European General Data Protection Regulation

How VMware NSX™ can help organisations comply with the new European data protection laws

WHITE PAPER

vmware®

Table of Contents

Executive Summary

In December 2015, the European Parliament and European Commission reached an agreement on the new Privacy and Personal data protection regulation, called the **"General Data Protection Regulation" (GDPR).** All existing local Data Protection laws and regulations in the 28 member countries will be superseded by the GDPR which sees the introduction of several new changes and enforcements regarding the security of processed personal data. The impact of these changes will affect enterprises and public bodies both inside and outside of Europe.

The GDPR will come into force in May 2018. Organisations have until then to review their processes and security strategies in order to comply with it. Failure to do so will expose them to significant sanctions in the event of a data security breach – fines of up to **20 Million Euros or 4% of global group revenue,** whichever sum is the greatest.

The purpose of this White Paper is to inform businesses about the GDPR and what steps need to be taken to prepare for compliance. It will share the best practice and processes that organisations should consider implementing in response to this new reality. Furthermore it will explain how VMware NSX, as part of a holistic security architecture in conjunction with VMware vRealize Operations, can help organisations operating in an ever changing security landscape face these challenges and how to comply with the new regulations.

VMware NSX changes the way applications in data centers are secured, by providing a zero-trust security model inside the datacenter and data-centric adaptive security. It allows enterprises to protect the sensitive data processed by their applications, control in real-time the security risk level of each workload and automate remediation in case of any compromised Virtual Machine (VM).

When it comes to complying with the GDPR, network micro-segmentation by NSX is not only operationally feasible, but also cost-effective. It enables the deployment of security controls inside the data center network for a fraction of the hardware cost required to deploy the same protection level with legacy security solutions.

What is the GDPR?

Data is considered to be the core business of today's digital economy. Collected, analysed and moved across the globe, personal data has acquired enormous economic significance. According to some estimates, the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020[1].

The GDPR is designed to protect all personal data collected for, or about, citizens and residents of the EU, in particular as it relates to processing, using, or exchanging data. It updates the principles set out in the 1995 directive, so as to keep pace with major changes in data processing brought about by the internet. It covers:

- Cloud computing
- Social networks
- Online shopping
- E-banking services
- Offline data processing: e.g. hospital and university registers, company registers of clients and personal data held for research purposes

The GDPR was introduced by the European Commission in January 2012, approved by the European Parliament in March 2014 and the European Union Council on 15th June 2015. The actual regulation texts were finally approved on 15th December 2015.

Once it receives formal adoption from the European Parliament and Council, the official texts will be published in the Official Journal of the European Union in all official languages. The new rules will become applicable in May 2018.

This data protection reform will come with three main innovations:

- **One continent, one law:** The regulation will establish a single, Pan-European law for data protection, replacing the current inconsistent patchwork of national laws.
- **One-stop-shop**: Companies will only have to deal with one single supervisory authority, not 28, making it simpler and cheaper for them to do business in the EU.
- **The same rules apply for all companies – regardless of where they were established**: Today European companies have to adhere to stricter standards than their non-EU competitors who also do business within the single European Market. All companies trading within the EU will have to comply with the GDPR.

European regulators will be equipped with strong powers to penalise non-compliance. Hefty fines of up to €20 million or 4% of their global group annual turnover, (whichever sum is the greatest), could be levied in the event of a security breach.

[1] http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

What are the main changes made by GDPR?

The main purpose of the GDPR is to harmonise the current data protection laws in place across the EU member states (28 different laws and regulations). It introduces guidance as to how customer data should be stored and, most significantly, how companies must respond in the event of a data breach. Many changes and enforcements are introduced by the new regulation. The main changes are:

Territorial scope:
The regulation applies if the data controller or processor (organisation) or the data subject (person) is based in the EU. The regulation also applies to organisations based outside the European Union if they process the personal data of EU residents.

The supply chain:
In existing laws, only Data Controllers are entirely accountable for the protection of Personal Data, even if some of that data is processed by third-party organisations acting as Data Processors. Under the GDPR, Data Processors will be required to comply with the new regulations meaning they share the liability of data-loss incidents and non-compliance.

Data Protection Officer:
The GDPR will force multi-national and large companies, processing more than 5,000 records of personal data per year, to appoint independent **Data Protection Officers (DPOs)** in order to comply. These DPOs will have a similar role to the Compliance Officers but they will also need to be proficient at managing IT processes, data security (including dealing with cyber- attacks) and other critical business continuity issues around the holding and processing of personal and sensitive data.

Data Protection Impact Assessment:
Organisations will be required to perform **Data Privacy Impact Assessments (DPIAs)** to identify how data handling procedures and processes (including what the personal data is used for) could impact the safety of information associated to data-subjects, and overall compliance of that information under the GDPR. The DPO will be legally obliged to provide the DPIA to the Supervisory Authority anytime it is requested (such as in the case of a Data Protection Audit) and, at least, once a year.

Data breaches – reporting without undue delay:
Under the GDPR, the independent Data Protection Officer (DPO) will be under a legal obligation to notify the Supervisory Authority and individual data subjects of all data breaches without delay, within 72 hours. Under the GDPR, no business will be able to hide a data breach from the public eye.

Financial sanctions:
In the event of a breach the GDPR enables companies to be fined up to €20 million, or 4% of their global turnover[2], whichever sum is the greatest.

Data protection by design and by default:
'Data protection by design and by default' will become an essential principle. It will incentivise businesses to innovate and develop new ideas, methods, and technologies for security and protection of personal data. Used in conjunction with data protection impact assessments, businesses will have effective tools to create technological and organisational solutions.

[2] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Summary of GDPR main changes:

Main change	Description
Territorial scope	Extended to organisations outside of EU processing data related to EU citizens (includes offering services or monitoring)
One stop shop	Replaces 'lead authority'
Supply chain	Controllers and Processors and 'Data Protection Seal'
Data Protection Officers	Appointed where data processed >5,000 records
Data Protection Impact Assessments (DPIA)	At least annually (and consultation with DPA/supervisory authority)
Data breach reporting	72 hours - without undue delay
Increased fines	Up to 4% global turnover/€20m
Consent	Must be freely given and obtained for a specific purpose
Security broadened	More than 'technical and organisational measures'
Personal data	Includes cookies and IP addresses
More transparency	Icon-based privacy notices
Pseudonymous and encrypted data	Still personal data but subject to less stringent requirements
International transfers	Adequacy criteria is amended by the GDPR

Potential economic impact of the GDPR

In December 2013, Deloitte UK, commissioned by the Data Industry Platform[3], issued a report[4] where they assessed the economic impact of the GDPR on four industry sectors which rely heavily on personal data in order to operate:

- Direct Marketing
- Online Behavioral Advertisement (OBA)
- Web Analytics
- Credit information

The report outcomes were striking. The survey suggests the GDPR could result in a major obstacle for European businesses wishing to use Direct Marketing, Web Analytics and OBA initiatives. Acknowledging that businesses would be able to offset some of this by reconfiguring their operations and redirecting some of the affected spend to other channels, European businesses are still expected to ***lose a total of €66 billion*** in sales. This estimate assumes that total budgets remain unchanged, but in practice marketing budgets may fall if they do not deliver adequate return on investment which means for business, the revenue losses could actually be greater.

For the Credit Information sector, the findings raise significant concerns over whether it would be able to continue to effectively assess credit risk. If it could not, then consumer credit could fall by as much as 19%.

The report concludes that the combined effects of reduced credit availability and sales losses across the four sectors could reduce GDP by €173 billion (1.34% of GDP in the EU-27).

What needs to change?

Going forward, enterprises will require organisation-wide changes in their business processes and the way they store, handle and exchange data. In addition, these changes will necessitate a significant transformation in their data center security model in order to address the GDPR challenges.

In order to comply with the 'Data protection by design and by default' regulation requirement, enterprises will have to move from legacy network-centric security to a data and application-centric security model. This ties the security policy to the application and VMs processing, exchanging and storing data inside their data centers.

Failure to prepare adequately for the new requirements will leave organisations at risk of significant fines due to non-compliance. In addition, by preparing for the GDPR now, organisations can take a measured approach to ensure that adequate due diligence is undertaken on the actions and budget required, in anticipation of the regulation coming into effect in early 2018.

[3] Data industry platform: a group of firms and associations from across Europe

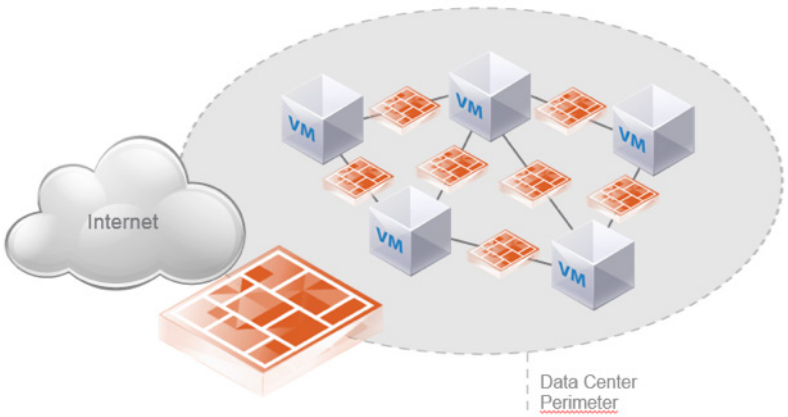
[4] Click here to find complete Deloitte report. Insights were collected from a survey of 6000 consumers and 750 businesses in major European markets: UK, France and Germany.

The evolving threat landscape

With a continuously evolving threat landscape, organisations have increased their expenses in security products without getting the expected protection level. This is not because of the ineffectiveness of installed security products or a lack of skills in their operational teams. The main reason is the security model itself and the way in which it is implemented inside the datacenter.

While recent attacks on Hilton, JP Morgan Chase, Target, Anthem, Home Depot, Sony and others have each been different, they all have one characteristic in common. Once inside the data center perimeter, the attacks were able to expand laterally from server to server where sensitive and personal data was collected and exfiltrated.

These cases highlight a major weakness of modern data centers. Security products are positioned at the perimeter or at the entry of DMZs inside the data center. Organisations require a more in-depth security with zero-trust zone architecture controlling lateral communications between workloads and applications. Zero-trust zone architecture addresses the "Data protection by design and by default" requirement of the GDPR by applying the security solutions to workloads and VMs.



Micro-segmentation – the new security model

Micro-segmentation provides the new application-centric security model. Filtering and inspection takes place at the network interface of each workload and VM, contextually adapting the protection level and proactively taking steps to avoid threat proliferation in the case of any compromised workload.

Micro-segmentation has not been operationally feasible in traditional data center networks with legacy security products. Traditional and even advanced next-generation firewalls implement controls as physical or virtual "choke points" on the network. As application workload traffic is directed to pass through these control points, rules are enforced and packets are either blocked or allowed to pass through.

Using the traditional firewall approach to achieve micro-segmentation quickly reaches some operational barriers – namely throughput capacity and operations/change management. Enhanced throughput capacity can be achieved by buying enough physical or virtual firewalls to deliver the capacity required to achieve micro-segmentation. However, in the increasingly dynamic nature of today's data centers, IT operations can quickly become overwhelmed if firewall rules need to be manually added, deleted and/or modified every time a new VM is added, moved or decommissioned.

In addition, traditional firewalls can deliver high isolation, based on their position in the network, but they lack visibility of the application and VM's context, as they are not directly connected to them and their policies are only IP-based. Adding a thick agent on the Workload or VM provides high visibility of their context but, as a part of the VMs, they could be stopped, bypassed or even compromised. In addition, the performance impact on the workload and the operational complexity when the number of VMs increases needs to be factored in.

VMware NSX Micro-segmentation

The leading use of the VMware NSX platform today is micro-segmentation. The NSX micro-segmentation approach delivers ubiquitous security enforcement providing high context and high isolation.

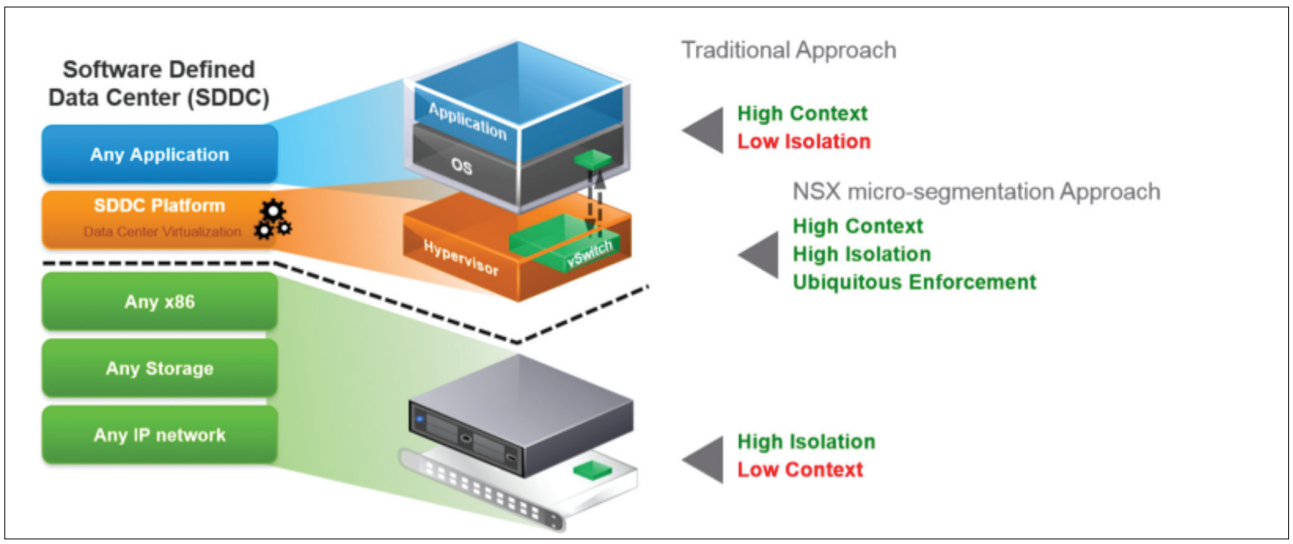
NSX Micro-segmentation provides control and visibility for workloads in virtualized networks:

- Security is shrink-wrapped around each workload.
- Firewall rules are enforced at the vNIC level of each VM creating a separate "micro trust zone" for each workload.
- NSX automatically assigns the appropriate security group and policy based on virtualization relevant context, rather than just physical topology.
- NSX can dynamically change the security group and policy based on changing context, including context provided from a third party, such as a malware or vulnerability assessment solution from VMware Security partners eco-system[5].

NSX offers new ways of grouping VMs and applying security policy. For example, it can secure workloads based on application types, network constructs, and/or infrastructure topologies. The security policy is no longer constrained to a single distributed virtual switch or port group but instead is orchestrated centrally, which reduces rule sprawl, and ensures that it is accurately and consistently applied. Furthermore, when a VM is provisioned, moved, or deleted – its firewall rules are also added, moved, or deleted. These changes happen automatically, with no human intervention. This new level of automation dramatically reduces the operational complexity and expense of managing security policies across workloads.

In addition, advanced security services (L7 inspection, vulnerability assessment, policy auditing) can be delivered through third party complementary security solutions that are natively integrated with NSX and able to consume security groups to provide the adapted protection level to workload context and comply with high security requirement for critical applications.

A VMware Software Defined Data Center (SDDC) approach leverages the NSX network virtualization platform to offer several significant advantages over traditional network security approaches – automated provisioning, automated move/add/change for workloads, distributed enforcement at every virtual interface and in-kernel, scale-out firewalling performance, distributed to every hypervisor and baked into the platform.



Operational cost reduction

With the SDDC approach, NSX not only makes micro-segmentation operationally feasible, it is also cost effective. Some customers have reported achieving it for approximately one-third of the cost of the traditional route. The entire NSX platform typically represents a fraction of the cost of the physical firewalls alone, and scales out linearly as customers add more workloads. VMware NSX maintains a consistent security policy, centrally managed and locally provisioned, simplifying operational tasks and reducing dramatically the number of changes and time spent on those changes.

NSX is fully integrated with VMware vRealize Automation, VMware vRealize Orchestrator or 3rd party automation tools. It enables the business to consume the Security and the Networking as a service, without compromising the protection level. This helps organisations to use the security as a business enabler while keeping operational costs to a minimum.

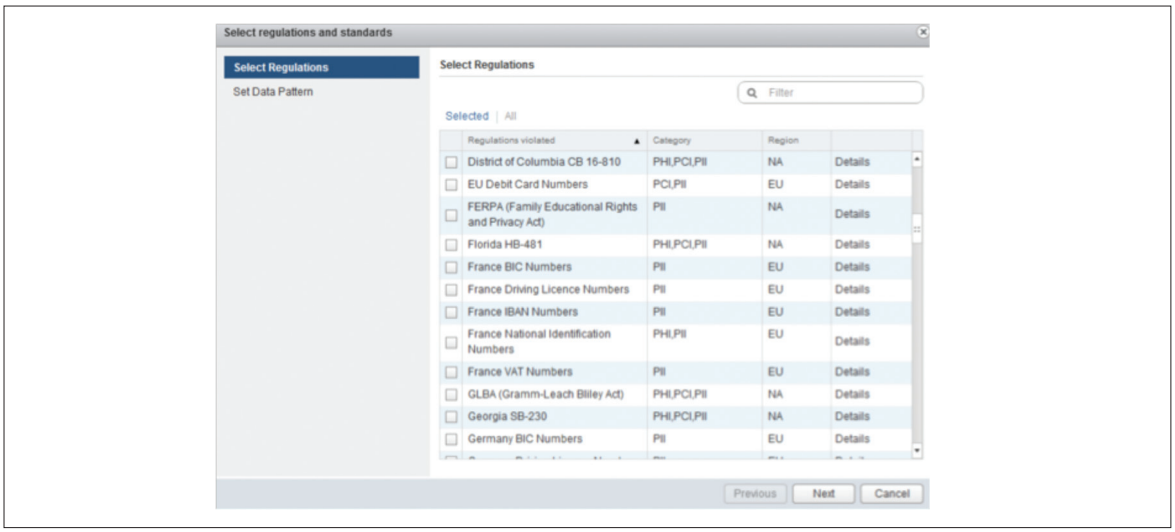
[5]NSX technology partners list available on the following link:
https://www.vmware.com/products/nsx/technology-partners

Minimise risk and impact of data breaches

NSX Micro-segmentation helps organisations to minimise the risks and avoid the costs associated with a data breach. These costs are typically as a result of engaging with forensic experts, in-house investigations, loss of customers and reductions in turnover. Add the considerable fines that will be levied in the event of non-compliance with the GDPR, (up to 20 Million Euro or 4% of global group turnover), and the potential effects of a data breach could be devastating.

Enhanced data monitoring

With micro-segmentation, NSX Data Security helps organisations build data-centric and adaptive security policies that will prevent against sensitive data exfiltration, by tagging VMs violating the data security policy. It essentially provides visibility into any sensitive data that is in the environment and helps to build real-time data risk assessment without increasing operational costs or impacting business agility. NSX Data Security provides a predefined set of regulations and sensitive data templates including a set of European data types. It helps to comply with over 70 regulations and scans over 100 file formats, as shown in the figure below:



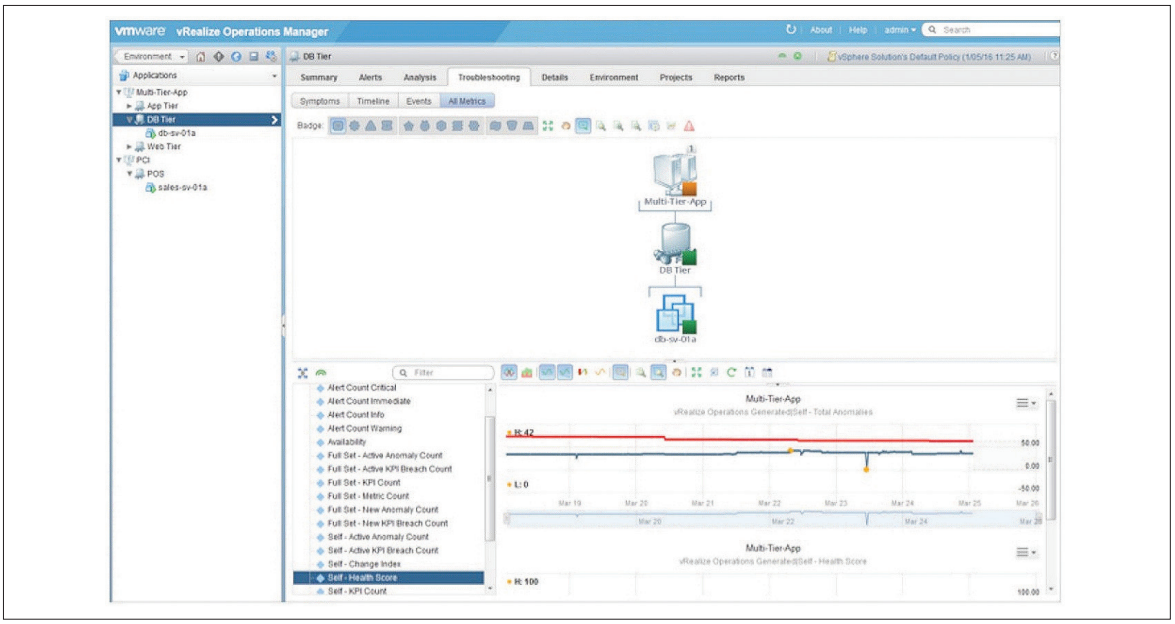
Demonstrating due diligence towards compliance with the GDPR

Whilst as part of the **Data Protection Impact Assessment (DPIA)** the **Data Protection Officer (DPO)** will determine a level of compliance at a specific point in time, maintaining compliance can only be accomplished through continuous monitoring of the environment in which personal data is stored. Proactive monitoring, reporting and alerting is therefore recommended to detect exceptions or compliance drift.

VMware vRealize Operations may be further enhanced through the use of the NSX management pack, therefore providing a robust offering for monitoring and maintaining security best practices. VMware vRealize Operations enables IT operations teams to manage the health, risk, efficiency, and compliance of dynamic workloads and heterogeneous infrastructure. It correlates data from applications to storage in a unified management solution that is easy to use and provides control over performance, capacity, and configuration standards. Predictive analytics drive proactive action and policy-based automation enables businesses to become more efficient and stay in compliance:

- Default or custom policies control, or trigger, the automation of key processes.
- Automated capacity optimisation reclaims overprovisioned capacity, increases resource utilisation, and eliminates scripts and spreadsheets.
- Flexible capacity modelling scenarios help IT teams better plan for resources based on service-level agreements (SLAs).
- Automated detection, enforcement, and remediation of security guidelines, configuration standards, and regulatory requirements reduces the risk of non-compliance.

VMware vRealize Operations can help enterprises demonstrate due diligence towards GDPR compliance by providing continuous audit capabilities, intelligent operations and predictive analysis of critical assets and applications handling personal data. Organisations will have the ability to provide consistent Data Protection Impact Analysis and avoid any post-data breach penalties or insurance invalidations.



Conclusion

The adoption of the GDPR will bring very significant changes to the data security landscape for businesses operating within the European Market. Now is the time for organisations to get prepared for compliance with the new regulations or potentially face the consequences should the worst happen.

VMware NSX, as part of a holistic security architecture in conjunction with vRealize Operations, will help organisations to be confident in their defence against an evolving threat landscape, whilst ensuring the highest levels of visibility and consistency in respect to compliance with best practice. It provides the most effective security solution to build zero-trust zone architecture inside data centers, by delivering adaptive data and application-centric micro-segmentation, advanced security services based on VMware security partners' eco-system, automation and policy management.

Finally, organisations choosing to use NSX to secure their data and applications will see it as a business enabler, inspiring confidence in their customers. They will also keep their security investments and operational costs to a minimum - a key driver for them to maintain their competitive edge in the European market.

For more information on how NSX can help comply with the GDPR, please visit:
http://www.vmware.com/go/EU-GDPR

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 4/16