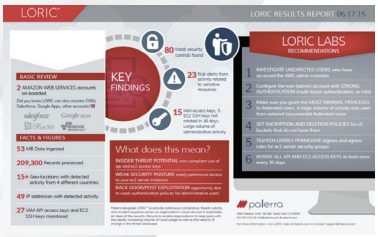
LORIC™ for box



Get a free assessment of usage, threats and compliance violations in your Box environment

Cloud Security is a Shared Responsibility

Cloud services are a growing target and in extreme cases, breaches have put companies out of business. Code Spaces is one such example where it had to close doors in June 2014 after hackers gained privileged access to its AWS environment and destroyed critical assets.

Protection of customer data is a priority for Box and it takes numerous steps to reduce risk. However, cloud security is a shared responsibility between the organization and the cloud provider. Security of the cloud infrastructure is Box's responsibility, while access and usage of the data stored in Box is the organization's responsibility.

Terms of Service for Box

You must immediately notify Box in writing of any unauthorized use of: (a) any Content (b) any account; or (c) the Service that comes to your attention. In the event of any such unauthorized use by any third party that obtained unauthorized access through you, you will take all steps necessary to terminate such unauthorized use.

An organization's obligations include being able to answer questions such as:

- Are privileged users and administrators making changes to Box security configurations?
- Are any users sharing confidential content?
- Are any users downloading an unusually large number of files from Box?

There are a number of challenges in meeting these obligations:

- Access to logs and metadata is limited reducing visibility into activities
- Detection of anomalous activity is challenging due to the volume of log data, lack of activity baselines, and lack of context
- Manual monitoring of security configurations and activities is laborious and error-prone
- Remediation requires subject matter expertise in Box

Security & Governance for Box

Palerra enables organizations to protect data within Box with LORIC™, the cloud security automation platform. It is the only solution to manage the entire security lifecycle of cloud data in a single platform.

VISIBILITY: Insights into Box adoption and usage

THREAT DETECTION: Monitoring for anomalous activities

COMPLIANCE MANAGEMENT: Monitoring of configurations and activities leading to policy violations

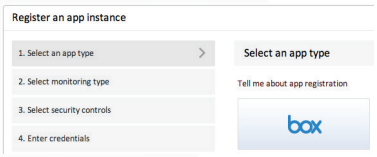
INCIDENT RESPONSE: Logging and remediation

Automation of threat detection, compliance management and incident response with LORIC increases operational efficiency and enables staff to focus on more strategic initiatives. It is delivered as a service and can be deployed in minutes. LORIC enables security and governance for Box without altering the native user experience for users.

palerra

3945 Freedom Circle Suite 560 Santa Clara CA 95054 /// 650 300 5222 /// info@palerra.com /// palerra.com

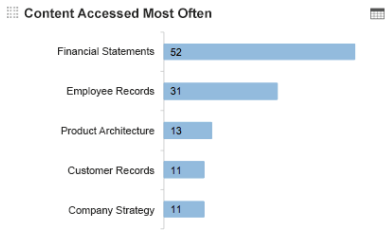
EFFORTLESS DEPLOYMENT



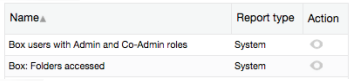
Get started in minutes by creating a Box service account for LORIC. No hardware, no software, no agents.

INSIGHTS

Instant insights into adoption and usage of Box, such as the most commonly accessed content.



ACTIVITY REPORTS

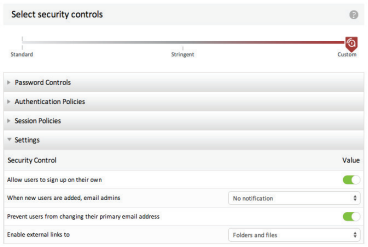


Ability to create custom reports as well as a rich set of predefined reports on potentially risky activities such as assignment of administrative privileges to users.

USER BEHAVIOR ANALYTICS

Studies activities such as logins, downloads, uploads, and sharing for each Box user to create baseline activity profiles. It then automatically flags any deviations in behavior exposing insiders and hackers.

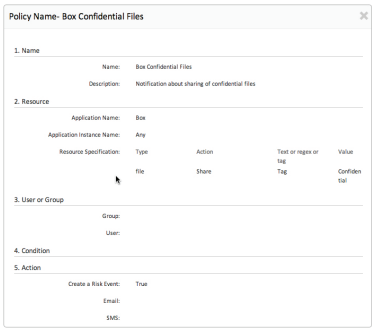
CONFIGURATION MONITORING



Continuously monitors and enforces security configurations within Box to ensure compliance – say goodbye to laborious manual audits.

MONITORING POLICIES

Ability to build custom policies as well as a library of predefined policies for real-time notifications about activities that may introduce risks, such as sharing of files tagged as "confidential".



AUTOMATIC INCIDENT RESPONSE

Category	Priority	Details
Anomalous Activity	Medium	IP Hopping Risk. IP address hopping between 2 geographical locations which are more than 1500 miles from each other
Anomalous Activity	Medium	IP Hopping Risk. IP address hopping between 2 geographical locations which are more than 1500 miles from each other
Anomalous Activity	Medium	IP Hopping Risk. IP address hopping between 2 geographical locations which are more than 1500 miles from each other
Anomalous Activity	Medium	User Behavior Risk. Login IPs and Login Geographical Locations show deviation from normal behavior
Anomalous Activity	Medium	User Behavior Risk. Login Actions and Login IPs show deviation from normal behavior
Cross Application Activity	High	Cross-application Risk. Fast IP Hopping detected with logins to multiple applications seen in the past 6 hours from more than 3 states

Automatically logs incidents and executes remedial actions within Box ensuring incidents are addressed immediately.

ECOSYSTEM INTEGRATION

Leverages existing IT investments by integrating with LDAP, single sign on, identity and access management, ticketing, and incident management solutions.