The Role of a Modern Enterprise DLP Solution in Facilitating GDPR Compliance

The General Data Protection Regulation (GDPR) came into effect in 2018 with the goal of providing Europeans with greater say in how their personal data is collected and managed, particularly in light of technological advances over the last 20 years. Under the GDPR, individuals have many rights, including access, rectification, and erasure of personal data held on them—the so-called "right to be forgotten"—and the right of data portability.

The GDPR applies to organizations that control or process personal data on EU residents. "Personal data" is defined in the law quite broadly. In general, it is data that identifies or can be used to contact a person, such as a name, email address, date of birth, phone number or user ID; identifies a unique device potentially used by a single person, such as an IP address; or reflects or represents a person's behavior or activity, such as location. The GDPR applies not only to organizations established in the EU, but also to organizations established outside the EU if they offer goods or services to EU residents or monitor the behavior of EU residents that takes place within the EU. In practical terms, this means any provider of services that process EU residents' personal data must be compliant.

Organizations subject to GDPR must implement processes and security tools to rightfully handle, continuously protect, and know the location of the information of EU residents. Failure to maintain compliance can result in serious penalties, reputational damage, and possibly private rights of action.

With more states and countries beginning to adopt more comprehensive data protection and data privacy regulations, it's more important than ever for organizations to take data protection and data privacy initiatives seriously. Yet, in spite of being aware, many organizations struggle to put necessary data security measures and procedures in place, lacking insight into a clear course of action. It can be challenging or nearly impossible to achieve compliance manually given the variety of sensitive information that can be associated with individuals and the number of places to control in a modern, highly distributed enterprise. This makes it a good time to invest in technologies that ease management of compliance requirements by improving data security best practices, risk management, visibility of data use and location, breach detection, and incident response planning.

Navigating the Current Data Landscape—an Uphill Battle

GDPR undoubtedly provides the impetus organizations need to improve how personal data or personally identifiable information (PII) is kept both private and secure. For many enterprises, however, implementing a structured data protection framework is challenging given the variety of sensitive PII associated with individuals—and the growing number of locations from which this information flows and is accessed.

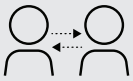
An increasing reliance on cloud computing and remote working further complicates the problem. In an irrevocably altered data landscape, both PII and sensitive business data stored or transmitted via software-as-a-service (SaaS) applications and private or public clouds is invariably susceptible to accidental exposure. In addition, the unusual new standard of working from home has created a legion of remote sites, making PII and sensitive business data even more susceptible to transmission and leakage due to unsuspected insider behavior or human error.

Three Areas of Cognizance

In a challenging data climate, where should CISOs and Information Security chiefs even begin with data compliance? We say: begin with cognizance. When architecting a data protection framework to be compliant with data protection regulations, security chiefs need clear cognizance in three areas:

1. **Recognizing what needs to be protected**. By this, we mean PII that can potentially identify any individual residing in the EU.
2. **Enabling preventive measures for what must be deterred**. Organizations should strive to protect regulated and sensitive personal data from external threats, malicious behavior from insiders, and unintentional exposure by negligent users. Leaks and breaches may trigger time-sensitive notice requirements to supervising authorities or individuals. Where required, failure to disclose in the time allotted may lead to additional fines, class-action lawsuits, and reimbursements to impacted parties for damages, not to mention the reputational damage the company is bound to incur.
3. **Taking all necessary security measures**. GDPR allows customers to access the PII that companies collect about them and request that PII be deleted, subject to certain exceptions. This means that organizations must be able to locate where such PII is stored, at all times, across every repository. Additionally, organizations will find it helpful to have tools in place to track PII as it travels through any communication vector, implement Zero Trust-based least-privileged access rules, and have strong data protection measures in place.

Recommendations



Engage with your board of directors; report on progress in addressing data privacy through your security program

Understand and tackle your big data privacy and security risks

Document what personal data you hold and ensure its lawful use

Identify where technology can help you achieve compliance

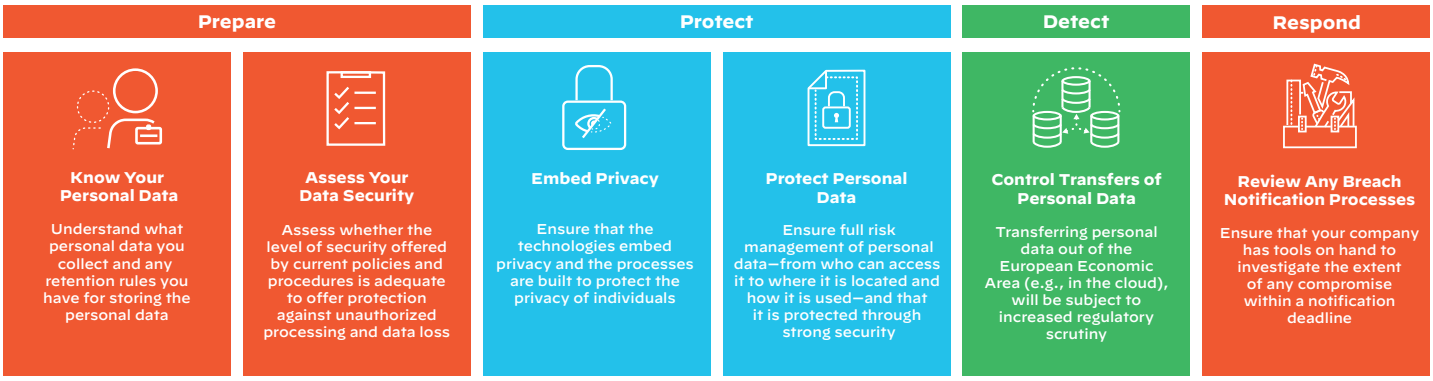


Figure 1: Tackle GDPR through four important steps

A Wall-to-Wall Approach to Data Security and Privacy

GDPR compliance demands more than a piecemeal approach to data protection. It requires a comprehensive and consolidated data security strategy that comprises any network location—on-premises, in the cloud, and across remote users—and lets you easily navigate through the full ambit of data protection obstacles:

- Identifying and monitoring PII wherever it lives or flows
- Protecting the data, ensuring only authorized access
- Helping prevent PII leaks and breaches
- Responding to incidents with timely remediation

Sensitive PII is subject to storing, sharing, and transmission from everywhere, be it from IT devices that your employees use or SaaS applications they access. Other than your own private cloud (data center), various public cloud platforms also store and share this type of sensitive data. Not only can this data exist everywhere; it also travels via many different transmission channels: encrypted and unencrypted web traffic, email, file sharing apps, public cloud storage, mobile devices, and many more. The multichannel data-at-rest and data-in-motion instances create your first challenge: **how can you identify and monitor PII wherever it lives and flows?**

Well-meaning yet negligent employees are an important vehicle for PII data loss. They may unintentionally expose sensitive data by transferring it through company-unsanctioned SaaS applications, oversharing it on cloud storage repositories, or sending it to untrusted third parties. Malicious activity by ill-intentioned insiders is another cause of data loss, creating your second challenge: **how can you ensure data is not overexposed and that only authorized users have access to your PII?**

Data leaks and security breaches wreak havoc on organizations, and the fallout can be debilitating. External cyberthreats that cause data leakage usually stem from phishing scams unleashed over email or from malware attacks mobilized via file downloads from the web. A leak is caused by some action of the party who owns the data. PII needs to be protected even when you are required to share it externally for legitimate business purposes with a partner or a vendor, so the question is: **how do you block or prevent data leaks and security breaches of PII and protect this data when it must leave the orbit of your network?**

The GDPR also introduces data breach notification requirements. This creates another obstacle: **how do you ensure incident response and remediation to investigate and mitigate the extent of a compromise within an allotted time frame?**

Leveraging Modern Enterprise DLP as a GDPR Compliance Tool

Modern and best-of-breed DLP technology is specially designed to help automatically discover, monitor, and protect sensitive data within your entire organization. In fact, it enables organizations to automatically find PII based on predefined and customizable detection rules and contextual conditions that align with the stringent regulation requirements of GDPR. The out-of-the-box specific policies for GDPR and other data protection regulations typically simplify the configuration process and shorten manual policy tuning cycles.

Modern DLP also provides visibility into the entire network and all traffic, including remote workers, sanctioned and unsanctioned cloud apps, and cloud storage repositories, to avoid blind spots and shadow IT problems. It helps organizations monitor how sensitive data is being used—or abused—and who is accessing it. When paired with other technologies like authentication, data governance, and rights management, this technology offers even stronger security to support a least-privileged access model and allow safer data sharing with third parties. When it comes to policy violations, modern DLP also helps with remediation actions. For example, it can automatically alert users to infringement, block unsafe data transfers, redact and encrypt information, or automatically limit file sharing of confidential information that is openly exposed on SaaS applications.

The GDPR-driven regulatory landscape makes it more pertinent than ever to invest in technologies that make it easier for data protection and privacy initiatives to meet compliance requirements, helping you overcome all data protection obstacles. **Luckily, evolving DLP technologies help organizations achieve otherwise insurmountable data security goals to adhere to the strict regulatory climate**.

Traditional DLP solutions fall short. They have become too complex over the years, are anchored by their on-premises infrastructure, and use a costly bolt-on approach to scale—and meanwhile, newly integrated DLP offerings are typically limited in coverage. A modern cloud-delivered, enterprise-grade DLP solution is the most effective way to address modern data protection challenges for network and cloud transformations. In fact, almost 40% of respondents in an ESG study expect their network security controls to be cloud-delivered within two years.[1] A modern DLP solution is deployed over a cloud native architecture and delivers key benefits across every control point on-premises and in the cloud with high efficacy, operational efficiency, scale, and economics.

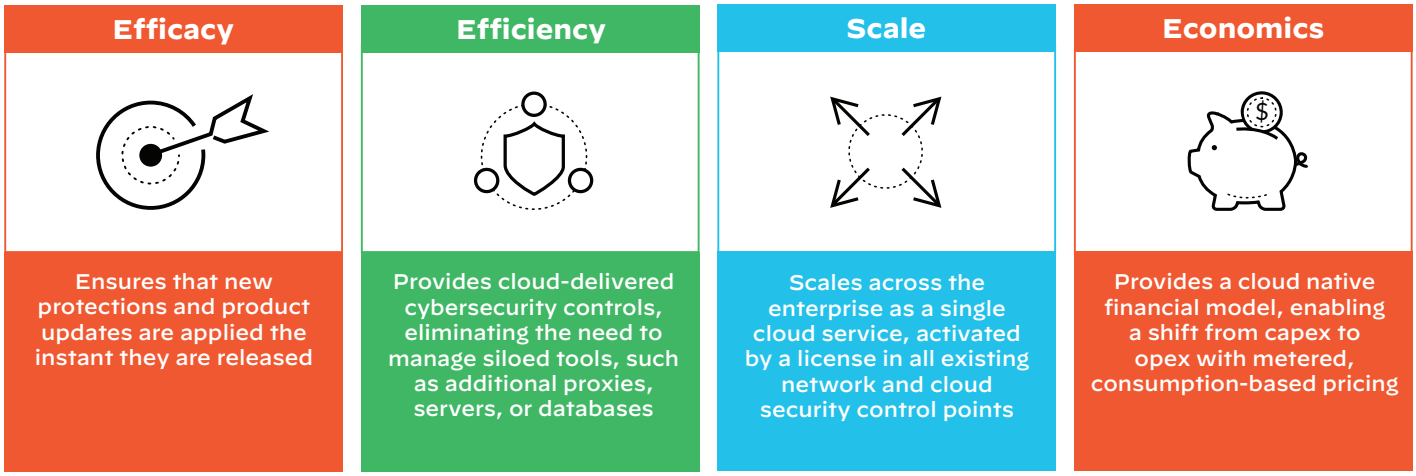


Figure 2: Key benefits of a modern cloud-delivered enterprise DLP solution

Introducing Enterprise DLP by Palo Alto Networks

Enterprise DLP by Palo Alto Networks is designed to effectively ease many of the challenges that come with data protection for the entire enterprise in a modern cloud-driven and highly distributed corporate environment. Innovated to automatically discover, monitor, and protect sensitive PII through a comprehensive cloud-delivered solution approach, it overcomes the challenges of legacy data protection technologies.

Right at the outset, the solution delivers predefined, granularly customizable detection rules and contextual conditions for highly reliable identification of sensitive data to align with fundamental GDPR requirements. These out-of-the-box policies simplify the configuration process and shorten manual policy tuning cycles.

As the industry's most comprehensive cloud-delivered enterprise DLP, the solution provides visibility into the entire network and all traffic—including remote workforces; branch offices; and software, infrastructure, and platform as a service (SaaS, IaaS, and PaaS)—to help avoid blind spots and shadow IT problems. Organizational GDPR policies are defined once and automatically synchronized everywhere the service is enabled, across all corporate on-premises and cloud environments, to ensure consistency across all environments and users as well as avoid unnecessary policy creation cycles as the organization expands.

By adding native integration of our new Enterprise DLP service within all form factors of our ML-Powered Next-Generation Firewalls—physical, virtual, and cloud-deployed—and the Prisma® suite of cloud security products, we have worked to help ensure your organization's sensitive data remains continuously and consistently protected throughout physical and virtual networks, cloud environments, including SaaS at rest, SaaS inline, cloud native IaaS, and across every user in any place—whether on campus, at branch locations, or working remotely. Through predefined and customizable GDPR policies, the solution automatically identifies GDPR-related data, monitors how that data is being used and transferred across secure environments or risky noncompliant locations, and protects it from loss and theft.

1. "Transitioning Network Security Controls to the Cloud," ESG, August 2020, https://www.esg-global.com/research/esg-research-report-transitioning-network-security-controls-to-the-cloud.

Simple to adopt, use, and maintain, Palo Alto Networks cloud-delivered Enterprise DLP doesn't require bringing in additional deployments of software, proxies, servers, databases, cloud connectors, and IT resources—delivering the most cost-effective solution and effectively lowering your total cost of ownership by at least three times compared to legacy DLP technologies.

Some technologies are tailored to assist with data privacy compliance, but one technology alone isn't enough for today's complex threat landscape. Organizations must protect networks, endpoints, clouds, and users, and we recommend doing so with a multilayered security approach.

Conclusion

As your organization continues to navigate data protection compliance requirements in a strict regulatory climate, consider how a modern cloud-delivered enterprise DLP solution could help meet your needs for the entire enterprise via a unified and comprehensive approach. To learn more, visit us online.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com