



Sarbanes-Oxley Compliance for Cloud Applications

What Is Sarbanes-Oxley?

Sarbanes-Oxley Act (SOX) aims to protect investors and the general public from accounting errors and fraudulent practices. For this purpose, corporations are required to implement processes (internal controls) to guarantee accuracy and reliability of their corporate financial data. Among the provisions, SOX mandated personal accountability to the senior leadership team for accurate and thorough financial reporting.

Sarbanes-Oxley (SOX) In The Cloud

With the growth of companies storing financial and other business critical information in the cloud, specifically the public cloud, the internal controls must provide management with a clear understanding of who owns and who is authorized to access and modify these financial documents.

Who Should Care

Entities subject to SOX compliance include:

- All US-based publicly traded companies
- International companies that have registered equity or debt securities with the Securities and Exchange Commission;
- Accounting firms that provide auditing services to the above entities.



What Is Sarbanes-Oxley?

Non-compliance implications can range from financial penalties to criminal prosecution and jail time. Further, this increased visibility can lead to reduced market and investor confidence.

A CEO or CFO who submits incorrect certification is subject to a fine up to \$1 million and imprisonment for up to ten years. If that certification was submitted “willfully”, the fine can be increased up to \$5 million and the prison term can be increased up to twenty years.

Complying with Sarbanes-Oxley

To comply, organizations must implement a suitable internal control framework that must be formally and periodically assessed. Not only should organizations determine if appropriate controls are in place and are effective, they should also select independent auditors who must assess the effectiveness of the internal controls. This assessment (audit report) must be included in all financial reports.



Impact on IT & Security

IT and security are inextricably linked into the overall financial reporting process. In this context, responsible individuals must:

- Understand the organization’s financial internal control program and its financial reporting process.
- Identify and localize data associated with these financial controls and financial reporting process, including within the cloud.
- Identify the system components that support those financial internal controls and the reporting process to the financial statements.
- Identify risks associated with these system components.
- Design and implement IT and security controls to mitigate the identified risks.
- Ensure that IT and security controls are updated and changed as necessary to correspond with changes in internal control or financial reporting processes.



Impact on IT & Security

SOX does not provide nor recommend a list of IT and Security controls, leaving organizations free to design and implement controls they deem sufficient. Such controls cover the following topics:

Strategic, Organizational & Compliance Controls	Technical Controls	Physical Controls
IT and security strategy	Access Management	Physical Security
Risk Assessment	Data protection	
Change Management	Data and system recovery	
Manage third-party services	Configuration Management	
People Management	Patch Management	
Training & Awareness	Malicious Software prevention	
Use of Administrative Privileges	Application Software	
Assets Inventory	Boundary defense	
Acquisition of system components	Wireless Devices	
Quality Assurance	Monitoring, and Analysis of Audit Logs	
Audits	Incident Response	

CloudLock Security Fabric

Sarbane-Oxley Compliance and Security in the Cloud

Meeting internal or external compliance regulations can be a tremendous challenge for any IT organization using software as a service (SaaS) applications. CloudLock provides the visibility and control needed to quickly detect and respond to risks of data that are sensitive, toxic, and/or subject to SOX regulation, while confidently working in the cloud.



CloudLock's cloud security solution helps organizations achieve SOX compliance through the following



Data Protection

- Identify and monitor sensitive data within your cloud apps in real time.
- Enforce strong encryption of documents containing sensitive data.
- Notify and educate users to encrypt sensitive information based on policy violations of over shared or inappropriately stored data.



Application Software

- Discover and control more than 77,000 cloud and third-party apps that matter.
- Gain insight which apps pose a risk to your organizations.



Access Management

- Enforce proper access controls for all relevant apps and data in the cloud.
- Provide ongoing verification and control of access rights.

- Protect your organization from malicious data extraction.
- Monitor access to your cloud apps and associated data.
Control and track addition, deletion, and modification of users.
Track inactive accounts.



Monitoring and Analysis of Audit Logs

- Monitor user activity to detect and surface potential anomalies, including suspicious logins.
- Use audited data as evidence of compliance to regulations and internal policies.
- Feed time-sensitive and critical security events into your enterprise-wide Security Incident and Event Management (SIEM) solutions for a consolidated security view.
- Gain real-time insight into the health of your public cloud applications in one unified dashboard.
- Leverage out-of-the box security and compliance reports to meet regulatory requirements with internal and external auditors.



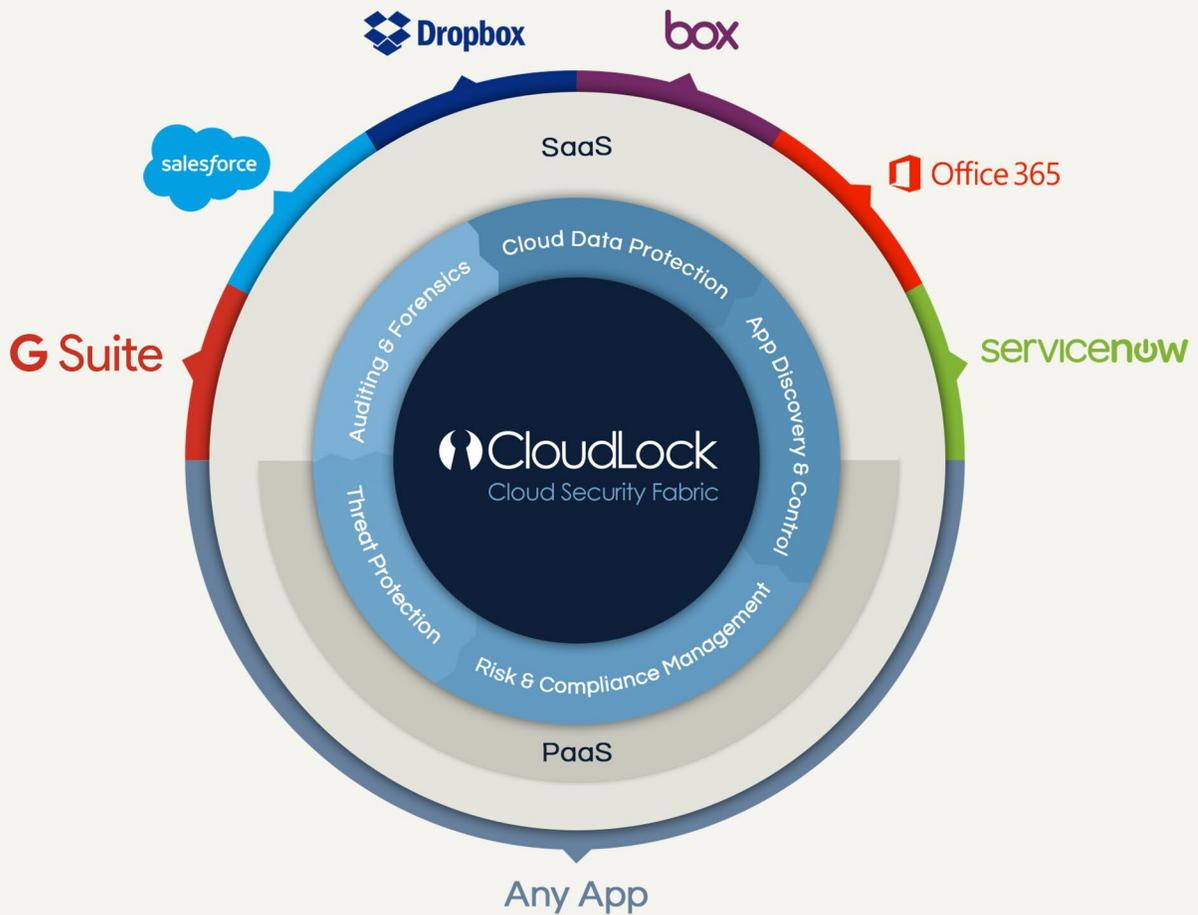
Incident Response

- Centrally manage all incidents based on unified policies.
Investigate flagged content and potentially toxic data in files and documents.
- View and filter incidents based on severity level, object type, cloud app, status, date, and other criteria.
Prioritize and track incidents based on business impact to your organization.
- Create incident reports.
- Automate response actions and notifications to your end users with CloudLock's fully automated remediation management capabilities.

The Cloud Security Fabric

CloudLock offers the cloud security fabric enabling enterprises to protect their data in the cloud, reduce risk, achieve compliance, manage threats, and increase productivity.

[Learn More](#)



By analyzing 750 million files for more than 6 million end users daily. CloudLock delivers the only complete, risk-appropriate, and people-centric approach to cloud security.