Parallels®

Data Security Challenges in the EU

White Paper | Parallels Remote Application Server | 2017

Table of Contents

Commonly known as the GDPR, the General Data Protection Regulation (Regulation [EU] 2016/679) will take full effect on May 25, 2018, replacing the national legislation for data protection1. After this date, data security for European businesses will become even more important, as data breaches and data misuse become more punishable. Under the GDPR, businesses will face penalties, fines, and public ire for their unwitting or irresponsible exposure of client or third-party personal and corporate information. Consequently, it is imperative that organizations tighten their data security to avoid facing these negative consequences.

The traditional network-centric security solutions, such as intrusion detection systems and firewalls, cannot protect data from hacking by privileged users and advanced persistent threats (APTs). There are other methods, such as security information and event management (SIEM) and database audit and protection (DAP), for event correlation. With stringent data regulations and increased data breaches, businesses have to move from network-centric solutions to data-centric solutions by integrating data-security intelligence and data firewalls to create a secure firewall around the data. Strong access controls, key management, and encryption augmented with security intelligence are a must, because once you move everything into the cloud, you only have a web browser as an interface.

A huge amount of data processed by organizations requires protection. This includes all personal data, which under the new regulations cannot be leaked or otherwise shown without authorization. Personal data also cannot be transferred to third countries without proper supervision and authorization—a problem for multinational establishments which now need to properly segregate data or face fines up to €10 million. Balancing security needs with employees' needs for quick access to data and applications is a key focus for IT professionals.

GDPR Compliance with Cloud Computing

In order to ensure an organization's compliance with the GDPR, the entire network must be securely deployed so unauthorized users cannot gain access. Moreover, it is important to hire reliable personnel to manage databases and administrate the system. When managing data, it is advisable to streamline processes so different privileges are assigned to different users based on their job roles. Data management has to be augmented with efficient technology that enforces system policies for secure access to data as well as its storage, retrieval, or manipulation.

Cloud computing allows organizations to centralize all data, improve the security of their network, easily protect data, and manage access through a central location. In cloud computing, data is safely hosted in a private, hybrid, or public cloud and is securely accessible through encrypted connections.

Cloud computing is a broad term that represents the different infrastructure and software solutions that enable ubiquitous access (often over the Internet) to shared pools of configurable resources (like computer networks, servers, storage, data, desktops, applications, and services). Application and desktop delivery is one of the most widely adopted cloud-computing solutions, since it allows employees to access centralized data from any location or device.

In application delivery, data and software are streamed into an isolated environment on the target device where they are executed. No local software installation or data storage is required on the client device. The user sends keystrokes and mouse clicks to the server and receives only screenshot updates. Access to data is granted only by authentication, and it can be secured further using two-factor authentication or granular filtering based on location, device type, or MAC address.

Removing the data from user devices substantially reduces the risk of data leakage or loss, helping the organization adhere to the new GDPR regulation. Moreover, businesses can also enjoy the scalability, agility, and mobility offered by the cloud, while security and business continuity are maintained at the highest level.

[1] Local legislation such us Dutch Data Protection Act ("DDPA"), British Data Protection Act (DPA), German Federal Data Protection Act, Swedish Personal Data Act (Sw. Personuppgiftslag (1998:204)) any other national personal data protection law.

Cloud Computing Advantages

As a result of the mobile IT revolution and the GDPR compliance requirements, many organizations are moving toward cloud computing to benefit from increased security, greater and easier scalability, a seamless mobile experience, and cost reduction.

- Security: Centrally storing data on a cloud system ensures GDPR compliance by eliminating the risk of physical data theft, the most common type of data breach.
- Scalability: Unlike traditional datacenters, companies can easily scale up their infrastructure through the cloud. Usually, businesses end up keeping personal data records for years. With a huge volume of personal data being stored, traditional datacenters might be overwhelmed.
- Mobility: Cloud computing allows employees to securely access data, applications, and desktops from any device and any location. This allows organizations to fully embrace bring-your-own-device (BYOD) and choose-your-own-device (CYOD) policies while gaining productivity and increasing data security.
- Cost Reduction: The adoption of cloud computing results in savings for businesses. Better hardware utilization means more efficiency. The centralized deployment of applications and desktops reduces IT staff's workload, which increases overall cost savings.

Build a Secure Cloud Computing Solution with Parallels Remote Application Server (RAS)

While cloud computing solutions provide efficient, scalable, and reliable systems, their full potential lies with the virtualization of applications, desktops, files, and folders that can be delivered to various devices. Through centralized application management, data storage, and maintenance, IT gains more control and can remotely ensure a strict separation between corporate and personal data.

Parallels® Remote Application Server (RAS) is an award-winning solution for virtual application and desktop delivery. It allows users to work securely from anywhere on virtually any device, including mobile Android and iOS®. Furthermore, it offers the required flexibility to build any cloud-computing infrastructure, since it works seamlessly with Microsoft® Remote Desktop Services (RDS), Citrix XenServer, VMware EXSi, Microsoft Hyper-V, Nutanix Acropolis (AHV), and KVM. Parallels RAS can be deployed on private, hybrid, or public clouds such as Amazon Web Services™ (AWS) and Windows Azure®.

To limit the risks of data leakage, access rules can be enforced and data can be segregated in restricted silos. This reinforces the division between the different user groups, departments, and regions.

Parallels RAS can centrally deploy critical OS updates and security patches to all users at once, reducing downtime while increasing security. In addition, it supports continuous availability, resource-based load balancing, and universal printing.

These features alongside strong data protection have led many organizations to choose Parallels RAS to provide access to applications, desktops, and data.

How Parallels RAS Increases a Business's Security

No Data Saved Locally: Data is stored in the company's cloud-based datacenter and securely accessed through encrypted connections. There is no data saved on the device; remote users only get a projection of the data, applications, and desktops hosted on the server.

Advanced Filtering: Parallels RAS integrates with Active Directory and offers advanced filtering options that prevent illegitimate user access. Filtering rules allow administrators to restrict access to sensitive data (such as cardholder details) by user or group, MAC address, IP address, and several other criteria.

Log-on: Two log-on modes are available: private and public. With the private log-on, user data (username and password) can be kept on the device. With public log-on, no user data can be retained on the device. This increases the security of shared workstations or tablets.

Data Segregation: Parallels RAS can create an unlimited number of farms and sites. A farm is a group of servers used to deliver applications to users, and a site is a group of farms; however, each site has an independent Activity Directory. No data can be shared between sites, guaranteeing perfect data segregation when needed.

Desktop Replacement: Parallels RAS offers businesses the ability to replace the desktop of a Windows machine, transforming it into a secure, pseudo thin client. The IT administrator can decide which applications are allowed to run locally based on security requirements. For maximum security, administrators can block any local operation on the machine and only allow operations remotely executed on the server.

Limitations for Copy and Paste: In order to avoid any unwanted data leakage from applications and desktops, copying and pasting data to a clipboard can be disabled.

Higher Security: All data is kept on the server side with centralized security and backup management. Only mouse clicks, keyboard keystrokes, and screen redraws are transmitted to and from the client device, thus preventing data leakages, viruses, Trojans, and other vulnerabilities on the clients.

Smart Card Authentication: Parallels RAS makes it easy to use a smart card to authenticate users on a virtual application. The redirection of virtual desktops and applications can be complicated; Parallels RAS increases security, allowing IT managers to use this technology when needed.

Two-Factor Authentication: Two-factor authentication provides a high level of protection by using different types of security tokens for a second level of authentication. Users are required to authenticate through two successive stages to access the application list. The second level of authentication can be provided by DualShield, SafeNet, or a RADIUS server.

SSL Certificate/Encryption: The Secure Client Gateway acts as a proxy between the Parallels Client software running on client devices and Parallels RAS. The gateway encrypts the communications using SSL.

Conclusion

Considered a Major Player in the virtualization technology solution sector, Parallels RAS enhances security and the end-user experience when accessing data, desktops, and applications on any device, anywhere. In fact, the secure solution has been awarded the prestigious Govies Government Security Award four years in a row. Not only that, Parallels RAS

has been chosen by thousands of businesses and organizations worldwide for its reliability, ease of use, and affordability.

By choosing Parallels RAS, both staff and users benefit from seamless, real-time access to virtualized applications on any device, including zero and thin clients, mobile workstations, and a vast selection endpoint machines.