UNISYS | Securing Your Tomorrow™

Addressing the Challenges of the New EU General Data Protection Regulation with Unisys Stealth Micro-Segmentation Solution

By: Salvatore Sinno and David Matthews

White Paper

Table of Contents

In recent years, the integration of social and economic elements and the overlapping of the private, public and business domains have led to an increased flow of personal data. At the same time, the exchange of personal data between the public and private sector, the rapid technological developments and globalization have brought new challenges to the protection of this data.

These challenges demanded a new data protection framework in the European Union: such framework, called General Data Protection Regulation (GDPR), was agreed in April 2016 and will apply from 25 May 2018.

The GDPR focuses on strong enforcement of compliance requirements stressing the importance of creating trust to allow the digital economy to grow inside the European Community. The GDPR brings consistency to the current data protection laws across EU member states, and provides guidance on how customer data should be stored and how companies must respond in the event of a data breach. The GDPR introduces new regulatory requirements for how institutions must manage the personal data they hold on their customers, including the segregation, obfuscation and encryption of data. GDPR requires businesses to implement security controls to address the risk presented by personal data processing, such as accidental or unlawful destruction, loss, alteration and unauthorized disclosure.

Organizations will be expected to demonstrate compliance at every stage of personal data processing, with potential heavy fines being levied by regulators on top of the high costs of dealing with data breaches. The GDPR imposes financial penalties on businesses for not protecting data, including fines of up to four percent of global revenue for the previous year, or €20 million – whichever is greater. Cloud providers and other data processors will be directly liable as the GDPR set direct security obligations such as confidentiality, integrity, availability, resilience, business continuity and regular testing and evaluation.

In conjunction with the heavy fines, the GDPR has mandatory data breaches reporting requirements; with the traditional challenges posed by data breaches and cybercrimes, businesses that collect, use and share data from European citizens must take adequate measures to ensure security of personal data and provide assurance that they meet the requirements set in the GDPR. As a result, there's been speculation about the struggle smaller cloud providers and other data processors will face in order to keep up with the financial burden and red tape associated with GDPR.

GDPR: Key Requirements

The GDPR Articulates Four Key Requirements:

- Controllers and processors must know the location where personal data is stored. GDPR poses limits on the ability to transfer personal data outside the European Economic Area (EEA); when this is allowed the transfer of personal data must comply with the data transfer rules of the GDPR.
- Companies whose core activities consist of processing on a large scale of personal data must appoint a Data Protection Officer (DPO). The DPO's role is similar to a Compliance Officer, and is expected to manage IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues relating to the holding and processing of personal and sensitive data.
- A Data Protection Impact Assessment (DPIA) to ensure overall compliance with the GDPR. This will involve identifying procedures, processes and technical controls such as encryption, network segmentation and data obfuscation.
- Personal data controllers and processors have to take adequate technical security measures to protect the personal data from loss, alteration or unauthorized processing. GDPR requires protection by design as well as by default. This means that data protection safety measures must be considered from the earliest stage of development.

To meet these requirements, CISOs and CIOs should adopt new security paradigms, methods, and technologies for the protection of personal data.

How Can Unisys Help?

To achieve an effective GDPR compliance, organizations need the following security capabilities:

- Security persistence
- Security ubiquity
- Security scalability
- More efficient and secure use of resources

Security persistence and ubiquity overcome the limits of the traditional security systems (physical firewalls, virtual firewalls and agent based security). These technologies are ineffective at securing all server-to-server, client-to-client, client-to-server traffic in and across data centers and cloud services.

Security scalability ensures that security controls can easily adapt to changing environments and threat conditions.

More efficient and secure use of resources reduce the costs of security controls and the overall compliance effort while increasing the organization resilience to security breaches. It is worth noting that a security breach of personal data is not a matter of if, but a matter of when. To reduce the impact of personal data breaches, businesses have to adopt technologies such as micro-segmentation and encryption that ensure that a break-in to one segment of the enterprise won't affect the security of other segments.

To meet these objectives organizations need to raise their security posture and work with a trusted security partner with a mature security service offering. Unisys is a trusted security adviser with a mature security service capability that provides effective GDPR compliance.

Unisys clients benefit from the following services to meet the GDPR requirements:

- Advisory and Consultancy Services (A&CS): the GDPR requires organizations to evaluate and document (annually) the risk inherent in the processing of personal data. Unisys provides organizations with security expertise to carry-out specific data protection impact assessment (Consequence Based Assessment) to evaluate the origin, the nature and the severity of the risks related to the processing of personal data. Unisys Consequence Based Assessment (CBA) establish long-term trusted advisor relationships with organizations and provide a strategic roadmap to meet the GDPR and identify the most effective protective measures. CBAs cover all areas of security, from roles and authorities of employees to technical and operational detail of physical security, IT security, and Industrial Control System security. Unisys use the outcome of this assessment to identify controls and demonstrate that the processing of personal data complies with the GDPR. These bespoke risk assessments offer a better view of the current risks and controls, including on-going vulnerability assessments; governance and risk compliance; business continuity; security strategy; architecture and response processes; and cloud security.
- Security Intelligence and Response (SI&R): to mitigate the impact of personal data security breaches, Unisys provides integrated solutions to plan and create a holistic end-to-end security ecosystem that detects and responds in real-time to security alerts. Unisys help organizations to meet GDPR by giving them a better understanding of what damage security incidents can do and provide incident response plans that make the difference between a security event and a reputational disaster. Unisys massive infra-structure correlates and monitors over 300 million client security events every day; as a result Unisys, as a trusted advisor, offload both day-to-day GDPR compliance activities, network and endpoint security management to a network of on-shore and off-shore security experts.
- Managed Security Service Provider (MSSP): the GDPR requires organizations to have an efficient process to provide detailed documentation and visibility of data breaches. This requires new and efficient security services to proactively monitor network and identify threat in real-time to prevent and stop cyber-attacks to fulfil the GDPR compliance requirements. Unisys as an MSSP delivers comprehensive real-time protection solutions orchestrating Security Information and Event Management (SIEM), Security Device Management (SDM), Governance Risk & Compliance (GRC), and Managed Identity and Access Management Services (IAM). As a MSSP, Unisys provides an integrated and cohesive ecosystem of security capabilities, integrating information and value flows. This helps organizations to manage overall GDPR compliance in a cost-effective manner. The integration with the Unisys security consultancy service provides additional value giving access to the right level of support at the right time in the most effective way. Unisys adds value by providing managed security services that are tailored to the customer GDPR needs.

To complement these service-based solution, and provide security protection by design, Unisys provides Stealth micro-segmentation as an integral part of its security solutions portfolio.

Stealth Micro-Segmentation

Unisys Stealth® is a software-based micro-segmentation solution that implements an effective "zero-trust" security model. Forrester Research is widely credited with coming up with the concept of the "zero-trust model", in which rules and policies can be assigned to workloads, VMs, or network connections. This means that only necessary actions and connections are enabled in a workload or application, blocking anything else.

Unisys Stealth allows businesses to meet GDPR requirements by deploying security controls inside the data center network and cloud environments (including public AWS and Azure) for a fraction of the cost of a hardware equivalent solution. Simple to implement and compliant with the new GDPR, Unisys Stealth is an advanced software-defined security solution that uses encryption to enable multiple "secure communities" to share the same network without other groups being able to access – or even see – their workstations and servers. These Communities of Interest (COI) enable logical segregation and isolation of network data and users without requiring multiple physical networks or inserting additional networking equipment such as firewalls, switches or routers.

The key differentiator for Unisys Stealth is identity-based key management for encryption. Stealth COI keys are assigned based on user identity or device identity (in case of servers) rather than the IP address. In doing so, access rights are tied to the user, and are not dependent on the network topology.

Stealth integrates with enterprise identity management systems such as Active Directory or LDAP so that the key distribution process is transparent to the user.

Stealth uses FIPS 140-2 compliant algorithms for encryption and key exchange. This makes it suitable for protecting sensitive personal data-in-motion and is compliant with GDPR requirements. As Stealth-enabled devices do not even respond to pings from non-COI members, they are cloaked from unauthorized users.

As Unisys Stealth establishes security policies for each workload rather than the network hardware, it enables businesses to meet three main requirements:

1. Security policies for personal data remain consistent in environments that are subjected to continuous change
2. Security control for personal data becomes available everywhere: in the cloud, in the traditional datacenter, on BYOD, and on mobile devices
3. Security becomes extensible and adapts to changes

As Unisys Stealth micro-segmentation solution assigns security policy at the workload level, the security can persist no matter how or where the workload is moved – even if it moves across cloud domains. Using Unisys Stealth micro-segmentation solution, administrators can program a security policy based on where a workload might be used, what kind of data it will be accessing, and how important or sensitive the application is. Security policies can also be programmed to have an automated response, such as shutting down access if data is accessed in an inappropriate way. All this reduce the burden of the organization to become GDPR compliant.

Regarding the use of cloud environment for personal data, traditional network segmentation strategies are complex or impossible to apply. As a result GDPR compliance becomes expensive and requires continuously reprogram of ACLs in routers, firewalls and switches and limit the adoption (and the realization of the related benefits) of 3rd party cloud solutions. In this case, Unisys Stealth micro-segmentation helps provide continuous protection for cloud instances, wherever they are hosted. Unisys Stealth segregates the workload from the rest of the cloud provider infrastructure allowing the provisioning of security for faster deployment. Unisys Stealth micro-segmentation is topology and network hardware independent allows the security model to extend seamlessly across the traditional data center and the public cloud. As a result businesses, can adopt Unisys Stealth micro-segmentation to allow the extension of the enterprise personal data security model to the cloud while maintaining control of the personal data in motion and remain compliant with the GDPR requirements.

Unisys Stealth controls the communication between workloads in the same subnet or on the same hypervisors, regardless of the location, infrastructure-type or workload type.

Unlike traditional VPNs which encrypt data only to the enterprise boundary, Stealth extends this encryption all the way to the server in the datacenter. This is achieved by a component called the Stealth Secure Remote Access (SRA) Gateway, which authenticates incoming connections from remote users, maps them to Communities of Interest based on user identity and creates a Stealth encrypted tunnel for each incoming connection all the way to the destination server in the data center. Therefore, a Stealth-enabled system can only be accessed over an encrypted tunnel, irrespective of whether access is from within the data center or remotely from a PC or mobile device or through a wrapped mobile application. As a result, processing personal data at different sensitivity levels can share the same infrastructure delivering agility, cost efficiency and GDPR compliance.

Conclusion

The GDPR can be the single most powerful force changing how business interact with their customer. For this reason, the GDPR is not only a compliance challenge, but touches all the aspects of an organization's value chain. Only if organizations plan their compliance strategy and review their personal data processing capabilities, can the GDPR become an opportunity to streamline the value chain and identify new ways to provide customers with value added services. To achieve these benefits, Unisys suggests a thorough review of organizations' security posture and data protection policies as well as roles and responsibilities. Unisys is the security trust advisor to meet such challenges with a broad range of cost effective services and solutions that support an organization's effort to meet the GDPR compliance requirements and reduce penalties associate with personal data breaches. It's important for businesses to not only have the technology in place, but for it to be with an organization – like Unisys – that has the credentials and pedigree to help manage this compliance.

Unisys security services and solutions can be deployed everywhere to protect servers in traditional data centers, cloud workloads, clients including mobile devices, and organization's operations:

- Unisys A&CS, SI&P, MSSP services provide comprehensive enterprise security capabilities that help organizations to measure and raise their security posture, and thus meet compliance and regulatory requirements set by the GDPR
- Unisys Stealth solution meets the GDPR requirements by enforcing granular network segmentation policies and strong encryption of data-in-motion to protect against lateral movement and network attacks inside data centers and cloud environments. It delivers fine-grained security at workload level without impacting existing applications, systems or network topologies. Such a solution is independent from any hypervisor, physical server or other network infrastructure components.
- Unlike other vendors that offer a hardware-based approach to micro-segmentation, Stealth offers software-defined security that is deployed on the existing network and does not require 'rip-and-replace' of existing network hardware. This leads to lower costs for GDPR compliance, as well as lower operating costs on power, cooling and hardware warranties.
- Unisys Stealth protects business investments as it adapts to changes in the network fabric and provides the agility to move workload across datacenters, public clouds and inside different zones of the network. Personal data security policies can follow the end-point from its inception to the decommissioning, while ensuring compliance with GDPR everywhere inside and outside the EU.
- Stealth deployment can also extend to public clouds such as Amazon Web Services (AWS) and Azure. Stealth secures data-in-motion all the way to the destination VM on the public cloud, and not just to the cloud boundary, thus ensuring GDPR security compliance in the public cloud.

For more information visit www.unisys.com

12/16 16-560