



INFRASTRUCTURE SECURITY AND COMPLIANCE

Sucuri Security owns and manages a custom built CDN Anycast Network that is primarily used for our CloudProxy (WAF) service. It consists of a half a dozen POPs (Points of Presence) throughout the US and Europe. We also utilize a custom designed cloud infrastructure that provides redundant services, custom CloudProxy configurations, and scalable options for customers with specific needs.

Sucuri's Management team maintains direct involvement with all operational tasks, incident management, change management, and compliance activities.

CLOUDPROXY INFRASTRUCTURE

Every Datacenter we operate from meets or exceeds all standards and compliance regulations:

- SSAE16 COMPLIANCE
- OHSAS 18001:2007
- PCIDSS PAYMENT CARD INDUSTRY STANDARD
- ISO CERTIFICATION
- ISO 9001:2008
- ISO 14001:2004
- ISO / IEC 27001:2005 AND 27001:2013
- ISO 50001:2011

NETWORK INFRASTRUCTURE

Sucuri's network consists of multiple transit providers at each location that is utilized for primary traffic routing, internal traffic routing, and redundancy.

Shared network with a primary and secondary termination for each connection to prevent a single point of failure.

OPERATIONS

- Daily device vulnerability scan performed internally
- Daily Vulnerability and Compliance scan performed by third parties
- In house Penetration Testing and third party testing
- Documentation, Practices, and Continuous Employee Education
- Firewall Change Management procedures
- Data classification and ownership
- Incident Management
- BCP (Business Continuity Plan) & DRP (Disaster Recovery Plan)
- Continuous Network and Log Monitoring and Review

MANAGEMENT AND HUMAN RESOURCES

- Mandatory security awareness training and review for each employee
- Strict least privilege access practices throughout teams
- Required Non-Disclosure & Confidentiality Agreements
- Background Checks and Skills Assessment
- Active Management in all aspects of the Security Community
- Stay current in the ever changing cyber world