LORIC™

The Cloud Security Automation Platform

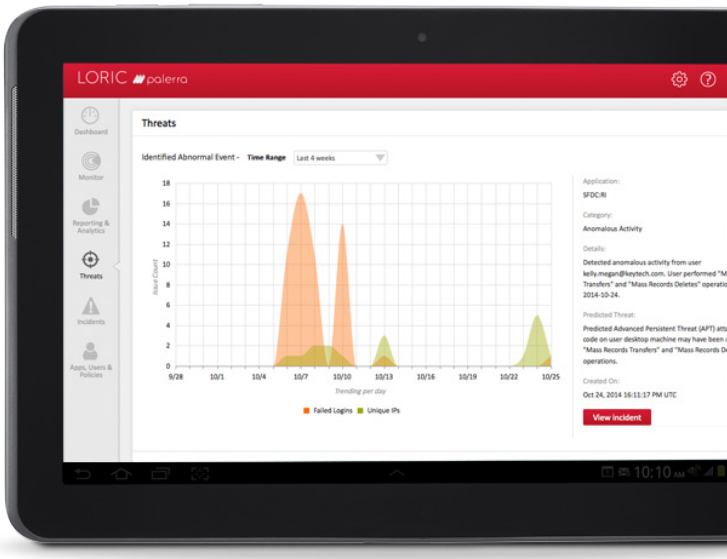
LORIC enables you to keep pace with the rapidly changing threat landscape by automating threat detection, predictive analytics, security configuration management, and incident response across your entire cloud footprint. It protects Software-as-a-Service applications such as Office 365 through infrastructure such as Amazon Web Services (AWS), and everything in between.

- **Threat visibility** in a single pane of glass across all your cloud services.
- **Regulatory compliance** through automated monitoring and enforcement of security configurations.
- **Automated threat response** with automated forensics, incident tracking and remediation.
- **Effortless deployment** without hardware, software and agents.
- **Seamless user experience** and no risk of productivity disruption as a result of LORIC's unobtrusive architecture (no proxies).

Enterprises across financial services, high technology, consumer hospitality services, and numerous other industries are using LORIC to secure their cloud footprints.

"We are really looking to use LORIC to address some of the gaps in our security monitoring and intelligence and visibility of users' activity, potential threats, and bad actors in the cloud."

– Steve Tout, Head of IAM, Architecture & Strategy Group at VMware



Security Configuration Management

LORIC eliminates labor intensive, error-prone manual processes by automatically managing security configurations within cloud services. As an example, it can enforce minimum password length or manage encryption settings for a cloud service.

DISCOVERY: Asynchronously assesses and models security configurations for each supported cloud service.

SEEDING: Pushes out-of-the-box, LORIC-recommended, or custom settings to each cloud service.

MONITORING: Continuously audits for configuration drift.

ENFORCEMENT: Instantly rectifies drift and restores configurations to a compliant state.

Threat Detection

LORIC identifies existing threats across your entire cloud footprint by detecting anomalous behavior. Sample risky scenarios include a user logging in from an unusual number of geo-locations in a 24-hour period and downloading or deleting data.

USER RISKS: Evaluates a variety of threat vectors including deviations from normal user behavior, suspicious locations, and non-compliant security configurations.

APPLICATION RISKS: Detects anomalous cloud service behavior to protect against threats proliferating from one service to another.

KEY SECURITY INDICATORS: Consolidation and correlation of data to provide instant insight into the security posture of your cloud services.

CUSTOM NOTIFICATIONS: Ability to define custom threat scenarios and receive notifications upon violations.

Predictive Analytics

LORIC stays a step ahead of threats with patent-pending modeling techniques that evaluate risks across hundreds of threat vectors to provide you with a concise summary of potential threats. An indication of an attack such as a compromised client might be that a user has an unusual number of failed logins from different geo-locations, each with different browsers and operating systems on the client device.

INTELLIGENCE FEEDS: Integrates real-time commercial, open source, LORIC proprietary, and contextual application feeds to refine analytics.

BEHAVIORAL ANALYSIS: Recognizes deviations of user and cloud service behaviors from baselines across recent as well as established periods.

MACHINE LEARNING: Performs real-time threat modeling using non-linear algorithms to automatically correlate hundreds of threat vectors including IP reputation, action velocity, anomalous behavior, and cross application intelligence.

Automated Incident Response

LORIC enables organizations to keep pace with new threats by automating forensics, incident management, orchestration and remediation through native capabilities as well as integration with existing technologies. For example, a user's Box account may be temporarily disabled if more than 20 continuous failed login attempts are detected.

INCIDENT MANAGEMENT: Automatically generates incident tickets for threat events.

REMEDIATION: Manually or automatically resolve incidents through built-in capabilities or by integrating with existing enterprise applications or change management processes.

ORCHESTRATION: Execute your preferred remediation processes through a native ticketing system and different remediation methods.