Enhance Your Data Security with Parallels RAS

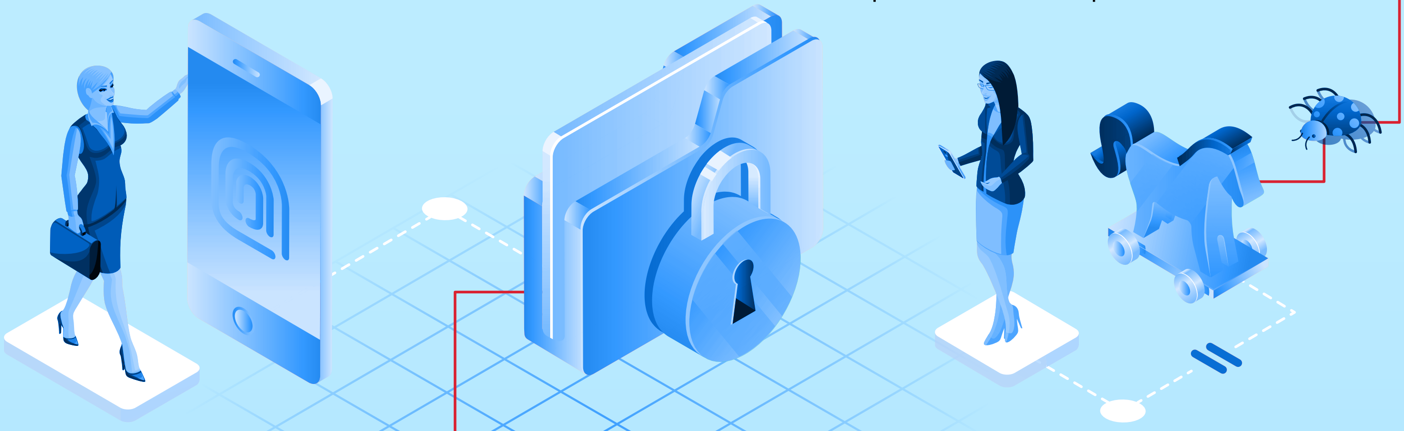
Deploying Parallels® Remote Application Server (RAS) reduces the risk of data loss and malicious activity by using policies that limit access based on user, group permissions, locations and devices.

INCREASE YOUR MOBILE WORKFORCE SECURITY

Organizations need to ensure that the devices and data accessed by remote workers are kept secure. Parallels RAS provides a high level of protection by enabling multifactor authentication (MFA) through providers such as Google Authenticator and Microsoft Azure. Client policies control what is accessed from devices to minimize data breaches.

PREVENT MALICIOUS SOFTWARE AND CYBER-ATTACKS

With Parallels RAS, IT administrators can control what users access—from a single pane of glass. A distributed denial-of-service (DDoS) prevention engine is built-in to block multiple attacks and allow only true traffic to go through the gateways. Access from known suspicious locations is blocked, and data is segregated to prevent data corruption or theft.



REINFORCE DATA ENCRYPTION AND COMPLIANCE

Encryption protocols such as SSL or FIPS 140-2 are enabled to help organizations adhere to data compliance policies such as PCI DSS, HIPAA and GDPR. Access to sensitive data is restricted with granular filtering rules, defining who in the organization can access specific published resources.

MONITOR AND CONTROL ACCESS

Parallels RAS incorporates an advanced monitoring and reporting engine that monitors the IT infrastructure and detects unauthorized access. It creates detailed reports about the server usage, the devices used, what applications are accessed and more. By scanning these reports, organizations can detect any malicious activity that might be occurring.

> *"Due to HIPAA and eHPI security requirements, Parallels RAS has been a solution we can offer our clients that both meets HIPAA and our management expectations as an MSP."*
> **Tracy Acord,** Sr. Network Engineer, Streamline IT Solutions

Parallels®

parallels.com/ras