Parallels®

PCI DSS Compliance

White Paper | Parallels Remote Application Server

Table of Contents

Introduction

IT security has always been a major concern for businesses that accept online credit card payments. They hold sensitive information that malicious hackers are after: cardholder data. This is why such businesses are legally obliged to build IT systems and networks that are PCI DSS compliant.

What Is PCI DSS?

PCI DSS is a security standard developed by the PCI Security Standards Council. Designed for businesses that do online transactions and hold customers' payment records, it helps them build and maintain secure IT systems and networks, ensuring the privacy and security of their customers' credit-card details and cardholder data.

The set of standards defined in the PCI DSS are the minimum required level of computer systems security that must be in place when processing credit-card data. These standards apply to merchants, processors, financial institutions, service providers, and any other entity that stores, processes, or transmits credit-card and cardholder information.

Why Businesses Need to Be PCI DSS Compliant

The challenges of building and maintaining a PCI DSS–compliant network are many and depend on several factors—for example, the type of software used, the network setup, and the procedures in place. If organizations that process credit-card payments and store cardholder details fail to build PCI DSS–compliant networks and computer systems, they risk being fined up to $500,000 per month—or even worse, having their trading licence revoked.

This white paper explains how using Parallels® Remote Application Server (RAS) can help organizations build scalable PCI DSS–compliant networks and also save on costs and administration overheads.

What Is Parallels RAS?

Parallels RAS is a server software that enables organizations to build a private secure cloud from which they can provide vendor-independent virtual desktop and application delivery from a single centralized platform. Parallels RAS extends and optimizes Windows Terminal Services and supports all major hypervisors from Microsoft, VMware, Citrix, and others.

All published applications and virtual desktops run on servers inside the datacentre. Users can access published applications and desktops using native Parallels RAS Clients or via HTML5-enabled web browsers. Since the user experience is provided via clients, the data and published resources never leave the private cloud, thus ensuring its security.

Apart from cutting down on costs, organizations using Parallels RAS also improve their productivity by being able to easily deliver applications, desktops, and data to anyone, anywhere.

How Parallels RAS Helps Build PCI DSS–Compliant Systems

PCI DSS is based on a set of twelve security requirements. Businesses and companies are required to implement these requirements to ensure security and protect cardholder data so they comply with the Payment Card Industry Data Security Standard.

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

PCI DSS–compliant networks require that all cardholder data flow across systems and networks—both trusted und untrusted—using secure protocols and network firewalls that allow incoming traffic from allowed devices only.

Parallels RAS simplifies this scenario; it allows administrators to easily allow or deny access to the data and published resources both at the gateway level and published resource level. IT administrators can specify which devices are authorized to connect to the environment and access data with the policy settings by limiting access based on gateway, MAC address, client type, IP address, user, or group.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Parallels RAS is completely integrated with Microsoft Active Directory, through which IT administrators can easily enable or disable users and set password-complexity requirements. On Parallels RAS, they can also control user access and logon times, as well as integrate the system with third-party authentication servers to enable strong authentication mechanisms such as two-factor authentication.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.
Parallels RAS equips IT administrators with all the tools and components required to build a secure setup on which they can run software to store cardholder data. All process flows and cardholder data stay in the datacenter, which eases being PCI DSS compliant and reduces security costs to protect the data.

Parallels RAS also provides a comprehensive client management solution that allows IT administrators to completely lock down client guests, configuring user policies that transform the client device into a thin client (kiosk mode).

Requirement 4: Encrypt transmission of cardholder data across open, public networks.
Parallels RAS supports both Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols to guarantee a secure communications channel between clients and the private cloud. Traffic is also encrypted if the user is connecting to the Parallels RAS site over the Internet.

IT administrators can choose either to set the SSL decryption process to be performed on the HALB appliance (SSL Offload)—which are also used to load balance incoming traffic—or tunnel the SSL connections directly to the Secure Client Gateways. In addition, SSL/TLS must be enabled and configured on the Parallels RAS Gateway to allow access from HTML5-enabled web browsers.

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs.
When using Parallels RAS, all infrastructure components and data are stored in the datacenter or the secure private cloud. This allows administrators to install anti-virus and similar protection software in a central location, thus making it very easy to ensure it is kept up to date and working. Running such software in a central location reduces the risks of having the network infected because of possibly outdated anti-virus software running on users' machines.

Since Parallels RAS allows all business applications to be configured to run in servers located in the datacenter, organizations reduce the risk of users running unwanted and dangerous applications, thus infecting the network with malware and other malicious software. Furthermore, client-side policies can limit a client (kiosk mode/thin client) or an HTML5-enabled browser, limiting users from running malicious software.

Requirement 6: Develop and maintain secure systems and applications.
Systems administrators know very well that applying security patches is a problematic task. Compatibility issues, software crashes, user permissions problems, unsupported hardware, and several other issues are just a few that administrators encounter when applying security patches. There is no way to avoid this; administrators must install the vendor-released security patches to ensure the security of their network and sensitive data.

With all business applications running in the datacenter and published through Parallels RAS, security is guaranteed. Operating systems and applications are centrally updated in a short space of time, and there is much less that needs to be updated. Also with Parallels RAS, users do not have access to install software, and the applications catalog is limited to the software each user can run. Parallels offers the option of verifying access to published applications prior to making them available to the end user, ensuring resources are available in the specified path and compatibility issues do not appear after the product's or operating system's patching process.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know.
To ensure critical information such as cardholder data can only be accessed by authorized personnel, Parallels offers a comprehensive set of policies to determine which clients can run which publish applications. Policies allow IT administrators to manage and define client requirements for users on the network who connect to a server in the farm. Based on different criteria such as client MAC address, client type, or Parallels RAS Gateway, different session settings can be defined for each client connected to the environment.

Requirement 8: Identify and authenticate access to system components.
PCI DSS–compliant solutions must provide a unique identification account to each individual user who connects to the infrastructure. Parallels RAS is completely integrated with Microsoft Active Directory, where each user has its own unique ID (User Principal Name).

Parallels RAS can be also integrated with multifactor authentication solutions that identifiy unique users in your network. One of the supported authentication providers is the Azure MFA Server. Assigning a unique identification to each user guarantees that each person is traceable for their actions.

Requirement 9: Restrict physical access to cardholder data.
Even though this is not something that Parallels RAS or any other software can help you with, since Parallels RAS stores all data centrally, it makes it much easier to restrict physical access to servers where cardholder data is stored.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.
Tracking end-to-end user activities is critical in detecting, preventing, and minimizing possible unauthorized access to applications or even to stored cardholder data. Parallels RAS offers both complete tracking configuration options for IT administrators' activity (audit log of what administrators are doing and changing in the environment configuration) and for the end-user connections (who logged in, when, what applications did they use, and more).

Apart from the default audit log, several other types of logs can be enabled in the Parallels RAS farm. Additionally, several monitoring features (such as the monitoring report or the client manager) can be used to help administrators keep track of all the events happening on their network, servers, and private cloud, and spot any suspicious behavior immediately.

Requirement 11: Regularly test security systems and processes.
This is not related to the network setup and Parallels RAS cannot help you with this requirement. However, because of the way Parallels works and can be set up, it is very easy for administrators to test the system and processes since everything is centralized in the datacenter or private cloud.

Maintain an Information Security Policy

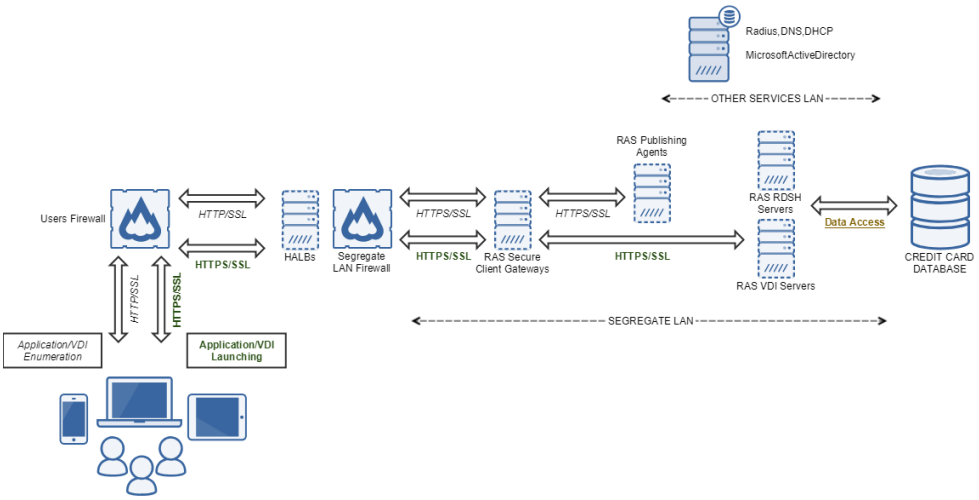
Requirement 12: Maintain a policy that addresses information security for all personnel.
Employees working in a cardholder-data environment should be aware of the sensitivity of data and their responsibilities for protecting it. The easier they can access the environment from client devices, the easier for IT administrators to avoid security problems. As all Parallels RAS infrastructure components can be in the company datacenter or private cloud, and client-side requirements are minimum, companies can easily document and establish simple user procedures to connect to their critical applications.

Sample Diagrams for PCI DSS Networks

PCI DSS–Compliant Local Network Implementation

The diagram below highlights how Parallels RAS can be implemented in a LAN environment to build a PCI DSS–compliant network. Some of the features that organizations can benefit from when using this scenario are:

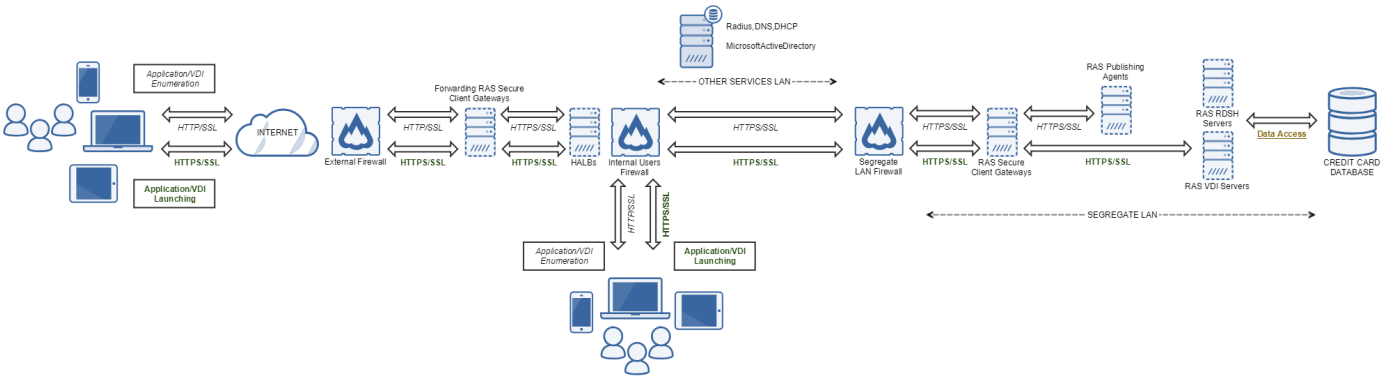
- Applications used to access cardholder data are segregated from the LAN.
- The cardholder data database is segregated from the LAN.
- All applications are only available through a central location: Parallels RAS.
- All sensitive data is stored in a central location.
- Users access applications and data over an encrypted channel.
- Sensitive cardholder data never leaves the private cloud.
- Only publishing data is transferred between the user and the private cloud.



PCI DSS Compliant Network with Remote Access Implementation

The diagram below highlights how Parallels Remote Application Server can be implemented to build a PCI DSS compliant network and provide access to remote users. These are some of the features organizations can benefit from:

- All of the benefits that apply to the local area network implementation mentioned in the previous section.
- Remote users can access applications and data by using the RAS Client, which can run on any modern operating system and mobile device.
- Remote users can access applications and data from a standard HTML5 browser over an HTTPS session.
- Multiple firewalls allow for segregation of private cloud, local area network, DMZ and corporate network



Other Notable Features that Make Parallels RAS Perfect for PCI DSS Networks

Installation and Setup: Time Investment

All the components required to set up the site are installed through a single MSI file, a very straightforward process for an "all-in-one" solution. Default setup is focused on helping businesses get started very easily with configured SSL certificates, remote access, and fully enabled HTML5 client support. Furthermore, Parallels RAS offers an all-in-place upgrade for all versions with minimal downtime. When using Parallels, your environment can be upgraded without affecting your users' productivity.

Flexibility in Deployment (On-Premise, Hybrid, and Cloud)

Parallels RAS supports on-premise, hybrid, and cloud deployments. It is readily available for both Microsoft Azure and Amazon Web Services™ (AWS) Marketplace as a Windows Appliance.

Simple Pricing and Low Licensing Costs

There is only one edition of Parallels RAS, and it includes all the enterprise features such as reporting, load balancing, and high availability. The affordable Parallels RAS licensing model depends only on the number of concurrent users connecting to the environment.

Centralized Configuration Console and Multisite Support

To manage, monitor, and scale up the Parallels RAS farm systems, administrators only use a single central interface, the Parallels RAS Configuration Console. This console also allows system administrators to centrally manage interconnected farms in different physical locations. This gives system administrators in a multisite environment the flexibility to better utilize all available resources, because users from one site can access published applications and virtual desktops on another site.

Multiple Administrators and Roles Make Delegation Easier

Delegating administrative tasks has never been easier. Administrators can assign different Parallels RAS roles to Active Directory users, so that each administrator account can configure and maintain a specific function. For example, an administrator can manage the publishing of applications and other resources for a specific site.

Best-in-Class BYOD Support for a Wider Variety of OSes and Mobile Devices

Parallels RAS client is available for Windows, Mac, and Linux operating systems. It can also be installed on virtually any type of mobile device, such as the popular Android and iOS phones. A HTML5-enabled browser allows users to view and launch remote applications or virtual desktops in a web browser, making Parallels RAS a client-independent solution that's perfect for bring-your-own-device (BYOD) scenarios.

Easy Partial and Full Recovery Options

Parallels RAS allows IT administrators to easily import or export configuration from the central Parallels RAS Console. If a backup needs to be restored, the process is simple, efficient, and fast, ensuring the least possible downtime.

High Availability

An out-of-the-box installation of Parallels RAS load balances all the incoming connections. Parallels RAS has a built-in and management-free High Availability Load Balancing (HALB). It can distribute load among servers and gateways based on the resources available, dramatically improving the user experience.

A Complete VDI Management Solution

In some scenarios, IT administrators may need to provide users with a full desktop instead of just a published application. Parallels RAS offers a complete virtual desktop infrastructure (VDI) solution included with its licensing plan. Furthermore, Parallels RAS supports desktop pool generation from linked clones, which in conjunction with RASprep technology allows absolute flexibility in the creation of new user desktops. It's easy to recycle machines and possible to generate new ones in case some have been infected by malicious software in a short space of time.

With Parallels RAS, It's Easier to Be PCI DSS Compliant

Parallels RAS allows administrators to build a secure private cloud where they can centralize all sensitive data, allow access through published applications and virtual desktops, and have a PCI DSS–compliant network. Since all data is centralized and only accessed via published resources, it is easier to manage, maintain, and audit the network. Because only published data is exchanged between the client and Parallels RAS servers, the security of the network is drastically improved.

The Parallels RAS Client is available for most popular operating systems and mobile devices. It's also integrated with HTML5-enabled browsers, which makes it a client-independent solution. A unique and simple licensing plan offers both published applications and a VDI solution. Complete integration with the latest machine cloning technologies allows IT administrators to easily deploy new machines to their environment or replace infected machines that may compromise network security.