OROCK SIEM AS A SERVICE WITH IBM QRADAR
Solution Overview

RAPIDLY DETECT ADVANCED SECURITY THREATS

Government agencies face an ever-increasing set of security threats without the required resources to protect mission-critical networks and infrastructure. Security Information and Event Management (SIEM) tools such as IBM QRadar are deployed widely across the government to address this challenge. But despite this wide adoption there is no FedRAMP-authorized SIEM available as a software-as-a-service (SaaS) offering in the cloud. As a result, federal CIOs and CISOs are limited in their choices to comply with FedRAMP guidelines and purchase software under an OpEx model.

SIEM HOSTED IN A FEDRAMP MODERATE CLOUD

To address these pressing security and compliance needs, ORock Technologies has introduced **ORock SIEM as a Service with IBM QRadar.** This powerful solution enables government agencies to detect threats across cloud-based and on-premises environments with a single, unified security analytics solution that is hosted in ORockCloud, a FedRAMP Moderate cloud, and delivered as a SaaS application.

Based on the industry-leading IBM QRadar SIEM solution and hosted in **ORockCloud**, ORock SIEM as a Service with IBM QRadar enables your security analysts to quickly detect anomalies and attacks from event data while eliminating many false positives. It can either be managed by your security staff or consumed as a fully-managed service operated by IBM certified professionals and backed by ORock's 24/7/365 NOC and SOC. With a cloud-based service now available, resource-constrained agencies can now have greater access to a platform with extensive out-of-the-box content for a broad selection of security use cases.

By leveraging this powerful SIEM solution in the ORockCloud, agencies can comply with mandates to move applications to the cloud, reduce hardware and storage costs, and stay within budgets with a predictable billing model. ORock anticipates FedRAMP Moderate and DoD Impact Level 4 provisional authorization for this solution as a SaaS offering in 2019, with FedRAMP High and DoD Impact Level 5 SaaS authorization expected in 2020.*

**Pending sponsorship by a government agency and FedRAMP authorization.*

SOLUTION BENEFITS

Gain visibility into high-risk network, application and user activity while consuming SIEM as a Service:

Data Ingestion
Gather a broad range of data from network devices, endpoints, clouds, users, applications, security controls and threat intelligence sources

Monitoring
Gain insight into who is on the network, what is happening, and what represents a potential risk

Detection
Correlate activity across the entire network and apply signature-based and behavioral-based detection methods to identify both known and unknown threats

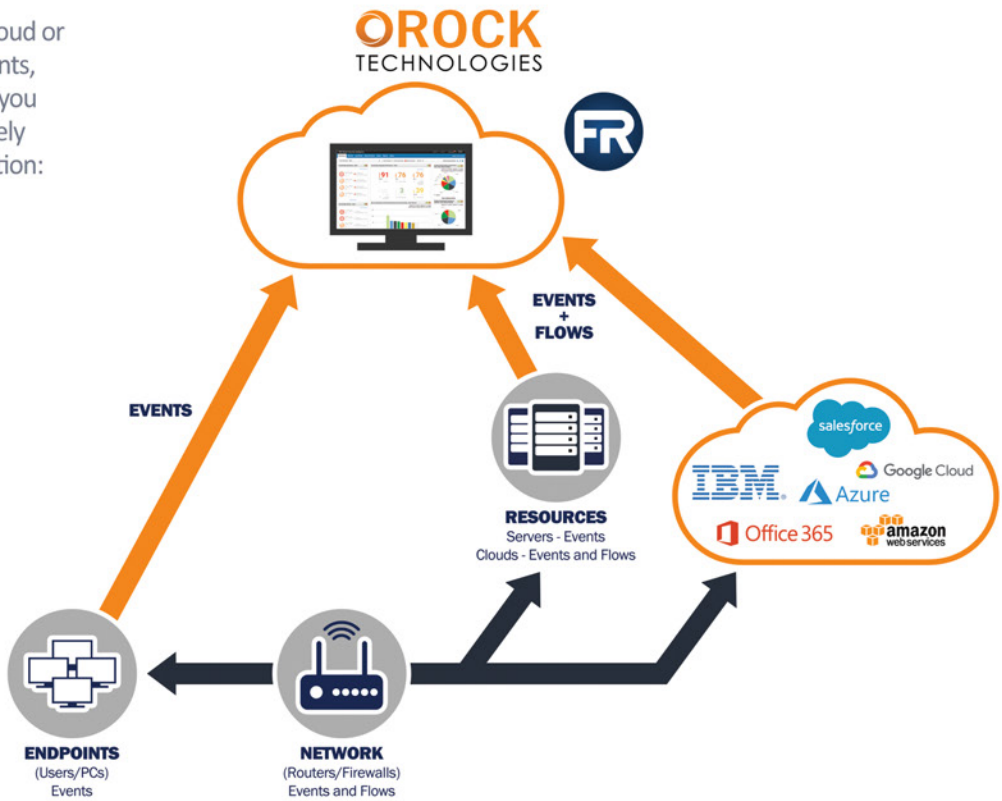
Investigation
Automate the investigation of observable threats to help analysts make faster, more informed decisions about what to do next.

ORock Technologies, Inc. | 571.386.0201 | sales@orocktech.com | www.orocktech.com

IDENTIFY THE SECURITY EVENTS THAT MATTER THE MOST

Whether you are just starting your journey to the cloud or you are already managing multiple cloud deployments, ORock SIEM as a Service with IBM QRadar can help you gain the comprehensive visibility needed to effectively detect, investigate and respond to threats. The solution:

- Correlates and analyzes security data, network traffic anomalies, threat intelligence and user behavior to help rapidly detect threats and potential breaches
- Automatically prioritizes alerts so you can more easily identify the most critical incidents
- Provides a single-pane-of-glass view into security events, vulnerability data and user activity across both on-premises and cloud-based environments



OROCKCLOUD: ARCHITECTED FOR GOVERNMENT WORKLOADS

Security

Government-grade security built-in from inception

325+ security controls

Operate outside DDoS attacks

FIPS 140-2 dual factor authentication

Prevent security breaches

Performance

Leverage ORock's private fiber optic network for fast data transmission

Monitor across most multi-cloud and on-prem deployments with connectivity at Layer 2

Enhance network speed and security

Predictable Cost

Flat rate for data transport

Improve cost predictability

Simplify billing

Avoid surprise charges or inflated exit costs

Backup and recovery and 24/7 NOC/SOC support included

Control

Federate your own security policies

Reduce movement of data within and between regions

Know where data is at all times

Avoid vendor lock-in

OROCK TECHNOLOGIES

Improve your security monitoring today.
Contact ORock Technologies at (571) 386-0201 or sales@orocktech.com.

Distributed by:
immixGroup
An Arrow Company