Paperspace

Security Primer
& Architecture Overview

Business Whitepaper

Paperspace
www.paperspace.com

Paperspace Virtual Desktops: A foundation for a secured IT environment

Overview

Security and Privacy as the Core of Your Business

Paperspace is designed with security as the primary consideration. We know that security is the cornerstone of all business and we are committed to providing the world's most trusted virtual desktop environment. In today's environment knowing that your company's data is secure, permissions managed, and totally isolated from possible attackers is an essential requirement for the move to the cloud. Paperspace exceeds on all fronts and can become a primary pillar of your secure IT infrastructure.

Data Security

Technical foundations for a zero knowledge platform

Paperspace is built with the mindset that only you have access to your data, and we work tirelessly to engineer solutions that live up to this goal. This happens at the **application layer**, the **network layer**, and at the **physical datacenter** (for our hosted offerings).

All communications to and from your Paperspace VM are secured over a fully encrypted channel.

- Encrypted stream between client and remote server (SSL/TLS) independent of platform — web, desktop or mobile.

- Traffic between our database, web servers, API and internal networks is also encrypted (SSL/TLS)
- Database secured with 256-bit AES or higher
- We use 2048 bit public keys in our certificates, and support only high-strength symmetric ciphers.

Network Security

Ensuring the secure transport of data

When you put a Paperspace VM on your network, it is likely that Paperspace will be the most secure machine on that network.

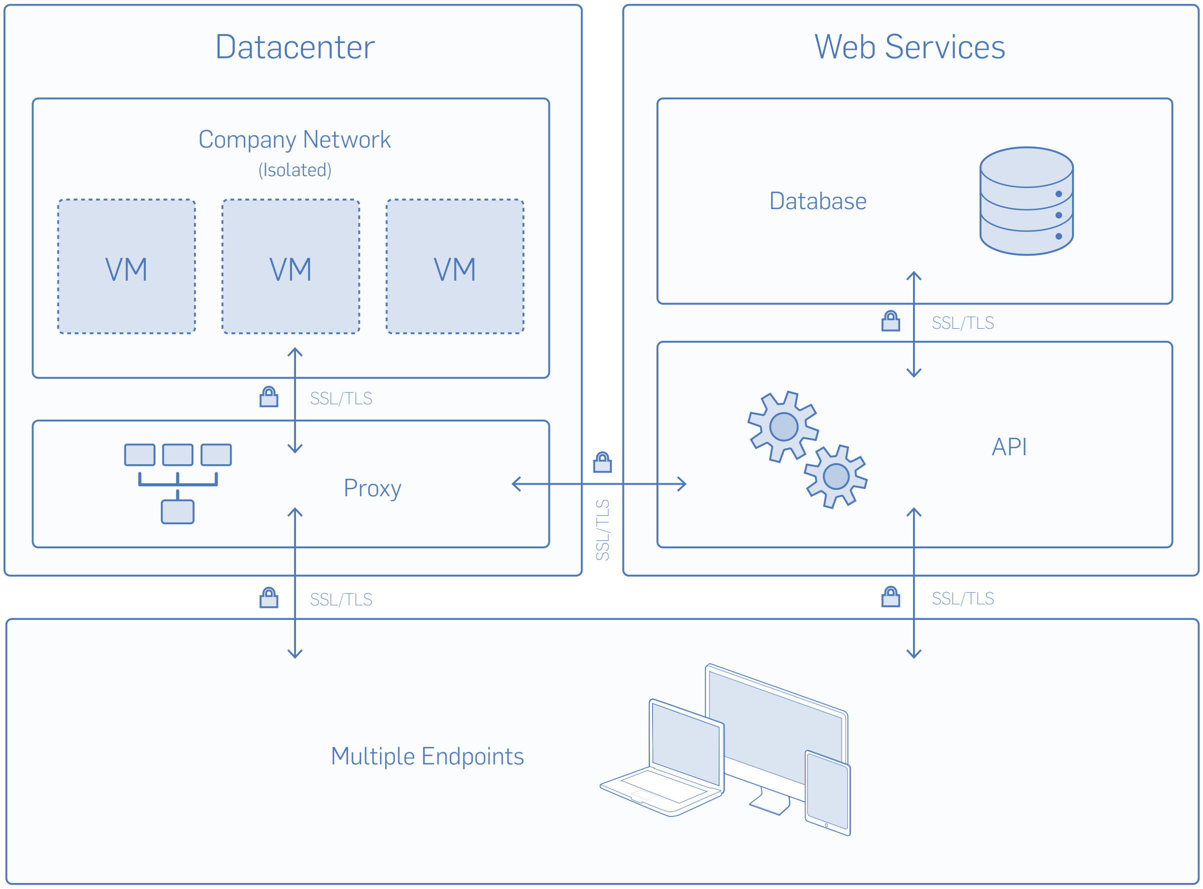
- 100% network isolation
- Configurable firewall (or run your own)
- Encrypted channel from VPN to VPN (IPSec/OpenVPN encrypted channel between Paperspace DC and your offices)
- 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces

Datacenter Standards and Compliance

Protecting and monitoring corporate servers

Our datacenters employ a variety of security mechanisms, including strict access policies plus secure vaults and cages.

- Paperspace datacenters are ISO and SSAE16 compliant (certified by independent auditors and third-party organizations).
- Our datacenters employ 24x7 on-site security including personnel, motion detection, a badge access system and closed-circuit video monitoring.
- Access to areas containing corporate servers is restricted to authorized personnel via elevated roles granted through the badge access system.
- Uninterruptible power and backup systems as well as fire/flood detection and prevention.



Users and Identity Management

Know Who, When, Where

Paperspace provides tools to centrally manage identity and collaborators with strong authentication and granular permissioning.

- A robust role-based permissioning system helps maintain tighter control (both machines and drives) over traditional on-premise systems.
- Active Directory integration for access control (optional)
- Advanced account management (sign out of all sessions remotely, alerting, etc)
- Login monitoring and access logs providing intelligence and visibility over all the content, users, devices and activity in your account.

Credit Card Security

Paperspace does not store credit card information

Credit card processing is handled by Stripe. Stripe complies with PCI standards and all traffic that interacts with their API is run over a secure channel (HTTPS).   Credit card information stored on their servers is encrypted using AES-256.

Mobility

Protecting against theft and loss of data

Paperspace's unique 'zero local storage' model is the most secure virtual desktop delivery system available. Since endpoints only render pixels streamed from a datacenter, information within the virtual environment cannot be extracted (from either machines or shared drives). Our zero local storage policy is enforced on all platforms (web, desktop, mobile) regardless of device.