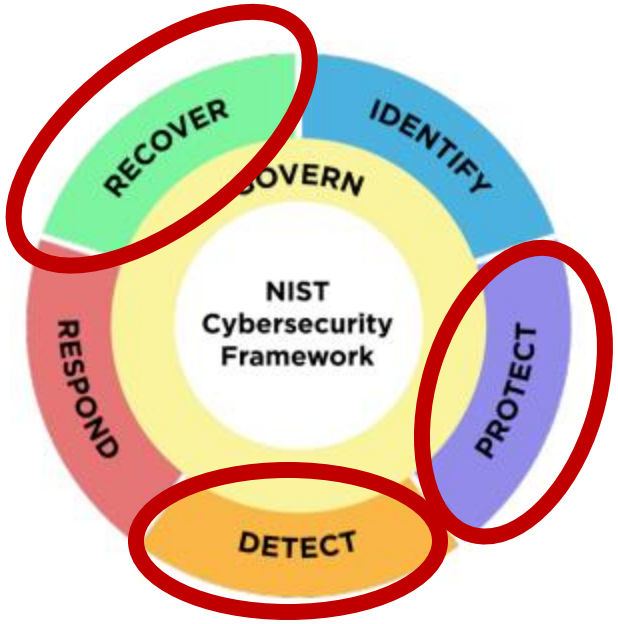
Hewlett Packard Enterprise

# Counter Ransomware Attacks With HPE Storage Solutions

2025 06

Martynas Skripkauskas
HPE Duomenų Centrų produktai

# The NIST Cybersecurity Framework




NIST 2.0 public draft: Link

## Ransomware is predominant class of Cyber Attacks

Our focus is on **Data Protection**. Data is one of the most important company asset

1. **GOVERN:** Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy.
2. **IDENTIFY:** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. Identify what should be protected and why.
3. **PROTECT:** Use safeguards to prevent or reduce cybersecurity risk and to lower the impact of adverse cybersecurity events. (Backup Immutability, Snapshots, Cyber-vault, …)
4. **DETECT:** Timely discover and analyze possible cybersecurity attacks. Monitor anomalies that may indicate that cybersecurity attacks are occurring. (Zerto 10 and Partners)
5. **RESPOND:** Take action regarding a detected cybersecurity incident. You need a plan to follow.
6. **RECOVER:** Restore assets and operations that were impacted by a cybersecurity incident.

NIST - National Institute of Standards and Technology - www.nist.gov

# Where is our focus for Ransomware Protection

**It is impossible to eliminate the risk of a successful ransomware attack**
**We want to implement the last line of defense, that reduces the damage when everything else failed.**

1) Traditional Data Protection solutions are designed against Natural Disasters
2) Data Protection needs to include new **specifically designed components** for ransomware attacks
3) Multiple protection layers is better than one. Immutable Snapshots, Immutable Backups, Tapes, …

Our focus is to **reduce the damage**


After a successful ransomware attack

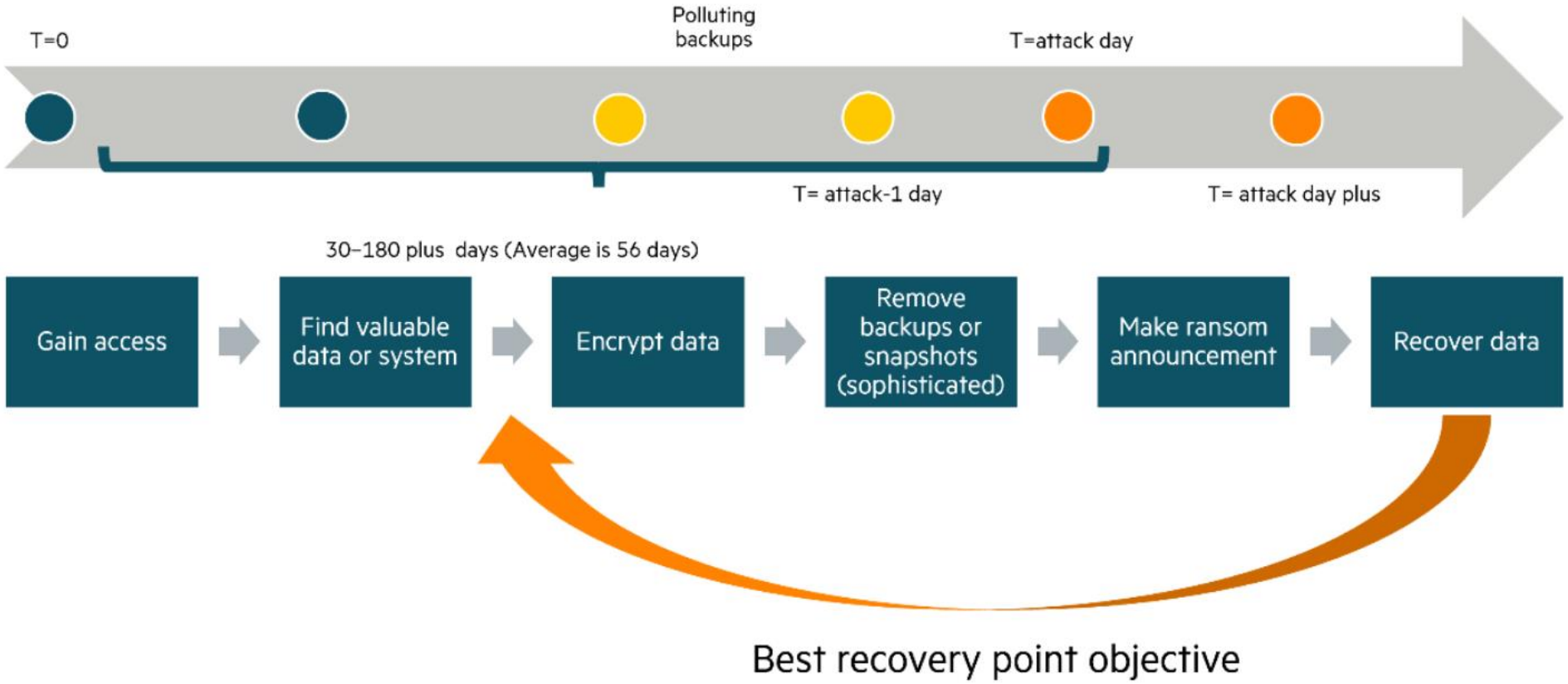
Main GOAL

**Recover production**
- **With minimal data loss**
- **As fast as possible**

# Ransomware protection rule-X:

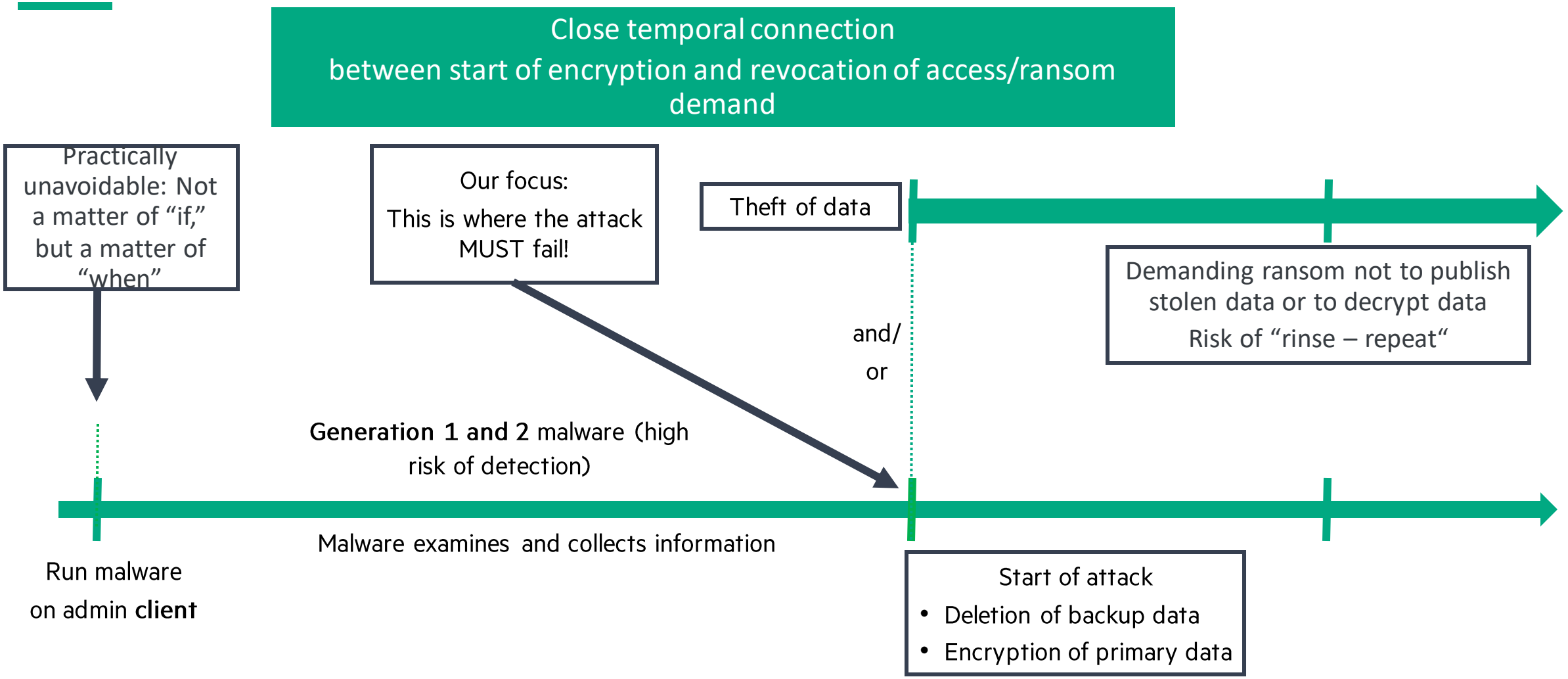
**“Your Backup and Snapshots are USELESS if the attacker deletes them”**

# Ransomware attack timeline (general)



# Ransomware attack timeline for older generations of ransomware

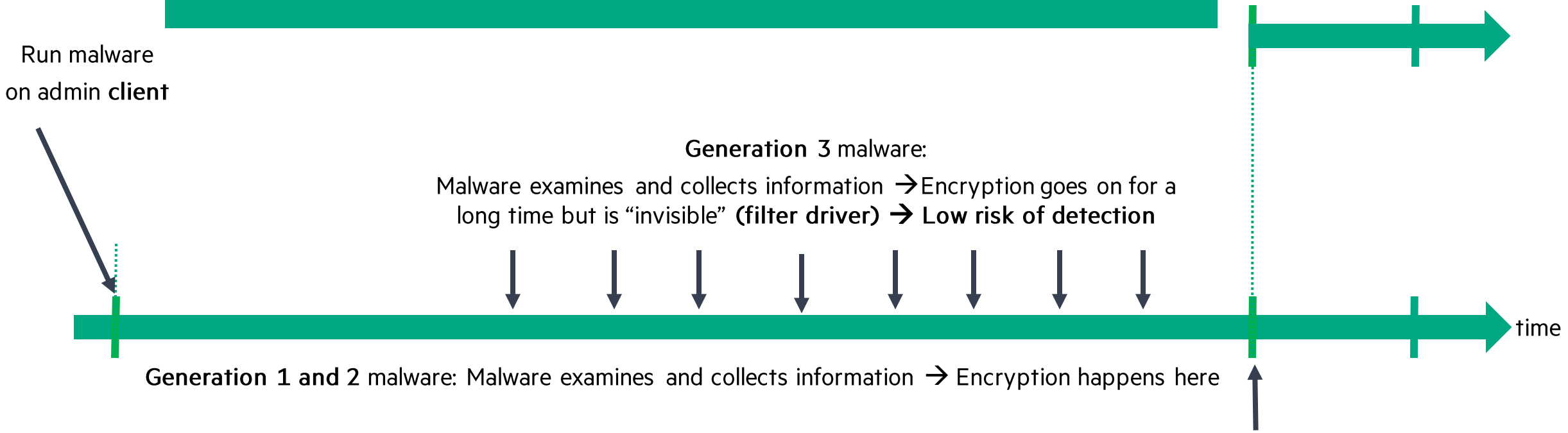
## Storage view




Zerto
a Hewlett Packard Enterprise company

# Ransomware attack timeline for new generation of ransomware
## Storage view

Weeks or months between start of encryption and revocation of access/ransom demand → backup poisoning!

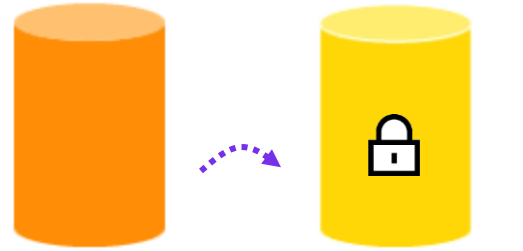


# HPE Storage Arrays – "Virtual Lock" immutable snapshots

## Snapshot Immutability

NEW 2024

- Originally on Primera, Alletra 9000
- Now also on Alletra MP and Alletra 5/6000




## Immutability: Read-only and Locked Snapshots to protect from

- Cybercrime incidents like ransomware attacks or insider attacks
- Nobody can delete or modify an Immutable/read-only Snapshot
- Storage Efficiency. For most use cases, 4 days of hourly snapshots requires less than 10% of additional capacity in total

## How to Create Immutable Snapshot

- **From backup applications** with Veeam V12.2, *Commvault in roadmap for 2024.*
  This is the preferred methodology because it offers Application consistency also for multi-homed VMs, and a variety of restore options
  NOTE: ISV Integration is not available on Nimble family and Alletra 5000/6000
- **Schedule a local policy** in the array via DSCC, SSMC, CLI or API
  NOTE: For Primary Storage, pay attention to VMs with VMDKs on multiple volumes
  NOTE: For Backup Target Repository see "Double layer of Immutability"

# In-line Ransomware detection, mitigation and recovery

Available with R5

- Realtime in-line write data scanning
- AI anomaly detection technology developed by HPE and Zerto
  - Multiple independent detection algorithms decreases the possibility of misses and false positives
  - Evolves over time (AI-based learning and tuning)
- Enabled and managed via DSCC, on-array UI, and CLI
- DSCC provides workflows to decide whether an action is necessary or not
- There is a single global, customer selectable confidence level
  - Medium – Default confidence level
  - High – Decreases the sensitivity and may cause the ransomware detection engine to delay the reporting of, or miss the presence of actual ransomware
  - Low – Increases the sensitivity but could lead to excessive numbers of false positive notifications
  - The level can be changed by the “RwareConfidence” system parameter
- Anomaly detection is supported with standard Virtual Volumes and VVOLs
  - Enabled and processed per VVOL (rware / no_rware policy) setvv -pol
  - Enabled per-VV Family, per-VV Set, or on the entire Storage System
- Leverages the Virtual Lock feature for easier data recovery
- Supported in air-gapped installations (no internet access required)
- Impact on storage performance is negligible (< 5%)

# B10000 Ransomware in-line detection
## How it works

Available with R5

The internal logic detecting anomalies in the entropy of observed data has several step

| | |
|---|---|
| **Training** | After ransomware protection has been set for a VV, the data stream anomaly algorithm begins a training period of 1 hour (by default) |
| **Sampling** | As data is written to virtual volumes the detection algorithm computes the Shannon entropy of randomly selected block samples |
| **Detecting** | Each sample is passed to two independent algorithms performing different statistical test, returning the indication if the sample consists of encrypted data |
| **Alerting** | If the detection logic suspects unexpected data encryption, and the conditions specified by the “Confidence Level” system parameter are met, the array raises an alert |
| **Reaction** | 1. Create an immediate immutable RO snapshot with the expiration and retention times set in the ”RwareRetentionTime” system parameter<br>2. Raise a major severity alert to the customer<br>3. Flag the RO snapshot with "v_rware_alert"<br>4. Flag the suspicious VV as degraded with "VV_ST_POSSIBLE_RWARE"<br>5. The VV and its snapshots remain fully functional |

# B10000 Ransomware in-line detection
## HPE Cyber Resiliency Guarantee

**Service Overview**

- In the event of an outage resulting from a ransomware incident, HPE support will connect the customer to an outage specialist in less than 30 minutes from the moment the customer calls in
- HPE guarantees that all Virtual Lock (also known as immutable) snapshots created by the customer will be available on the storage array for the duration of the retention period set by the customer

**Terms of the HPE Cyber Resiliency Guarantee**

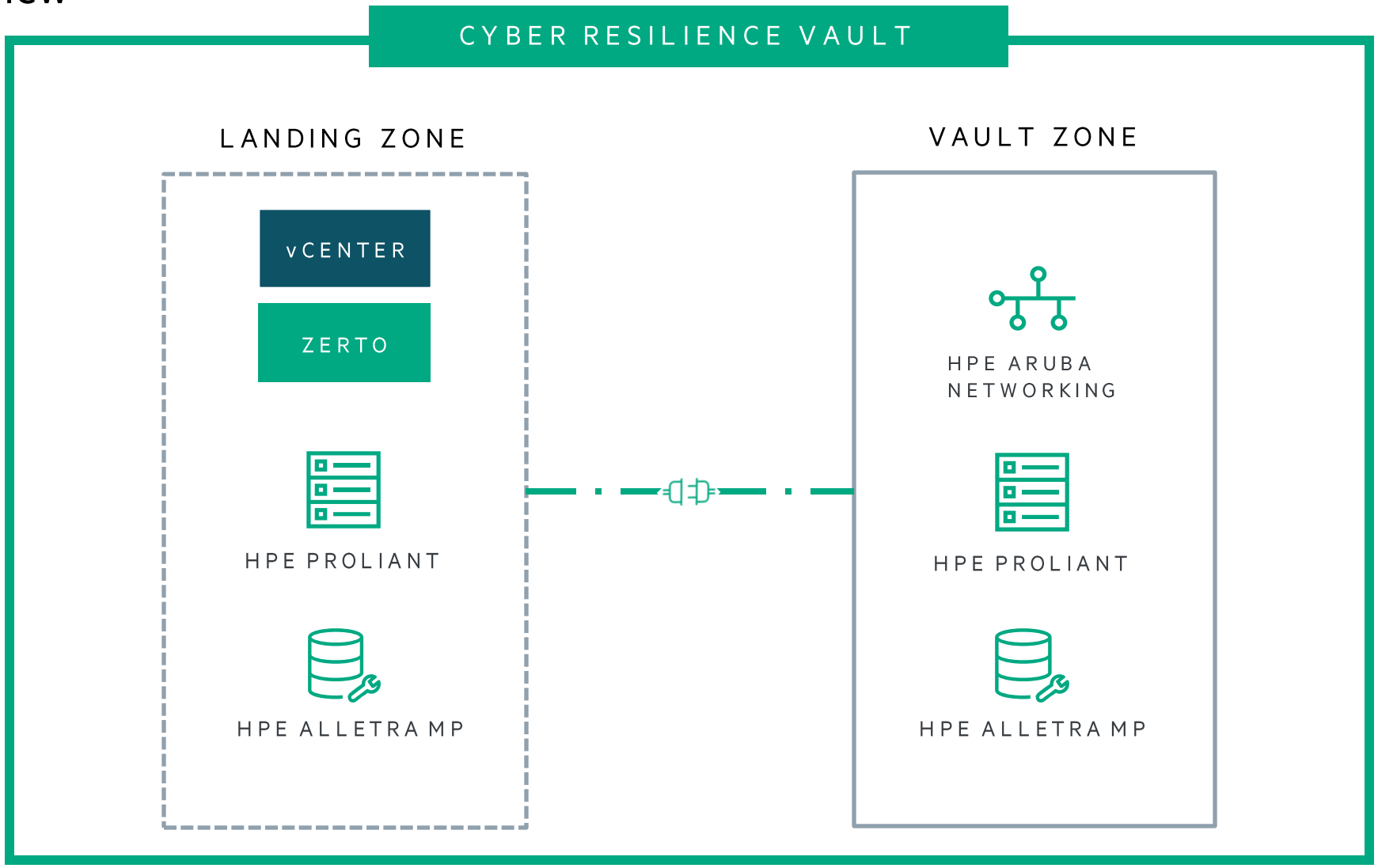
- The B10000 needs to be on OS version 10.5.0 and above
- An active B10000 HPE Tech Care Service Essential or above support contract for 3 years or more is required
- The B10000 should stay connected to Data Services Cloud Console (DSCC), call home (sending telemetry metadata), and be able to receive notifications
  - Ransomware incidents that happen while the system is not connected and not sending data logs back to HPE will not qualify for the guarantee.
- All HPE critical and recommended software updates or OS releases must be applied within 30 days of notification
- Customer must provide timely access for HPE to resolve any issues, including remote access
- In the unlikely event that HPE fails to meet the HPE Cyber Resiliency Guarantee, we will provide you access to free support and SaaS subscription, as determined by HPE at its discretion


HPE Cyber Resiliency Guarantee Brochure

HPE Cyber Resiliency Guarantee Data Sheet

# Zerto Cyber Resilience Vault architecture

## High-level overview



# Veeam hardened Linux repository

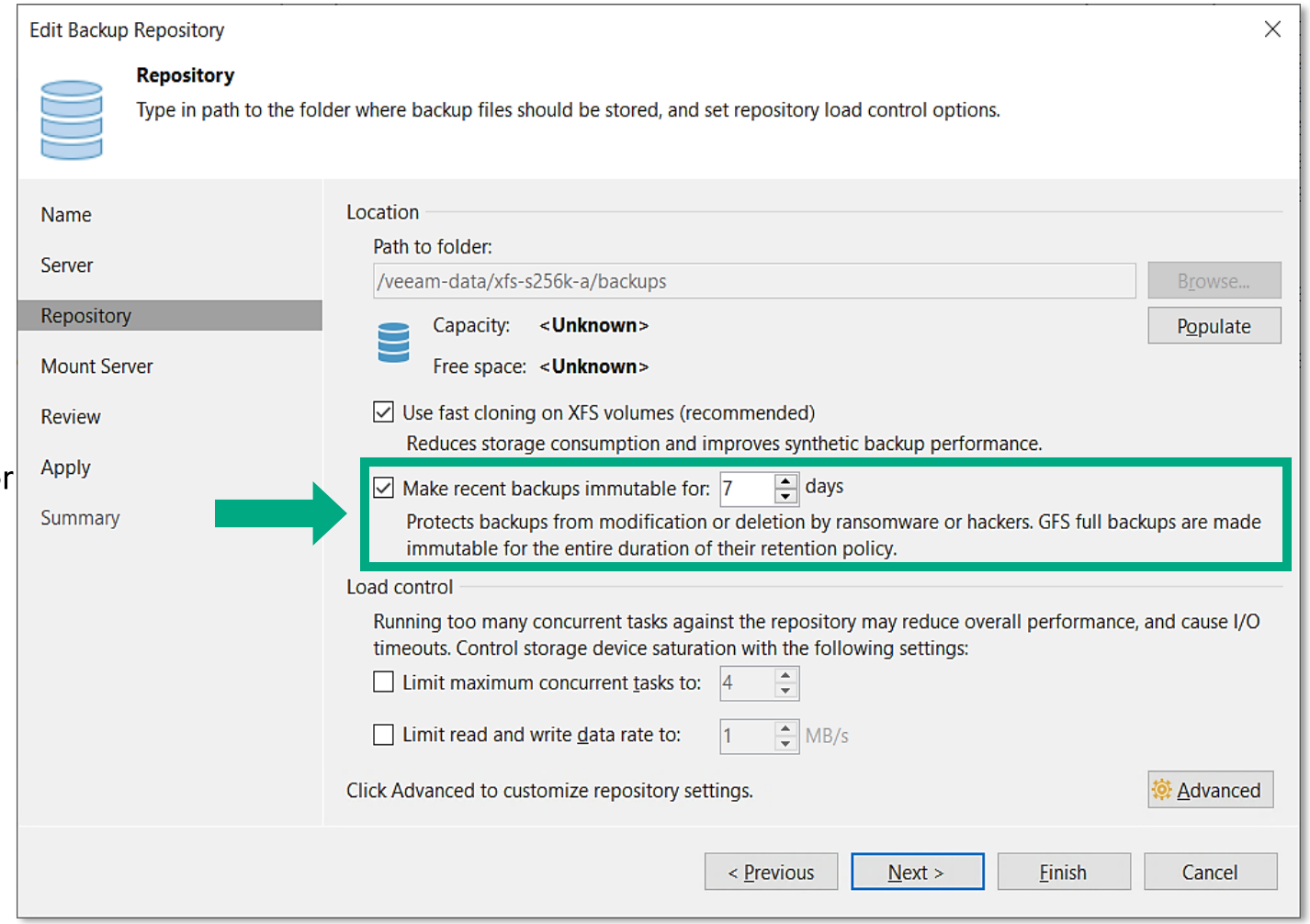
## On-premises immutability for ransomware protection on HPE Alletra 4120 and 4140

### Why HPE Alletra 4120 and 4140?

- High performance and cost-effective for Windows and Hardened Linux
- Optimized backup performance (35 TB/h and 62 TB/h for HPE Alletra 4120 and 4140, respectivey)
- Legendary ProLiant reliability

### Keep your backup on immutable repositories

- Ransomware cannot delete/encrypt your backup
- A hacker using the Veeam GUI cannot delete backup
- Don't use root for prevention as a key-logger can copy it
- Protect your Linux from pkexec privilege escalation




* Measured in HPE lab, June 2022.

Verify: HPE supported Linux distributions

# Scality Ring and Artesca as Veeam repositories

## The enterprise solution for on-premises object storage

SCALITY

VEEAM READY Object

VEEAM READY Object with Immutability

### Tiering and direct backup to object

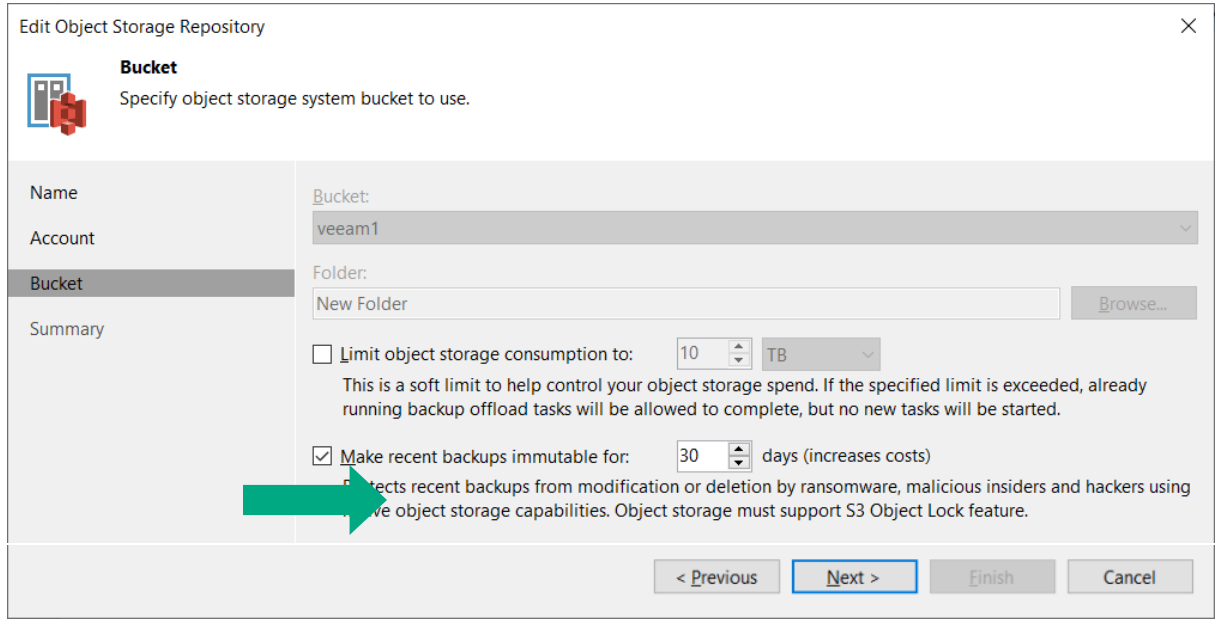
- Direct-backup to on-premises and high-performance S3 repositories
- Immutability and compliance for ransomware protection
- Rich scale-out, clustered, and distributed configurations

### Hardware enforced Immutability

- Veeam-controlled S3 object locking
- No one can remove or change the lock's expiration date
- Designed for ransomware protection

### Use cases

- Backup to on-premises object storage
- Storage-based replication, no need for backup copy jobs
- Customers asking for highly-available scale-out configuration




**Note:** Server with internal disks or HPE StoreOnce is probably still best for price/performance.

Read Veeam article and watch BrightTalk.

# Air-gap and Long-Retention with HPE StoreEver and LTO-9

**3-2-1-1 rule** (3 copies, 2 different media, 1 offsite, 1 offline)

**Air-gap** (offline)

i. Make a backup to Tape,

ii. Eject Tapes from the Library and manually store in a Vault,

iii. One of the moat effective air-gap, but manual handling is prone to human errors.

LTO Ultrium Tape Drive

MSL 1/8 Tape Autoloader

MSL2024 Tape Library

MSL3040 Tape Library

MSL6480 Tape Library

HPE T950

HPE TFinity ExaScale

| | ENTRY LEVEL | SMB & DISTRIBUTED ENVIRONMENTS | | MID-RANGE | | ENTERPRISE | |
|---|---|---|---|---|---|---|---|
| **Form factor** | Half Height | 1U Form Factor | 2U Form Factor | Scales from 3U-21U | Scales from 6U-42U | 47U Form Factor | |
| **Max. slots** | 1 slots | 8 slots | 24 slots | Scales from 40-280 slots | Scales from 80-560 slots | 50 to 10,020 LTO slots<br>45 to 7,614 TS11xx slots | 50 to 53,460 LTO slots<br>45 to 40,680 TS11xx slots |
| **Max. drives** | 1 | 1 | 2 | 1-21 Half Height | 1-42 Half Height | 120 Full Height<br>120 Half Height (T950V only) | 144 Full Height |
| **Max. capacity** | 45 TB LTO-9*<br>30 TB LTO-8*<br>15 TB LTO-7*<br>6.25 TB LTO-6*<br>3 TB LTO-5** | 360 TB LTO-9*<br>240 TB LTO-8*<br>120 TB LTO-7*<br>50 TB LTO-6* | 1.1 PB LTO-9*<br>720 TB LTO-8*<br>360 TB LTO-7*<br>150 TB LTO-6* | 12.6 PB LTO-9*<br>8.4 PB LTO-8*<br>4.2 PB LTO-7*<br>1.75 PB LTO-6* | 25.2 PB LTO-9*<br>16.8 PB LTO-8*<br>8.4 PB LTO-7*<br>3.5 PB LTO-6* | 450.9 PB LTO-9*<br>380.7 PB TS1160*<br>300.6 PB LTO-8*<br>285.5 PB TS1155*<br>190.3 PB TS1150*<br>150.3 PB LTO-7*<br>62.62 PB LTO-6* | 3.05 EB LTO-9*<br>2.03 EB TS1160*<br>1.6 EB LTO-8*<br>1.52 EB TS1155*<br>1 EB TS1150*<br>801.9 PB LTO-7*<br>334.12 PB LTO-6* |

*2.5:1 compression
**2:1 compression

**LTO-9 Tape Media: 18 TB native – up to 45 TB compressed**
**400 MB/s native – up to 1000 MB/s compressed**

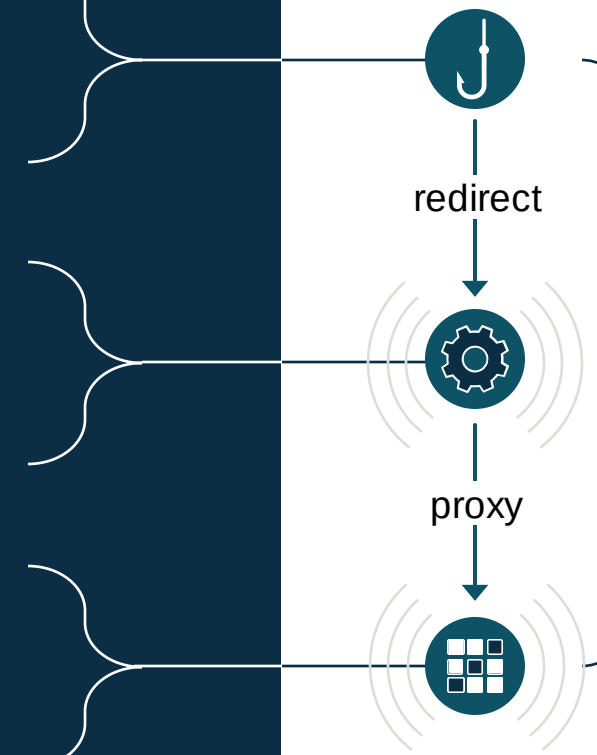
# Metallic ThreatWise

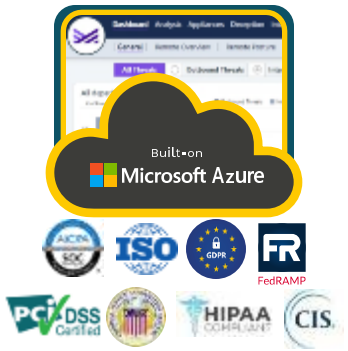
- see NIST SP 800-53, Revision 5

## Lures and Honey-Pots
artifacts that redirect attack toward sensors
- Files, Cached credentials, Bookmarks, etc.
- Unlimited use – no agents

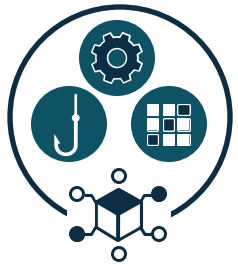
## Sensors
microservices of native interactions
- Clone production assets
- Highest scalability and agility

## Full System
full interaction decoy
- Unlimited interaction
- Fit for specific use cases




## TSOC
ThreatWise Security Operations Console
- Managed and monitored from a secure SaaS environment
- Alerts integrated with SIEM, SMS or Email



## Virtual Appliance / Container
- On-premise, Cloud, IoT and OT
- 100's of Deceptive Assets configured and deployed through each

# iLO protection best practices (1/2)

## iLO must be protected

### What is iLO

- Integrated Lights-Out ("ILO") is a ProLiant technology that enables FW update, and Remote access.
- Most server vendors have similar solutions, iLO is one of the most advanced
- Note: iLO access is considered equivalent to a physical access to the system.

### FW update protection: Protected by the HPE Silicon Root of Trust

1) It is a Firmware technology that protects against firmware attacks, detects compromised firmware or malware
2) It creates an immutable fingerprint in the silicon that verifies the firmware code is valid
3) It includes control on PCI cars FW upgrades

### Remote access protection: Customer ownership to avoid ISO boot attacks

1) The attacker could steal the iLO administrative credentials using a key-logger or other means.
2) The attacker uses a guest in LAN to connect to the target iLO and reboot the system on a ISO image, such as SPP
3) The attacker can delete data in several ways, including using the SmartArray utility to format all disks.

**Note:** All server-based solutions require protection: StoreOnce, Veeam hardened Linux, Commvault HSX, Scality Ring/Artesca, …

Next slide for solution options →

# iLO protection best practices (2/2)

## Problem solution *(multiple options)*

Each of the configuration/best practice below offers effective protection for the ISO boot attack.
Multiple layers may offer better protection, but simplicity is important too. See here for more details: Link1, Link2

1) **iLO with Kerberos and MFA**: Link
   iLO authentication can be forced to use Kerberos with MFA.
   Hackers cannot bypass the MFA protection
2) **iLO Smartcard authentication**: Link
   iLO authentication can be forced to require a CAC Smartcard.
   The hacker cannot physically insert the card in the reader.
3) **iLO with MFA protected VPN**:
   iLO network can be connected to a VPN requiring MFA which is disconnected after a short period of inactivity
   For the hacker it is difficult to take control of a system with an active VPN connection, that was left open.
4) **iLO disconnected**:
   Disconnecting the iLO network cable provides the strongest protection, but it reduces the HW monitoring capabilities.
   StoreOnce doesn't need iLO for HW monitoring because it includes API for direct BIOS communication.

# Considerations for ransomware recovery strategies
## Common best practices independent of attack type (1 of 2)

1) Reserve enough free space on your primary storage to perform the recovery process.
   - Optimal: 50%, acceptable: 35%
   - You need additional space for restoring from a backup
   - Without additional space, you must overwrite the previous data
     (Perhaps not every file is encrypted, and maybe in the future there will be a way to decrypt encrypted files as well.)
   - Be aware of the impact of a full restore on storage snapshots:
     After a full-restore, a storage snapshot uses a lot of capacity. Primary storage deduplication can reduce the impact, but without enough free capacity, you might be forced to delete all snapshots.
   - Acquiring capacity after a ransomware attack makes the recovery time much longer
2) Keep a long-enough backup retention — nine weeks at least, four months optimal.
   - HPE StoreOnce deduplication greatly reduces cost of the additional retention
3) Old data protection rules are not enough for the new threats. Your strategy requires periodic validation.
   - An HPE consultant can help

# Considerations for ransomware recovery strategies
## Common best practices independent of attack type (2 of 2)

4) To recover, you need critical documentation.
   - Save it to off-line storage (you don't want to have it encrypted)
   - Save a document with the list of your servers, OS, IPs, installed SW, PWD
   - If your backup is encrypted, save your PWD offline
5) Have a recovery plan.
   - Assign roles to employees
   - Prepare a list of tasks: disconnect internet, shut down servers and VMs, take storage snapshots, reinstall priority, and so forth
6) It helps to have a contract with a cybersecurity company that can quickly provide a team of experts when a cyber attack occurs to work side-by-side with the local IT team.
7) Test the process at regular intervals. TEST! TEST! TEST!
8) Beware: Cloud storage is not 100% immutable. (Try "forgetting" to pay the next monthly bill … )