Hoop.la Security

Rev. 1 / May 15, 2017

A. General Philosophy

Our philosophy at Social Strata is that you, the customer, own your data.

It's our job to protect the integrity of that data and ensure that it's only accessible to those to whom you've granted access. Social Strata complies with the EU-U.S. Privacy Shield Framework, and our data centers are SOC2 and/or ISO 27001:2013 certified.

We have been providing online community services for over 18 years, supporting marquee customers like Rodale, Dun & Bradstreet, Time Warner Cable, and Monster. We are currently supporting hundreds of millions of page views across multiple environments and thousands of customers. Social Strata's service has been consistently reliable and can accommodate high levels of traffic, including the types of spikes that can occur during unique media events or celebrity chats.

B. Privacy and Compliance

Social Strata takes privacy of customer data very seriously, which is why we are a participant in the EU's Privacy Shield program. We also have a Privacy Policy that clearly states what data we collect and how we may use your data.

Privacy Shield

https://www.privacyshield.gov/participant?id=a2zt000000001NuAAI&status=Active

Social Strata Privacy Policy

https://assets.socialstrata.com/docs/privacy_policy.php

EU General Data Protection Regulation (EU GDPR)

We plan to offer compliance with the new EU GDPR before it becomes effective in May 2018. Compliance, however, will likely require that your account include the Premium Security add-on, and it may also require additional optional services (TBD), which may incur additional fees.

C. Network and Platform Security Details

Social Strata's network infrastructure is built on the latest networking technology available. The multi-homed network uses Cisco routers at its core. All servers are

connected on a gigabit backbone via Cisco switches.

Hoop.la's environments are protected from malicious users and attacks by state-of-the-art firewalls. All internal network access is restricted to Social Strata employees using the latest in SSH encryption technology.

Encryption

Hoop.la's Enterprise plan includes TLS/SSL for encryption of data transmitted across the Internet. The customer will need to procure the security certificate for the community domain name, and Social Strata will install and manage the certificate as part of the service offering.

Hoop.la's data is stored in multiple systems including MySQL, MongoDB, and distributed file systems for media and attachments. User passwords are encrypted with strong, oneway cryptography utilizing Blowfish hashing with a randomized salt to ensure the security of user sign-in credentials.

Virtualization

We are able to deploy new servers quickly, responding to new requirements or community growth through our virtualized environment. New equipment is at the ready should the need arise.

Software

Social Strata's software is proprietary. The source code is not available to the public or to customers.

D. Monitoring Tools

We have a geographically diverse monitoring system deployed to ensure that our systems team is notified immediately in the event of any reachability or performance issues. We are constantly evaluating new ways to expand the overall capacity and throughput of our systems at various layers, including equipment, network, and software.

Hoop.la's architecture has built-in tools to monitor performance and overall health of the software system. Our dev/ops team uses these tools to identify and correct any hotspots that may be causing user impact.

Our monitoring systems record uptime statistics throughout the month, and those statistics are used by our billing department each month to ensure that we meet our required Service Level Agreement uptime guarantees.

E. Uptime

Hoop.la Enterprise customers are guaranteed 100% uptime SLA. We have an excellent uptime track record across the entire platform.

F. Backups and Disaster Recovery

Hoop.la includes redundant databases with multi-layered backup protection. Backup options include daily data backup, point-in-time backups, and redundant storage arrays. Includes online and offline backups. Weekly off-site backups are performed.

All off-site backups are encrypted before being transferred across the wire.

Backups are multi-tiered: local database/file server backups, local replicated backups (2 copies), and one off-site Disaster Recovery backup.

G. Operating System Patching

Regular OS patching is one of the most effective ways to mitigate against the risk of compromise as many exploits specifically target OS deficiencies. This includes all applicable vendor supplied security and critical OS patches and updates.

H. Premium Security

Hoop.la offers an optional “Premium Security” add-on that provides a very high level of security. We recommend this for all customers, but especially any customers storing sensitive data or that consider their online communities mission critical. Here are some of the benefits that are included with Premium Security:

Total Data Encryption

With Total Data Encryption, every bit of data is encrypted both in transit throughout the internet and Hoop.la environment as well as at-rest on the file system. This includes data stored in databases as well as files that have been uploaded as clips, attachments, etc.

Active Cyber Defense

Hoop.la's Premium Security environment is protected by numerous proactive Cyber Defense mechanisms such as IP Reputation Management, DoS/DDoS protection/mitigation, Web Application Firewalls, and Intrusion Detection. Additionally, vulnerability scans are performed regularly to detect and identify any potential risks or threats to the system. Finally, server logs are managed, monitored, and audited regularly to ensure systems are secure and functioning without incident.

IP Reputation Management (IPRM)

IPRM prevents network access from known bad IP addresses and networks, eliminating a large majority of typical threats to customer environments. The IPRM database is updated multiple times per day.

Denial-of-Service Mitigation (DoS/DDoS)

Powerful redundant, multi-stage systems provide early detection and mitigation for combating denial and distributed denial of service attacks. Thresholds are set that automatically trigger blackholing of DoS traffic in excess of 1Gbps and alert NetOps to the issue. NetOps then facilitates mitigation through DDoS equipment.

Web Application Firewall (WAF)

The WAF protects against many types of malicious application layer attacks over TCP ports 80 (HTTP) and 443 (HTTPS). Mitigated attacks include SQL injection, cross-site scripting (XSS) and cross-site request forgery (CSRF). Both detective and preventive rules are included in the ever evolving rule set according to the OWASP Top Ten list.

Network Intrusion Detection Services (IDS)

Network traffic that has passed through the network is inspected for malicious and anomalous behavior. Traffic between the Internet and customer servers (north-south monitoring) and traffic between servers within the environment (east-west monitoring) is monitored and inspected. Alerts generated by IDS are investigated by our vendor's SecOps team in conjunction with information from our other security services to determine which are valid and may be considered an Indicator of Compromise (IOC). IDS data is used in digital hunting efforts to provide additional context for potential compromises.

Anti-Malware

Malware infections continue to represent a significant source of compromise and having protection against this threat vector is key to a strong security program. Premium Security provides a fully managed anti-malware service that is based on Trend Micro's Deep Security product. All alerts generated are investigated by our vendor's SecOps team to determine the nature of the malware. Often this involves SecOps using information from our other security services to provide more detail on the nature, extent and source of the malware.

Log Monitoring and Management Service

Centralized log aggregation for operating system (OS) logs. Agents are installed on all customer servers that collect and forward system, audit and authentication logs to the centralized system. Basic log analysis is performed every 24 hours. If anomalies are detected during this process we are notified for further investigation.

Isolated Firewalls & Network

With Premium Security, all customer environments are completely isolated from each other on their own private networks. The Hoop.la server environment is protected behind Enterprise-class firewalls that are deployed in a closed state by default; only traffic necessary to provide the service (such as HTTP/S traffic) is allowed through. Database servers are also isolated from front-end servers by firewalls.

File Integrity Monitoring (FIM)

File integrity monitoring lets us know whenever a critical OS file has been changed and is typically reviewed when other anomalous activity is detected to confirm a compromise by determining if changes were made to critical OS files. It is facilitated via the same Trend Micro Deep Security agent as is used for the anti-malware service.

Secure Administrative Access

Customer environments are only accessible to authorized Social Strata employees using SSH encryption over an SSL VPN with mandatory two-factor authentication (2FA).

Disaster Recovery

Continuous data replication, powered by Zerto Virtual Replication (ZVR), delivers an enterprise-class, hypervisor-based solution for proven business continuity. It's the only secure disaster recovery solution for mission-critical applications. Premium Security includes ZVR to increase competitive advantage, ROI, and make failover and disaster recovery testing easy. Data is replicated in real-time across geographical regions to provide a rock solid recovery plan in the event of a disaster.

HIPAA Compliance

Hoop.la's Premium Security add-on allows customers to sign a HIPAA Business Associates Agreement so that further data protections are in place for electronic Protected Health Information (ePHI) that might be shared within your community. HIPAA compliance is only available to customers based in the United States with hosting also in the United States.

I. Data Center Security Details

The specifics of the data center(s) we use for your account will vary, depending on the service level and the data hosting location requirements for your account.

For "Premium Security" customers, however, here are the current specifications:

Facility

- 75,000 sq. ft. facility size
- 35,000 sq. ft. raised floor

Physical Security

- ISO/IEC 27001:2013 certification
- On-site personnel 24/7
- Electronic and physical security
- Biometric and card access security system
- CCTV video surveillance system with DVR recording
- Man-trap entry and badge-only access
- SSAE16 SOC 1 Certified

Power Management

- 2N Electrical infrastructure
- (6) MW ONCOR single electrical feed
- (3) 3750 kVA GE redundant transformers in ring configuration
- (4) HOLT/CAT 2,000 kW diesel generators
- 72+ hours fuel supply onsite
- System is pre-engineered to add (4) more generators as growth requires
- (8) Emerson-Liebert 750kvA modules in 2N configuration
- (34) Emerson/Liebert Power Distribution Units (PDU)

Connectivity

- Meshed, multi-vendor Internet transit connectivity
- Multiple ILEC and CLEC access providers
- Diverse fiber entry and intra-building fiber paths
- Redundant internal network distribution platforms Media supported for circuit hand-offs (CAT, Coax single-mode and multi-mode fiber)
- (13) Telco carriers

Environmental Controls

- N+1 Trane centrifugal chillers
- (33) 30-ton chilled water CRAC units on the raised floor
- (13) 30-ton split system-DX (direct exchange) CRAC units
- (12) Liebert roof top units VESDA (Very Early Smoke Detection Apparatus)
- FM-200 fire suppression system
- Dry-pipe pre-action sprinkler system
- Electrical monitoring
- Under the floor water detection system
- Control and monitor 32,000 points in the facility

Note that some details may change over time (for instance, the specific facility size), but we will maintain this document, as appropriate to reflect minimum values over time.

If you are not utilizing Premium Security for your account, please request the specifics about your data center(s) from an account representative.