Hewlett Packard Enterprise

NonStop Technical Boot Camp 2022 TBC22-TB43 You did everything right, but… Can you recover from a ransomware attack?

Richard Conine

November 2022

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

You do everything right …

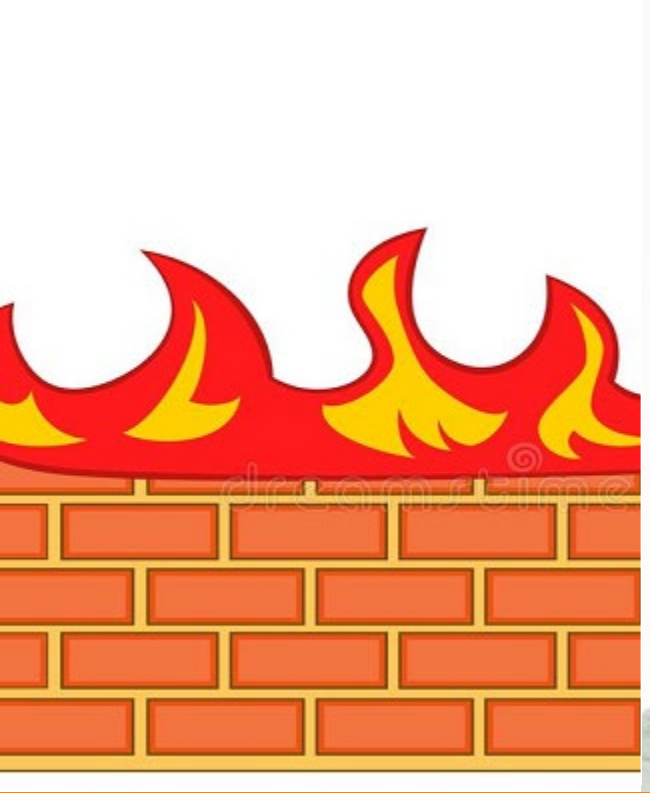
Something happened, you got hacked! “Pwned!” And they want money. Lots of it. Or else.

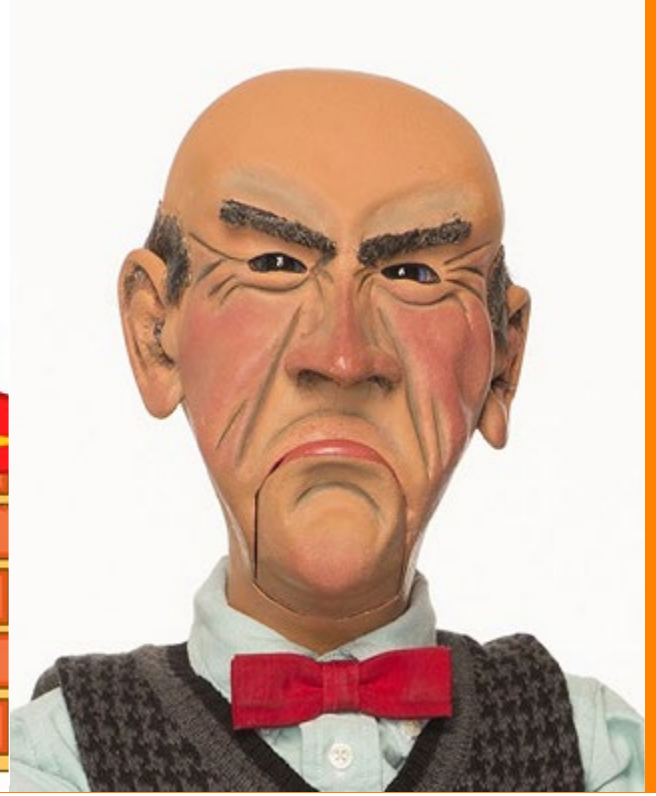
What is Ransomware?

Who would do this?

What are my options?

Recovery architecture, an insurance plan.





Introduction

- You've done it all right. Firewalls, grumpy auditor, password hygiene, the best security, and you've realized Bill Gates or the Nigerian Prince aren't going to give you money. And please don't click on the cat videos, no matter what!

The Myths of Ransomware Attacks and How To Mitigate Risk

…57% of security leaders expect to be compromised by within the next year.

…remote work and the cloud have made it more difficult to spot a ransomware attack, as well as how deploying behavioral-anomaly-based detection can help mitigate ransomware risk.

The growing trend is that attackers understand IT infrastructure really well. For example, lots of companies are running Windows or Linux machines or have entities on-premises. They might also be utilizing *cloud services or cloud platforms* or different endpoints. Attackers understand all that. So they can develop malware that follows those IT infrastructure patterns. *And in essence, that's where they're evolving, they're getting wise to our defenses.*

https://thehackernews.com/2022/05/the-myths-of-ransomware-attacks-and-how.html?m=1

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.*

MORE ≡ > SCAMS AND SAFETY > COMMON SCAMS AND CRIMES FBI Search FBI

SCAMS AND SAFETY

Protecting Your Kids | On The Internet: Be Cautious When Connected | Common Scams And Crimes | Sex Offender Registry Websites

Ransomware

Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware.

Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More menacing versions can encrypt files and folders on local drives, attached drives, and even networked computers.

Most of the time, you don't know your computer has been infected. You usually discover it when you can no longer access your data or you see computer messages letting you know about the attack and demanding ransom payments.

Tips for Avoiding Ransomware

The best way to avoid being exposed to ransomware—or any type of malware—is to be a cautious and conscientious computer user. Malware distributors have gotten increasingly savvy, and you need to be careful about what you download and click on.

Other tips:

- 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.

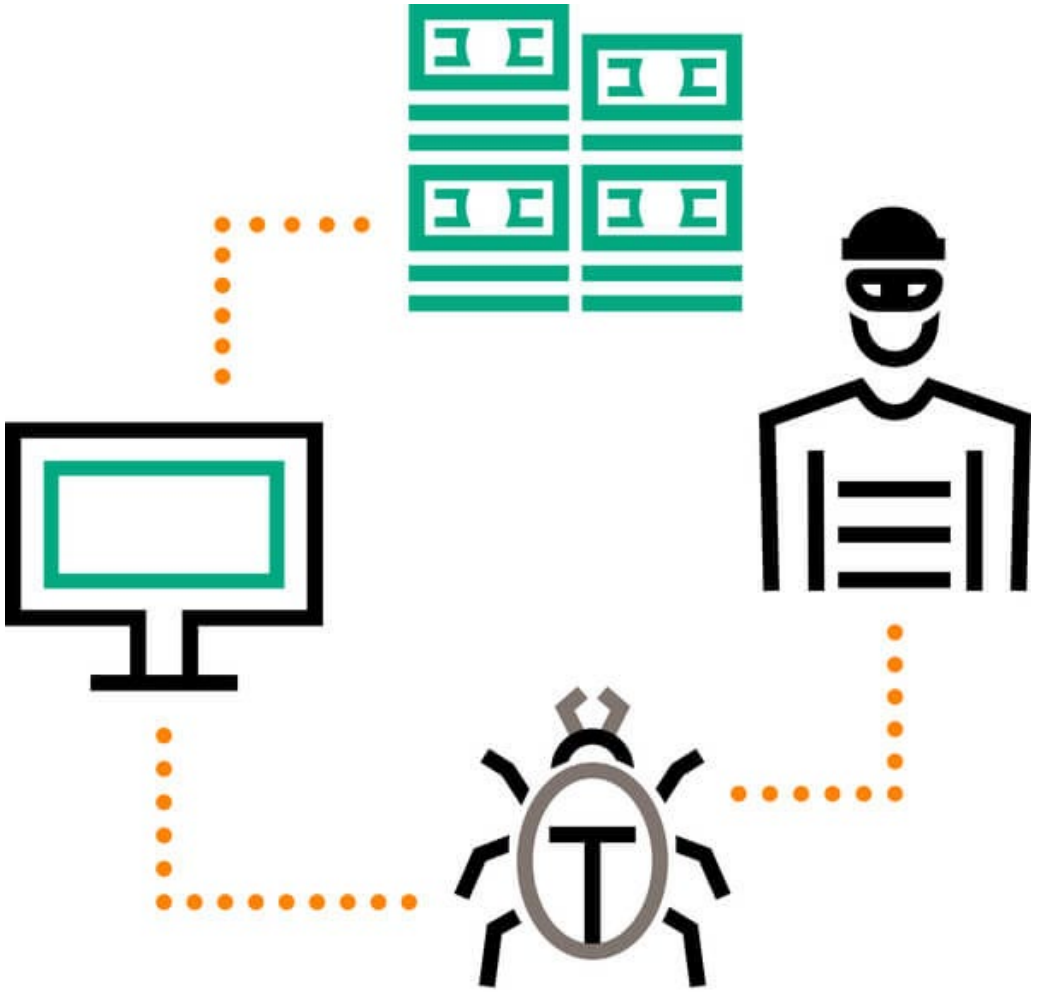
How to Respond and Report

The FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity.

If you are a victim of ransomware:

- Contact your local FBI field office to request assistance, or submit a tip online.
- File a report with the FBI's Internet Crime Complaint Center (IC3).

What is Ransomware?



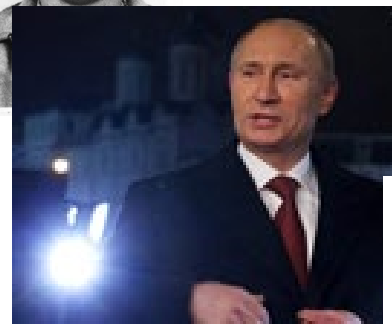
What is Ransomware?

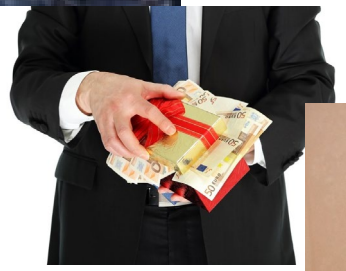
- “Malware with a ransom note”

- According to the report “Combatting Destructive Malware”, on average, a single ransomware attack costs large multinational companies USD $239 million and destroys 12,316 computer workstations. The cyber threat landscape is constantly evolving and expanding with new ransomware due to the complexity of networks, the cloud, remote virtualization, and the IoT.*

*https://www.ibm.com/topics/ransomware

Attack Vectors





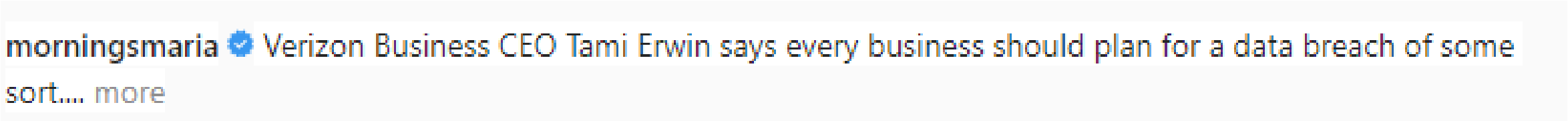
PEOPLE

- Bad actors
- Nation state infiltration
- Bribery/Blackmail
- Snowden/Assange/Winner
- Perceived moral outrage, revenge for $40m CEO package, layoffs

Attack Vectors: Who?

- Nation state infiltration
- Traditional bad actors (extortion, kidnapping, etc.)*
- Bribery/Blackmail opportunists (attack staff?)
- Self-proclaimed “Whistle blowers” Snowden/Assange/Winner
- Perceived moral outrage, revenge for $40m CEO package, layoffs

**See also Justin Simonds presentation on Detecting Human Trafficking, TBC22-TB08*



Attack Vector: How?

Phishing - Still number one

- The first quarter of 2022 saw phishing attacks hit a record high, topping one million for the first time, according to data from the Anti Phishing Working Group (APWG)
- The industry, law enforcement and government coalition's new Phishing Activity Trends Report also revealed that March was the worst month on record for phishing, with 384,291 attacks detected
- The financial sector was the worst hit, accounting for 24% of all detected attacks, although webmail and SaaS providers were also popular targets

https://www.infosecurity-magazine.com/news/phishing-hits-all-time-high-q1/

DOJ Seizes Web Domains used to sell stolen data

- The database consisted of seven billion indexed records featuring names, email addresses, usernames, phone numbers, and passwords for online accounts that could be accessed through different subscription tiers

DOJ Seizes 3 Web Domains Used to Sell Stolen Data and DDoS Services

June 01, 2022 Ravie Lakshmanan

The U.S. Department of Justice (DoJ) on Wednesday announced the seizure of three domains used by cybercriminals to trade stolen personal information and facilitate distributed denial-of-service (DDoS) attacks for hire.

This includes weleakinfo[.]to, ipstress[.]in, and ovh-booter[.]com, the former of which allowed its users to traffic hacked personal data and offered a searchable database containing illegally amassed information obtained from over 10,000 data breaches.

The database consisted of seven billion indexed records featuring names, email addresses, usernames, phone numbers, and passwords for online accounts that could be accessed through different subscription tiers.

Evolving Examples

- Malware, extortion, bribery taken from the headlines

Phishing still top attack method

https://securityintelligence.com/posts/why-phishing-still-top-attack-method/

Russian man “Plead guilty to offering a Tesla employee $1M to cripple battery plant ….” –ABC news, March 19, 2021

IoT devices being attacked

https ://www.theregister.com/2022/06/01/ransomware_iot_devices/

Ransomware aaS providers becoming more sophisticated and cross-platform

https ://thehackernews.com/2022/07/hive-ransomware-upgrades-to-rust-for.html?m=1

PDF documents found to contain malware

https ://www.theregister.com/2022/05/24/hp-pdf-phishing-malware/

77% of security leaders fear we’re in perpetual cyberwar from now on

https ://www.theregister.com/2022/08/27/in-brief-security/

Evolving Examples

- Malware, extortion, bribery taken from the headlines

Business found to neglect Cybersecurity until it's too late
https://www.infosecurity-magazine.com/news/cybersecurity-seriously-breach/

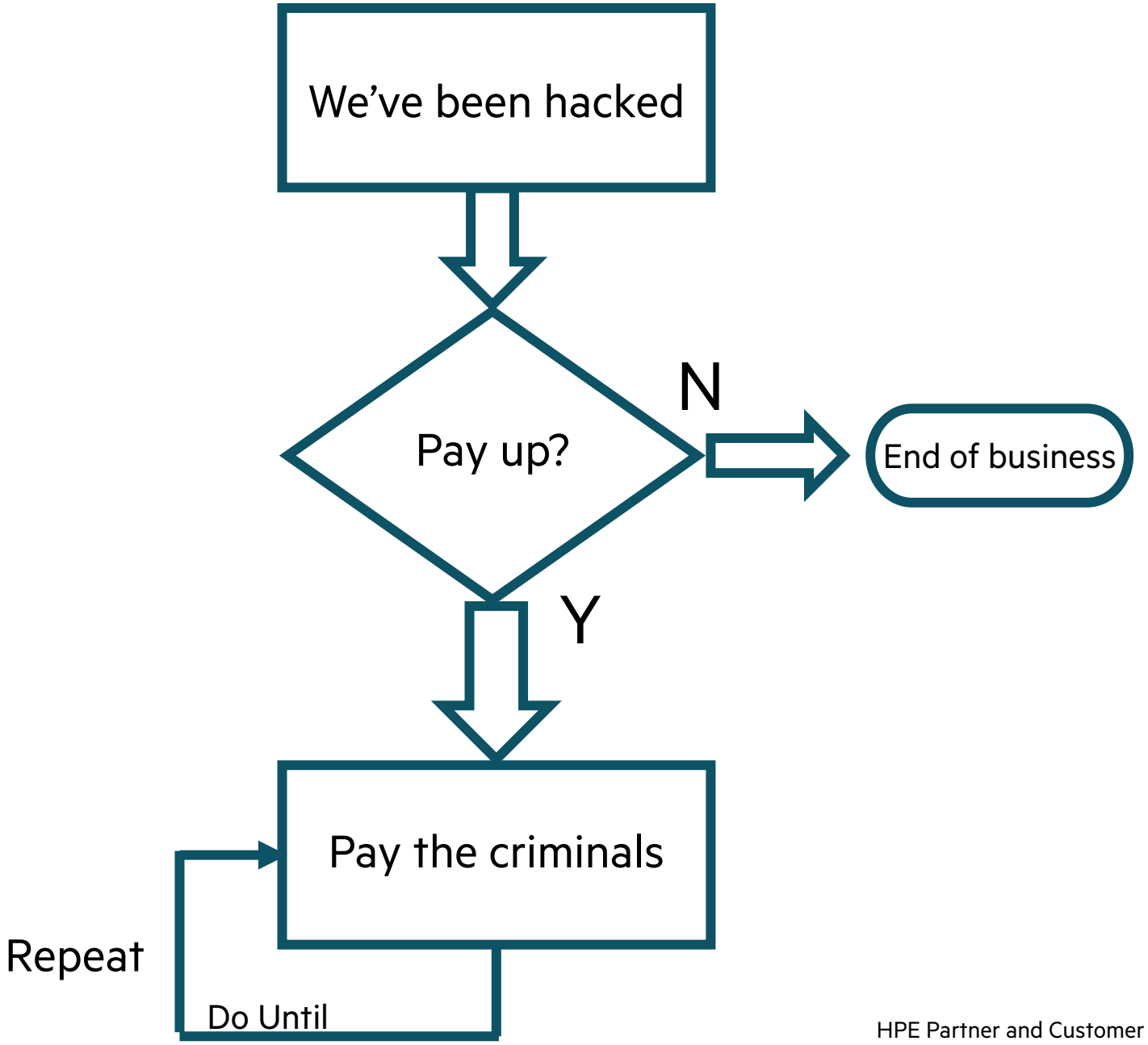
Researchers war of large-scale AiTM attacks targeting enterprise users
https://thehackernews.com/2022/08/researchers-warns-of-large-scale-aitm.html

Three-quarters of Security Pros believe Current Cybersecurity Strategies Will shortly be obsolete
https://www.infosecurity-magazine.com/news/security-pros-cybersecurity/

HackerOne bug bounty platform employee defrauded customers
https://www.infosecurity-magazine.com/news/hackerone-insider-defrauded/

New GwisinLocker ransomware encrypts Windows and Linux ESXi servers
https://www.bleepingcomputer.com/news/security/new-gwisinlocker-ransomware-encrypts-windows-and-linux-esxi-servers/

What are my options?



Plan now

Is the mirror/DR system compromised?
(how do you know?)

Can I recover from a backup?
(which backup is good?)

Is it cheaper to just pay the money?
(they have you now, will they have you again?)

Case study: Recovery Architecture for an Insurance Plan

- (Near) Immediate recovery, 47 mins
- Preserve evidence

How do you do “Recovery”

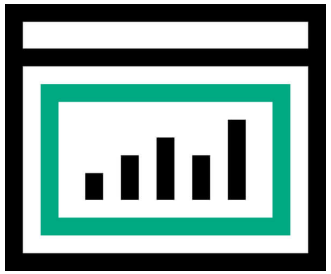
Hardware

- How do you know you’ve gotten rid of the ransomware? Is it hiding in firmware?
- What else is corrupted?
- Is the DR system compromised?
- Sectors of disk data

1.New factory-clean system

Software

- When were the last patches?
- What OS version is the vendor running?
- Production configuration files



2.Up-to-date current OS, middleware, database, and application

Data/Storage

- How do I know backup is good?
- Sector backups don’t preserve ACID database principles and could contain malware (binary/executable code)
- Transactional backup has only data.

3.Clean, transaction-based secure data

Data recovery: Sector vs. Transaction

Sector vs Transaction

Snapshot

- Fast “snapshot”
- Complete sectors, laid down in PHYSICAL order of the disk
- Data, programs, garbage, malware?, etc.

- What part of the database got restored? From which snapshot? Are you fingerprinting files?

ACID Transactions

- Atomicity: All or none
- Consistency: Data will be valid according to the database rules
- Isolation: Not affected by other transactions
- Durability: Once committed, is permanent

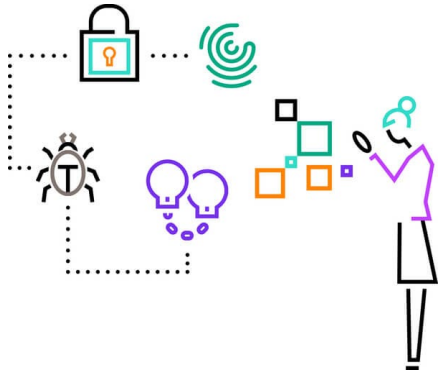
Avoiding Roadblocks to Recovery

Steps to Recovery	Roadblock
• Order, ship, and install system	• System corruption (firmware, hidden malware). Start with factory-fresh system.
• Install OS and relevant patches	• Install and test new OS
• Install, configure, and test application	• Application configure and startup
• Recover data from latest backup	• Restore backup. Is it good?
• Fix and clean restored data	• Sector-based backups will leave database in inconsistent state, ACID properties not maintained. Digital data may hide malware.

Architectural Principles

Business View

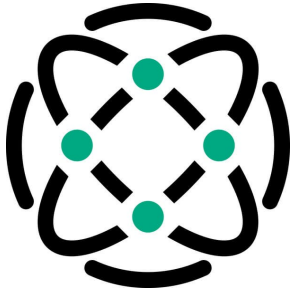
1. In the event of a ransomware attack, we return to processing in 47 minutes, not hours.
2. We preserve evidence of the attack for forensic analysis.



Architectural Principles

Functional Structure

- We use an isolated “standby system” for recovery purposes.
- We have the option of using the standby system for other purposes, but it must be sanitized before returning to “ready/standby.”
- Our standby system is covered by HPE NonStop standard M&S (Maintenance and Support) with the GNSC and CE team.



Architectural Principles

Technical Design (platform)

1. Our standby system is a 3rd mirror of our two production systems.
2. Our standby system is not connected to the Internet or the corporate LAN. It is “air gapped” from networks and people.
3. Our standby system can be brought online quickly to recover from an attack, or to support the production environment.
4. Our standby system is kept up-to-date (OS and Application) and in a “ready/standby” state according to our specifications by HPE GMS (GreenLake Management Services).

Recovery Data, Shadowbase offers tools

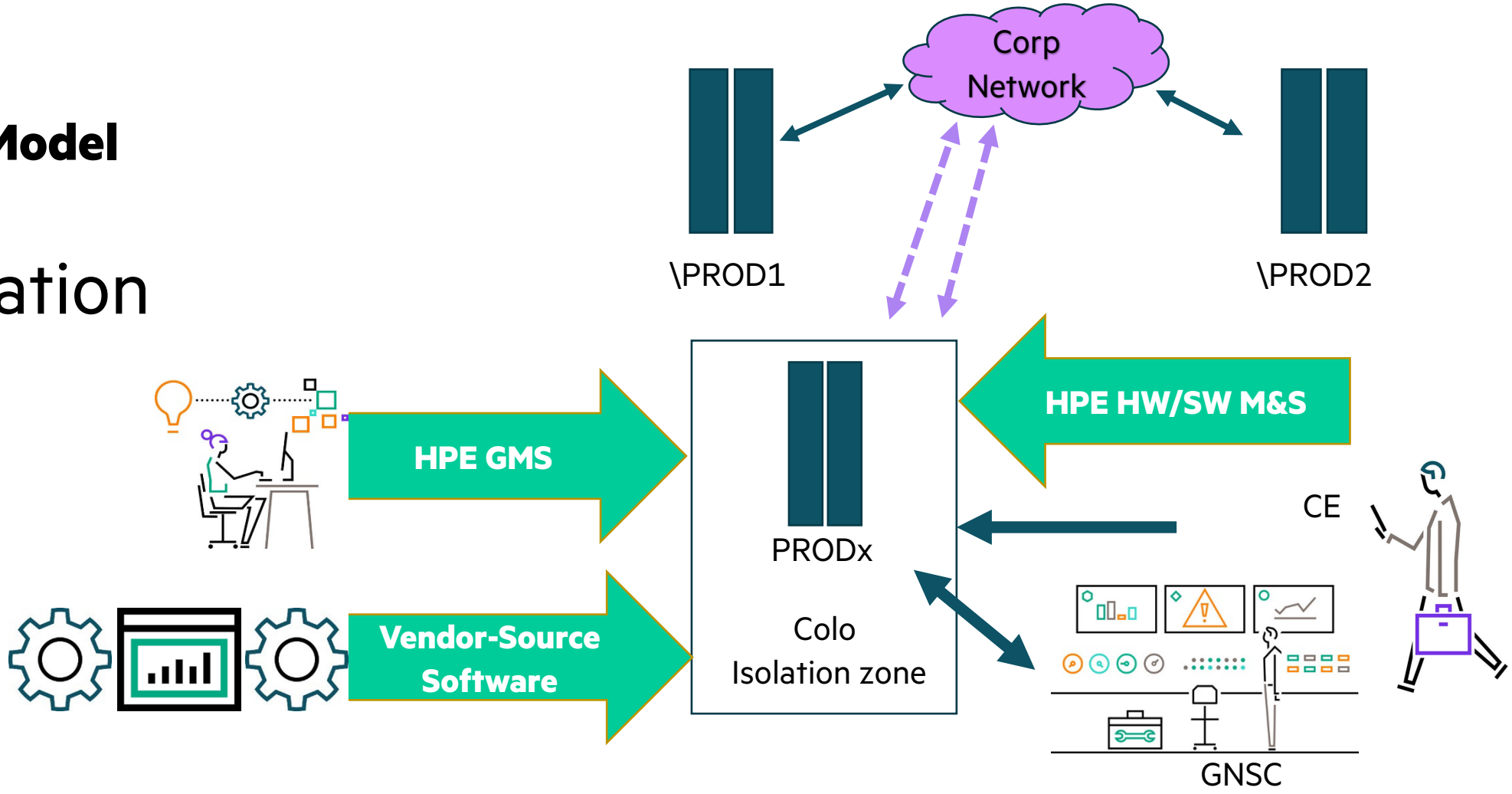
Technical Design (database)

- The opposite of “Sizzling Hot Take Over”, our standby system is brought online only when needed.
- An Immutable Database of Change captures transactions from production environment and moves them, under our control, to the standby system
- Our transactions are a secure, immutable blockchain ledger of transactions exported from production in character format. (possibly in JSON or XML character format—not binary)
- We preserve all database ACID properties using TMF AuditTrails
- We can play transactions forward as our recovery plan dictates (continuously, periodically or at failover).

GRAVIC®
HPE Shadowbase

Architectural Model

Implementation Plan



1. In the event of a ransomware attack, we return to processing in minutes, not hours.
2. We preserve evidence of the attack for forensic analysis.

Business Requirements

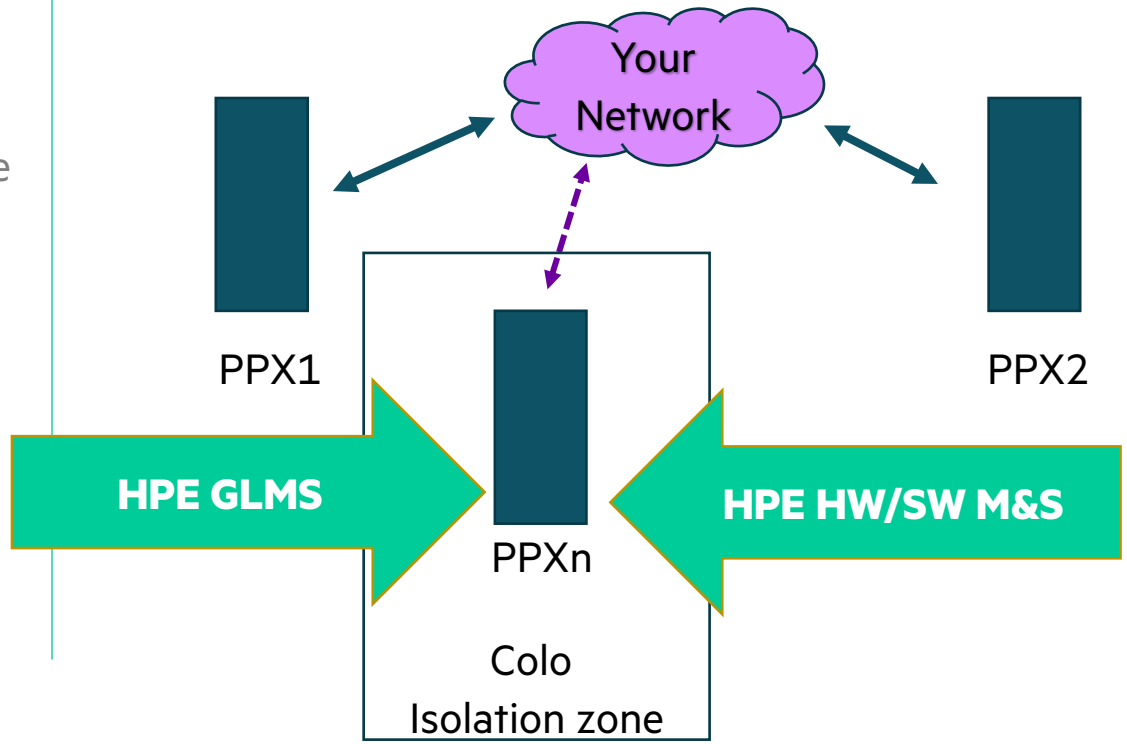
1. We use a “standby system” for recovery purposes
2. We have the option of using the standby system for other purposes, but it must be sanitized before returning to “ready/standby.”
3. Our standby system is covered by HPE NonStop standard M&S (Maintenance and Support) with the GNSC and CE team.

Functional Structure

Technical Design

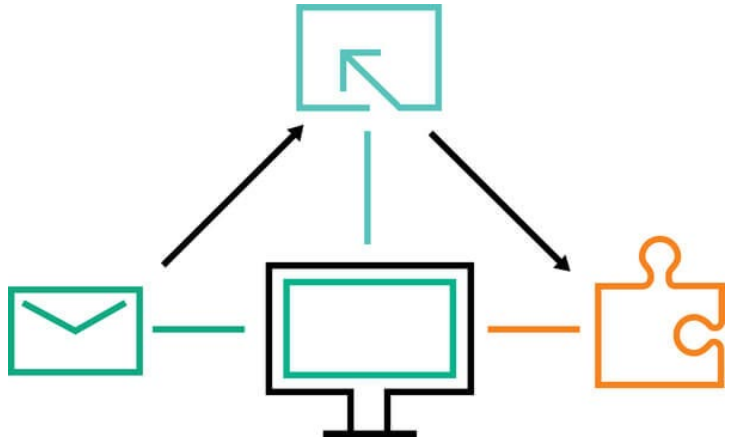
1. Our standby system is a 3rd mirror of our two production systems.
2. Our standby system is not connected to the Internet or the corporate LAN. It is “air gapped”.
3. Our standby system can be brought online quickly to recover from an attack, or to support our production environment.
4. Our standby system is kept up-to-date (OS and Application) and in a “ready/standby” state according to our specifications by HPE GLMS (GreenLake Management Services).

Implementation Plan



HPE As-a-Service Solution, by Greenlake

- Monthly pre-paid or billed monthly (Cap-X or Op-X)
- Private cloud pay-as-you-go costs and implementation, with dedicated system
- Monthly pricing, billed in arrears
- Billing starts AFTER the system is ready to put in “standby/ready” state
- Standby system hardware/software clone of production systems
- Hardware Maintenance/Software Support, GNSC and HPE CE (Pointnext)
- GreenLake Management Services to monitor and maintain OS and application
- Isolated colo, non-accessible by staff or contractors



File integrity is a cybersecurity fundamental

Detect Malicious Attacks

- Detecting unauthorized modification of objects and files is the best defense against malware and ransomware
- Provides critical input to threat detection and incident management

Identify Human Error

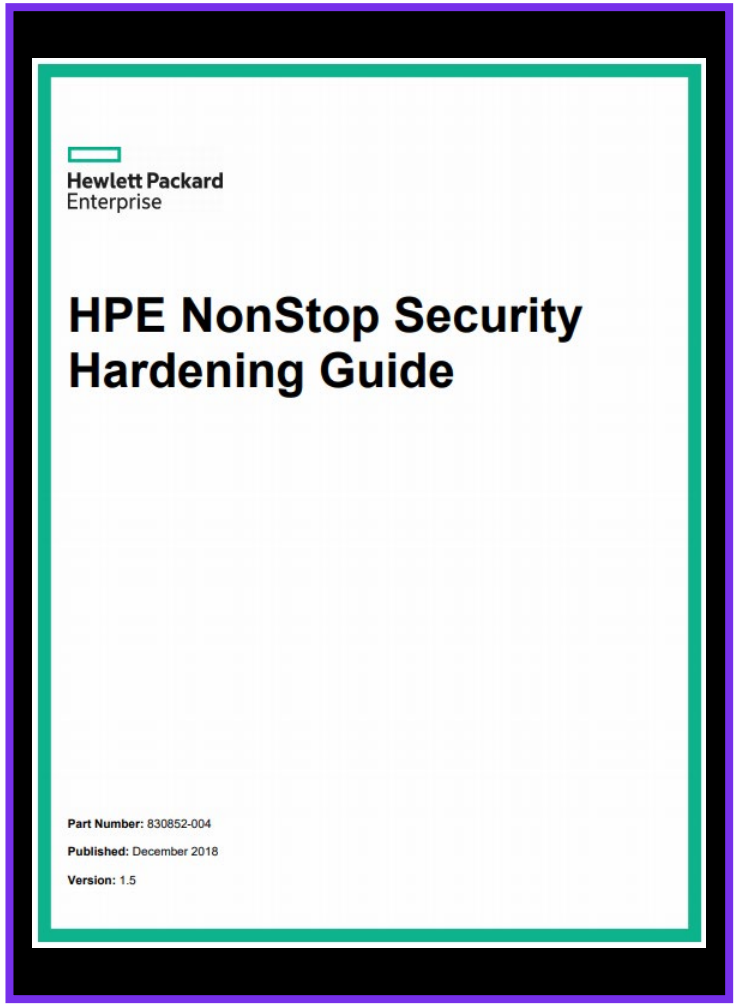
- Detect mistakes before they cause irreparable damage

Necessary for Compliance

- PCI, GDPR, SOX, HIPAA, GLBA, FISMA, NIST and other frameworks

Recommended by HPE NonStop Hardening Guide

- “Ensuring the integrity of critical operating system files and settings is an important part of your security strategy.”
- “Centralized monitoring and reporting and file integrity checking both assist you in demonstrating compliance to security regulations such as PCI DSS, SOX and HIPAA.”



Recovery As Insurance

Assured clean environment

- Air-gapped known good recovery system
- Running, but “lukewarm” standby
- Maintained and updated “off the net”
- Normally, no Internet connection
- Not part of standard operations
- Supported and configured by GMS under customer direction

Assured clean data

- How do I know backup is good or which one to restore?
- What if I restore the malware?
- Secure, immutable database of change
- Transactional backup (not sectors!)
- Play it forward as required (continuously, periodically or at failover)

Semper Vigilans

NonStop Partnership– It's a Beautiful Thing!

Thank you for attending this talk TBC22-TBT43 You did everything right, but… Can you recover from a ransomware attack?

Richard Conine
NonStop Technical Solutions Architect

512-284-1277
Richard.Conine@hpe.com

HPE Slides and Materials Usage

This content is protected

This presentation is the property of Hewlett Packard Enterprise and protected by copyright laws of the United States. The material in this presentation is provided to attendees of the NonStop Technical Boot Camp 2022 as part of their registration and attendance at the event. Attendees are free to use this material and share it with others within their own company.

This material may not be quoted, copied, communicated or shared with third parties or mutual customers without permission from HPE. To request permission to share material in this presentation outside of your company, send an email to ozen.ercevik@hpe.com explaining the usage you are intending and your request will be considered.