



Datensicherheitsstandard in der Zahlungskartenbranche Compliance (PCI DSS)

Whitepaper | Parallels Remote Application Server (RAS)

Inhalt

Einführung	3
Was ist PCI DSS?	3
Warum Unternehmen PCI DSS-konform sein müssen	3
Was ist Parallels RAS?	3
So unterstützt Parallels RAS den Aufbau von Systemen, die mit PCI DSS kompatibel sind.....	3
Aufbau und Wartung eines sicheren Netzwerks und sicherer Systeme	4
Schutz der Karteninhaberdaten.....	4
Pflege eines Programms zum Management von Schwachstellen.....	5
Implementierung von strengen Zugangskontrollmaßnahmen	5
Regelmäßige Überwachung und Prüfung von Netzwerken.....	6
Aufrechterhalten einer Richtlinie zur Informationssicherheit	7
Beispieldiagramme für PCI DSS-Netzwerke.....	7
Weitere bemerkenswerte Features, die Parallels RAS perfekt für PCI DSS-Netzwerke machen.....	8
Mit Parallels RAS ist es einfacher, PCI DSS-konform zu sein	10

Einführung

IT-Sicherheit ist seit jeher ein wichtiges Anliegen für Unternehmen, die Online-Kreditkartenzahlungen akzeptieren. Sie speichern sensible Daten, hinter denen böswillige Hacker her sind: Karteninhaberdaten und Kundeninformationen. Deshalb sind Unternehmen gesetzlich verpflichtet, PCI DSS-konforme IT-Infrastrukturen aufzubauen.

Was ist PCI DSS?

PCI DSS ist ein Sicherheitsstandard, der vom Payment Card Industry (PCI) Security Standards Council entwickelt wurde. Er wurde für Unternehmen entwickelt, die Online-Transaktionen durchführen und die Zahlungsdaten ihrer Kunden aufbewahren. Der Standard unterstützt sie bei Aufbau und Wartung einer sicheren IT-Infrastruktur und gewährleistet Privatsphäre und Sicherheit der Karteninhaberdaten.

Die im PCI DSS definierten Standards sind das Mindestmaß an Sicherheit der Computersysteme, das bei der Verarbeitung von Kreditkartendaten gewährleistet sein muss. Diese Standards gelten für Händler, Verarbeiter, Finanzinstitute, Dienstleister und alle anderen Unternehmen, die Kreditkarten- und Karteninhaberinformationen speichern, verarbeiten oder übertragen.

Warum Unternehmen PCI DSS-konform sein müssen

Die Herausforderungen bei Aufbau und Wartung von PCI DSS-konformen Netzwerken sind vielfältig und hängen von mehreren Faktoren ab. Zum Beispiel die verwendete Software, die Netzwerkeinrichtung und die vorhandenen Verfahren. Wenn Unternehmen, die Kreditkartenzahlungen verarbeiten und Karteninhaberdaten speichern, es nicht schaffen, PCI DSS-konforme Netzwerke und Computersysteme aufzubauen, riskieren sie eine Geldstrafe von bis zu 500.000 US-Dollar pro Monat – oder noch schlimmer, dass ihnen der Gewerbeschein entzogen wird.

In diesem Whitepaper wird erläutert, wie der Einsatz von Parallels® Remote Application Server (RAS) Unternehmen beim Aufbau skalierbarer PCI DSS-konformer Netzwerke unterstützen und Kosten und Verwaltungsaufwand sparen kann.

Was ist Parallels RAS?

Parallels RAS ist eine Serversoftware, die es Unternehmen ermöglicht, eine private, sichere Cloud aufzubauen, aus der sie herstellerunabhängige virtuelle Desktops und Anwendungen von einer einzigen zentralen Plattform aus bereitstellen können. Parallels RAS erweitert und optimiert Windows RDSH-Hostpools und unterstützt alle wichtigen Hypervisoren von Microsoft, VMware, Citrix und anderen.

Alle veröffentlichten Anwendungen und virtuellen Desktops laufen auf Servern im Rechenzentrum. Benutzer können über native Parallels RAS-Clients oder über HTML5-fähige Webbrowser auf veröffentlichte Anwendungen und Desktops zugreifen. Da die Benutzererfahrung über Clients bereitgestellt wird, verlassen die Daten und veröffentlichten Ressourcen niemals die private Cloud und gewährleisten so deren Sicherheit.

Neben der Kostensenkung verbessern Unternehmen, die Parallels RAS einsetzen, auch ihre Produktivität, indem sie Anwendungen, Desktops und Daten einfach und überall bereitstellen können.

So unterstützt Parallels RAS den Aufbau von Systemen, die mit PCI DSS kompatibel sind

PCI DSS basiert auf einer Reihe von zwölf Sicherheitsanforderungen. Unternehmen werden aufgefordert, diese Sicherheitsmaßnahmen umzusetzen, um die Einhaltung des Datensicherheitsstandards der Zahlungskartenindustrie sicherzustellen.

Aufbau und Wartung eines sicheren Netzwerks und sicherer Systeme

Anforderung 1: Installieren und warten Sie eine Firewall-Konfiguration, um die Daten der Karteninhaber zu schützen.

PCI DSS-konforme Netzwerke erfordern, dass alle Karteninhaberdaten über Systeme und Netzwerke fließen – sowohl vertrauenswürdige als auch nicht vertrauenswürdige –, unter Verwendung sicherer Protokolle und Netzwerk-Firewalls, die nur eingehenden Datenverkehr von zulässigen Geräten zulassen.

Parallels RAS vereinfacht dieses Szenario. Es ermöglicht Unternehmen, den Zugriff auf die Daten und veröffentlichten Ressourcen sowohl auf Gateway-Ebene als auch auf Ebene der veröffentlichten Ressourcen einfach zu kontrollieren. Administratoren können festlegen, welche Geräte berechtigt sind, sich mit der Umgebung zu verbinden und auf Daten mit den Richtlinieneinstellungen zuzugreifen, indem sie den Zugriff auf Basis von Gateway, MAC-Adresse, Client-Typ, IP-Adresse, Benutzer oder Gruppe beschränken.

Anforderung 2: Verwenden Sie keine vom Hersteller vorgegebenen Standardwerte für Systempasswörter und andere Sicherheitsparameter.

Parallels RAS ist in Microsoft Active Directory integriert, über das Administratoren einfach Benutzer aktivieren oder deaktivieren und Anforderungen an die Passwortkomplexität festlegen können. Auf Parallels RAS können sie auch die Zugriffs- und Anmeldezeiten der Benutzer steuern und das System in Authentifizierungsserver von Drittanbietern integrieren, um starke Authentifizierungsmechanismen wie die Zwei-Faktor-Authentifizierung zu ermöglichen.

Schutz der Karteninhaberdaten

Anforderung 3: Gespeicherte Karteninhaberdaten schützen.

Parallels RAS bietet Unternehmen ein komplettes Toolset zum Aufbau einer sicheren Umgebung, in der sie Software zur Speicherung von Karteninhaberdaten ausführen können. Alle Prozessabläufe und Karteninhaberdaten bleiben im Rechenzentrum, was die PCI DSS-Konformität erleichtert und die Sicherheitskosten zum Schutz der Daten reduziert. Parallels RAS bietet auch eine umfassende Client-Management-Lösung, die es Administratoren ermöglicht, Client-Gäste vollständig zu sperren, indem sie Benutzerrichtlinien konfiguriert, die Endpunkte in einen Thin Client umwandeln (Kiosk-Modus).

Anforderung 4: Verschlüsselung der Übertragung von Karteninhaberdaten über offene, öffentliche Netze.

Parallels RAS unterstützt sowohl Secure Socket Layer (SSL) als auch Transport Layer Security-Protokolle (TLS), um einen sicheren Kommunikationskanal zwischen Kunden und der Kunden-Cloud-Infrastruktur zu gewährleisten.

Administratoren können wählen, ob sie den SSL-Entschlüsselungsprozess für die High Availability Load Balancing (HALB) Appliance (SSL Offload) – die auch zur Lastverteilung beim eingehenden Datenverkehr verwendet wird – festlegen oder die SSL-Verbindungen direkt zu den Secure Client Gateways kanalisieren möchten. Darüber hinaus muss SSL/TLS auf dem Parallels RAS-Gateway aktiviert und konfiguriert sein, um den Zugriff über HTML5-fähige Webbrowser zu ermöglichen.

Pflege eines Programms zum Management von Schwachstellen

Anforderung 5: Schützen Sie alle Systeme vor Malware und aktualisieren Sie regelmäßig Antivirensoftware oder -programme.

Bei der Verwendung von Parallels RAS werden nicht alle Infrastrukturkomponenten und Daten auf dem Endpunkt-Client-Gerät gespeichert. Auf diese Weise können Administratoren Antiviren- und ähnliche Schutzsoftware an einem zentralen Ort installieren und so sehr einfach sicherstellen, dass sie auf dem neuesten Stand gehalten wird und funktioniert. Der Betrieb einer solchen Software an einem zentralen Ort reduziert das Risiko von Datenverstößen. Darüber hinaus bietet Parallels RAS für mobile Benutzer den HTML5-Zugang mit sehr strengen Zugriffsregeln.

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen.

Administratoren wissen sehr gut, dass das Einspielen von Sicherheitspatches eine problematische Aufgabe ist. Kompatibilitätsprobleme, Softwareabstürze, Probleme mit Benutzerberechtigungen, nicht unterstützte Hardware und einige andere Probleme sind nur einige, auf die Administratoren beim Einspielen von Sicherheitspatches stoßen. Es gibt keine Möglichkeit, dies zu vermeiden; Administratoren müssen die vom Hersteller freigegebenen Sicherheitspatches installieren, um die Sicherheit ihres Netzwerks und sensibler Daten zu gewährleisten.

Parallels RAS verfügt über Richtlinien, die es Administratoren ermöglichen, die Zuordnung von Desktops und die Trennung von Unternehmensnutzern zu verwalten. So kann beispielsweise nach der Abmeldung eines Benutzers je nach den Richtlinien der Benutzer-Desktop heruntergefahren, ausgesetzt oder neu gestartet werden. Dies ermöglicht nicht nur eine vollständige Kontrolle über die Zuordnung der Desktops, sondern auch eine effiziente und optimale Nutzung der Unternehmensressourcen.

Da alle Geschäftsanwendungen in der Enterprise Cloud ausgeführt und über Parallels RAS veröffentlicht werden, wird die Eindämmung von Sicherheitsbrüchen zu einer kostengünstigeren Aufgabe. Betriebssysteme und Anwendungen werden in kurzer Zeit zentral aktualisiert, und es gibt viel weniger zu aktualisieren. Außerdem haben Benutzer mit Parallels RAS keinen Zugriff auf die Installation von Software. Der Anwendungskatalog ist auf die Software beschränkt, die jeder Benutzer ausführen kann, und die laufenden Prozesse auf jedem VDI-Benutzer können zentral verwaltet werden. Parallels bietet die Möglichkeit, den Zugriff auf veröffentlichte Anwendungen zu überprüfen, bevor sie dem Endbenutzer zur Verfügung gestellt werden, um sicherzustellen, dass Ressourcen im angegebenen Pfad verfügbar sind und Kompatibilitätsprobleme nicht nach dem Patch-Prozess des Produkts oder Betriebssystems auftreten.

Implementierung von strengen Zugangskontrollmaßnahmen

Anforderung 7: Den Zugriff auf die Daten des Karteninhabers nach Geschäftsanforderungen beschränken.

Um sicherzustellen, dass wichtige Informationen wie Karteninhaberdaten nur autorisiertem Personal zugänglich sind, bietet Parallels ein umfassendes Paket von Richtlinien an, um festzustellen, welche Kunden welche Anwendungen ausführen dürfen. Richtlinien ermöglichen es Administratoren, Client-Anforderungen für Benutzer im Netzwerk zu verwalten und zu definieren, die eine Verbindung zu einem Server in der Farm herstellen. Basierend auf verschiedenen Kriterien wie Client-MAC-Adresse, Client-Typ oder Parallels RAS-Gateway können für jeden mit der Umgebung verbundenen Client unterschiedliche Session-Einstellungen definiert werden.

Anforderung 8: Den Zugriff auf Systemkomponenten identifizieren und authentifizieren.

PCI DSS-konforme Lösungen müssen jedem einzelnen Benutzer, der eine Verbindung zur Infrastruktur herstellt, ein eindeutiges Identifikationskonto zur Verfügung stellen. Parallels RAS ist vollständig in Microsoft Active Directory integriert, wobei jeder Benutzer seine eigene eindeutige ID (User Principal Name) hat. Ergänzend dazu ist die neue Windows10-PIN-Entsperrfunktion vollständig in den RAS-Client „Single Sign On“ integriert.

Parallels RAS kann auch in Multifaktor-Authentifizierungslösungen von Drittanbietern wie DualShield, Safenet, RADIUS oder Azure Multi-Factor Authentication integriert werden. Google Authenticator, der den Algorithmus Time-Based One-Time Password (TOTP) verwendet, wurde kürzlich auch als MFA-Anbieter hinzugefügt. Die Zuordnung einer eindeutigen Identifikation zu jedem Benutzer garantiert, dass jede Person für ihre Aktionen nachvollziehbar ist.

Ihre im Unternehmen veröffentlichten Ressourcen können nur über die RAS-Infrastruktur zugänglich gemacht werden, was die Sicherheit Ihres Unternehmens erhöht und unzulässige Zugriffe verhindert.

Anforderung 9: Den physischen Zugriff auf die Daten des Karteninhabers beschränken.

Auch wenn Parallels RAS oder eine andere Software Ihnen dabei nicht helfen kann, da Parallels RAS alle Daten zentral speichert, ist es damit viel einfacher, den physischen Zugriff auf Server zu beschränken, auf denen Karteninhaberdaten gespeichert sind.

Regelmäßige Überwachung und Prüfung von Netzwerken

Anforderung 10: Alle Zugriffe auf Netzwerkressourcen und Karteninhaberdaten verfolgen und überwachen.

Das Verfolgen von End-to-End-Benutzeraktivitäten ist entscheidend für die Erkennung, Verhinderung und Minimierung eines möglichen unbefugten Zugriffs auf Anwendungen oder sogar auf gespeicherte Karteninhaberdaten.

Parallels RAS bietet vollständige Optionen zur Tracking-Konfiguration für die Aktivitäten der Administratoren (Audit-Log, was Administratoren tun und was sich in der Umgebungskonfiguration ändert) und protokolliert, was in der RAS-Konsole geändert wird, um beispielsweise unbefugte Zugriffsrechte zu vermeiden. Neben dem Standard-Auditprotokoll können mehrere andere Arten von Protokollen in der Parallels RAS-Farm oder in Multi-Farmen aktiviert werden. Protokollrotation und andere Einstellungen können auf jedem Host je nach Sicherheitsanforderungen konfiguriert werden.

Darüber hinaus können mehrere Benutzerüberwachungsfunktionen (wie der Überwachungsbericht oder der Client-Manager) und maßgeschneiderte Berichte verwendet werden, um Administratoren dabei zu unterstützen, den Überblick über alle Zugriffe, Anwendungsnutzungen und Ereignisse auf ihrer Infrastruktur zu behalten, um verdächtiges Verhalten sofort zu erkennen.

Darüber hinaus verfügt Parallels über ein Tool zum Löschen aller Informationen über einen bestimmten Benutzer, das die Einhaltung der Compliance-Anforderungen der Allgemeinen Datenschutzverordnung (DSGVO) erleichtert.

Anforderung 11: Regelmäßige Überprüfung der Sicherheitssysteme und -prozesse.

Dies hängt nicht mit der Netzwerkinstallation zusammen und Parallels RAS kann Ihnen bei dieser Anforderung nicht helfen. Aufgrund der Funktionsweise von Parallels und der Möglichkeit, Parallels einzurichten, ist es für Administratoren jedoch sehr einfach, das System und die Prozesse zu testen, da alles im Rechenzentrum oder in der privaten Cloud zentralisiert ist.

Aufrechterhalten einer Richtlinie zur Informationssicherheit

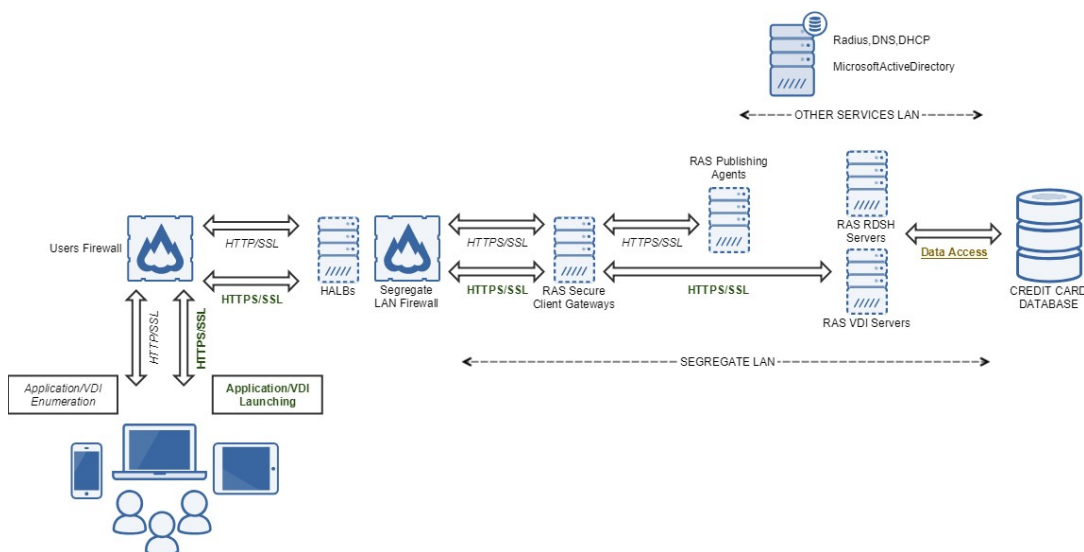
Anforderung 12: Eine Richtlinie aufrechterhalten, die sich mit der Informationssicherheit für alle Mitarbeiter befasst. Mitarbeiter, die in einer Umgebung mit Karteninhaberdaten arbeiten, sollten sich der Sensibilität der Daten und ihrer Verantwortung für deren Schutz bewusst sein. Je einfacher sie von Client-Geräten aus auf die Umgebung zugreifen können, desto einfacher ist es für Administratoren, Sicherheitsprobleme zu vermeiden. Da sich alle Parallels RAS-Infrastrukturkomponenten im Rechenzentrum oder in der privaten Cloud des Unternehmens befinden können und die Anforderungen auf der Clientseite minimal sind, können Unternehmen einfach dokumentieren und einfache Benutzerverfahren für die Verbindung zu ihren kritischen Anwendungen einrichten.

Beispieldiagramme für PCI DSS-Netzwerke

PCI DSS-konforme Implementierung eines lokalen Netzwerks

Das folgende Diagramm zeigt, wie Parallels RAS in einer LAN-Umgebung implementiert werden kann, um ein PCI DSS-konformes Netzwerk aufzubauen. Einige der Funktionen, von denen Unternehmen bei der Verwendung dieses Szenarios profitieren können, sind:

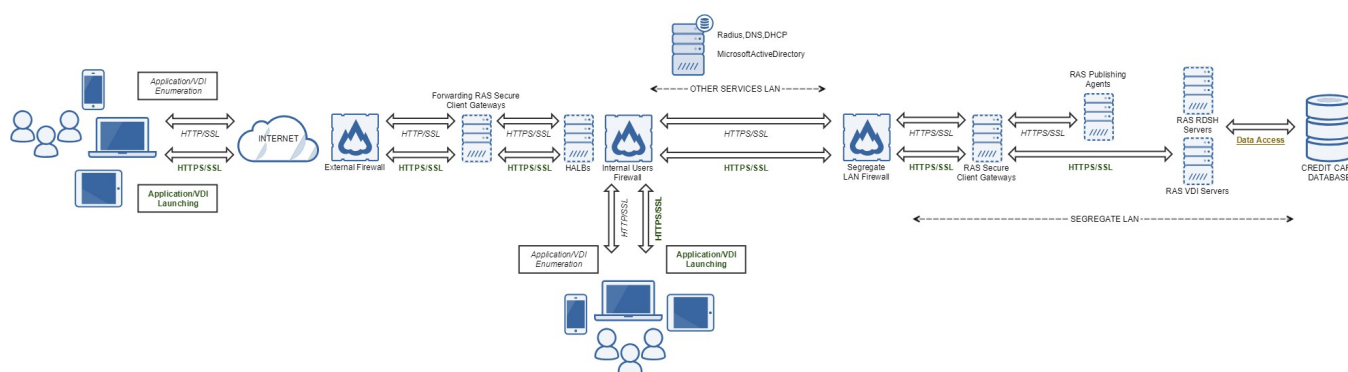
- Anwendungen für den Zugriff auf Karteninhaberdaten werden vom LAN getrennt
- Die Datenbank der Karteninhaberdaten ist vom LAN getrennt
- Alle Anwendungen sind nur über eine zentrale Stelle verfügbar: Parallels RAS
- Alle sensiblen Daten werden an einem zentralen Ort gespeichert
- Benutzer greifen über einen verschlüsselten Kanal auf Anwendungen und Daten zu
- Sensible Karteninhaberdaten verlassen nie die private Cloud
- Es werden nur Veröffentlichungsdaten zwischen dem Benutzer und der Private Cloud übertragen



PCI DSS-konformes Netzwerk mit Remote Access-Implementierung

Das folgende Diagramm zeigt, wie Parallels Remote Application Server implementiert werden kann, um ein PCI DSS-konformes Netzwerk aufzubauen und Remote-Benutzern Zugriff zu gewähren. Dies sind einige der Funktionen, von denen Unternehmen profitieren können:

- Alle Vorteile, die für die im vorherigen Abschnitt erwähnte Implementierung des lokalen Netzwerks gelten.
- Remote-Benutzer können mit dem RAS-Client, der auf jedem modernen Betriebssystem und mobilen Gerät ausgeführt werden kann, auf Anwendungen und Daten zugreifen.
- Remote-Benutzer können über eine HTTPS-Sitzung von einem Standard-HTML5-Browser aus auf Anwendungen und Daten zugreifen.
- Mehrere Firewalls ermöglichen die Trennung von Private Cloud, Local Area Network, DMZ und Corporate Network



Weitere bemerkenswerte Features, die Parallels RAS perfekt für PCI DSS-Netzwerke machen

Installation und Einrichtung: Zeitaufwand

Alle Komponenten, die für die Einrichtung der Site erforderlich sind, werden über eine einzige MSI-Datei installiert, ein sehr einfacher Prozess für eine „All-in-One“-Lösung. Die Standardeinrichtung ist darauf ausgerichtet, Unternehmen bei der einfachen Einführung mit konfigurierten SSL-Zertifikaten, Fernzugriff und voll aktiviertem HTML5-Client-Support zu unterstützen. Darüber hinaus bietet Parallels RAS ein All-In-Place-Upgrade für alle Versionen mit minimalen Ausfallzeiten. Wenn Sie Parallels verwenden, kann Ihre Umgebung aktualisiert werden, ohne die Produktivität Ihrer Benutzer zu beeinträchtigen.

Flexibilität bei der Bereitstellung (On-Premise, Hybrid und Cloud)

Parallels RAS unterstützt On-Premise-, Hybrid- und Cloud-Bereitstellungen. Es ist sowohl für Microsoft Azure als auch für Amazon Web Services™ Marketplace (AWS) als Windows-Appliance verfügbar.

Einfache Preisgestaltung und niedrige Lizenzkosten

Von Parallels RAS gibt es nur eine Edition. Diese enthält alle Unternehmensfunktionen, wie z. B. Berichterstellung, Lastausgleich und Hochverfügbarkeit. Das erschwingliche Parallels RAS-Lizenzmodell hängt nur von der Anzahl der gleichzeitigen Benutzer ab, die sich mit der Umgebung verbinden.

Zentralisierte Konfigurationskonsole und Multisite-Unterstützung

Für Verwaltung, Überwachung und Skalierung der Parallels RAS-Farm-Systeme verwenden Administratoren nur eine einzige zentrale Oberfläche, die Parallels RAS Configuration Console. Diese Konsole ermöglicht es Systemadministratoren auch, vernetzte Farmen an verschiedenen physischen Standorten zentral zu verwalten. Dies gibt Systemadministratoren in einer Multisite-Umgebung die Flexibilität, alle verfügbaren Ressourcen besser zu nutzen, da Benutzer von einer Site aus auf veröffentlichte Anwendungen und virtuelle Desktops an einer anderen Site zugreifen können.

Mehrere Administratoren und Rollen erleichtern das Delegieren

Das Delegieren von Verwaltungsaufgaben war noch nie so einfach. Administratoren können Active Directory-Benutzern verschiedene Parallels RAS-Rollen zuweisen, sodass jedes Administratorkonto eine bestimmte Funktion konfigurieren und pflegen kann. So kann beispielsweise ein Administrator die Veröffentlichung von Anwendungen und anderen Ressourcen für eine bestimmte Site verwalten.

Erstklassige BYOD-Unterstützung für eine größere Vielfalt an Betriebssystemen und mobilen Geräten

Der Parallels RAS-Client ist für die Betriebssysteme Windows, Mac und Linux verfügbar. Es kann auch auf praktisch jeder Art von mobilen Geräten installiert werden, wie z. B. den beliebten Android- und iOS-Handys. Ein HTML5-kompatibler Browser ermöglicht es Benutzern, entfernte Anwendungen oder virtuelle Desktops in einem Webbrowser anzuzeigen und zu starten, was Parallels RAS zu einer mandantenunabhängigen Lösung macht, die perfekt für Bring-Your-Own-Device-Szenarien (BYOD) geeignet ist.

Einfache partielle und vollständige Wiederherstellungsoptionen

Parallels RAS ermöglicht Administratoren den einfachen Import oder Export von Konfigurationen aus der zentralen Parallels RAS Console. Wenn ein Backup wiederhergestellt werden muss, ist der Prozess einfach, effizient und schnell und sorgt für möglichst geringe Ausfallzeiten.

Hohe Verfügbarkeit

Eine „Out-of-the-Box“-Installation der Parallels RAS-Last gleicht alle eingehenden Verbindungen aus. Parallels RAS verfügt über ein integriertes und verwaltungsfreies High Availability Load Balancing (HALB). Es kann die Last auf Server und Gateways auf der Grundlage der verfügbaren Ressourcen verteilen und so die Benutzerfreundlichkeit erheblich verbessern.

Eine komplette VDI-Management-Lösung

In einigen Szenarien müssen Administratoren den Benutzern möglicherweise einen vollständigen Desktop anstelle einer veröffentlichten Anwendung zur Verfügung stellen. Parallels RAS bietet eine komplette Virtual Desktop Infrastructure-Lösung (VDI), die im Lizenzplan enthalten ist. Darüber hinaus unterstützt Parallels RAS die Generierung von Desktop-Pools aus verknüpften Klonen, was in Verbindung mit der RASprep-Technologie absolute Flexibilität bei der Erstellung neuer Benutzer-Desktops ermöglicht. Es ist einfach, Computer zu recyceln und neue zu generieren, falls einige davon innerhalb eines kurzen Zeitraums mit bössartiger Software infiziert wurden.

Unterstützung von Windows Server 2019

Alle Komponenten der RAS-Infrastruktur sind mit Windows Server 2019 kompatibel. Darüber hinaus können Virtual Desktop Infrastructure-Desktops (VDI) und Remote Desktop Session Host-Server (RDSH) auf Microsoft Hyper-V 2019 bereitgestellt, skaliert und gepflegt werden.

Sitzung vorab starten

Mit RAS können Administratoren die Vorstartfunktion für Sitzungen aktivieren, um die Startzeit der Anwendung zu verkürzen. Durch die Verwendung modernster Artificial Intelligence-Technologie (KI) werden RDP-Sitzungen nur wenige Minuten vor dem normalen Start der Anwendungen automatisch gestartet, um die Benutzerfreundlichkeit zu verbessern und Wartezeiten zu reduzieren.

VDI-Lösung für Scale Computing HC3-Unterstützung

Neben der vollständigen Liste der unterstützten Hypervisoren, wie VMware ESXi und Microsoft Hyper, unterstützt RAS auch Scale Computing HC3 für VDI-Bereitstellungen. Scale Computing HC3 ist eine neue hyperkonvergente Infrastruktur, die Computing, Speicherung, Virtualisierung, Backup und Disaster Recovery in einem einzigen System vereint. Mit Scale Computing HC3 können RAS-Administratoren schnellere VDI-Lösungen zu einem günstigeren Preis anbieten.

Mit Parallels RAS ist es einfacher, PCI DSS-konform zu sein

Parallels RAS ermöglicht es Administratoren, eine sichere Private Cloud aufzubauen, in der sie alle sensiblen Daten zentralisieren, Zugriff über veröffentlichte Anwendungen und virtuelle Desktops ermöglichen und über ein PCI DSS-konformes Netzwerk verfügen können. Da alle Daten zentralisiert sind und nur über veröffentlichte Ressourcen auf sie zugegriffen wird, ist es einfacher, das Netzwerk zu verwalten, zu warten und zu überprüfen. Da nur veröffentlichte Daten zwischen dem Client und den Parallels RAS-Servern ausgetauscht werden, wird die Sicherheit des Netzwerks drastisch verbessert.

Der Parallels RAS-Client ist für die meisten gängigen Betriebssysteme und mobilen Geräte verfügbar. Er ist auch in HTML5-fähige Browser integriert, was ihn zu einer mandantenunabhängigen Lösung macht. Ein einzigartiger und einfacher Lizenzplan bietet sowohl veröffentlichte Anwendungen als auch eine VDI-Lösung. Die vollständige Integration mit den neuesten Technologien zum Klonen von Computern ermöglicht es Administratoren, neue Computer einfach in ihrer Umgebung einzusetzen oder infizierte Computer zu ersetzen, die die Netzwerksicherheit beeinträchtigen können.