Hewlett Packard Enterprise

Server infrastructure security solutions for GDPR compliance

GDPR, NIST 800-53, ISO 27001, and IT

Contents

Technical white paper

Disclaimer

The purpose of this document is to help organizations understand how the HPE solutions can be utilized to help comply with certain elements of the EU General Data Protection Regulation (GDPR) requirements. The information contained in this document is not intended and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines.

Introduction

The trend toward more security regulations can, in part, be explained by the rise in data breaches and cybersecurity incidents. The GDPR is a new European privacy law that introduces new and more stringent requirements for organizations that collect and use personal data and significant penalties for compliance failures.

GDPR key provisions

The GDPR contains 99 articles and 173 recitals covering process and the operational aspects of data protection, including requirements that directly impact the way organizations implement IT security.

Organizations must be able to show how data is acquired, how it is handled, stored, and secured and how it is treated at end of life.

Some of the key areas include:

- Privacy by design: By default, data protection should be included from the onset of the design of systems. Store and process only that data, which is absolutely necessary.
- Consent: If an organization relies on consent it must be explicit. It will no longer be possible to rely on implied consent to individuals having the option to opt-out.
- Breach notifications: Mandatory notification to regulators is now required for personal data breaches within 72 hours of the organization becoming aware. Individuals must also be notified if there is a high risk that the rights and freedom of individuals could become compromised.
- Right to be forgotten: A new right that enhances existing rights for an individual to require an organization to erase their personal data.

If an organization fails to comply with the GDPR they are at risk of fines up to or greater than €20 million or 4% of the annual worldwide company turnover. Damages claims can also be brought by individuals or a consumer organization on their behalf.

Who needs to comply

The GDPR has a broad territorial scope and applies to all organizations established in the EU, regardless of whether the data is processed inside or outside the EU. It also includes organizations established outside the EU that offer goods and services to individuals in the EU.

Any company that handles European personal data must begin preparing now if they haven’t already. That includes multinational organizations working across the EU, many of whom will need to designate a data protection officer (DPO) to manage GDPR compliance across all corporate operations and IT systems.

GDPR and technology

GDPR is not specific when it comes to technologies to be deployed. It is up to organizations to determine that the technology they use to process personal data complies with the GDPR. In the case of security, Article 32 requires organizations to implement “appropriate technical and organizational measures to ensure a level of security appropriate to the risk.” It goes on to suggest the following as examples of what may be appropriate—“The pseudonymization and encryption of data; ability to ensure confidentiality, integrity, availability, and resilience of processing; the ability to restore data after an incident; and a process for testing, assessing, and evaluating effectiveness of security.”

GDPR introduces mandatory breach notifications for breaches of security that lead to the unauthorized or unlawful destruction, loss, alteration disclosure, or access to personal data. National DPAs must be notified of these breaches. Depending on the nature and severity of the breach, including the effectiveness of the controls in use to protect the data, they may also need to notify the affected individuals.

Time to assess infrastructure risk

For many organizations, the increased compliance risks presented by the GDPR will be the catalyst to assess the robustness of data protection processes and server infrastructure security.

Cyber attacks are becoming more sophisticated. The traditional perimeter and prevention response to threats is no longer realistic. Adversaries possess sophisticated levels of expertise and significant resources to achieve their objectives by using multiple attack vectors (such as cyber, physical, and deception). Objectives typically include establishing and extending footholds within the IT infrastructure for purposes of exfiltrating information, undermining business operations, or positioning itself to carry out these objectives in the future.

Today, cybercriminals typically gain access to data not by penetrating the impenetrable perimeter but rather through human error or social engineering. For example, someone's curiosity is piqued by a USB stick found in a parking lot, or someone opening a very authentic looking email and unwittingly giving away network credentials, and so on. A 2016 Harvard Business Review cybersecurity study found that 60% of security breaches in the data center were the result of employees or contractors. Of those internal breaches, 75% were conducted with malice or criminal intent and 25% from negligence. For a hacker with low ethical standards, this is the most surefire way to gain access to sensitive data—people will always be people. Nobody is hyper-vigilant all the time, and hackers will be waiting to take advantage.

Given the world we live in, where no server is safe and all data is exploitable, the focus of IT should expand from "protect" only to "protection, detection, and recovery." Assuming malware is going to find its way into a data center, how quickly can an organization detect the threats? Furthermore, how prepared is an organization to respond by removing the threat and recovering from the damage?

Fortunately, tools and standards do exist to provide a framework that can be tailored to an organization's specific regulatory requirements. This paper will discuss security controls described by the US National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).

National Institute of Standards and Technology

The NIST is becoming more well known outside of North America through cooperative initiatives such as the one with the EU Joint Research Centre's Institute for the Protection and Security of the Citizen focusing test methods and assessments of security for physical infrastructure.

NIST is part of the U.S. Department of Commerce and is one of the oldest physical science laboratories in the U.S. that provides technology, measurement, and standards across a wide range of products and services.

Part of their charter is to implement practical cybersecurity and privacy through outreach and effective application of standards and best practices, designed primarily for federal agencies that are appropriate to meet the GDPR requirements.

NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations is a publication that recommends security controls for federal information systems and organizations. It is a catalog of security controls that provide a holistic approach to information security and risk management. What's more, it strengthens information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber attacks and other threats.

The catalog of security controls in NIST 800-53 can be effectively used to protect information and information systems from traditional and advanced persistent threats in varied operational, environmental, and technical scenarios. The controls can also be used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements.

ISO/IEC 27001

ISO/IEC 27001 specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information risks. The ISMS is an overarching management framework through which the organization identifies, analyzes, and addresses its information risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities, and business impacts.

The standard covers all types of organizations (such as commercial enterprises, government agencies, non-profits, and more), all sizes (from micro-businesses to huge multinationals), and all industries or markets (for example, retail, banking, defense, healthcare, education, and government). Organizations adopting ISO/IEC 27001 are free to choose whichever specific information security controls are applicable to their particular information risks, drawing on those listed in the menu and potentially supplementing them with other options (sometimes known as extended control sets).

The security controls structure in NIST 800-53 is very similar to that of ISO 27001. Its 256 controls are organized into 18 families (against the 114 controls organized into 14 categories on ISO 27001), each one containing controls related to the general topic of the family such as ISO 27001. Controls in each family may cover aspects related to policy, oversight, supervision, manual processes, and actions by individuals, or automated mechanisms, depending upon their application (for example, management, operational, or technical). Additionally, NIST 800-53 also provides one family of 16 controls to the 256 security controls, which manages information security programs, and 14 controls, grouped into three families, for privacy protection.

The entire NIST 800-53 controls apply to an ISO 27001/2 certification. NIST provides mapping tables to provide organizations with a general indication of security control coverage.

Secure infrastructure solution from HPE and NIST 800-53 controls

Hewlett Packard Enterprise has taken steps to provide customers with a strong server infrastructure security baseline by contracting an outside firm to apply NIST 800-53 security controls to an HPE solution set of servers, networking, and storage. This is a rigorous process that includes integration, security control development, documentation, risk assessment, and vulnerability/penetration testing of a complete stack of HPE and partner technologies against NIST standards and controls.

This information will allow organizations to leverage the solution for assist with GDPR compliance. Additionally, this provides a ready-made Authority to Operate (ATO) accreditation package, which includes over a dozen documents and hundreds of pages. It's likely to shorten the accreditation cycle by more than 50% and provide assurance that the systems will stand up to the rigors of their agency accreditation and ongoing Continuous Diagnostics and Mitigation (CDM) processes.

The solution includes HPE 3PAR storage, HPE ProLiant, and HPE Apollo servers enclosed in the HPE rack system. It includes a full stack of cloud-enabling software such as Arista EOS and CloudVision, DoubleTake, Red Hat® KVM Hypervisor, Red Hat CloudForms, Red Hat OpenShift, Red Hat Ansible, Red Hat Ceph, AlienVault USM, Cloud Cruiser, and Aruba ClearPass.

The rigor and broad acceptance of the NIST standards and Risk Management Framework (RMF) provide broad applicability for controls across industry verticals including healthcare (HIPAA), energy (NERC CIP), retail (PCI), financial (GLBA), and EU personal data (GDPR/ISO 27001).

In summary, all the controls in the NIST framework can be leveraged directly toward achieving ISO 27001 series accreditation. As customers prepare for the enforcement of GDPR, the NIST controls that Hewlett Packard Enterprise is providing will also help organizations establish a strong server infrastructure security baseline.

HPE Gen10 Server Security

An organization's security plan should include locking down the data center, devices on the edge, the perimeter, along with the infrastructure that houses, computes, and manipulates data. That data, whether at rest, in use, or in flight, requires the highest levels of protection. Absolute protection has to begin with absolute trust. And absolute trust must be rooted in the silicon to protect against the lowest level of attacks. HPE Gen10 servers include silicon root of trust that provides protection as soon as the server is powered on.

HPE Integrated Lights-Out (HPE iLO) startup code includes a cryptographic algorithm (hash) that is permanently burned into the silicon. The silicon validates the HPE iLO 5 firmware code before it is fetched and executed. If any malware or compromised code has been inserted in the firmware, the silicon will detect it because any infected firmware code would be altered and, therefore, not match up with the hash burned into the silicon. From there, the HPE iLO 5 firmware validates the rest of the server firmware, namely the Unified Extensible Firmware Interface (UEFI), System Programmable Logic Device (SPLD), Innovation Engine (IE), and Management Engine (ME). The UEFI then validates the connection to the operating system through Secure Boot, completing a chain of trust anchored in the silicon. More than a million lines of firmware code run before the operating system starts, making it essential to confirm that all server essential firmware is free from malware or compromised code.

During operation of the server, Hewlett Packard Enterprise has a unique technology that conducts run-time firmware verification to check the firmware stored in the server. At any point during operation, if compromised code or malware is inserted in any of the critical firmware, an HPE iLO audit log alert is created to notify the customer that a compromise has occurred. This is achieved by storing HPE iLO 5 and UEFI firmware in non-volatile flash memory, which is thoroughly scanned at regular user-determined intervals and stored in a separate lock-box location inside the server. The contents of the firmware stored in memory must be correct, right down to the individual part, or else it is flagged as compromised. The recovery will begin on a previous version of the firmware that is known to be authentic and good.

HPE Storage

GDPR compliance depends on a manageable, scalable, simple, and reliable data protection strategy that manages both data and storage as one cohesive entity. Our portfolio of HPE 3PAR StoreServ, HPE Nimble Storage, and HPE StoreOnce Systems can create a firm foundation for a comprehensive data protection strategy. Recently acquired HPE Nimble Storage is ideal for advanced, flash-optimized data services, including all-flash, hybrid-flash, and multi-cloud support, underpinned by machine learning-based predictive analytics.

HPE 3PAR StoreServ storage arrays centralize and consolidate production data. Optimized for flash and high availability, as well as offering the best snapshot and replication technologies available, the storage arrays ensure production applications and data are available and protected. The HPE StoreOnce appliances complement the HPE 3PAR StoreServ arrays by providing the availability, scalability, and flexibility that organizations need for short- and long-term data preservation and retention. HPE Recovery Manager Central (RMC), integrates HPE 3PAR StoreServ all-flash arrays with HPE StoreOnce Systems to make the data management and movement seamlessly work together—centrally managing all of the product features and the movement of data between each product. It augments traditional backup approaches, combining the performance of snapshots with the protection of backups.

HPE 3PAR StoreServ Data-at-Rest Encryption protects data from both internal and external security breaches. HPE 3PAR StoreServ can be configured with self-encrypting drives (SEDs) and optional enterprise secure key management. HPE 3PAR StoreServ Data-at-Rest Encryption solution supports Federal Information Processing Standard (FIPS) 140-2 Level 2. The FIPS 140-2 standard for SED ensures that a product uses sound security practices, such as approved, strong encryption algorithms, and similar methods.

HPE 3PAR StoreServ Data-at-Rest Encryption provides data protection to ensure it's not accessed on stolen, discarded, or replaced disks. It provides a software-based encryption solution, which encrypts data on a per-store basis for HPE StoreOnce Catalyst, NAS, and VTL solutions. HPE 3PAR StoreServ Data-at-Rest Encryption delivers industry-standard compliance with the AES-256 encryption algorithm and is FIPS 140-2 level 1 capable.

HPE StoreOnce solutions offer both local key management and external key management, but for the most secure solution, we highly recommend that external key management is employed for authentication.

Whenever encryption is used to protect data at rest, a strong key management system is essential for the control and preservation of the underlying cryptographic keys over the life of the data. If keys are compromised, data is compromised. If keys are lost, data is lost and business operations are impacted. Customers can reduce the cost and complexity of managing encryption keys across a distributed infrastructure with consistent security controls, automated key services, and a single point of management. HPE 3PAR StoreServ Storage and HPE StoreOnce both support industry-standard key managers and the OASIS Key Management Interoperability Protocol (KMIP) Standard.

Internet Protocol Security (IPSec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network. Utilizing IPSec, data-in-flight encryption delivers secure data transfer over the LAN/WAN between HPE StoreOnce appliances, either physical or virtual.

HPE StoreOnce secure erase (data shredding) delivers leading industry-standard compliance with NIST SP 800-88 standards. It provides protection against recovery of deleted data by allowing you to securely erase confidential information. This is especially important when you are using virtual machines and need to repurpose your hardware or spin down VMs. Secure erase gives you an option to securely erase all the data from the device or only delete the individual datastore that needs to be removed.

HPE Cloud28+ community

Initiated by Hewlett Packard Enterprise approximately three years ago, HPE Cloud28+ first started in Europe as a means to accelerate enterprise cloud adoption across borders, while respecting local and regional regulatory environments. Today, HPE Cloud28+ is a growing community of around 600 partners leveraging the HPE technology, who have created a federated catalog of cloud services for customers anywhere in the world. With over 360 data centers within the HPE Cloud28+ community network and HPE-certified partners in more than 50 countries, customers can easily find the right partner and solutions that meet their unique data sovereignty, security, and workload requirements.

By facilitating both local service provisioning and the easy comparison of a greater choice of trusted enterprise offerings, there are currently more than 20,000 services in its worldwide catalog. HPE Cloud28+ enables customers to optimize their IT service purchasing while helping them to identify and engage with the partners best positioned to accompany them.

Leveraging the HPE Cloud28+ digital platform (cloud28plus.com/emea), customers can read GDPR-related articles to learn more about how they can leverage GDPR to advance their IT best practices. It's free to join the community and there are no brokerage fees should a customer choose to contact a partner member.

Summary

There may not be a better business case for organizations to fortify their cybersecurity and risk management portfolios than the GDPR. The need to meet the higher data protection standards of the GDPR will offer organizations the opportunity to streamline IT, enhance server infrastructure security, and improve data management.

When organizations take steps to comply with new legislation, they may be required to perform a "spring clean" of their data, which can in turn boost operational efficiency. Streamlining information improves the way firms carry out data analytics and can even result in additional revenue streams. At the same time, getting data in order for GDPR compliance encourages replacement of less secure legacy systems and adoption of Hybrid IT making business more agile.

For enterprises with multiple lines of business, forgetting a customer is not a simple task. If a client asks to be removed from a database, it will involve multiple files, formats, and locations including redundant and obsolete information. Consider how this potentially complex area of compliance could be turned into a positive for the business, by reducing the size of its data lake to make information easier to find, reducing the cost of storage, as well as the cost of powering storage infrastructure and back-up expenses.

It goes far beyond reducing costs. Organizations that take a holistic view of IT security, data security, and information management can accelerate their digital business with more confidence and better protect their brand and reputation. Better protection of the digital enterprise is a real competitive advantage and a means by which firms can build trusted customer relationships that drive loyalty, retention, and revenues.

As the security of personal data becomes ever more central to economic growth and for society at large, the organizational costs of losing or misusing it are increasing and can be devastating from reputational and financial perspectives.

Hewlett Packard Enterprise is focused on the new world of threats and how to best protect against them. HPE server infrastructure security solutions can assist with GDPR compliance.

Security built-in

HPE Gen10 servers have built-in security with a silicon root of trust implemented early in the production process.

Encryption to protect data

Hewlett Packard Enterprise has a comprehensive encryption strategy, at scale, with HPE Smart Array encryption, HPE 3PAR self-encrypting drives, and compatibility with Atalla ESKM.

Resiliency to recover from data loss or theft

The HPE auto-recovery features help start that process by recovering the server firmware.

Prompt notification of a security breach

Hewlett Packard Enterprise is the only server manufacturer to monitor server firmware every 24 hours to aid in that prompt awareness of a breach and, therefore, promotes notification to the authorities.[1]

Learn more at

hpe.com/security

[1] Based on external firm conducting cyber security penetration testing of a range of server products from a range of manufacturers, May 2017

Sign up for updates

a00029111ENW, October 2017