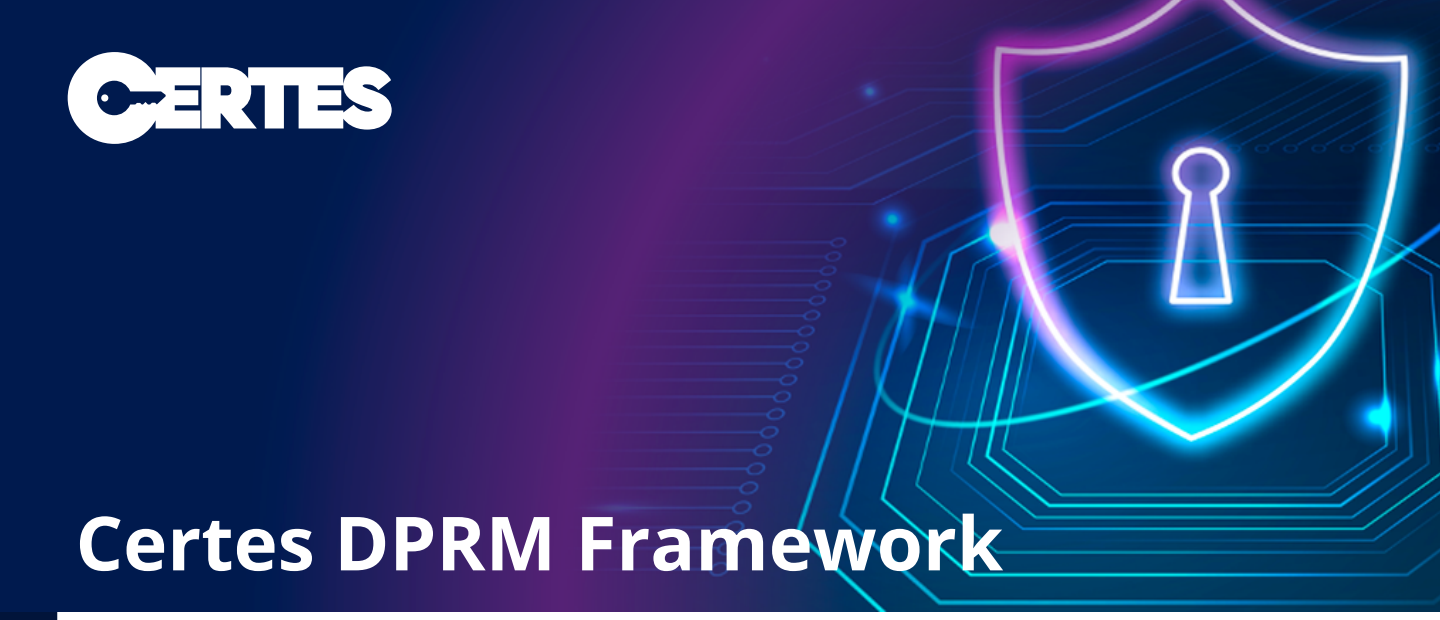

Certes DPRM Framework

In a world dominated by increasing digital threats, conventional network security approaches are falling short of safeguarding an organisation's critical asset - its data. Despite 61% of risk executives saying data protection and privacy regulations were their biggest priorities, traditional network security measures remain fixated on securing the network and identity perimeter, assuming its sufficient in ensuring data safety. Network and data access are distinct entities and should be managed separately.

With the average data breach costing globally $4.45 million, relying solely on a secure perimeter for data protection is a costly mistake. Despite the technical ingenuity of these tools, they all share the same flaw - they are retrospective in action, reporting on past and current events, rendering them insufficient in the dynamic field of data protection. In the world of data protection, if you detect a breach, it is already too late.

A secure perimeter does not automatically guarantee the safety of the data. You cannot fix a data problem with an infrastructure solution. A different approach is needed, and businesses need to act now. ‘Bad actors’ seek valuable customer data, and existing solutions, such as infrastructure protection, only serve as obstacles to their goals - obstacles they are finding easier to overcome with the increased use of AI.

> **Pressure to implement truly protective measures is rising and today, we’re seeing authorities respond to breaches handing out substantial fines and, even in certain jurisdictions, resorting to criminal actions.**
>
> *Simon Pamplin – CTO, Certes*

Traditionally, regulators overseeing sensitive, personally identifying, or regulated data had little in the way of fines to make companies take data protection seriously, but with the ongoing mass digitisation surge in recent years, we’re seeing a huge shift in regulatory attitudes to data protection all over the world. Pressure to implement truly protective measures is rising and today, we’re seeing authorities respond to breaches handing out substantial fines and, even in certain jurisdictions, resorting to criminal actions.

This is why Certes recommends DPRM - a data-centric framework for Data Protection and Risk Mitigation, comparable to what SASE (Secure Access Service Edge) is for infrastructure.

What is DPRM?

DPRM is made up of four functions that seamlessly work together to safeguard data, ensuring protection throughout its journey and mitigating the impact of regulatory fines in the event of a breach. This is achieved by ensuring that even in the aftermath of a breach, only the Data Controller or Customer possesses the capability to access the data, rendering it valueless to ‘bad actors'.

In this highly digitised world, data fills every aspect – and for a business owner, a customer, or a service provider, control over every network segment that data travels over is impossible. Protecting data across its intended path becomes a daunting task, especially if it's stolen or misdirected (Man-in-the-Middle or DNS spoofing attacks). The only way to truly prevent regulatory penalties is to gain 100% control over the data itself. It is logical to implement protective measures directly around the data, ensuring that only you, whether as the Customer or Data Controller, have authority over who can access that data. This protection should be seamlessly integrated without disrupting the existing infrastructure tools you've deployed.

Certes DPRM consists of:

1. **Layer 4 Data Payload Protection:** Safeguarding the actual data regardless of the infrastructure it traverses
2. **Separation of Key and Policy Ownership:** Placing 100% control with the Customer or Data Controller instead of a vendor or service provider
3. **Crypto-Segmentation:** Logically segmenting individual data flows through separate policies and strong cryptography, ensuring data sovereignty irrespective or physical geographical limits
4. **Data Security Unified Reporting:** Providing a clear view of protected, blocked, and allowed data flows as proof points for audit and record-keeping

Patented technology applies protection to the Data Payload without impacting any other part of the IP packet information, so all traditional network security and reporting tools function the same after DPRM is inserted into the network as it did before. It is transparent to other network devices.

It is not merely a technology solution, instead, it is a business risk mitigation solution. By safeguarding customer data, it ensures that control over the risk from regulatory, legal, and financial penalties firmly sits with the Customer or Data Controller. The presence of a data-centric control is crucial for effectively mitigating these risks.

Countries around the world are applying stronger data protection regulations and most are following those already deployed in the US and Europe. Fines per breach can escalate exponentially, coupled with potential criminal prosecutions for company officers - risks and consequences are rising and more action needs to be taken globally to protect customer data. Certes cites GDPR, DORA, HIPAA, NIS2, PCI, and PII PLDP as examples, each wielding significant financial implications for negligence in safeguarding sensitive data.

DPRM is applicable to any vertical dealing with sensitive, personally identifying, or regulated data. With an effective DPRM solution, sensitive data is protected in motion no matter where it travels or is taken.

DPRM represents a comprehensive approach to data protection and risk mitigation, aligning seamlessly with the challenges faced by modern enterprises. By prioritising the protection of data over any infrastructure, Certes provides organisations with a data-centric control, enabling them to navigate complex regulatory landscapes and fortify their defences against ransomware attacks and data breaches.

How do you protect your sensitive data? It's time you took the DPRM approach

CERTES

PSI

Product Source International Datacomm
330 Franklin Turnpike
Mahwah, NJ 07430
201.488.6000 Tel
www.psitec.com / sales@psitec.com