SYNCONSET

SECURITY + COMPLIANCE WHITEPAPER

3 Introduction
4 The SyncOnSet Product Suite
5 Empowering Studios and Users to Take Control of Security
5 Access Control
5 User Management
6 User Authentication
6 Web Access Revocation
7 Mobile User Authentication
7 Mobile Access Revocation
8 Technology Designed Around Security
8 Network Security
8 Intrusion Detection & DDOS Mitigation
9 SSL
9 Data Storage Security and Redundancy
9 Data Storage
9 Data Center Redundancy
10 Storage Backups
10 Data Removal
10 Data Transmission
11 Physical Security
11 Data Centers
11 Office
12 Organizational Security
12 Employee Background Check
12 Security Training
13 Risk Management
13 Vulnerability Management
13 Monitoring
13 Incident Management
14 Internal Policies
14 Administrative Data Access
14 InfoSec Highlights
14 Audit and Review
14 Internal Review
15 External Review
16 Business Continuity and Recovery
16 Availability
16 Incident Response
16 Conclusion
17 About SyncOnSet

Introduction

This whitepaper outlines SyncOnSet Technologies' approach to security and compliance for all of its cloud-based solutions for TV and film productions and studios.

As a cloud-based system, SyncOnSet operates very differently from previous on-premise and analog solutions. Rather than residing on one crew member's personal device, content is now managed on secure servers, accessible from any authorized user's device. Prior to SyncOnSet, production data was frequently lost, stolen, or destroyed. Today, however, productions have solutions that not only protect data from unauthorized access, but eliminate the risk of data loss.

Security drives SyncOnSet's organizational structure, training priorities, and hiring processes. Security is the cornerstone for how SyncOnSet handles customer data, account controls, compliance audits, and certifications. SyncOnSet fully understands the security implications of the cloud model. Our cloud services are designed to deliver stronger security than existing on-premise solutions.

Each studio must assess whether the security controls and compliance of any cloud solution meet their individual requirements, and therefore must understand how SyncOnSet protects and processes production data under the highest standards of security.

The SyncOnSet Product Suite

For Production

SyncOnSet for Production is an award-winning web and mobile application that helps creative departments on film and TV productions manage their workflow and communicate with their team throughout production. Departments can use SyncOnSet throughout production from prep (script breakdown and budgeting), to shoot (continuity notes and photos), through wrap (wrap inventory and reports).

Asset Hub

SyncOnSet Asset Hub is the first physical asset system designed specifically for studio workflows - connecting crew, accounting, and studio divisions. With the Asset Hub, studios can track disposition of all physical assets across series, franchises, and warehouses. Asset Hub's intelligent recommendation engine reconciles assets with financial transaction imports from standard accounting systems.

Admin Panel

SyncOnSet's Admin Panel provides studios greater control and access to SyncOnSet for Production. Studio admins can view all active and inactive production accounts, monitor production usage and stats (number of users, last activity date, photos, and inventory), remove/change Production Owners, and grant access into any wrapped productions within the Studio Admin Panel.

Empowering Studios & Users to Take Control of Security

SyncOnSet's main priority when it comes to security is maintaining a delicate balance between securing content, without getting in the way of the creative process on set. Studios have looked to SyncOnSet as the creative friendly solution to production security. We keep the crew in mind in all security discussions to maximize the ease of use for crew both on set and in the production office.

As the industry adapts to the chaning technological landscape, there has been a major shift in thinking among major studios and productions alike to a growing awareness of the importance of security to both physical and digital production. This shift, coupled with the rise of new technologies on set, has allowed the studios more control over the tools used by the crews. When a studio and SyncOnSet come to together to solve existing security flaws, a filmmaker's creative process is virtually unaffected and the world of filmmaking is better and more secure.

Access Control

User Management

SyncOnSet is the most advanced system for controlling access to production data. The account administrator can grant and remove access to the appropriate users as needed.
Whether SyncOnSet is accessed via a web browser or our mobile app, the permissions are thoroughly enforced. Each department has its own access permissions, preventing unauthorized members of one department from viewing production data created by another department

Within departments sensitive information has its own access controls, limiting access to only the proper members. Finally, both department heads and account administrators control who can edit data.

In addition, SyncOnSet supports photo watermarking to prevent users from distributing confidential production photos and/or to identify the source of photos in case of a breach.

User Authentication

SyncOnSet employs strict user authentication to make sure only users with the proper credentials can utilize its access points. SyncOnSet monitors and logs all access attempts, allowing our security team to investigate any suspicious activity.

We take additional measures to prevent any user from being vulnerable to external attacks, even if individual users do not take the proper precautions. SyncOnSet requires a re-authenticaten after periods of inactivity. Additionally, we prevent cross-site request forgery and cross-site scripting. That is, if a third party tries to access SyncOnSet through a user's computer, SyncOnSet recognizes the unauthorized request and blocks it.

Passwords have strict requirements and we disallow frequently used weak passwords that otherwise meet length requirements. In order to protect login credentials user passwords are encrypted using a one-way hash. Even when two users have the same password their encrypted passwords appear distinct, making it impossible to decipher the original password.

In addition to passwords, SyncOnSet supports mobile phone-based two factor authentication. Two factor authentication requires a user to enter an additional code made available only on their mobile phone before being able to log in.

Web Access Revocation

If a user loses a device connected to SyncOnSet or for any other reason believes their account to be compromised, we can instantly and remotely revoke access. Because SyncOnSet is a web application and not downloaded to the user's hard drive, when access is revoked unauthorized parties will not be able to access your data, immediately.

Mobile User Authentication

Mobile users can access their SyncOnSet accounts through mobile browsers or through phone and tablet apps on both iOS and Android. All data passed between the server and the mobile application is encrypted using SSL.

The mobile application performs user authentication via the OAuth 2.0 protocol. OAuth 2.0 employs three-legged authentication, which uses a secret token replacing a password. This token has a short lifetime and when it expires a refresh token is used to authorize a new secret token. Other services that support OAuth2 include Box, Facebook, Foursquare, GitHub, Google, Salesforce and Windows Live.

Mobile Access Revocation

As with the web application, if a mobile device is lost or stolen, SyncOnSet administrators can revoke access preventing the user from logging in or connecting to the server.

Technology Designed Around Security

Network Security

Intrusion Detection & DDOS Mitigation

We maintain system, network, and application log reporting and analysis as well as baseline network standards. This allows us to perform continuous internal monitoring and to employ network intrusion detection systems.

SyncOnSet undergoes regular third party penetration testing and remote vulnerability scanning to ensure that we have implemented the strongest measures to secure our network. We use a full scale monitoring system to record and notify our development and security teams of any irregular application activity or exceptions.

We use a complete firewall solution which is configured to default deny mode. Database servers are accessible only by the application servers and files from the file servers must pass a permission check on the application server before being displayed.

SSL

SyncOnSet uses Symantec Secure Socket Layer (SSL) Certificates powered by Verisign. We use a full 256-bit AES encryption to encode all data between SyncOnSet's servers and our users. In addition, Symantec performs daily website malware scanning to protect our users.

These SSL certificates secure more than one million web servers worldwide. Symantec has a rigorous authentication process and is audited annually by KPMG.

For more information on Symantec SSL certificates please visit: http://www.symantec.com/verisign/ssl-certificates

Data Storage Security and Redundancy

Data Storage

SyncOnSet operates its own proprietary data store utilizing a variety of Amazon Web Services including EC2, RDS, EBS and S3. This system was developed to provide the highest class of scalability and security. This data store is designed strategically to ensure that data from one production is not cross-contaminated or de-duped with others.

Data Center Redundancy

In addition to taking the strongest possible precautions to ensure a secure environment, we protect against hardware failure by utilizing multiple physically separate data centers in parallel.

Through load balancing and DNS routing SyncOnSet takes advantage of using multiple data centers to be highly available.

Storage Backups

SyncOnSet's databases are backed up in real time, providing a complete change log of all actions performed. Real-time change logs are kept for one week, after which hourly backups extend for another week. Daily backups extend for a further ninety days. Like our application servers, SyncOnSet maintains synchronous copies of our database in multiple data centers. If for any reason there is an outage on the master database, SyncOnSet automatically switches over to one of the backup instances.

Data Removal

SyncOnSet protects your data not only throughout the life of your production, but also long after your production has finished. You will continue to have read-only, archive permission to access your production for as long as the production administrator decides. If at any time the account administrator requests in writing or via email and confirmed via telephone, that their production be deleted, SyncOnSet will remove all production data from our servers within 7 days. This includes all original data as well as all replicated backup copies on local storage and secondary data centers.

Data Transmission

SyncOnSet uses 256-bit AES encryption to encode all data during transmission from both the web application and the mobile application. 256- bit AES encryption is the data standard used by the most secure institutions in the world.

SyncOnSet ensures that unsecure third party consumer services are not required and offers a secure replacement for email. With SyncOnSet's "Production Dashboard", read-only access can be strictly controlled and your data never needs to leave the system.

Physical Security

Data Centers

SyncOnSet utilizes data centers that follow the most stringent security standards and control frameworks. AWS is compliant with various certifications and third party audits, including: ISO 270001 certification of the Information Security Management System (ISMS) covering infrastructure, data centers and services; SAS70 Type II, which specifies detailed controls and independent auditor opinion about these controls.

AWS only provides data center access and information to employees and contractors with legitimate business need for privileges and utilizes state of the art fire detection and suppression, power, and climate and temperature control.

For more information on physical security please visit:

https://aws.amazon.com/security/

Office

SyncOnSet does not store any production data locally. Our offices are private with multiple levels of security. All visitors must have an official purpose and are escorted by an authorized employee. Stringent administrative access control is in place, and we maintain policies for corporate facility access, removable media, corporate and production passwords, access privileges, security training, system configuration, and change management.

Organizational Security

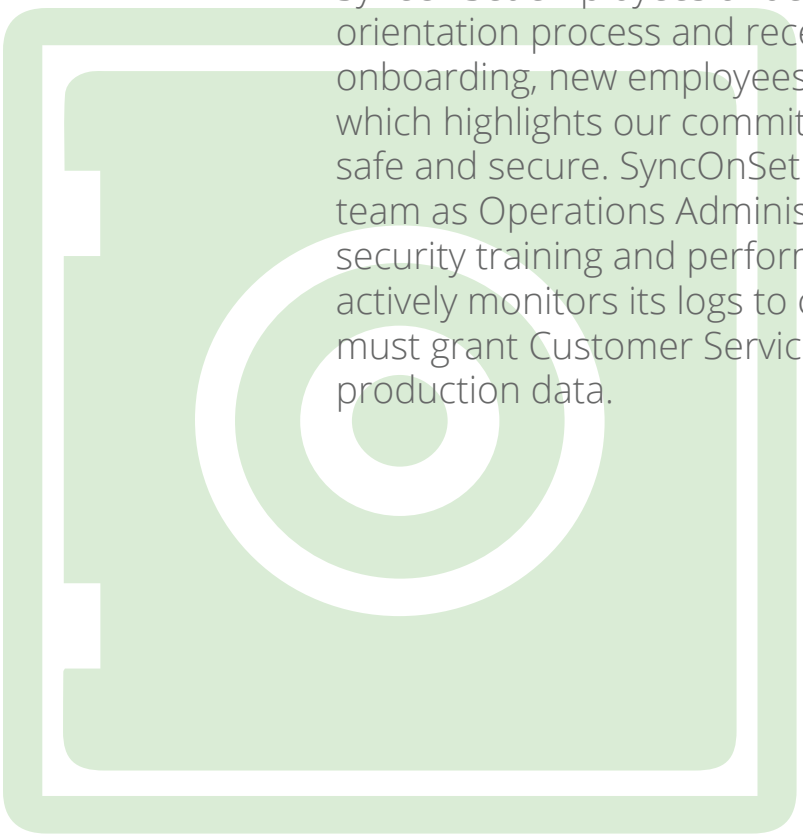
Human Resources

Employee Background Checks

SyncOnSet has established formal policies to delineate levels of access. All SyncOnSet employees undergo third party background checks as permitted by law commensurate with the employee's position and level of access.

Security Training

SyncOnSet employees undergo security training as part of the orientation process and receive ongoing security training. During onboarding, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. SyncOnSet designates key members of the team as Operations Administrators, who undergo additional security training and perform system maintenance. SyncOnSet actively monitors its logs to confirm administrator activities. Users must grant Customer Service representatives explicit access to production data.



Risk Management

Vulnerability Management

SyncOnSet works with third party assessment teams to determine adequate remediation to any internally detected vulnerability. In addition, along with our partners we monitor applicable vendor flaws and relevant new patches.

Monitoring

SyncOnSet utilizes a variety of tools to monitor and provide significant protection against traditional network security issues. These include Man in the Middle Attacks, IP Spoofing, Port Scanning, Packet Sniffing and Distributed Denial of Service Attacks. In addition, general uptime monitoring is performed each minute.

Incident Management

SyncOnSet has a specified incident management team that utilizes industry-standard diagnostic tools to resolve business-impacting events. Leadership at the highest level is involved and leads the incident management team. Incident management plans are reviewed by the senior executive team periodically.

Formal Incident Management policies are available upon request of appropriate parties.

Internal Policies

Administrative Data Access

SyncOnSet employees can never access productions unless invited in by an authorized member of the production company. Only a small group of SyncOnSet employees have access to customer data stored in our database, primarily used for communication with customers. Access rights are based on job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities

InfoSec Highlights

SyncOnSet periodically reviews information security policies. New employees are trained in these policies and existing employees undergo periodic reviews. InfoSec policies include data sharing and access, appointed section leaders, best practices for securing data, data transmission guidelines and notification procedures.

Audit and Review

Internal Review

SyncOnSet employs agile development with stringent code review, automated and manual quality assurance as well as strict change management processes. In addition, our developers receive periodic security review training and regular roundtable discussions.

External Review

SyncOnSet engages in quarterly external security assessments. These assessments include two stages: automated and manual penetration testing and source code analysis and review. The penetration testing begins with network, operating system, and web server level scans to search for known vulnerabilities and common incorrect configurations.

Engineers then perform an application discovery process to gather information about the application and search for information disclosure vulnerabilities. The bulk of the testing is conducted manually, consisting of input validation tests, impersonation (authentication and authorization) tests and session state management tests. The purpose of this security assessment is to illuminate security risks by leveraging weaknesses within the environment that lead to the obtainment of unauthorized access and/or the retrieval of sensitive information.

Source code analysis involves directly analyzing source code in an attempt to expose vulnerabilities. This allows for guided penetration testing based on back-end knowledge.

SyncOnSet also frequently works with partner studios to conduct ad hoc security and penetration tests.

Business Continuity and Recovery

Availability

SyncOnSet utilizes multiple data centers in multiple regions in a resilient architecture. SyncOnSet designed its systems to be fault tolerant in order to minimize the impact of a disaster and achieve uptime goals even in local service disruptions.

Incident Response

SyncOnSet has a specified incident response team to confirm and manage the response to any incident. In addition, we work with individual studio contacts to communicate incidents and response plans.

Conclusion

We believe that SyncOnSet offers a level of security and protection that previous methodologies just cannot match. Because protecting production data while making film and television more efficient is part of our core business, we are constantly adding tools that eliminate the security flaws of the past.

Because security is of the utmost importance to our clients, we constantly make extensive investments in new security measures. From third party penetration tests to enhanced security features for our studio partners, we are committed to delivering world-class software that meets and exceeds today's security standards.

For these reasons and more, thousands of productions, spanning six continents trust SyncOnSet with some of their most valuable data. SyncOnSet will continue to invest in our software in order to allow crews, studios, and other partners more efficient and secure productivity tools each and every day.

About SyncOnSet

SyncOnSet Technologies is an Emmy-Award winning technology company that offers modern software solutions to TV and film productions and studios.

For productions and crews, SyncOnSet's web and mobile app help creative departments optimize workflows and secure communication throughout the project. Departments use SyncOnSet's production apps throughout their entire production from prep (script breakdown and budgeting) to shoot (continuity notes and photos), through wrap (wrap inventory and reports).

For studios, SyncOnSet designed the first physical asset system specifically for studio workflows, Asset Hub. With Asset Hub, studios track the dispositions of all physical assets across series, franchises, and warehouses. In addition, SyncOnSet offers enterprise solutions for increased oversight and control over production data and content.

SyncOnSet is trusted by thousands of TV series and films around the world. The Company is based in Los Angeles, CA and Boston, MA.

WINNER OF 2016
ENGINEERING EMMY AWARD

SyncOnSet.com
1.800.470.7962
contact@synconset.com