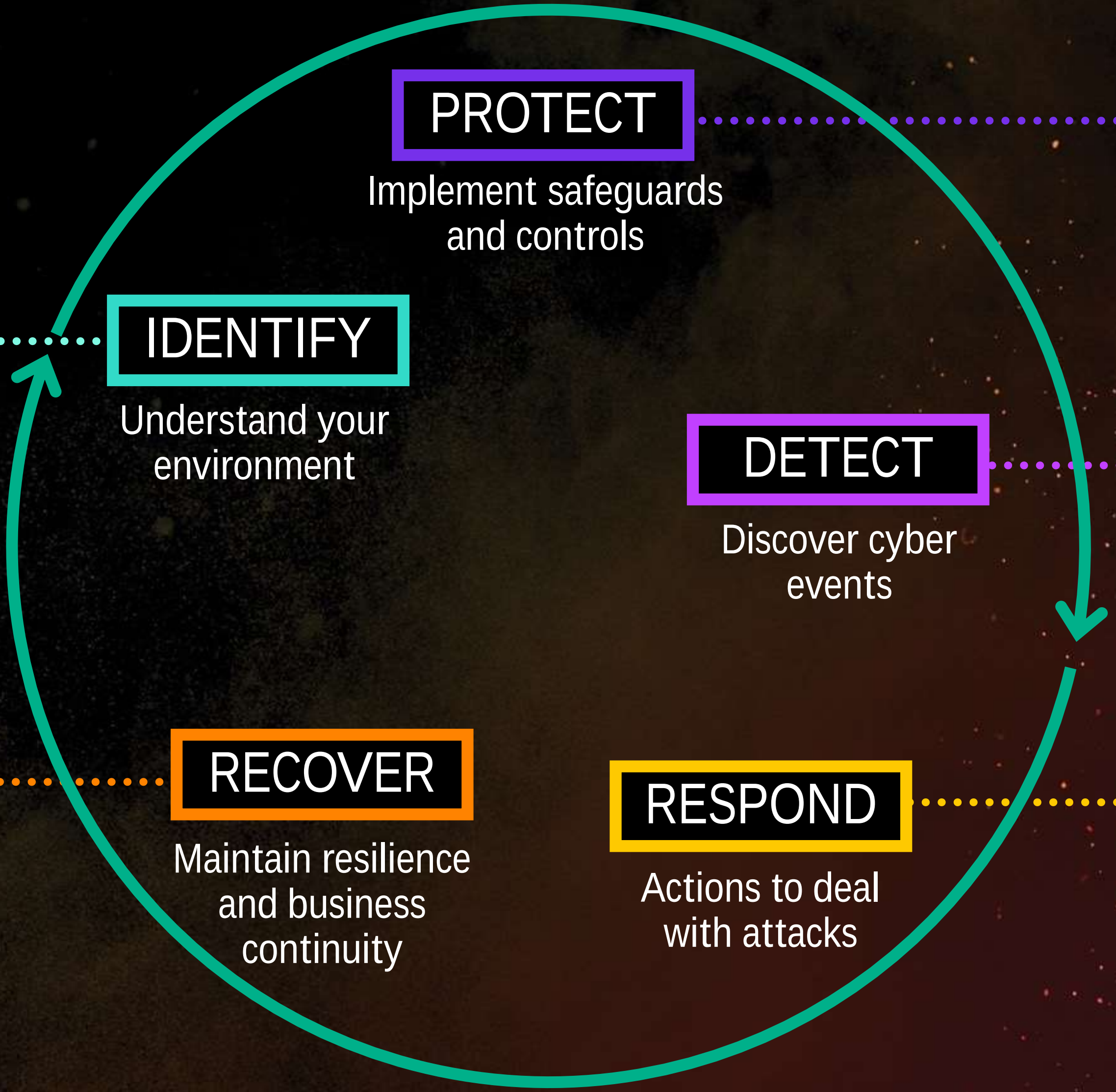
- fca.org.uk
  - National Crime Agency (NCA) strongly advises you not to pay
  - Regularly review the controls
  - Provide your staff with continuous cyber resilience training
  - Identify and resolve your vulnerabilities quickly
  - Regularly check that your cyber incident response plans
  - Maintain 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

HPE Digital Resiliency Framework



IDENTIFY

Understand your environment

- Identify assets to protect

PROTECT

Implement safeguards and controls

- Zero Trust Security
- Data Protection
- Rigorous security hardening

DETECT

Discover cyber events

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

RESPOND

Actions to deal with attacks

- Standard operating procedures

RECOVER

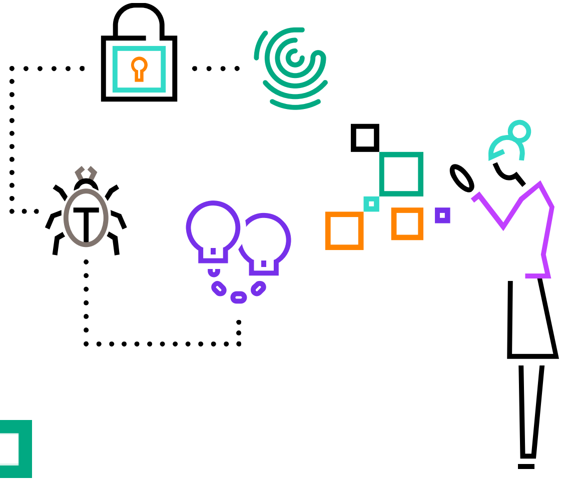
Maintain resilience and business continuity

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

Protection and Recovery – two pillars of digital resilience

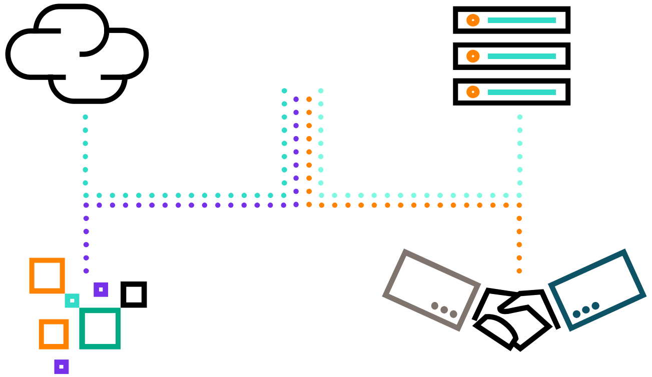
Protect and Monitor

- Fine grained access control
- MFA for system access
- Integrate user management with Enterprise IAM
- File Integrity Monitoring
- Data protection – at rest and in transit
- Security monitoring
  - AI/ML driven
  - Integrated with enterprise SOAR



Business continuity

- A DR infrastructure for business continuity in the event of a Cyberattack
- Isolated infrastructure for managing recovery resources and spring back to service
  - Recommended to also isolate it administratively
- Simulated tests run regularly and under supervision of neutral experts



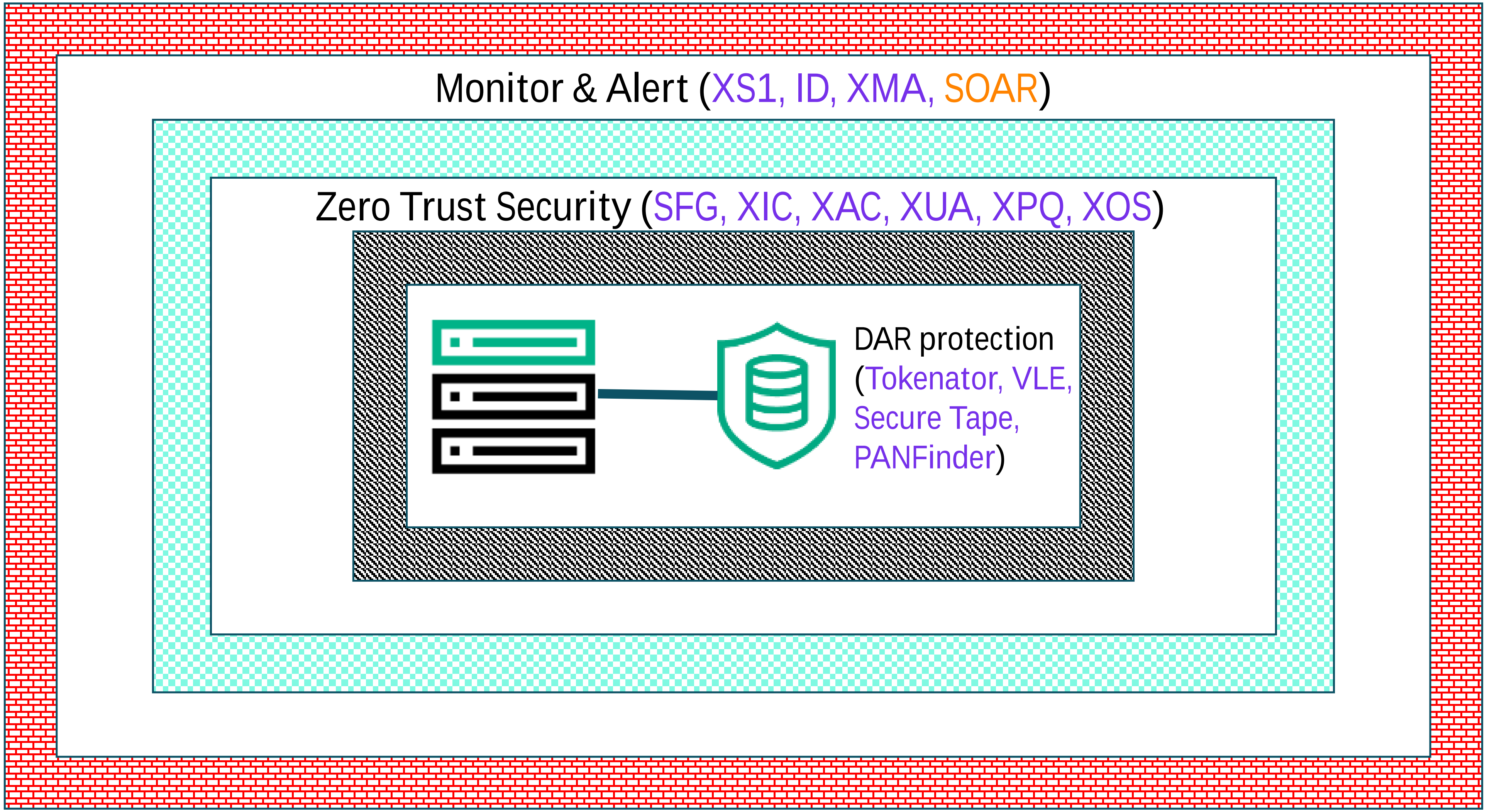
Digital resilience strategies for HPE NonStop

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)

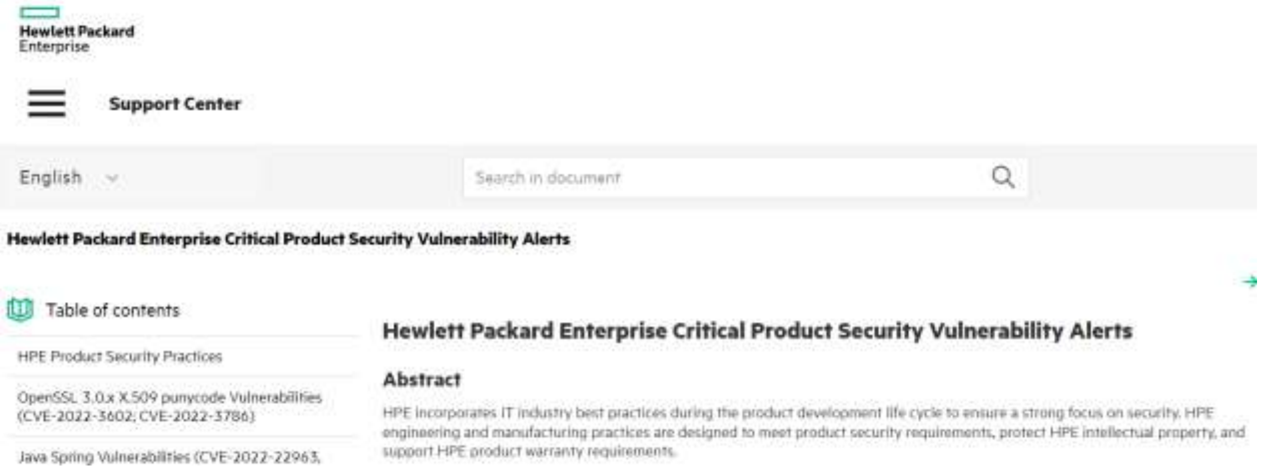
DAR protection (Tokenator, VLE, Secure Tape, PANFinder)

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 admins
- Refer security hardening recommendations of ISV products

HPE Vulnerability bulletins
Subscribe & Act

- HPE now 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

HPE Product Security Practices

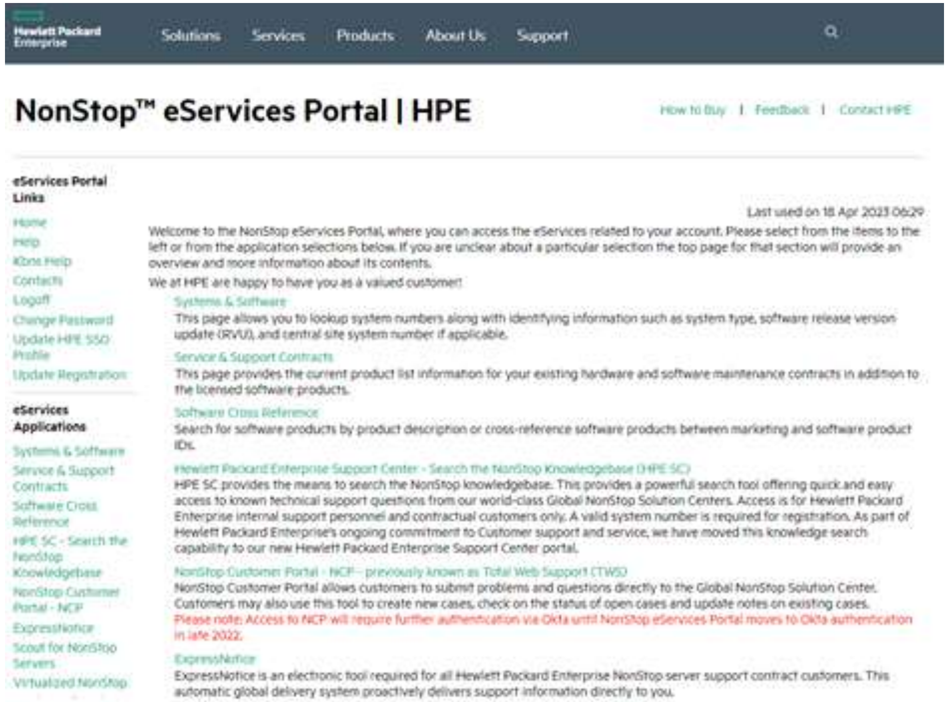
OpenSSL 3.0.x X.509 punycode Vulnerabilities (CVE-2022-3602; CVE-2022-3786)

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

Terminologies

Immutable

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

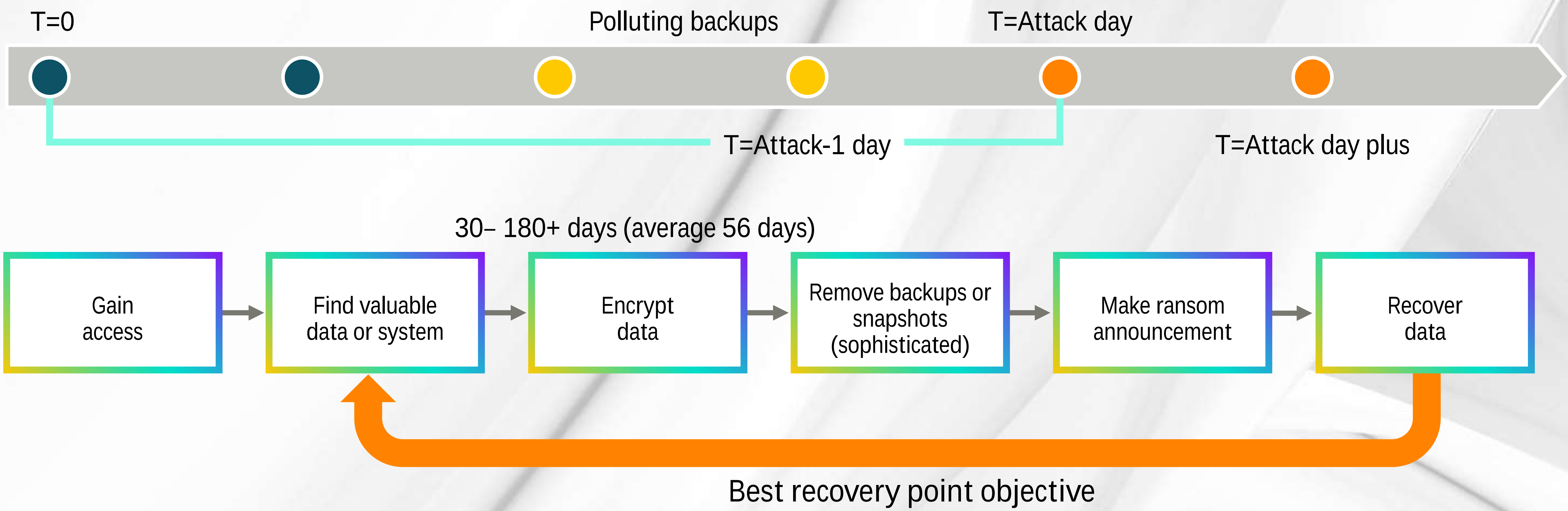
Air gapped systems

- 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).

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).

Ransomware attack



T=0

Polluting backups

T=Attack day

T=Attack-1 day

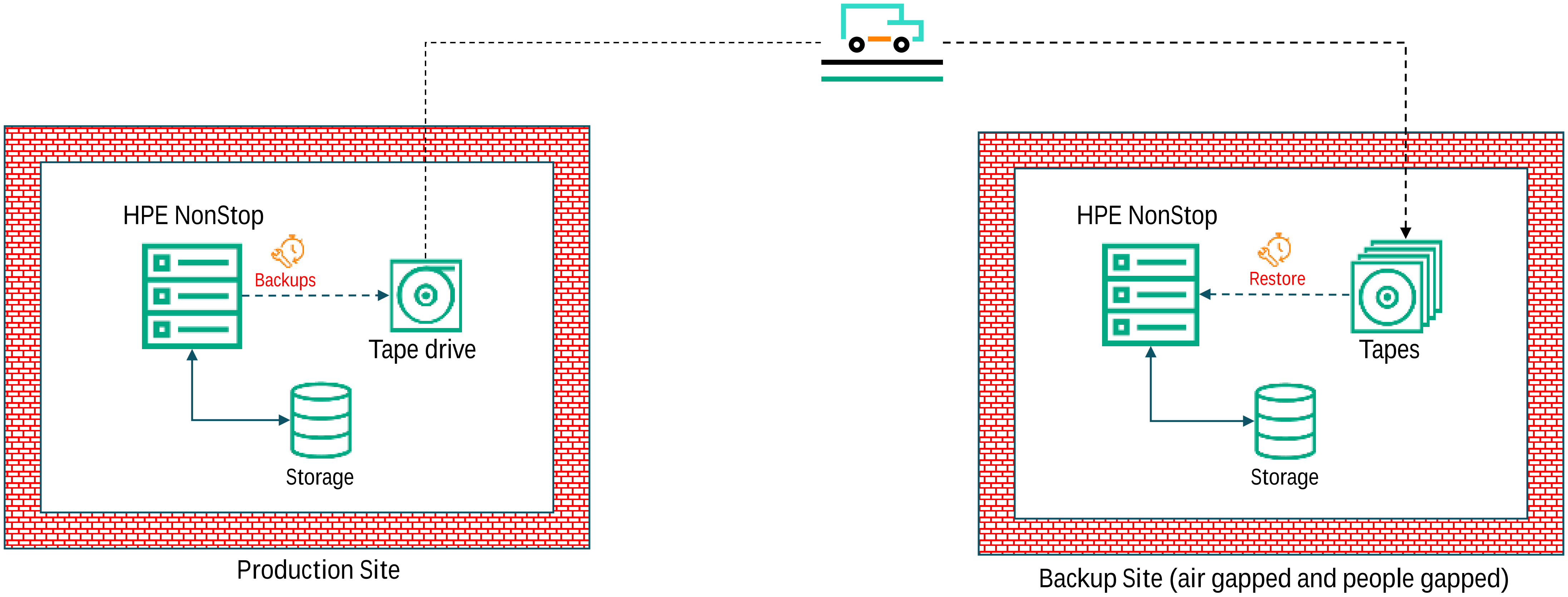
T=Attack day plus

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

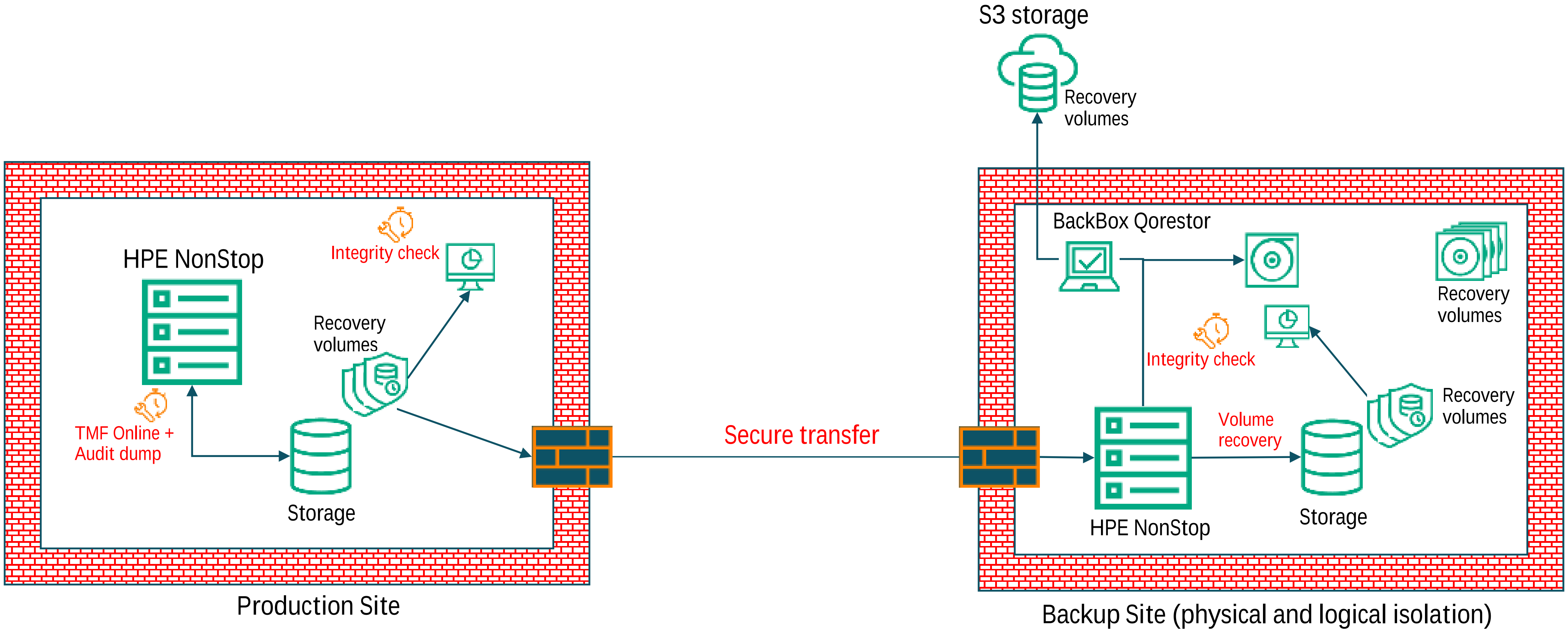
Best recovery point objective

Ransomware recovery – option 1

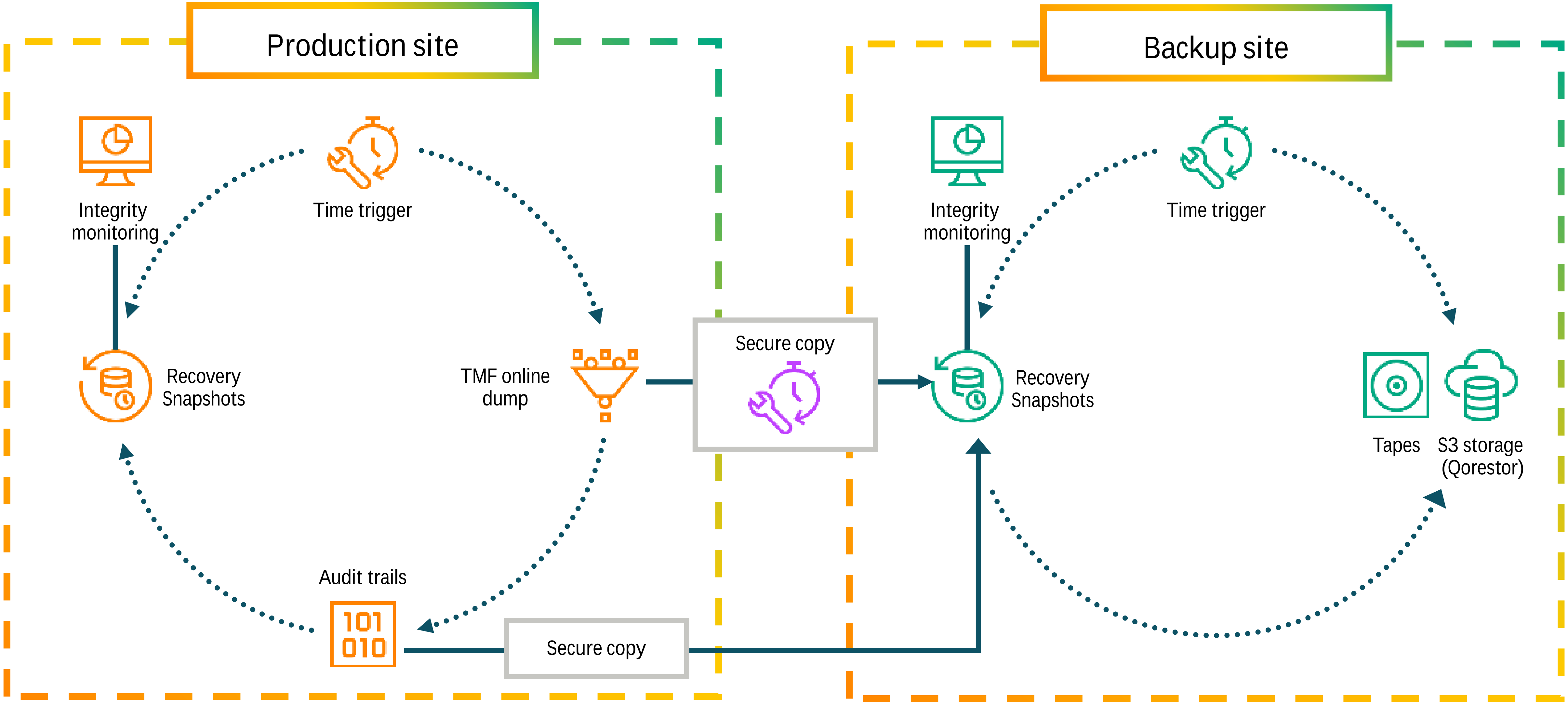


Ransomware recovery– option 2

3-2-1-1 rule as translated to NonStop

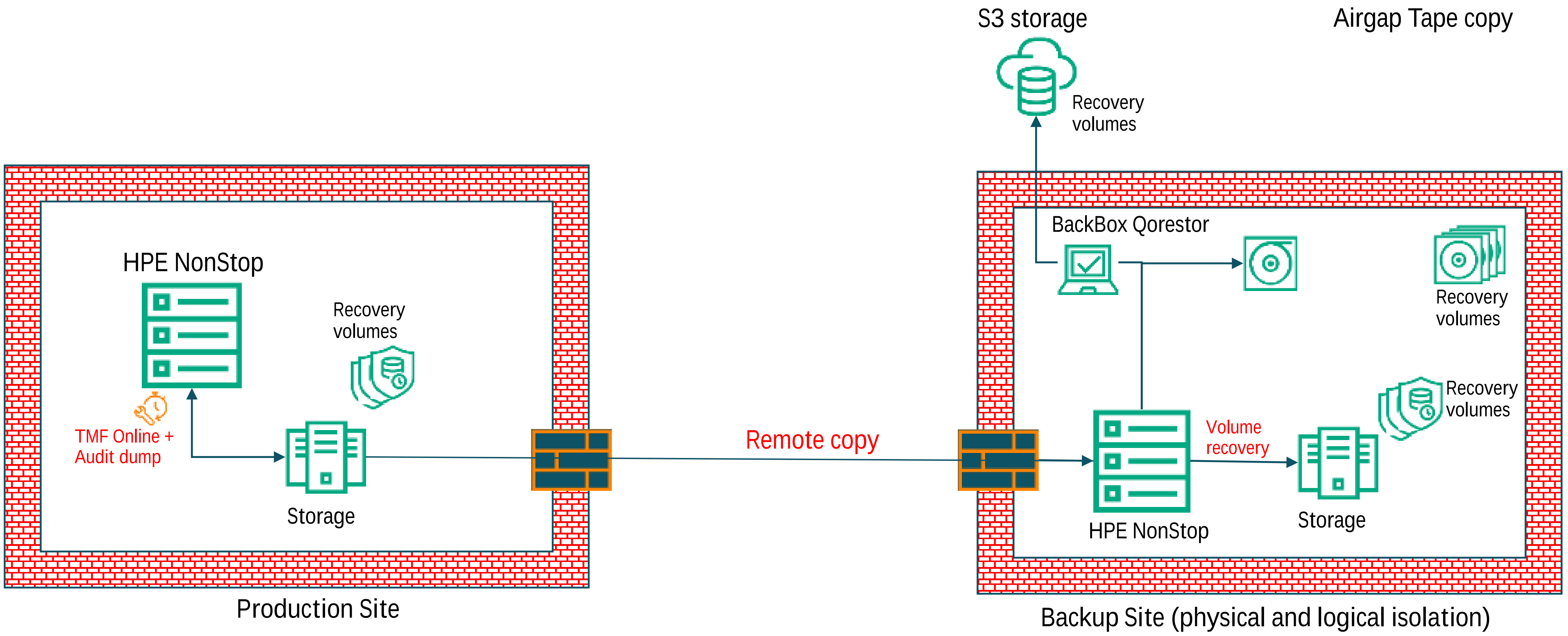


Workflow


Production site
Integrity monitoring
Time trigger
Recovery Snapshots
TMF online dump
Audit trails
Secure copy
Secure copy
Backup site
Integrity monitoring
Time trigger
Recovery Snapshots
Tapes
S3 storage (Qorestor)

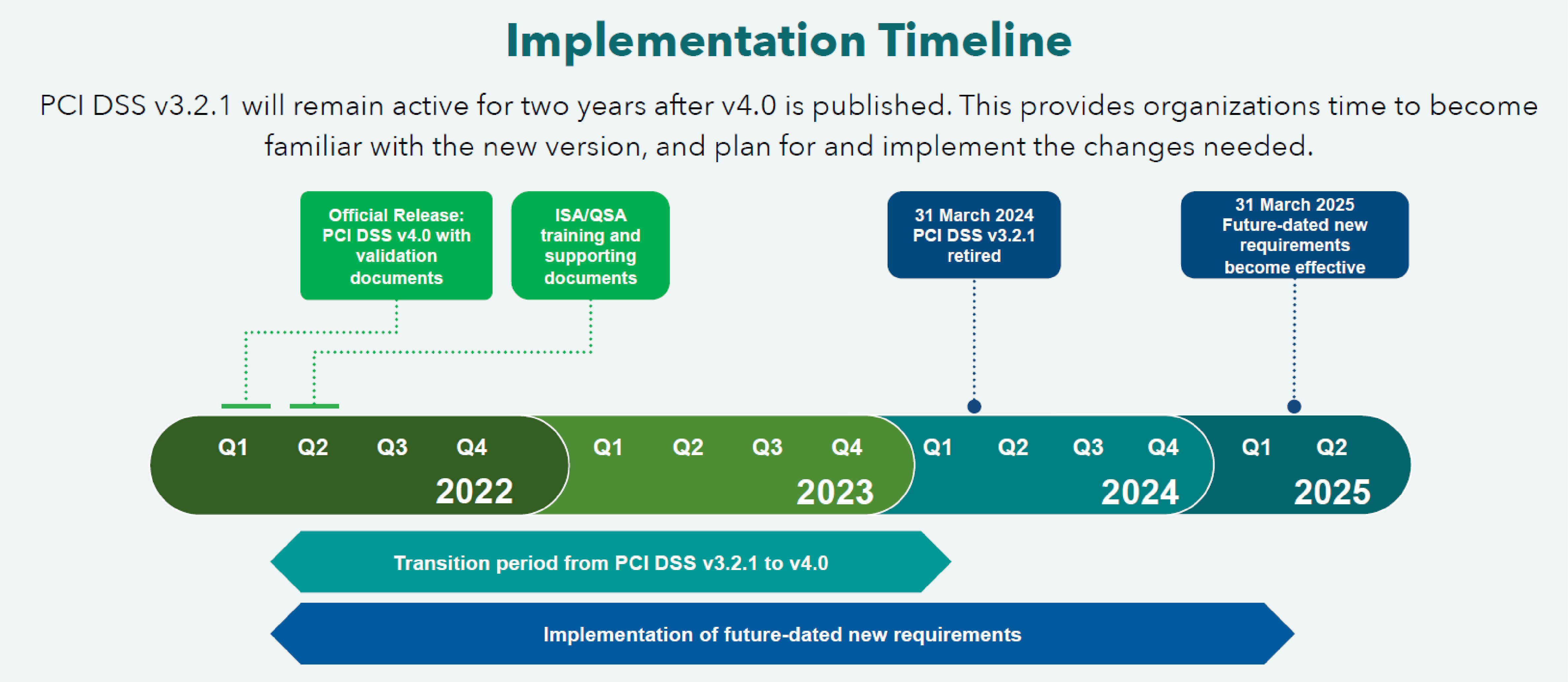
Ransomware recovery – option 3

Immutable volumes in XP



More on security

PCI DSS 4.0 has arrived!



Implementation Timeline

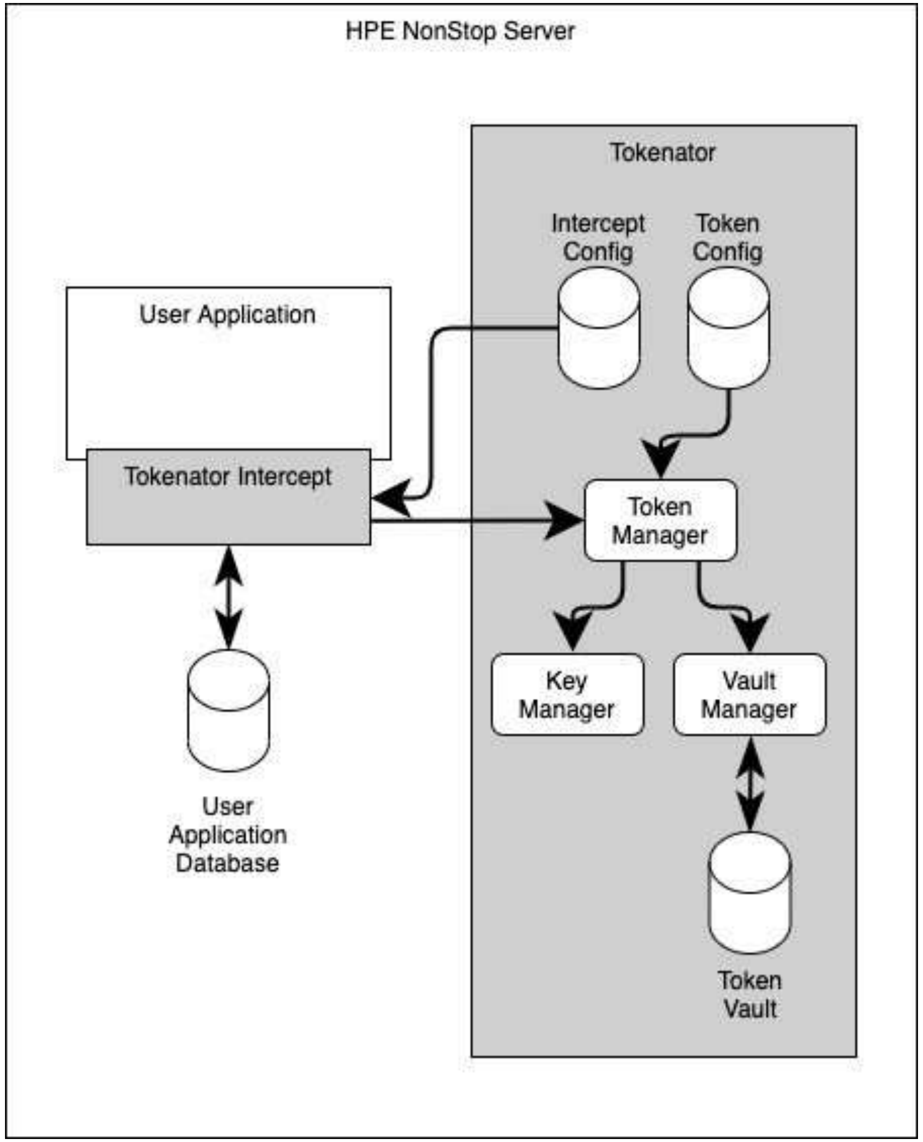
PCI DSS v3.2.1 will remain active for two years after v4.0 is published. This provides organizations time to become familiar with the new version, and plan for and implement the changes needed.

Official Release: PCI DSS v4.0 with validation documents
ISA/QSA training and supporting documents
31 March 2024 PCI DSS v3.2.1 retired
31 March 2025 Future-dated new requirements become effective
Q1 Q2 Q3 Q4
2022
Q1 Q2 Q3 Q4
2023
Q1 Q2 Q3 Q4
2024
Q1 Q2
2025
Transition period from PCI DSS v3.2.1 to v4.0
Implementation of future-dated new requirements

Source: https://www.pcisecuritystandards.org/documents/PCI-DSS-v4-0-At-A-Glance.pdf

TOKENATOR
Futures

- Tokenizes sensitive data in Enscribe files transparently
- Working principle
  - Intercept file I/Os
  - Locate sensitive data (E.g. PAN, DoB)
  - Tokenize/detokenize data prior to write/read
- What are tokens?
  - A randomized value representing the sensitive data
  - Irreversible by an attacker and hence offers no gain
  - Often has the same format as that of the sensitive data it represents (eliminates application changes)
- No change required to applications
- No external hardware required
- Uses industry standard cryptographic algorithms to store token vaults
- Supports sensitive data masking for usages such as report generation
- Offers minimal latency overhead



Data at rest protection - SQL/MX
Futures

- User level encryption support through DBMS_CRYPTO
  - DBMS_CRYPTO: Contains cryptographic functions and procedures
  - Applications can encrypt the data using algorithms such as AES before writing data to the DB
- Transparent Data Encryption (TDE)
  - Encrypts data at rest in SQL tables and requires no application change

Stay ahead and protect yourself

Thank you!

HPE Slides and Materials Usage

This content is protected