PANTHEON SECURITY

PANTHEON®
Website Management Platform

Pantheon gives security-conscious organizations everything they need to keep their websites safe.

- ✓ Container-based infrastructure
- ✓ One-click core updates
- ✓ Denial of service protection
- ✓ Automated security monitoring
- ✓ Network intrusion protection
- ✓ HTTPS with custom certificate
- ✓ End-to-end encryption
- ✓ Resource isolation
- ✓ SAML/SSO/2FA
- ✓ Role-based site access
- ✓ Automated backup and retention
- ✓ Secure code and database access
- ✓ Secure integration to resources
- ✓ Secure datacenters
- ✓ PCI compliance

Pantheon is built on containers, making it easy to scale and deploy infrastructure-wide fixes. Embraced by companies like Google App Engine and Heroku, they allow lightweight partitioning of the OS into isolated spaces where applications can safely run.

Resource Isolation

Pantheon uses control groups, a kernel-level facility for resource isolation for memory, disk, cpu, and other server resources. This means that process and memory-level isolation are effective for all customer processes, from PHP to MySQL.

Automated Site Monitoring

Pantheon runs over a million checks a day to proactively monitor network, server, and application resources. Uptime data is always available at status.getpantheon.com.

One-Click Core Updates

Update Drupal and WordPress core with a single click. Pantheon's built-in dev, test, and live environments allow developers to push updates to production safely and quickly.

Network Intrusion Protection

Pantheon's intrusion prevention system (IPS) adds a layer of protection, using a x.509-based public key infrastructure to add authentication and encryption to the Rackspace network. IPS runs for any service with user-chosen passwords—dashboard, SFTP, git, drush—detecting failed logins and preventing unauthorized host access.

Denial of Service Protection

Pantheon works with Rackspace and CloudFlare to provide management of denial-of-service attacks, filtering ongoing attacks and isolating traffic streams through Riverbed load balancers for each site and environment.

SAML and Two-Factor Authentication

Pantheon supports SAML integration, enabling additional security features like two-factor authentication and single sign-on. Customers can also enforce settings like minimum password strengths or authentication audit logs.

Role-Based Access to Site Resources

Pantheon's Change Management feature allows site owners to manage organization-wide settings and selectively grant or deny developer access to deploy to production.

Anti-Malware

Pantheon prevents malware installation by running a Linux OS. We use only established vendor repositories for software, verify software package signatures, perform cryptographic validation of platform code, and maintain auditable change management. ClamAV antivirus protection ensures our system's integrity and to prevent malware from spreading through customer websites.

Find out more at pantheon.io/security

> **Pantheon runs their website infrastructure as if no single aspect of the web can be trusted. This approach helps ensure that all of their servers and services have the highest degree of isolation.**
>
> -Luke Probasco, Drupal General Manager, Townsend Security

No compromising on website security. We protect you from a hostile internet with secure infrastructure, carefully configured access to resources, and best practices around data safety and retention.

Pantheon Employee Administrative Access

Pantheon grants access according to least privilege. Employees can interact with servers via a secure API without actual server access—when they do need it, SSH-key based authentication is used and activity is recorded in a central log.

Releasing Patches and Updates

Pantheon continually deploys new container host instances with the latest supported kernel, OS and packages. Containers are migrated to the updated instances automatically and the older systems are retired. Core CMS application updates and security patches are tested internally before being deployed to our customer base through our one-click update workflow.

Vulnerabilities and Incident Response

Security issues identified by Pantheon are immediately communicated to affected parties. Details of any significant disruption are posted status.getpantheon.com and tweeted by @pantheonstatus. We always conduct a post-incident review of security events to improve the effectiveness of our response to future incidents.

Datacenter Security

Pantheon's primary datacenter is managed by Rackspace. Rackspace provides 24/7 direct support access on any hardware issue. Access to data centers is granted though both keycard and biometric scanning protocols and protected by round-the-clock surveillance monitoring. Every Rackspace data center employee undergoes thorough background security checks before hiring.

Redundancy

Many of Pantheon's core components are fully redundant and highly available with no single point of failure: the internal Pantheon API, the edge routing layer, DNS, and files directory storage. Where redundancy is not feasible, we maintain automated tools to facilitate recovery. Pantheon's internal services are designed to tolerate process and server-level failure. We maintain a minimal server footprint in multiple datacenters to facilitate restoration in the event of a datacenter-level failure. When possible, we use redundant providers for upstream services like DNS.

Customer Content Durability

Pantheon uses industry-standard practices for on-disk storage, including writing to multiple physical disks with hardware-level RAID. For further protection, customers can make automated backups on the platform. Backups have over 99.99% durability and availability, are stored in multiple datacenters, and are encrypted at-rest.

Backups

Backups can be automated or triggered manually. Each backup, containing all site-related customer data, is shipped to Amazon S3 as a compressed archive. Backups are encrypted during transfer and at-rest with 256-bit Advanced Encryption Standard ciphers, storing private keys and encrypted backup data on separate servers. Users have the ability to test restoration via the dashboard for any site for any manual or scheduled backup. They also have the ability to restore from a backup to a new site, on Pantheon or elsewhere.

Meet Your Industry's Highest Standards

Stay secure and compliant on Pantheon. We allow you to meet standards for the payment card industry, healthcare's FERPA, data security standards, and the safe harbor act.

PCI — Payment Card Industry (PCI) Data Security

FERPA — Family Educational Rights and Privacy Act (FERPA)

SOC 2 Type II and SOC 3 and ISO 27001
US-EU Safe Harbor