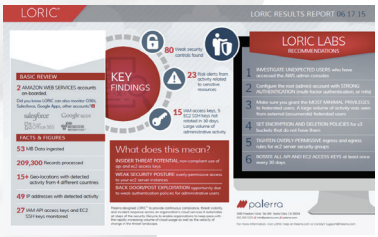
LORIC™ for Office 365



Get a free assessment of usage, threats and compliance violations in your Office 365 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 Microsoft 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 Microsoft's responsibility, while access and usage of the data stored in Office 365 is the organization's responsibility.

> ### Service Level Agreement for Microsoft Online Services
> *This SLA and any applicable Service Levels do not apply to any performance or availability issues:*
> *... 5. That result from your unauthorized action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices;*

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

- Knowing when a new Exchange administrator account is created which could be a potential backdoor to the environment
- Knowing if privileged users disable Office 365 data loss policies
- Detecting anomalous activity such as when a user performs an unusually large number of administrative changes in a short period of time

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 Office 365

Security & Governance for Office 365

Palerra enables organizations to protect data within Office 365 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 Office 365 adoption and usage

THREAT DETECTION: Monitoring for anomalous activities

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

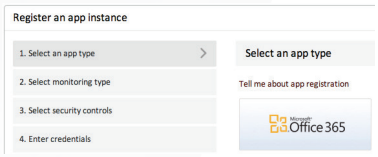
INCIDENT RESPONSE: Logging and remediation

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 Office 365 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

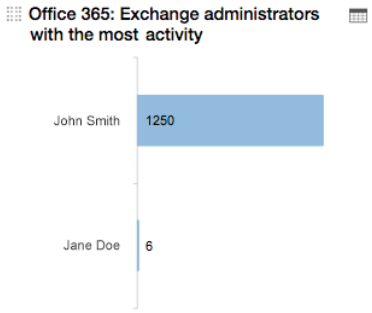
EFFORTLESS DEPLOYMENT



Get started in minutes by creating an Office 365 service account for LORIC. No hardware, no software, no agents.

INSIGHTS

Instant insights into adoption and usage of Office 365, such as administrators with the most activities.

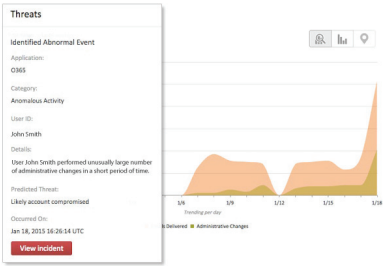


ACTIVITY REPORTS

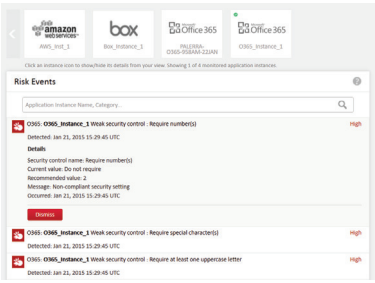
Ability to create custom reports as well as a rich set of predefined reports on potentially risky activities such as commonly run cmdlets.

USER BEHAVIOR ANALYTICS

Studies activities such as logins and administrative changes for each Office 365 user to create baseline activity profiles. It then automatically flags any deviations in behavior exposing insiders and hackers.



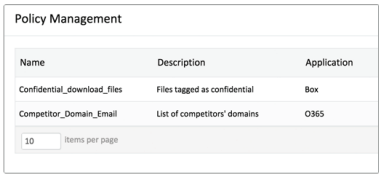
CONFIGURATION MONITORING



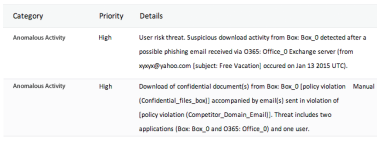
Continuously monitors security configurations within Office 365 to ensure compliance – say goodbye to laborious manual audits.

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 changes to Exchange transport rules.



AUTOMATIC INCIDENT RESPONSE



Automatically logs incidents and executes remedial actions within Office 365 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.