Zerto
a Hewlett Packard Enterprise company

Achieving NIS2 Compliance with Zerto

The current threat and regulatory landscape pressures organizations to establish capabilities to prepare for and manage a cyberattack effectively and efficiently. During recent years, we have noticed that cyberattacks targeting critical infrastructure have increased worldwide. Additionally, the explosion of remote work opened new vulnerabilities, resulting in an increase in individuals who fell for phishing attacks.

As organizations navigate the evolving landscape of cybersecurity regulations, compliance with NIS2 becomes critical. Zerto, a Hewlett Packard Enterprise company, is a leader in the disaster recovery and data protection industry and aligns with these regulations to enhance overall security.

Understanding NIS2

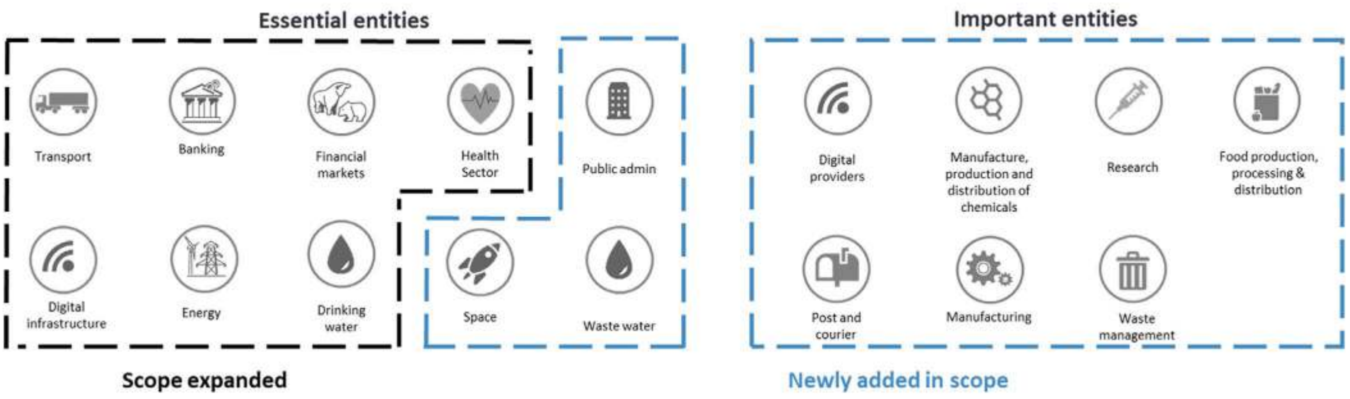
NIS2 (Network and Information Systems Security Directive 2)

a. Objective: NIS2 aims to improve the security and resilience of critical infrastructure across various sectors, ensuring the networks and systems they use to deliver services and conduct their activities attain a higher level of cybersecurity.

b. Requirements: Entities will be required to put governance structures in place to manage cybersecurity, comply with breach reporting obligations, implement risk management practices, and monitor the supply chain for cybersecurity risks.

    i. Essential entities, including the energy, transport, health, digital infrastructure, and cloud sectors, will be subject to greater scrutiny and up-front regulations. Regulators will be able to perform audits and carry out inspections. Fines can go up to €10,000,000 or at least 2% of total annual turnover.

    ii. Important entities, including medical devices, chemicals, electronic and social networks, will only be subject to investigation where there is evidence of non-compliances. Fines can go up to €7,000,000 or at least 1.5% of annual turnover.



Source: EY.com

How Zerto Can Help NIS2 Compliance

> **Article 21, Cybersecurity Risk Management Measures**
>
> Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.

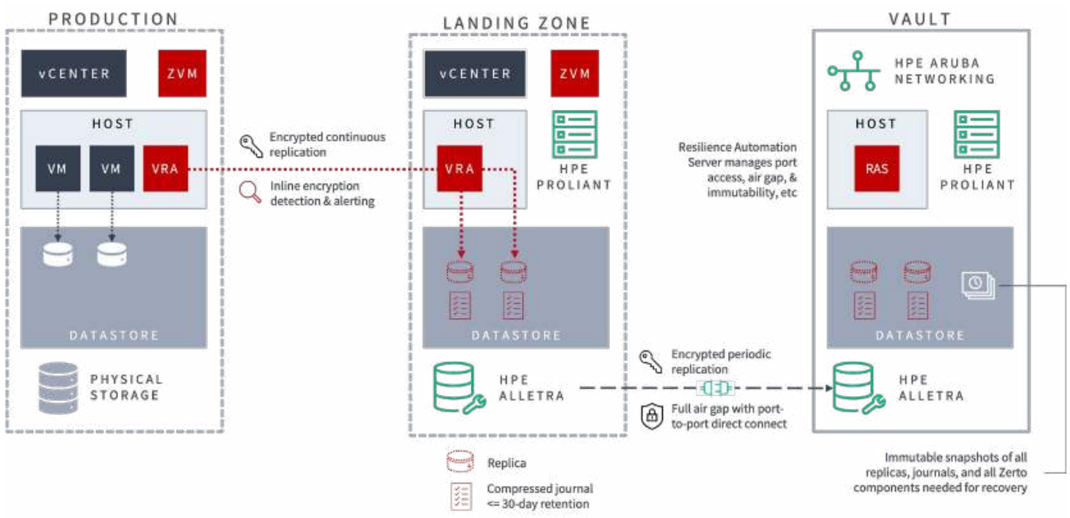
Continuous Data Protection

Zerto delivers resilience, continuity, and availability through high-performance continuous data protection (CDP). CDP continuously tracks and mirrors data changes automatically, replicating every version of the data to a local or remote site. Journal-based technology logs all the changes that occur in a specified timeframe, enabling point-in-time recovery in increments of seconds. With thousands of restore points throughout the journal history, CDP minimizes the risk of data loss. Zerto reduces operational impact in event of a cyber event.

Real-Time Encryption Detection

With the growing threat of ransomware, the risk of potential breaches couldn't be higher. Zerto addresses this vulnerability with real-time encryption detection, leveraging algorithmic intelligence to swiftly alert users to encryption anomalies indicative of ransomware initiation. This feature not only provides notifications within seconds but also automates the tagging of checkpoints in the journal to facilitate the distinction between recovery points before and after the anomaly, as well as to indicate the proposed blast radius.

Cyber Resilience Vault


PRODUCTION
vCENTER
ZVM
HOST
VM
VM
VRA
DATASTORE
PHYSICAL STORAGE
Encrypted continuous replication
Inline encryption detection & alerting
LANDING ZONE
vCENTER
ZVM
HOST
VRA
HPE PROLIANT
DATASTORE
HPE ALLETRA
Replica
Compressed journal <= 30-day retention
Resilience Automation Server manages port access, air gap, & immutability, etc
Encrypted periodic replication
Full air gap with port-to-port direct connect
VAULT
HPE ARUBA NETWORKING
HOST
RAS
HPE PROLIANT
DATASTORE
HPE ALLETRA
Immutable snapshots of all replicas, journals, and all Zerto components needed for recovery

The Cyber Resilience Vault is a comprehensive solution that empowers essential and important entities to implement appropriate technical and operational measures for effective cybersecurity risk management. The vault is positioned as a key player in achieving rapid air-gapped recovery post-ransomware attacks, utilizing a combination of HPE Alletra, HPE ProLiant, HPE Aruba Networking, and Zerto.

The vault serves as an isolated cleanroom, ensuring complete air-gapping through a proprietary protocol for point-to-point replication, boasting aggressive RPO and RTO. Inside the vault, the Resilience Automation Server takes charge of crucial cyber resilience measures, overseeing port management, snapshot creation, and activity logging. Zerto's vault addresses various key items outlined in Article 21, such as emphasizing risk analysis, security, security in network and information systems acquisition, and policies and procedures to assess the effectiveness of cybersecurity risk management measures.

> ### Article 23, Reporting Obligations
>
> The competent national authorities or the CSIRT shall provide, without undue delay and where possible within 24 hours of receiving the early warning referred to in paragraph 4 point (a), a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures.

Testing and Reporting

Zerto provides fully automated, nondisruptive, and granular failover testing in a sandbox environment for recovery assurance, with detailed reporting functionality to document proof of compliance during audits and inspections. A single person can test recovery operations in minutes without impacting the production site. For multi-cloud and multisite monitoring, you can leverage Zerto Analytics to analyze and report on the data streaming in from all protected sites and applications.

Achieving Regulation Readiness

Zerto stands at the intersection of NIS2, offering a comprehensive solution that enhances both organizational security and product security. For businesses seeking robust disaster recovery and data protection, Zerto is a proven reliable partner for navigating the complexities of the EU cybersecurity regulations.

This document is a snapshot of how Zerto can assist with NIS2 compliance. The solution has additional features beyond those specified above. With Zerto, businesses are better equipped to navigate the complex landscape of compliance, ensuring a resilient and sustainable digital future.

Learn more about how we handle compliance.

Learn More

About Zerto

Zerto, a Hewlett Packard Enterprise company, empowers customers to run an always-on business by simplifying the protection, recovery, and mobility of on-premises and cloud applications. Zerto eliminates the risk and complexity of modernization and cloud adoption across private, public, and hybrid deployments. The simple, software-only solution uses continuous data protection at scale to solve for ransomware resilience, disaster recovery, and multi-cloud mobility. Zerto is trusted by over 9,500 customers globally and is powering offerings for Amazon, Google, IBM, Microsoft, and Oracle and more than 350 managed service providers.
www.zerto.com