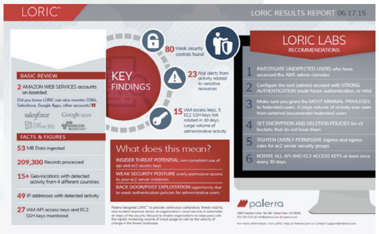
SOLUTION BRIEF

LORIC™ for Google™ Apps



LORIC™ LORIC RESULTS REPORT 06.17.15

BASIC REVIEW

2 AMAZON WEB SERVICES accounts on-boarded.

Did you know LORIC can also monitor O365, Salesforce, Google Apps, other accounts?

FACTS & FIGURES

53 MB Data ingested

209,300 Records processed

15+ Geo-locations with detected activity from 4 different countries

49 IP addresses with detected activity

27 IAM API access keys and EC2 SSH keys monitored

KEY FINDINGS

80 Weak security controls found

23 Risk alerts from activity related to sensitive resources

15 IAM access keys, 5 EC2 SSH keys not rotated in 30 days. Large volume of administrative activity

What does this mean?

INSIDER THREAT POTENTIAL non-compliant use of api and ec2 access keys

WEAK SECURITY POSTURE overly-permissive access to your ec2 server instances

BACK DOOR/POST EXPLOITATION opportunity due to weak authentication policies for administrative users

Palerra designed LORIC™ to provide continuous compliance, threat visibility, and incident response across an organization's cloud services. It automates all steps of the security lifecycle to enable organizations to keep pace with the rapidly increasing volume of cloud usage as well as the velocity of change in the threat landscape.

LORIC LABS RECOMMENDATIONS

1 INVESTIGATE UNEXPECTED USERS who have accessed the AWS admin consoles

2 Configure the root (admin) account with STRONG AUTHENTICATION (multi-factor authentication, or mfa)

3 Make sure you grant the MOST MINIMAL PRIVILEGES to federated users. A large volume of activity was seen from external (assumerole) federated users

4 SET ENCRYPTION AND DELETION POLICIES for s3 buckets that do not have them

5 TIGHTEN OVERLY-PERMISSIVE ingress and egress rules for ec2 server security groups

6 ROTATE ALL API AND EC2 ACCESS KEYS at least once every 30 days

palerra

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

For more information: Visit LORIC Help at Palerra.com or Contact Support@Palerra.com

Get a free assessment of usage, threats and compliance violations in your Google Apps 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 Google 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 Google's responsibility, while access and usage of the data stored in Google Apps is the organization's responsibility.

Google Apps Terms of Service

> *"Customer will use commercially reasonable efforts to prevent unauthorized use of the Services' and to terminate any unauthorized use."*

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

- Knowing if privileged users are changing security configurations within Google Apps
- Knowing if sensitive corporate data is being shared externally via Google Drive
- Reporting on third party application and mobile device access to data within Google Apps for audit purposes

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 Google Apps

Security & Governance for Google Apps

Palerra enables organizations to protect data within Google Apps 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 Google Apps adoption and usage

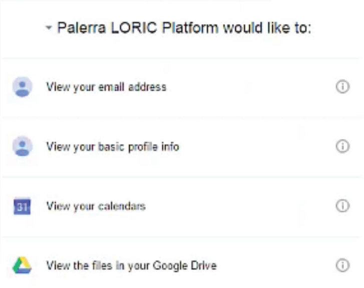
THREAT DETECTION: Monitoring for anomalous activities

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

INCIDENT RESPONSTE: 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 provides security and governance for Google Apps without altering the native user experience for users.

SERVICE ACCOUNT SUPPORT



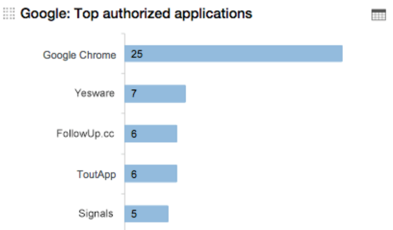
▾ Palerra LORIC Platform would like to:

- View your email address ⓘ
- View your basic profile info ⓘ
- View your calendars ⓘ
- View the files in your Google Drive ⓘ

Monitoring of all activities within Google Apps including user, administrator and API-driven interactions.

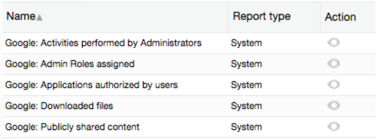
INSIGHTS

Instant insights into adoption and usage of Google Apps, such as details of publicly shared content or third party application access.



Google: Top authorized applications

ACTIVITY REPORTS

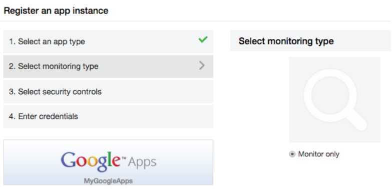


Name▴	Report type	Action
Google: Activities performed by Administrators	System	◎
Google: Admin Roles assigned	System	◎
Google: Applications authorized by users	System	◎
Google: Downloaded files	System	◎
Google: Publicly shared content	System	◎

Ability to create custom reports as well as a rich set of predefined reports on risky activities such as assigning admin roles and adding new members to a group.

CONFIGURATION MONITORING

Continuously monitors security configurations within Google Apps to ensure compliance – say goodbye to laborious manual audits.



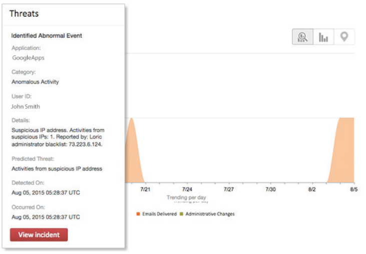
Register an app instance

1. Select an app type ✓
2. Select monitoring type >
3. Select security controls
4. Enter credentials

Select monitoring type

● Monitor only

USER BEHAVIOR ANALYTICS



Threats

Identified Abnormal Event

Application: GoogleApps

Category: Anomalous Activity

User ID: John Smith

Details: Suspicious IP address. Activities from suspicious IPs: 1. Reported by: Loric administrator blacklist: 73.223.6.124.

Predicted Threat: Activities from suspicious IP address

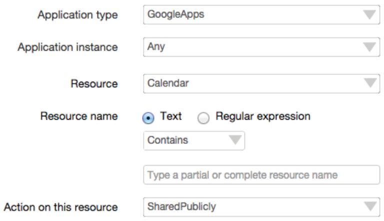
Detected On: Aug 05, 2015 05:28:37 UTC

Occurred On: Aug 05, 2015 05:28:37 UTC

Studies activities such as logins, communication and collaboration for each Google Apps user to create baseline activity profiles. It then automatically flags any deviations in behavior exposing insiders and hackers.

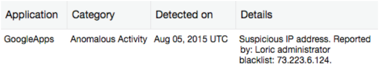
MONITORING POLICIES

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 a calendar with the public or sharing content with an external user.



Application type	GoogleApps
Application instance	Any
Resource	Calendar
Resource name	● Text ○ Regular expression Contains Type a partial or complete resource name
Action on this resource	SharedPublicly

AUTOMATIC INCIDENT RESPONSE

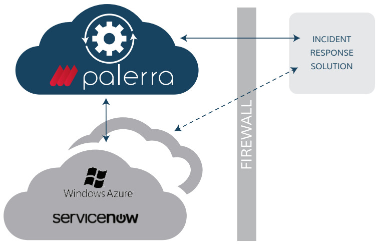


Application	Category	Detected on	Details
GoogleApps	Anomalous Activity	Aug 05, 2015 UTC	Suspicious IP address. Reported by: Loric administrator blacklist: 73.223.6.124.

Automatically logs incidents and executes remedial actions within Google Apps service 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.



palerra
Windows Azure
servicenow
FIREWALL
INCIDENT RESPONSE SOLUTION