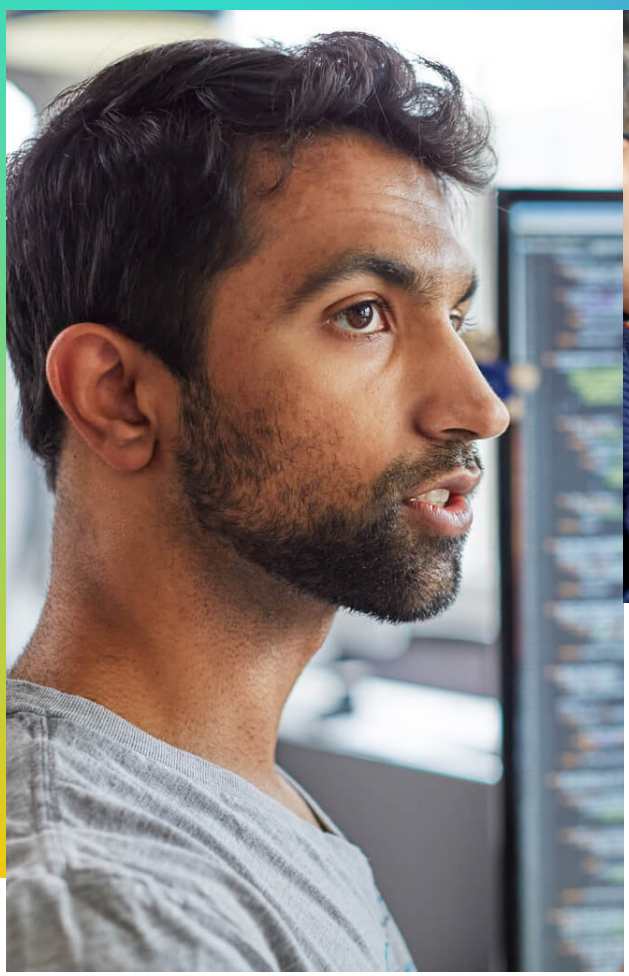






Building digital resilience against ransomware for mission-critical workloads

HPE GreenLake

Growing challenge for cybersecurity — ransomware attacks

In today's digital world, ransomware has emerged as a rapidly growing and pressing cyber-threat that is causing significant concerns for organizations of all shapes and sizes. The magnitude of this problem has elevated to the point where it has become a board-level challenge. It is estimated that by 2031, there will be a ransomware attack on a business, consumer, or device every two seconds, resulting in a total cost of $265 billion.[1]

Banks and financial institutions (FIs) are the preferred targets of ransomware and cyberattacks due to the sensitivity and value of financial data that can be accessed. While FIs have taken steps to implement robust cybersecurity practices, the rapid advancements in ransomware and its potentially devastating consequences necessitate that every institution review and update its controls continuously. FIs are one of the highly regulated entities by national governments because of their preeminence for the financial health of a nation and its citizens. Due to the nature of the threat that ransomware poses, governments have introduced regulations defining the measures that these institutes must put in place to protect themselves against the threat. For instance, the Digital Operational Resilience Act (DORA), the new European Union (EU) regulation, brings new digital resilience requirements that aim to safeguard sensitive data and protect FIs against cyber-threats. DORA mandates all financial entities make sure they can withstand, respond to, and recover from information and communication technology (ICT)–related disruptions. It also applies to critical third parties, which provide ICT-related services to financial entities such as cloud platforms, solution/software vendors, data analytics and audit services. Similarly, there are regulations/guidelines set by governments and federal regulatory bodies in the United States, UK, India, and others across the world.







When and where to recover from a ransomware attack

Recovery-point objective (RPO) (how much data you can afford to lose) and recovery-time objective (RTO) (how fast you can recover your data) are vital for your business continuity plan, and ransomware can cause hours of downtime and data loss. According to Statista, the time to recover from a ransomware attack can be as high as 20 days or more. For businesses that rely on mission-critical workloads, a prolonged recovery period can be devastating. That is why it is crucial to put safeguards in place to protect your production environment and data against ransomware attacks. In addition, contingency plans must be put in place to minimize downtime and ensure a quick and efficient recovery of the production environment (application stack) and also the complete recovery of valuable data so that operations can resume expeditiously.

[1] "Digital resilience against ransomware for payment switching providers," HPE, 2023

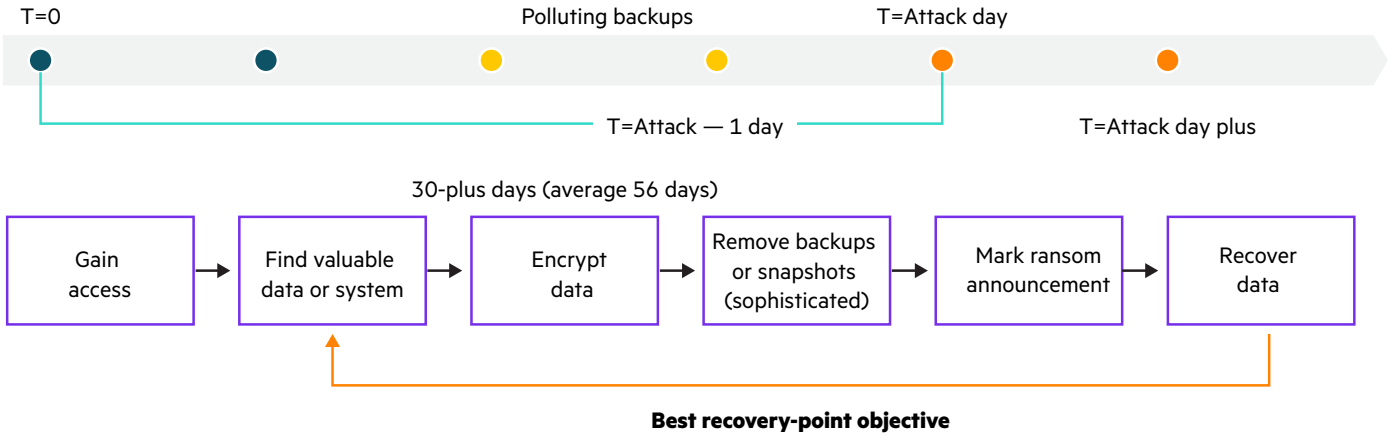


Figure 1. Timeline of a ransomware attack

Ransomware attacks are insidious, hidden, and can be ongoing for a long time before being detected. Data must be protected for a period longer than an attack that has been occurring to ensure there is a copy of data to recover from. Figure 1 provides perspective on the timeline of a ransomware attack. According to a Sophos report, the attacker is typically in the system anywhere from three days to two months to six months — also called the dwell time — wherein that person goes about encrypting data and any backup points available.[2] Once the attacker is confident that the target does not have a possible recovery point, they announce a successful ransomware attack and demand ransom. So, a recovery strategy should have a deep archival of data recovery points, at least for six months, so that, should the customer decide to go far back, it's possible to do so. For customers and use cases where resumption of operations (low RTO) is important and requires little or no data recovery (very low RPO), such as payment switch providers, we have a separate service outlined in "Digital resilience against ransomware for payment switching providers" document, where an air-gapped and isolated standby system is kept ready (and managed for you) to take a transaction processing in very less time (with just having a copies of endpoint and routing data as the main verified / backed-up source).

[2] news.sophos.com/en-us/2023/04/25/2023-active-adversary-report-for-business-leaders/

A digital resilience framework for HPE NonStop systems

To neutralize the effects of such cyber-threats including ransomware attacks, Hewlett Packard Enterprise follows the digital resilience framework as set by the National Institute of Standards and Technology (NIST). The goal of this framework is to protect IT environments to help minimize downtime, allowing customers to bring up their mission-critical workloads quickly and efficiently in case of a ransomware attack.

The digital resilience framework as defined by NIST and applied for HPE NonStop systems consists of the following five stages (see Figure 2):

- **Identify:** Discover the customer environment and identify how to meet regulatory and compliance requirements, prioritize risk management efforts, and streamline operations to reduce time and resources required to manage and maintain. HPE offers services on the HPE NonStop platform to help you perform this exercise in a systematic manner using smart tools.

- **Protect:** Based on the findings from the identify stage, implement best practices from various compliance frameworks and security controls to reduce the identified attack surface. HPE has a rich portfolio of security products to help you achieve this important step. Three key elements to keep in mind are:
  - Have zero trust security, control access to each resource and control changes to its settings through diligent measures
  - Protect data, the treasure that is the main target of attack
  - Harden every product you use in your environment for security and refresh your knowledge periodically. Review your security settings periodically, at least once a year, to explore further improvement measures.
- **Detect:** A rigorous security monitoring goes a long way in identifying latent threats and malicious actions before they could cause harm. Customers need to implement a comprehensive security management and analytics solution for HPE NonStop systems and applications, with real-time risk management, threat detection, vulnerability assessment, compliance reporting, and integrity monitoring resulting in improved threat identification and quicker security incident alerting.
- **Respond:** Establish standard operating procedures to respond to critical security events which point toward harm or impending harm. Identify the possible actions to take under different scenarios and practice them regularly through simulated alerts. It could be isolating the resources, disabling user access, stopping optional workloads, and perhaps many more.
- **Recover:** Establish a sophisticated recovery strategy to recover workloads and recover data. Implement a backup solution based on our best practices to recover from a ransomware attack by meeting your company's RPO and RTO requirements. If possible, divide your workloads and data into multiple tiers. The most important tier is the one you need in order to come back to service, which your customers (and regulators) expect to be available the soonest post an attack. HPE recommends the **3-2-1-1 rule for data recovery**, which is covered in a later section.

Let us look at some of the details of implementing the previously mentioned framework in terms of protection and recovery for HPE NonStop workloads.

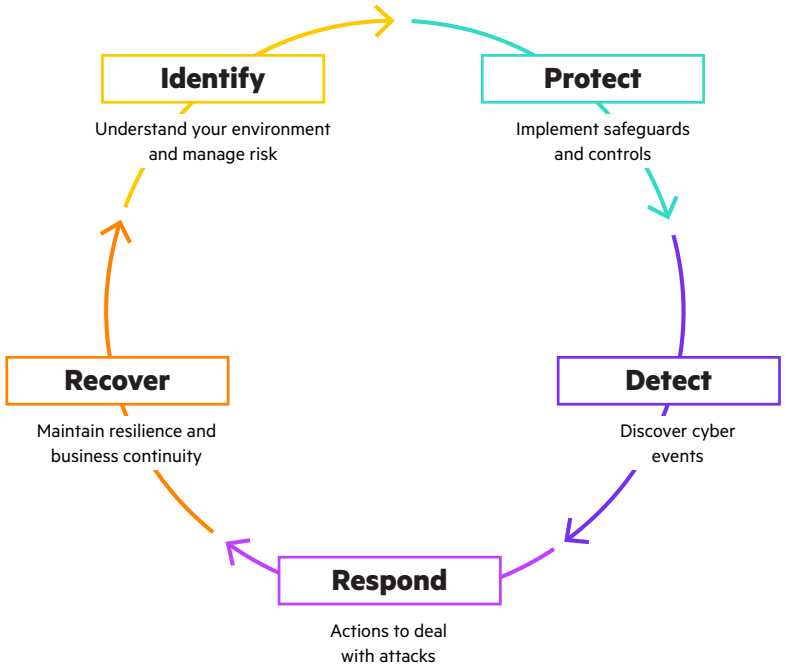


Figure 2. Five-stage digital resilience framework for HPE NonStop systems

Protection and recovery — the two pillars of digital resilience

Good news is that HPE NonStop customers have been implementing robust security and data protection measures and also complying with regulations such as Payment Card Industry Data Security Standard (PCI DSS) and General Data Protection Regulation (GDPR). Much of these can be leveraged for implementing compliance with ransomware protection regulations such as DORA.

Implementing zero trust security requires fine-grained access control, division of responsibility — administrator versus data, multi-factor authentication (MFA) without exception (now a PCI 4.0 requirement), watertight user administration, password vaulting for privileged accounts, and control/traceability to changes in user settings.

The importance of file integrity monitoring (FIM) is paramount with regard to ransomware protection — ransomware is just foreign, unauthorized software in your system. Integrity monitoring solutions are meant specifically to detect attempts to change/introduce unauthorized objects and actions. Ransomware attacks are typically low and slow. The attacker operates below the radar to determine your environment, identify the recovery points, access them, and block their access before taking control of production data and encrypting it. Detecting this by manual review of daily logs is not only tedious but can also be ineffective against sophisticated attacks such as advanced persistent threats. Sophisticated monitoring, built with the power of artificial intelligence (AI) / machine learning (ML) is the solution to look for, and HPE NonStop together with their partners has such capabilities.

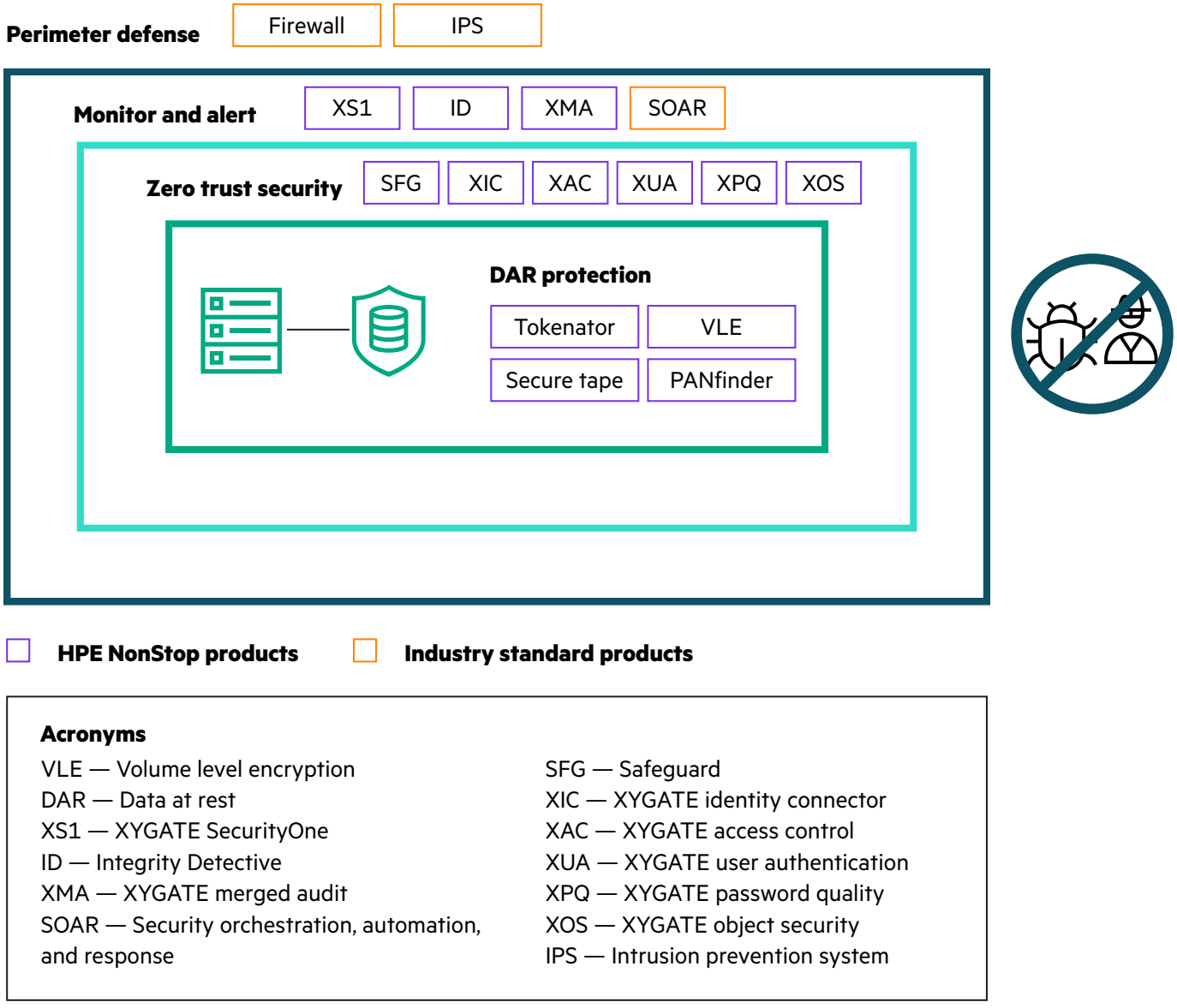


Figure 3. Multi-tier protection for HPE NonStop environment

Ransomware recovery architecture for HPE NonStop



The ability to recover from a ransomware attack without having to pay a ransom is becoming a requirement for enterprises. Ransomware protection is more important because a ransomware attack can infect and render unusable not only the primary production site data but also the disaster recovery (DR) site data, and even backup data, making recovery impossible unless special precautions are taken to protect the data. This means that a typical disaster-tolerant or DR solution is not sufficient to protect the data and enable recovery from a ransomware attack.

The recovery strategy in such a case would involve a separate HPE NonStop backup system, maintained in an air-gapped site — physically isolated with no network connectivity but having resources required to do the setup if this system were to take over the workload. It is also recommended to administratively isolate this system, which means that the users/administrators accessing the system should be different from those managing the production site, to improve security. In addition to maintaining an air-gapped system, implement our recommended 3-2-1-1 rule that says to maintain three copies of your data and use two different media types, one off-site copy to the cloud and one off-site copy to the tape. The principle of operation for HPE NonStop is as follows:

1. Divide your data into tiers based on the criticality of their need to establish the bare minimal operation post a successful ransomware attack.

2. On a regular basis create HPE NonStop transaction management facility (TMF) online dumps. Generate them more frequently for those files/volumes that are most critical for your service resurrection.

3. Rebuild those files/volumes using TMF dumps and audit trails. Successful rebuilds through TMF imply that those files are valid recovery points. Of course, this does assume that dumps/audit trails encrypted through ransomware lead to the failure of rebuilding those files through TMF.

4. Maintain the history of these files up to a short period — a few days or weeks in your production site. These are the first set of candidates to recover, in case of a successful ransomware attack. These files should be under the watch of a file integrity check that would detect any attempts to alter them.

5. Securely FTP the TMF dump files and audit trails to the remote backup site. Ensure that the client pulling the data from HPE NonStop is in a separate physical LAN with firewalled access to the system.

6. Like how you build the files in the production site, build them in the backup site as well. Keep your backup site resources administratively isolated so that there are no common set of users and administrators having access to both the primary and backup sites. Consider using HPE Managed Services to manage the backup system and resources to perform these tasks.

7. Once successfully built, using fingerprint comparison, ensure that the recovery files/volumes created in primary and backup sites are identical so that the data are not tampered with before being transferred to the backup site. This site can have data in greater depth — running into several months. This is to have a viable recovery option should an attacker manage to encrypt the production site data. Place these volumes under integrity check to detect any attempt to alter them. From this site, backup these volumes to immutable cloud storage such as Amazon S3. Alongside, also create a backup of these into tape drives, physically remove those tapes from the tape drives, and keep them in an air-gapped location. This will be the last line of defense, that is, should all your recovery points be invalidated/encrypted, the tapes (because they are not accessible through any datapaths) have the highest chance of survival.

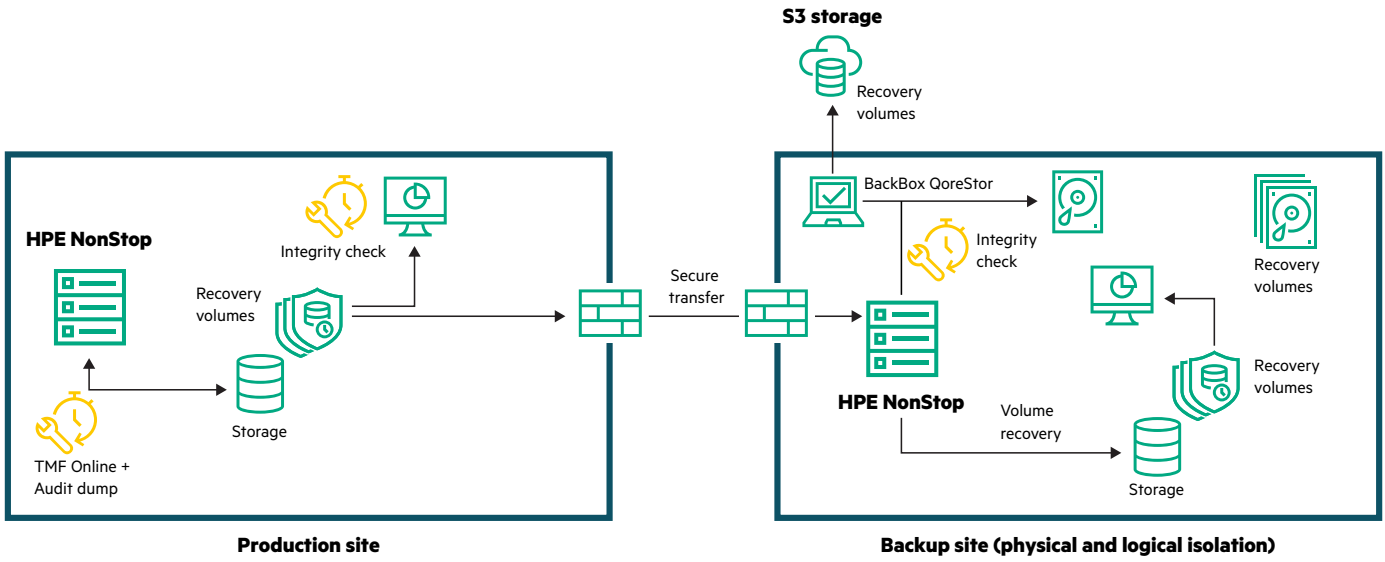


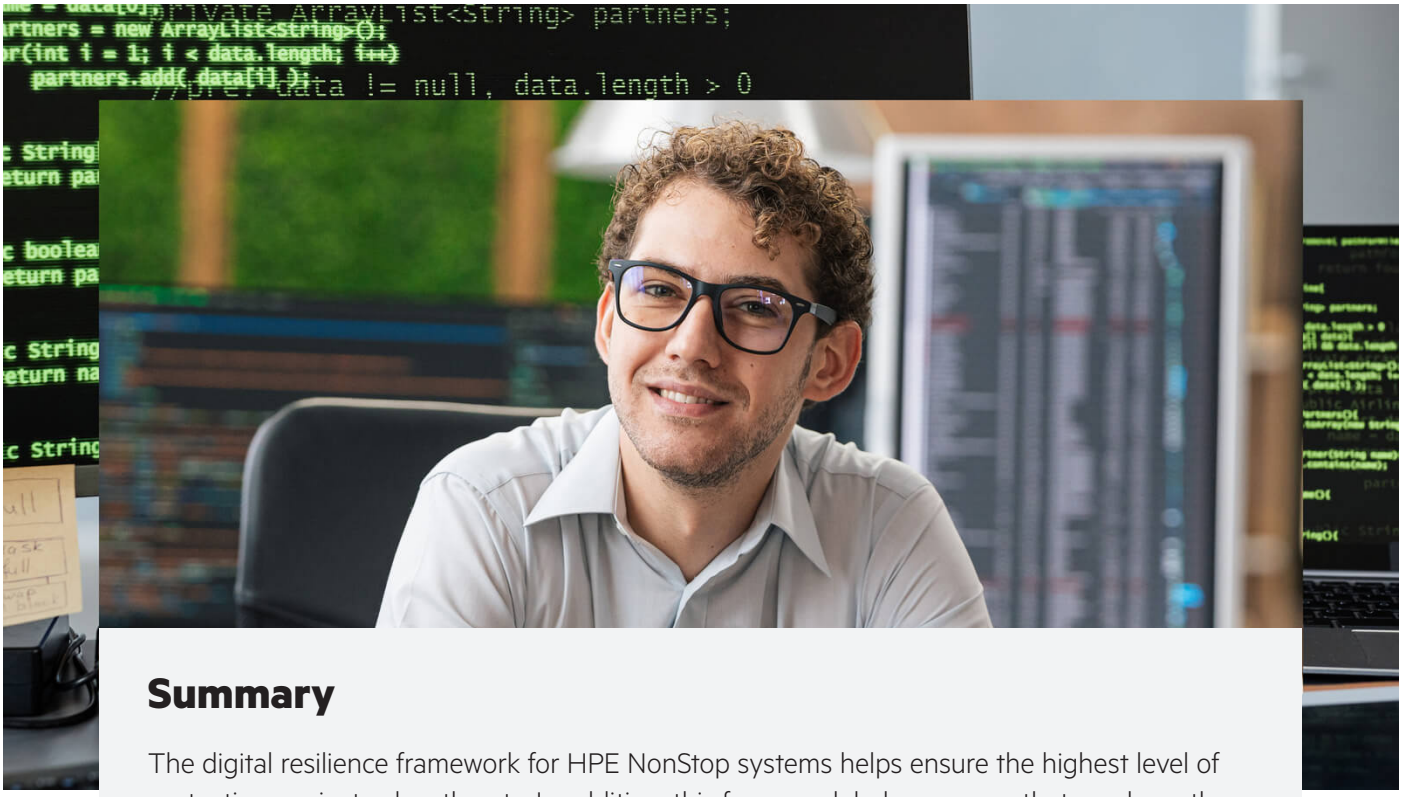
Figure 4. Ransomware recovery 3-2-1-1 rule as applied to HPE NonStop

A sample implementation of the digital resilience framework

A generalization and summary of the process to navigate compliance and regulatory requirements while also strengthening the security is described in Table 1. This process needs to be highly customized for each customer since the requirements are so unique and different based on existing customer environments.

Table 1. Sample framework implementation

Framework category	Solution / service details	Stakeholder/timelines	Customer benefit
Identify	Security gap assessment (scan, identify, and assess security misconfiguration, compliance status, and other attack vectors)	HPE: 10–14 weeks Customer: 6–8 weeks	Prioritization of cost and effort
Protect	Security hardening service (implementing best practices based on findings from the gap assessment)	HPE: 10–14 weeks (parallel with detect and respond phase) Customer: 6–8 weeks	Reducing the attack surface based on gap analysis; Data at rest encryption to protect from physical theft
Detect **Incident response**	Deploying tools for complete security management based on customers' IT environment (includes risk management, threat detection, vulnerability assessment, compliance reporting, and integrity monitoring)	HPE: 10–14 weeks (parallel with protect phase) Customer: 6–8 weeks	Comprehensive real-time visibility of the environment and apps via automation, management, and reporting
Recover	Workshop to understand backup and recovery options and how they work	HPE and Customer: 3–4 days	Understand gaps, needs, and actions around backup architectures/implementation
	Understanding (and moving to) on-prem and cloud immutable storage options	HPE: 3–4 days (planning and migration)	Helping ensure backup data security
	Ready-to-go relief system (third site) for risk mitigation against an actual attack	To be assessed (working closely with all stakeholders)	Air-gapped isolated systems, untouchable until used in a disaster scenario
	Fast recovery/replication to backup/ relief system	To be assessed	Reducing recovery time



Summary

The digital resilience framework for HPE NonStop systems helps ensure the highest level of protection against cyber-threats. In addition, this framework helps ensures that you have the right data protection solution in place to recover your mission-critical workloads from any potential ransomware attack.

Learn more at

HPE.com/info/NonStop

Visit **HPE GreenLake**

Chat now (sales)

Hewlett Packard Enterprise

© Copyright 2023 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a50008913ENW