Paperspace

Security Primer
& Architecture Overview

Business Whitepaper

Paperspace infrastructure & services: 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 infrastructure and services. In today's environment, knowing that your company's data is secure, permissions are managed, and your network is completely isolated from possible attackers, are essential requirements. 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 are secured over a fully encrypted channel.

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

20 Jay St. Suite 312
Brooklyn, NY 11201

- 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 access move workloads to Paperspace, we guarantee the following:

- Configurable firewall rules (or run your own) and whitelisting.
- Encrypted channel from VPN to VPN (IPSec encrypted channel between Paperspace and your other environments).
- For virtual machines, we offer 100% network isolation and 802.1q VLANs. This dedicated connection can be partitioned into multiple virtual interfaces.

Standards and Compliance

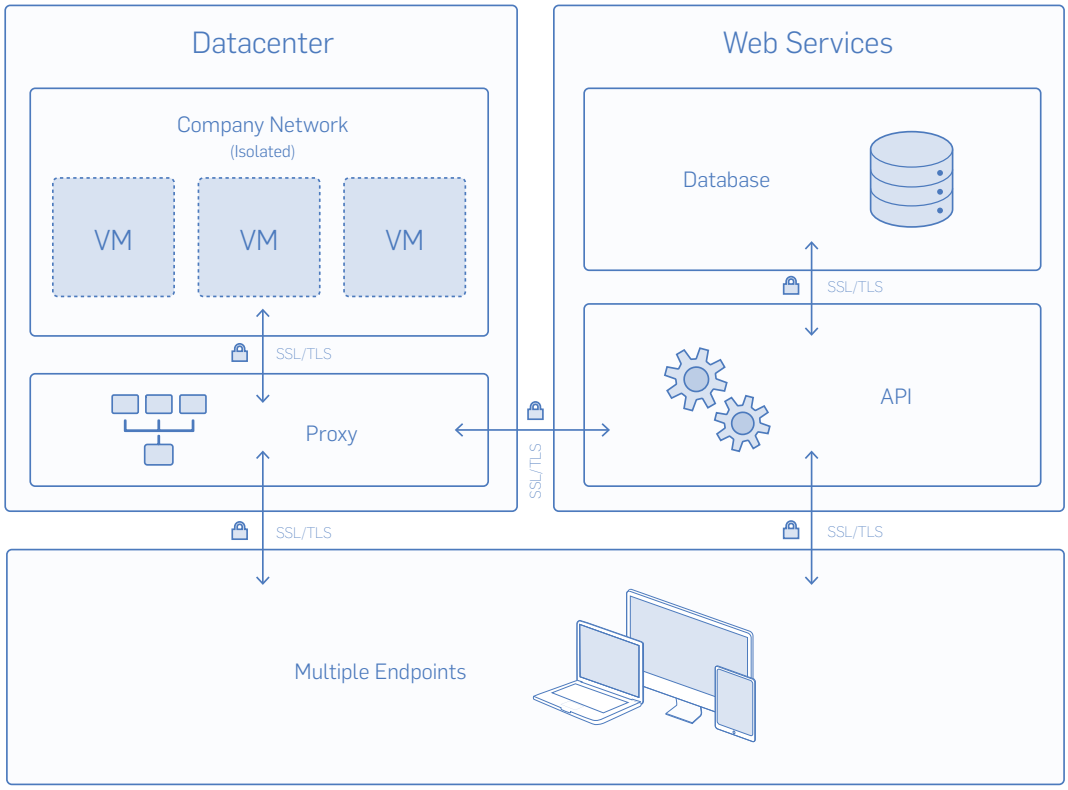
Protecting and monitoring our environment

Our systems employ a variety of security mechanisms, including strict access policies, intrusion detection, and more.

- As a Paperspace customer, you will benefit from a system architected to protect your information, identities, applications, and data. Paperspace has an established track record of successfully protecting customers across both our multi-cloud and on-premise environments.
- Our enterprise customers can run in their own cloud VPC or on-premise networks for maximum control.
- For our hosted offerings, our 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

20 Jay St. Suite 312
Brooklyn, NY 11201

video monitoring. Access to areas containing corporate servers is restricted to authorized personnel via elevated roles granted through the badge access system.



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.

20 Jay St. Suite 312
Brooklyn, NY 11201

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 which is the most secure delivery system available. Information within the virtual environment cannot be extracted (from either virtual machines or other services). Our zero local storage policy is enforced on all platforms (web, desktop, mobile) regardless of device.

20 Jay St. Suite 312
Brooklyn, NY 11201