Hewlett Packard
Enterprise

NonStop Technical Boot Camp 2023
TBC23-TB75 Establishing a Secure and Resilient Operating Environment on HPE NonStop

Ozen Ercevik (HPE), Richard Conine (HPE)

September 2023

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.

Agenda

Cybersecurity trends

Digital resilience strategies for HPE NonStop – Protect & Detect

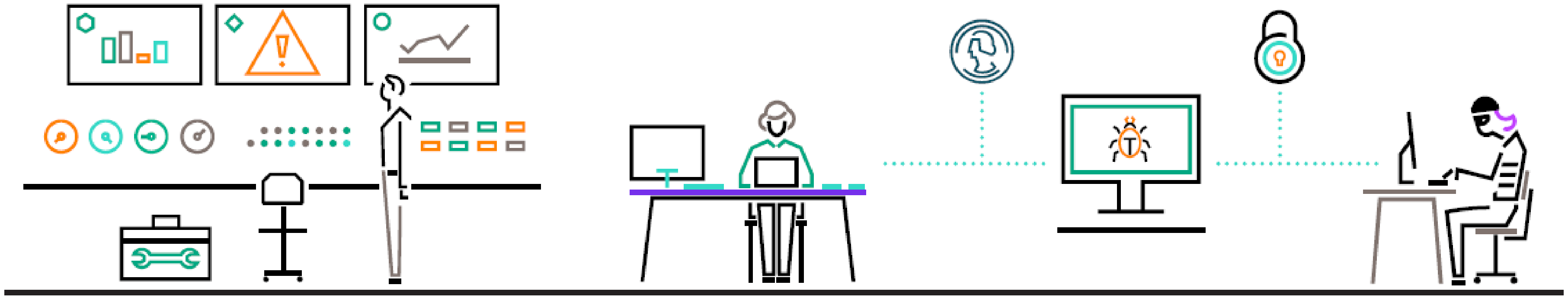
Digital resilience strategies for HPE NonStop – Respond & Recover

HPE Managed Services for protection against ransomware

Cybersecurity trends

Cybersecurity in 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[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.

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

[3] “Cyber Crime & Security,” Statistica.

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.***
  - ***<u>Create a continuity plan in case your business or organization is the victim of a ransomware attack</u>.***

- **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**

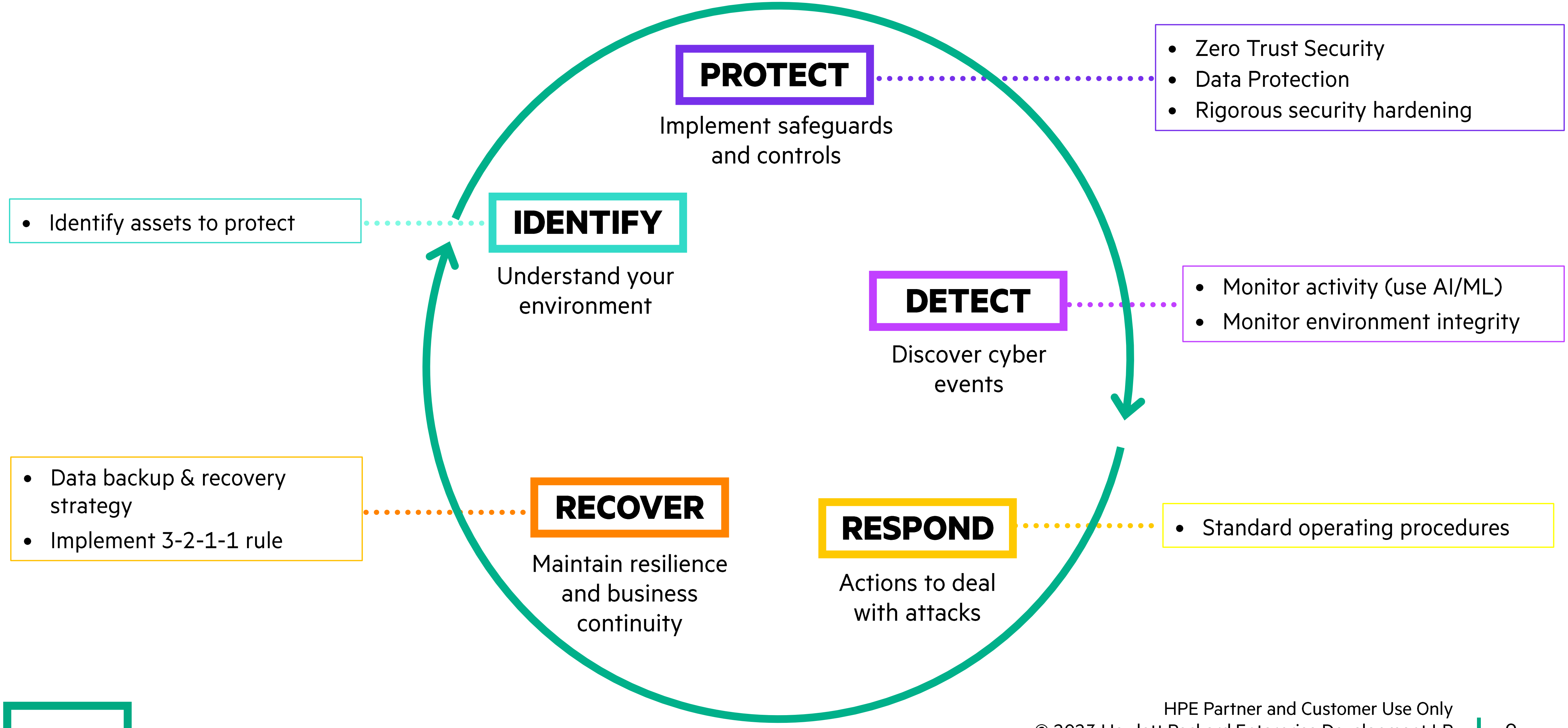
- **eur-lex.europa.eu**
- ***Digital Operational Resilience Act (DORA)***
- ***Coverage***
  - ICT Risk management
  - ICT-related incident management, classification and reporting
  - ***Digital operational resilience testing***
  - ***Managing of ICT third-party risk***
  - Information-sharing arrangements

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 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 based on NIST guidelines



- Identify assets to protect

IDENTIFY

Understand your environment

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

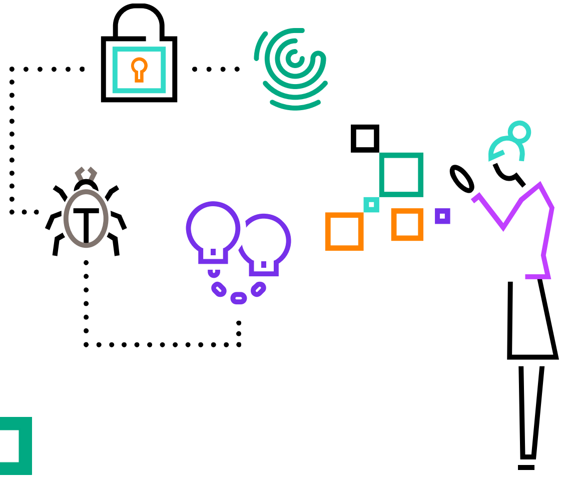
- Data backup & recovery strategy
- Implement 3-2-1-1 rule

HPE Partner and Customer Use Only

Protection and Recovery – Two Pillars of Digital Resilience

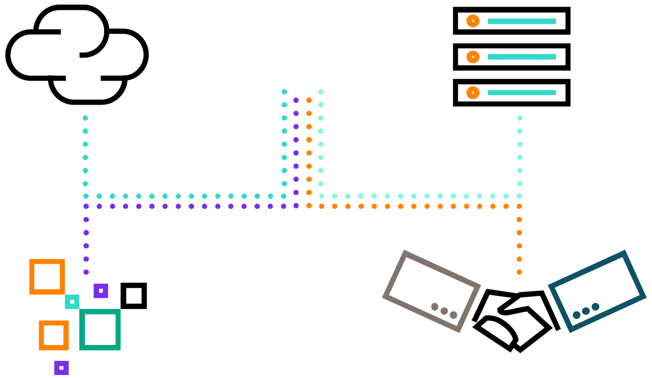
Protect and Detect

- 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



Recover

- A recovery 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

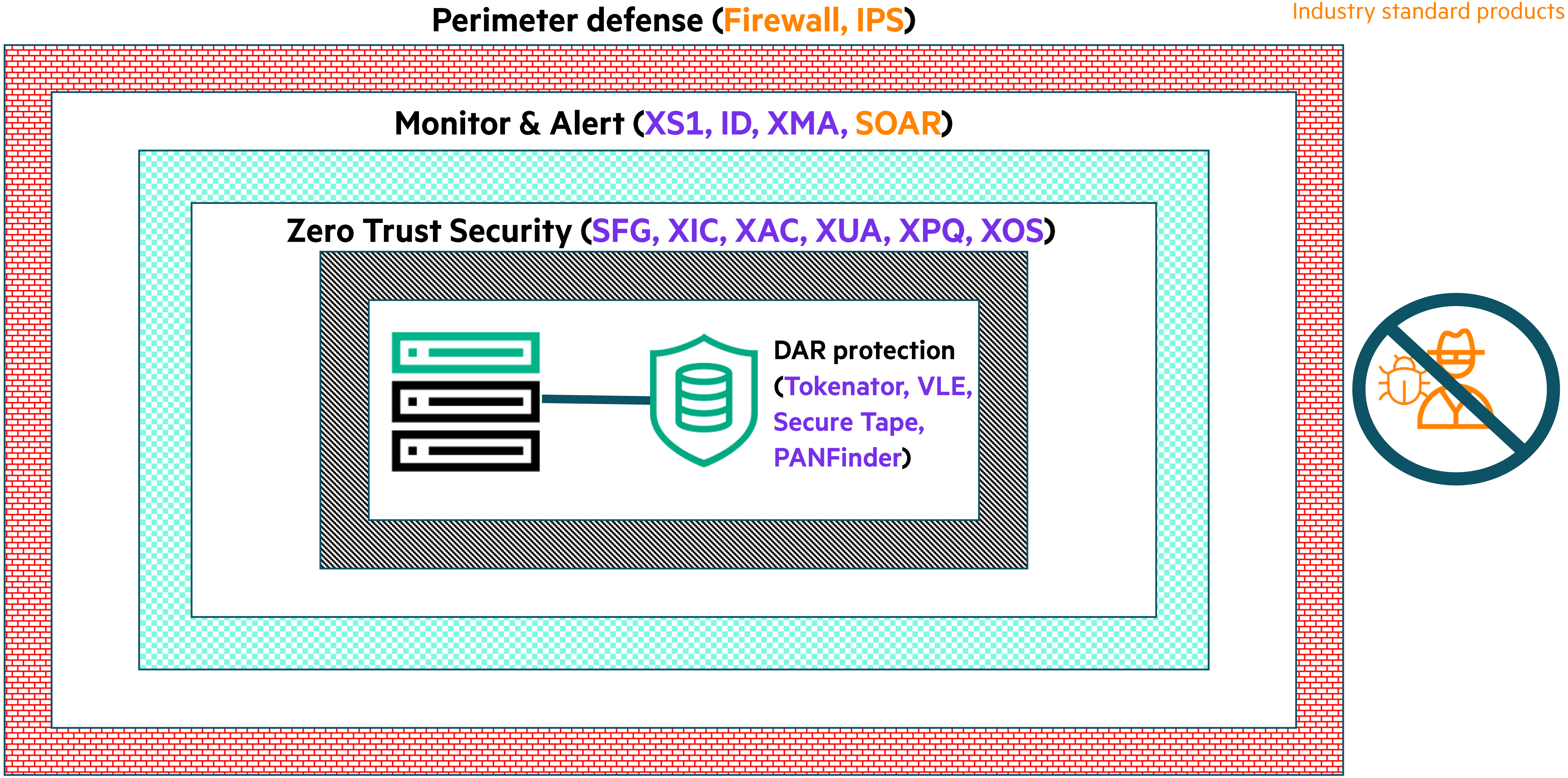


Digital resilience strategies for HPE NonStop

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)

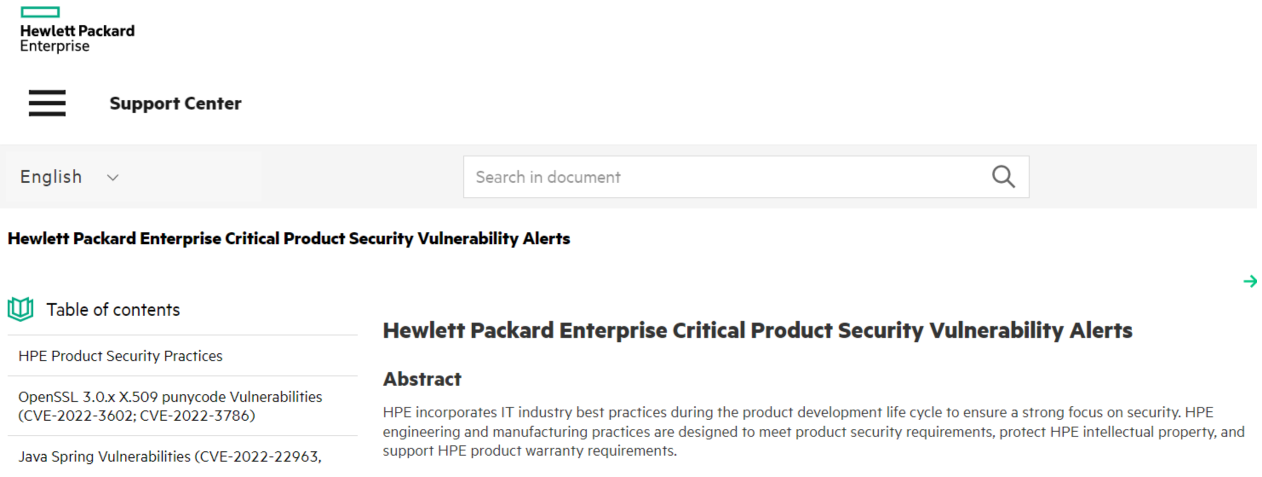
HPE NonStop Security Hardening Guide

- A comprehensive guide on how to secure HPE NonStop
- 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

Table of contents

HPE Product Security Practices

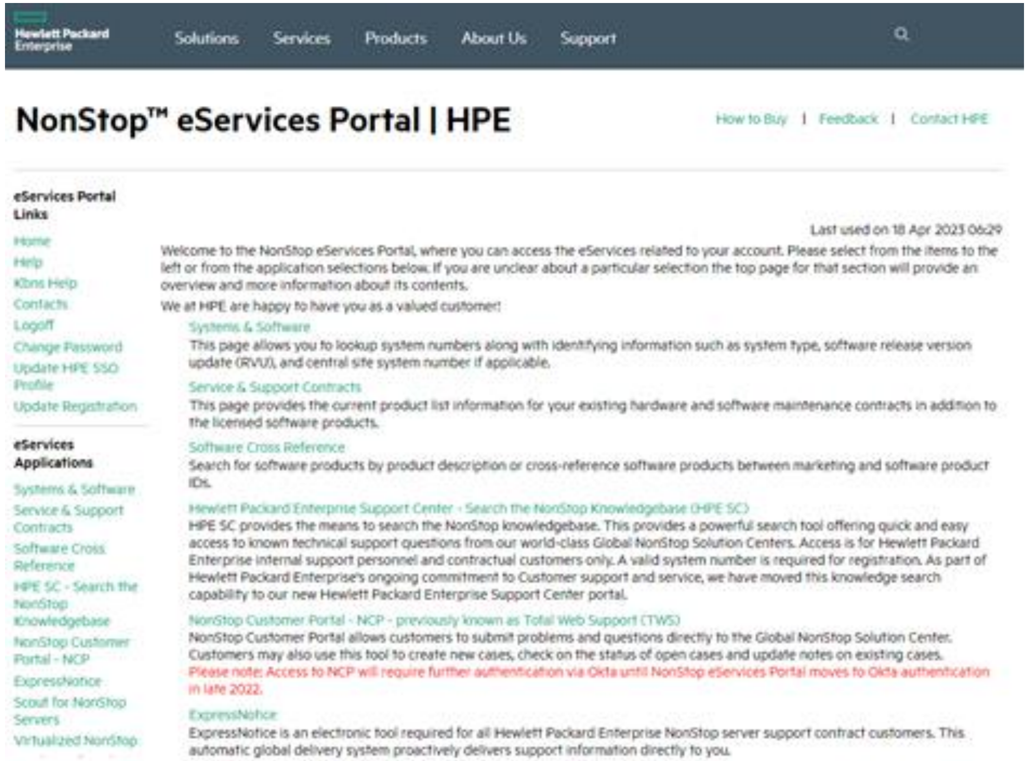
OpenSSL 3.0.x X.509 punycode Vulnerabilities (CVE-2022-3602; CVE-2022-3786)

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

eServices Portal Links

Home
Help
Kbns Help
Contacts
Logoff
Change Password
Update HPE SSO Profile
Update Registration

eServices Applications

Systems & Software
Service & Support Contracts
Software Cross Reference
HPE SC - Search the NonStop Knowledgebase
NonStop Customer Portal - NCP
ExpressNotice
Scout for NonStop Servers
Virtualized NonStop

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.

HPE Partner and Customer Use Only

Digital resilience strategies for HPE NonStop

Recover

Terminology

Immutable

Data that can only be written, not modified or deleted

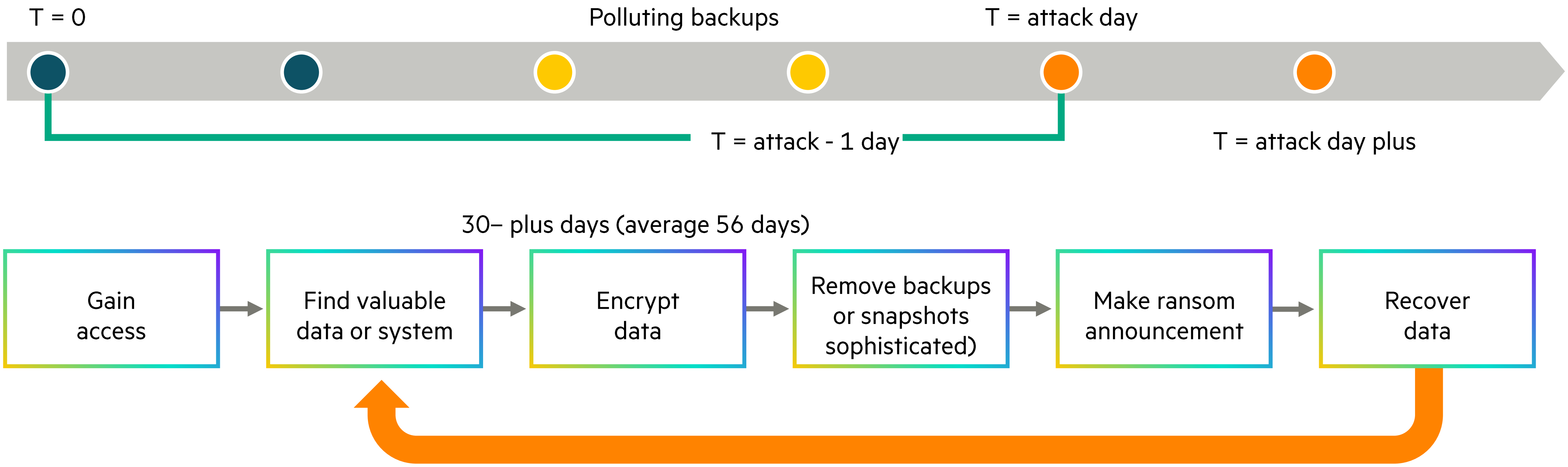
Air Gapped Systems

An interface between two systems at which they are **mostly** not connected physically

3-2-1-1 Rule

- ✓ **Three** copies of data
- ✓ **Two** different forms of media
- ✓ **One** off-site copy to the cloud
- ✓ **One** off-site copy to tape

A Typical Ransomware Attack Timeline

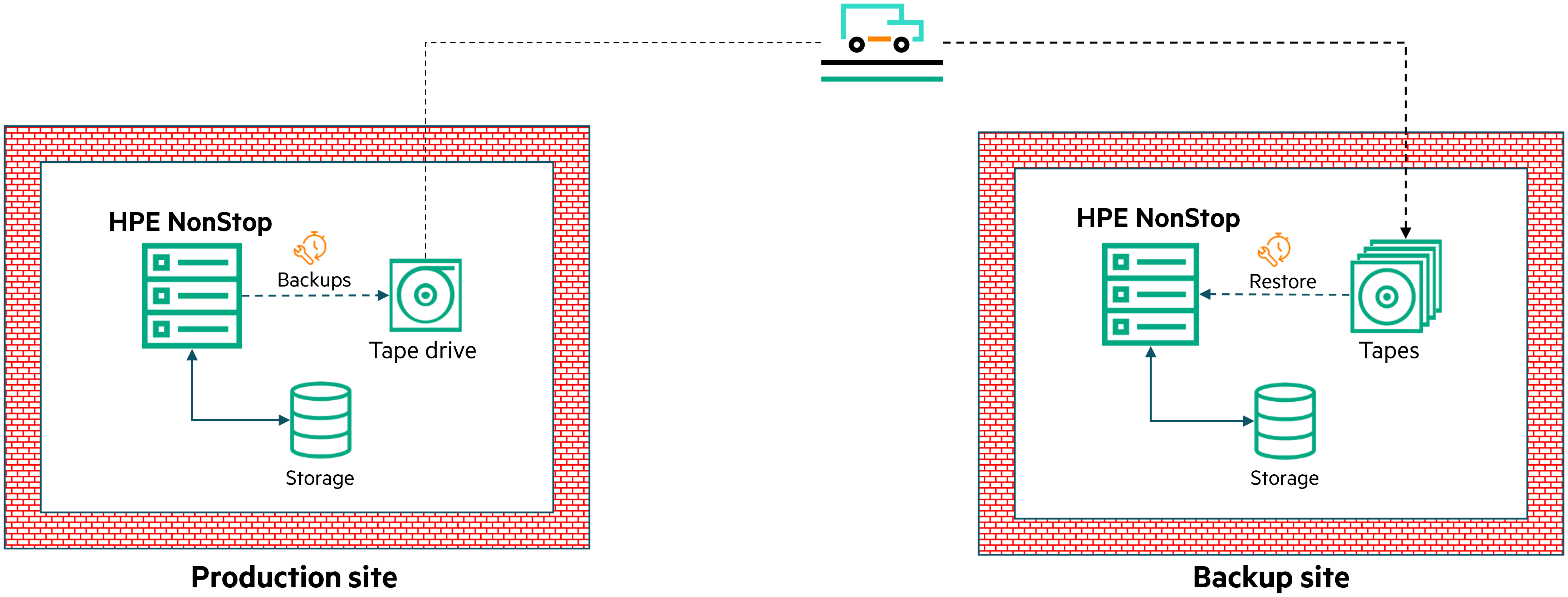


Best Recovery Point Objective - RPO

HPE Partner and Customer Use Only

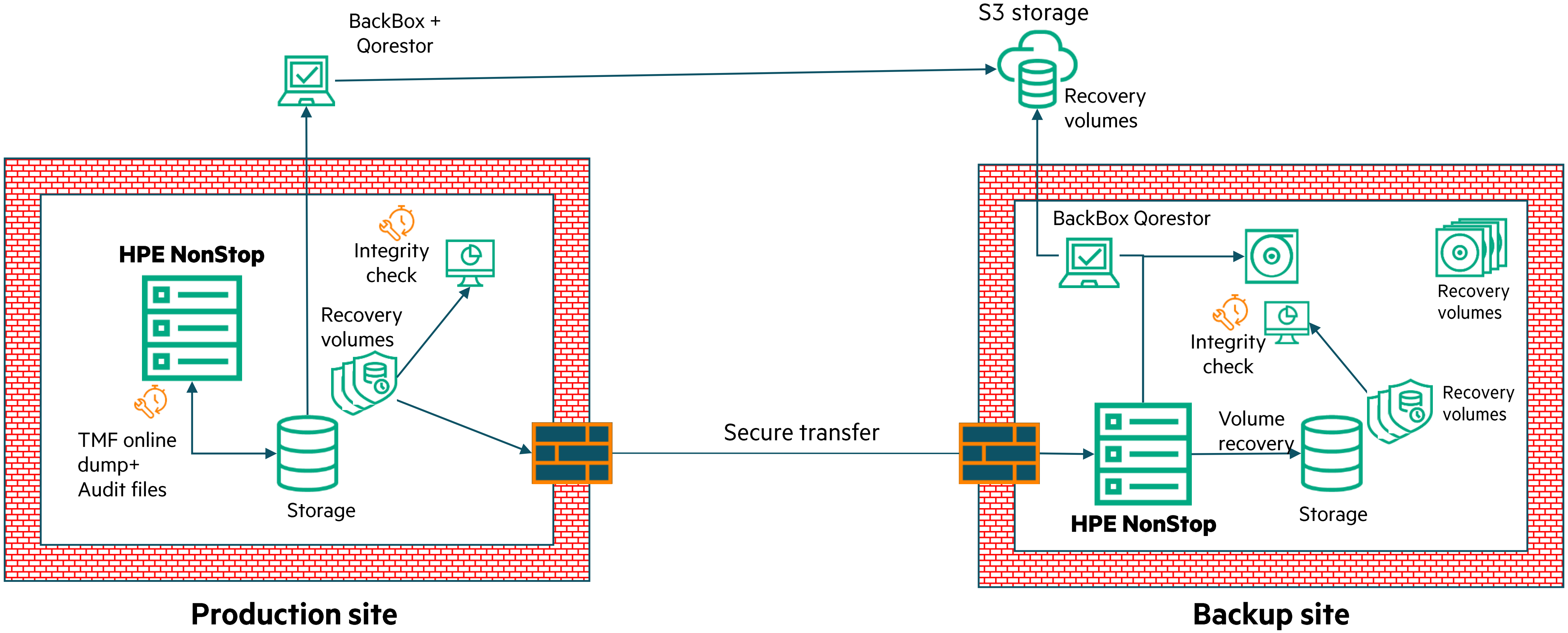
Ransomware Recovery Using Physical Media

Solution 1



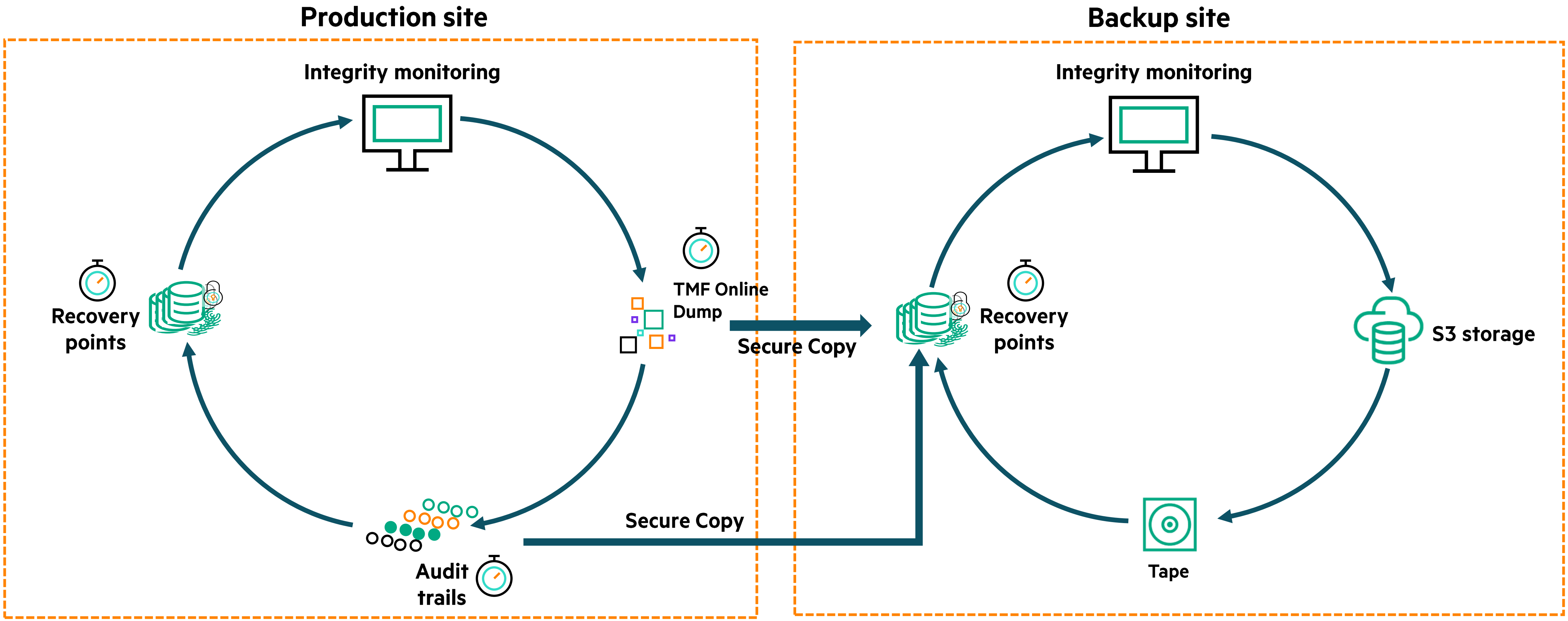
Ransomware Recovery Using 3-2-1-1 rule

Solution 2a – Standard TMF Online Dump and Audit Files



HPE Partner and Customer Use Only

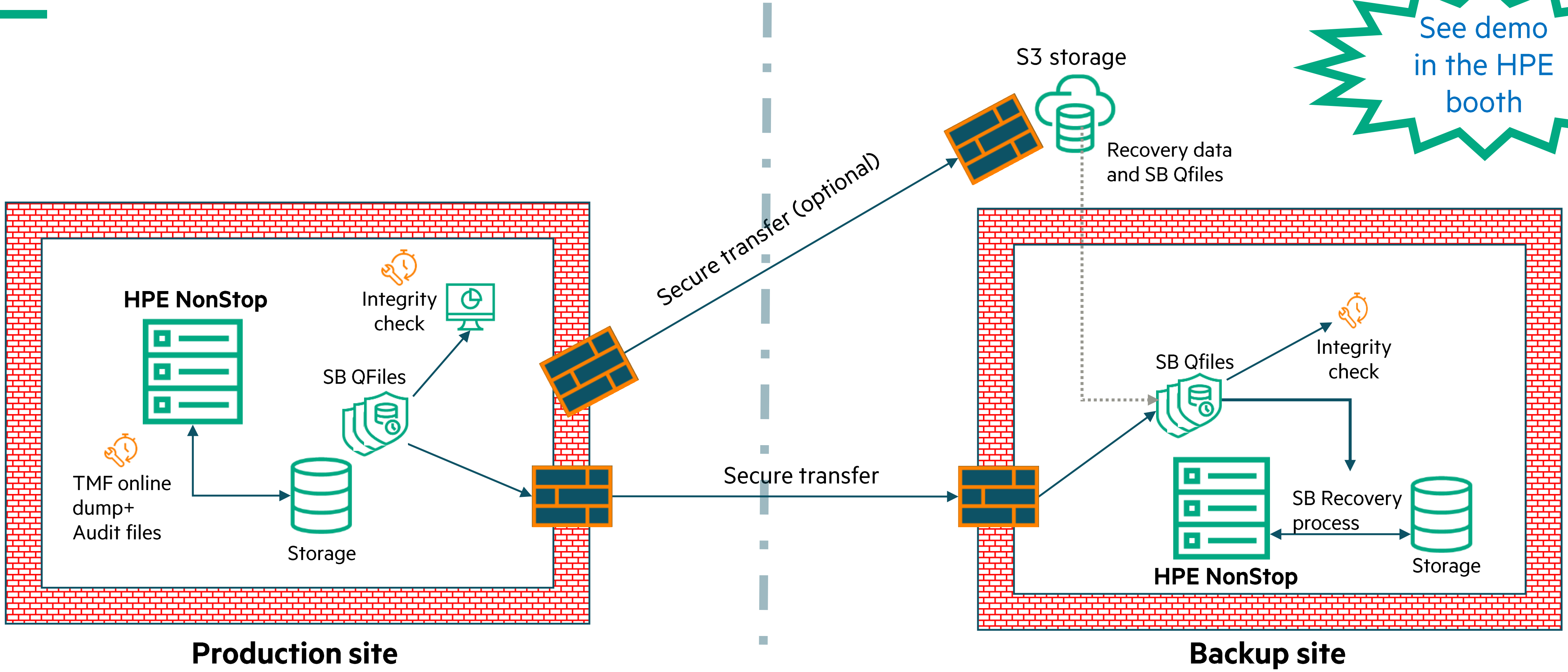
Workflow


Production site
Integrity monitoring
Recovery points
TMF Online Dump
Secure Copy
Audit trails
Secure Copy
Backup site
Integrity monitoring
Recovery points
S3 storage
Tape

Ransomware Recovery Using 3-2-1-1 rule

Solution 2b - HPE Shadowbase Qfiles

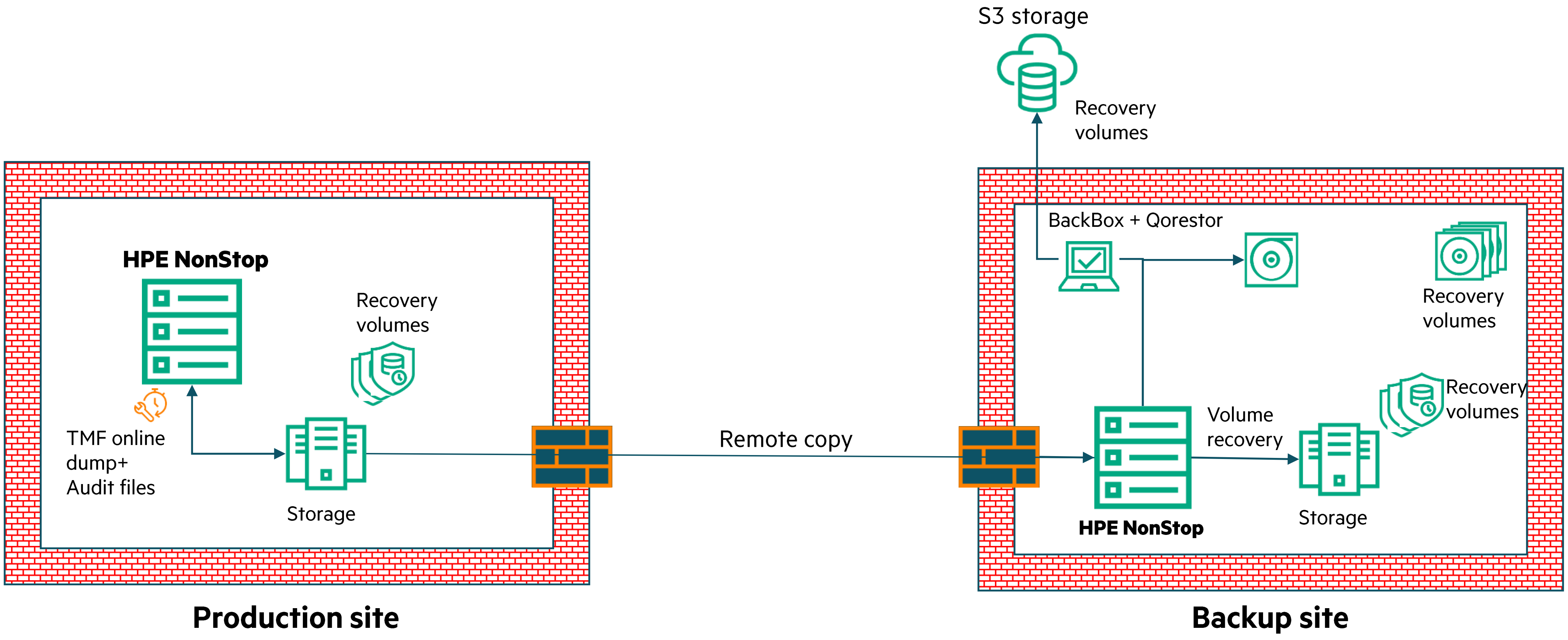
See demo in the HPE booth



“Air Gapped” - NO Expand
Only private network and controlled internal port access
Backups site stasis is version N-minus user defined last good

Ransomware Recovery Using XP

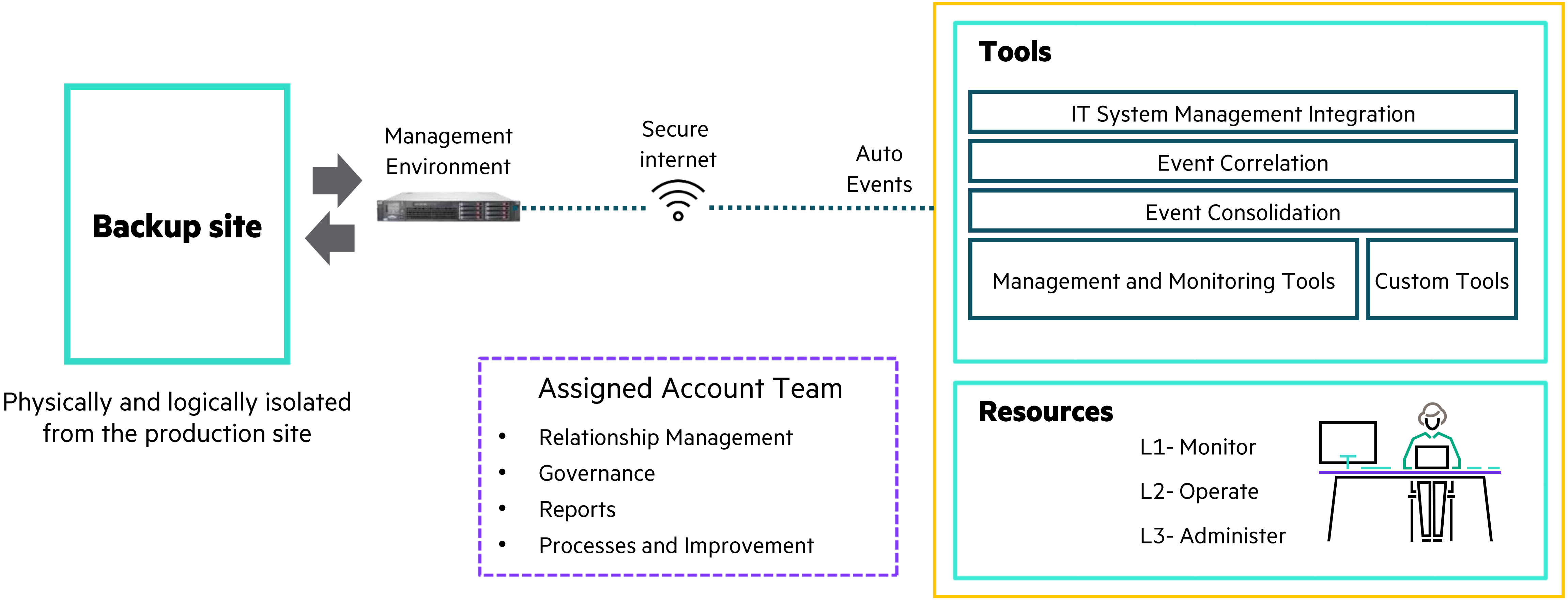
Solution 3



HPE Managed Services for Protection against Ransomware

HPE Managed Services

Safeguarding your NonStop environment from ransomware threats



Backup site

Physically and logically isolated from the production site

Management Environment

Secure internet

Auto Events

Tools

- IT System Management Integration
- Event Correlation
- Event Consolidation
- Management and Monitoring Tools
- Custom Tools

Assigned Account Team

- Relationship Management
- Governance
- Reports
- Processes and Improvement

Resources

L1- Monitor

L2- Operate

L3- Administer

TBC sessions

- **TBC2023-VT4**: HPE Shadowbase: Maximize NonStop Digital Resilience with Data Replication, Integration, and Validation
  - Paden Holenstein (Gravic)
  - Tue Sep 12, 2023
  - 1:00 PM - 2:00 PM
  - Denver 4

- **TBC2023-CFP7:** Practical Ransomware Vectors
  - Randall Becker (Nexbridge)
  - Tue Sep 12, 2023
  - 2:15 PM - 3:15 PM
  - Denver 6

- **TBC2023-VT9:** Identify, Protect, Detect - A ZERO Trust Approach to Ransomware Protection
  - Steve Tcherchian (XYPRO)
  - Wed Sep 13, 2023
  - 1:30 PM - 2:30 PM
  - Denver 1-2

- **TBC2023-VT13**: NTI Embraces Continuous Adaptation, Delivers Business Resilience
  - Richard Buckle (NTI)
  - Wed Sep 13, 2023
  - 1:30 PM - 2:30 PM
  - Denver 4

- **TBC2023-VT5**: Ransomware Protection and Data Recovery
  - Paul J. Holenstein (Gravic), Kenneth Scudder (Gravic)
  - Wed Sep 13, 2023
  - 4:00 PM - 5:00 PM
  - Denver 1-2

- **TBC2023-VT6**: Helping You Tick The Compliance Checkboxes While Providing Full Cyber Resilience
  - Greg Swedosh (4tech)
  - Wed Sep 13, 2023
  - 4:00 PM - 5:00 PM
  - Denver 6

Thank you for attending this talk NonStop Technical Boot Camp 2023 TBC23-TB75 Establishing a Secure and Resilient Operating Environment on HPE NonStop

ozen.ercevik@hpe.com
richard.conine@hpe.com

HPE Partner and Customer Use Only

HPE Slides and Materials Usage

This content is protected