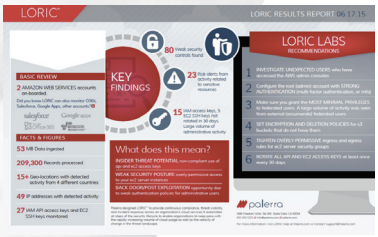
LORIC™ for salesforce®



Get a free assessment of usage, threats and compliance violations in your Salesforce environmentt

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 Salesforce 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 Salesforce's responsibility, while access and usage of the data stored in Salesforce is the organization's responsibility.

Master Subscription Agreement for Salesforce

4.3 Your Responsibilities. You will ... (c) use commercially reasonable efforts to prevent unauthorized access to or use of Services and Content, and notify Us promptly of any such unauthorized access or use

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

- Are privileged users and administrators making changes to security profiles, roles, groups, and users?
- Are any users creating risk by exporting data from Salesforce?
- Are any users tampering with data within standard and custom objects?

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 Salesforce

Security & Governance for Salesforce

Palerra enables organizations to protect data within Salesforce 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. LORIC leverages the Salesforce Event Monitoring functionality to provide:

VISIBILITY: Insights into Salesforce adoption and usage

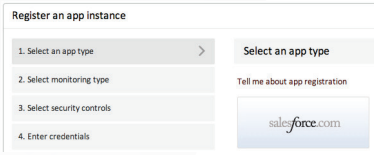
THREAT DETECTION: Monitoring for anomalous activities

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 Salesforce without altering the native user experience for users.

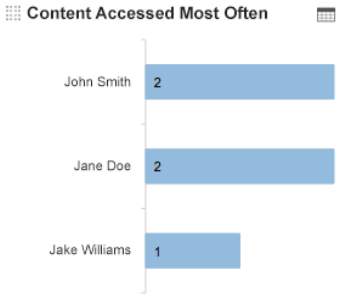
EFFORTLESS DEPLOYMENT



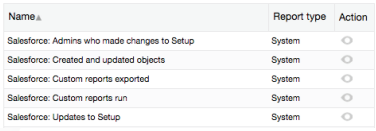
Get started in minutes by creating a Salesforce service account for LORIC. No hardware, no software, no agents.

INSIGHTS

Instant insights into adoption and usage of Salesforce, such as administrators with the most activities.



ACTIVITY REPORTS

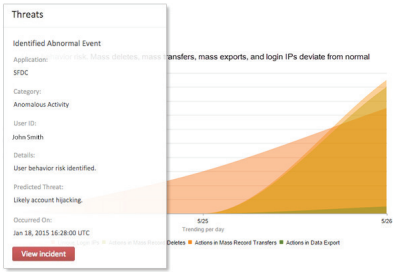


Name	Report type	Action
Salesforce: Admins who made changes to Setup	System	
Salesforce: Created and updated objects	System	
Salesforce: Custom reports exported	System	
Salesforce: Custom reports run	System	
Salesforce: Updates to Setup	System	

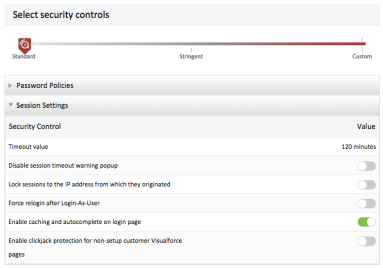
Ability to create custom reports as well as a rich set of predefined reports on potentially risky activities such as exported reports.

USER BEHAVIOR ANALYTICS

Studies activities such as logins, record deletions, and data export for each Salesforce user to create baseline activity profiles. It then automatically flags any deviations in behavior exposing insiders and hackers.



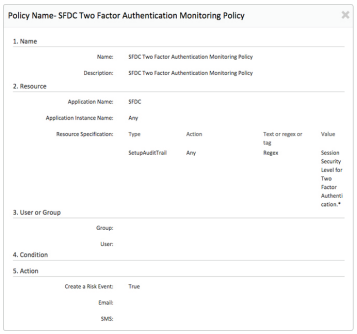
CONFIGURATION MONITORING



Continuously monitors security configurations within Salesforce 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 mass record download at the end of a fiscal quarter.



AUTOMATIC INCIDENT RESPONSE

Category	Priority	Details
Anomalous Activity	High	Brute force attack risk
Anomalous Activity	Medium	IP hopping risk. IP address hops between 2 locations that are more than 1500 miles apart
Security Control	High	The security control value should be stronger
Cross Application Activity	High	Cross application risk detected. Please review account activity for further confirmation

Automatically logs incidents and executes remedial actions within Salesforce 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.