SECURITY & PRIVACY DOCUMENTATION

(last updated March 26, 2018)

Scalyr's Commitment to Security & Privacy

Scalyr is committed to achieving and preserving the trust of our customers, by providing a comprehensive security and privacy program that carefully considers data protection matters across our products and services, including data submitted by customers to our online service ("Customer Data").

Covered Services

This documentation describes the security-related and privacy-related audits and certification received for, and the administrative, technical, and physical controls applicable to, the Scalyr server monitoring and log analysis service ("Service"). This documentation does not apply to free trial services made available by Scalyr.

Architecture, Data Segregation, and Data Processing

The Service is operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The Scalyr architecture provides an effective logical data separation for different customers via customer-specific "Organization IDs" and allows the use of customer and user role-based access privileges.

Additional data segregation is ensured by providing separate environments for different functions, such as for testing and production.

Scalyr has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Scalyr and its sub-processors.

Security Controls

The Service includes a variety of configurable security controls that allow Scalyr customers to tailor the security of the Service for their own use. The Scalyr Agent can be configured to redact sensitive information before it leaves the customer's server to protect customer data. The Scalyr Agent has no facility for receiving external instructions to collect data outside of the customer's control. Scalyr limits its own capability to access and edit customer accounts for maintenance purposes only.

1. Security Assessments and Compliance.

Scalyr's ISMP includes adherence to and regular testing of the key controls, systems and procedures of its ISMP to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing includes:

- Internal risk assessments;
- SOC2 (or successor standard) audits annually performed by accredited third-party auditors ("Audit Report").

2. Security Audit Report.

Scalyr provides its customers, upon non-disclosure ageement, with a copy of Scalyr's then-current Audit Report.

3. Assigned Security Responsibility.

Scalyr assigns responsibility for the development, implementation, and maintenance of its Information Security Management Program, including:

- Designating a Chief Information Security Officer and Chief Privacy Officer with overall responsibility; and
- Defining security and privacy roles and responsibilities for individuals with security and privacy responsibilities.

4. Relationship with Sub-processors.

Scalyr conducts reasonable due diligence and security assessments of sub- processors engaged by Scalyr in the storing and/or processing of Customer Data ("Sub-processors"), and enters into agreements with Sub-processors that contain provisions similar or more stringent than those provided for in this security and privacy documentation.

5. Background Check.

Scalyr performs background checks on any employees who are to perform material aspects of the Service or have access to Customer Data.

6. Security Policy, Confidentiality.

Scalyr requires all personnel to acknowledge in writing, at the time of hire, that they will comply with the Information Security Policy (ISP) and protect all Customer Data at all times.

7. Security Awareness and Training.

Scalyr has mandatory security awareness and training programs for all Scalyr personnel that address their implementation of and compliance with the ISP.

8. Disciplinary Policy and Process.

Scalyr maintains a disciplinary policy and process in the event Scalyr personnel violate the ISP.

9. Access Controls.

Scalyr has in place policies, procedures, and logical controls that are designed:

- To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
- To prevent personnel and others who should not have access from obtaining access; and
- To remove access in a timely basis in the event of a change in job responsibilities or job status. Scalyr institutes:
    - Controls to ensure that only those Scalyr personnel with an actual need-to-know will have access to any Customer Data;
    - Controls to ensure that all Scalyr personnel who are granted access to any Customer Data are based on least-privilege principles;
    - Periodic (no less than semi-annually) access reviews to ensure that only those Scalyr personnel with access to Customer Data still require it.

10. Physical and Environmental Security.

Scalyr leverages Infrastructure-as-a-Service (IaaS) provider's controls that provide reasonable assurance that access to physical servers at the production data center is limited to properly-authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes. These controls include:

- Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;
- Camera surveillance systems at critical internal and external entry points to the data center;
- Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and
- Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

11. Data Encryption.

Encryption of Transmitted Data: Scalyr uses Internet-industry-standard secure encryption methods designed to encrypt communications between its server(s) and the customer browser(s), and between its servers and customer's server(s).

12. Disaster Recovery.

Scalyr maintains policies and procedures for responding to an emergency or a force majeure event that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

- Data Restoration: A procedure for restoring data from backup and restore services to meet the Recovery Point Objective described below;
- Disaster Recovery: A formal disaster recovery plan for the production environment designed to minimize disruption to the Service, which includes requirements for the disaster plan to be tested on a regular basis, currently four times a year;
- RPO / RTO: Recovery Point Objective is no more than 4 hours and 15 minutes and Recovery Time Objective is no more than 4 hours and 30 minutes.

13. Malware Control.

Scalyr employs antivirus software on company endpoints that support production systems.

14. Data Integrity and Management.

Scalyr maintains policies that ensure the following:

- Segregation of Data: The Service includes logical controls, including encryption, to segregate each customer's Customer Data from that of other customers; and
- Data Replication: Customer data is continuously replicated across data centers using an automated replication system. The Service makes a continuously updated tertiary copy that can be used for recovery if both primary instances are lost.

15. Vulnerability Management.

Scalyr maintains security measures to monitor the network and production systems, including error logs on servers, disks and security events for any potential problems. Such measures include:

- Infrastructure Scans: Scalyr performs monthly vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis;
- Application Scans: Scalyr performs weekly application vulnerability scans. Vulnerabilities are remediated on a risk basis;
- External Network Penetration Tests: Scalyr engages third parties to perform network penetration testing on an annual basis.

16. Change and Configuration Management.

Scalyr maintains policies and procedures for managing changes to production systems, applications, and databases. Such policies and procedures include:

- A process for documenting, testing and approving the promotion of changes into production; and
- A security patching process that requires patching systems in a timely manner based on a risk analysis.

17. Secure Deletion.

Scalyr maintains policies and procedures regarding the deletion of Customer Data in compliance with applicable data protection laws, taking into account available technology so that Customer Data cannot be practicably read or reconstructed.

18. Incident Management.

Scalyr has in place a security incident response plan that includes procedures to be followed in the event of any unauthorized disclosure of Customer Data by Scalyr or its agents of which Scalyr becomes aware to the extent permitted by law (such unauthorized disclosure defined herein as a "Security Breach"). The procedures in Scalyr's security incident response plan include:

- Roles and responsibilities: formation of an internal incident response team with a response leader;
- Investigation: assessing the risk the incident poses and determining who may be affected;
- Communication: internal reporting as well as a notification process in the event of a Security Breach;
- Recordkeeping: keeping a record of what was done and by whom to help in subsequent analyses; and
- Audit: conducting and documenting a root cause analysis and remediation plan.

Scalyr publishes system status information on the Scalyr Status website, at http://status.scalyr.com/. Scalyr typically notifies customers of significant system incidents by email to the listed admin contact,

and for availability incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Scalyr's response.

19. Security Breach Management.

- Notification: In the event of a Security Breach, Scalyr notifies impacted customers of such Security Breach. Scalyr cooperates with an impacted customer's reasonable request for information regarding such Security Breach, and Scalyr provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.
- Remediation: In the event of a Security Breach, Scalyr, at its own expense, (i) investigates the actual or suspected Security Breach, (ii) provides any affected customer with a remediation plan, to address the Security Breach and to mitigate the incident and reasonably prevent any further incidents, (iii) remediates the effects of the Security Breach in accordance with such remediation plan, and (iv) reasonably cooperates with any affected customer and any law enforcement or regulatory official investigating such Security Breach.
- Unsuccessful Security Incidents: An unsuccessful Security Incident will not be subject to this Section 19. An unsuccessful Security Incident is one that results in no unauthorised access to Customer Data or to any of Scalyr's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents; and (ii) Scalyr's obligation to report or respond to a Security Incident under this Section 19 is not and will not be construed as an acknowledgement by Scalyr of any fault or liability of Scalyr with respect to the Security Incident.

20. Logs.

Scalyr provides procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports. Scalyr (i) makes a continuously updated tertiary copy of logs that can be used for recovery if both primary instances are lost (ii) implements commercially reasonable measures to protect such logs from unauthorized modification or erasure, and (iii) retains such logs in compliance with Scalyr's data retention policy.