

# Cloud Security Monitoring

## Proactive Monitoring for Security Threats

By moving to the cloud, organizations will realize improved security efficiencies due to more effective controls over information access, reduced risk of data and system compromise, shared legal and compliance responsibilities, and secure environments for their business-critical assets. However, organizations also need full visibility into their cloud environment (IaaS, Paas, SaaS) to adequately assess their security posture and minimize risk.

At Protiviti, we believe companies must shift from a reactive approach to a proactive and preventive cloud security strategy. This prioritizes the design and implementation of deterrent, detective and corrective security controls that help protect the cloud ecosystem and its services from being exploited by attackers.

**Enabling  
complete  
visibility for  
reduced risk**

### Key Themes of Cloud Security Monitoring



#### Identity Management is Key

Organizations should assess their security posture from an identity perspective and evaluate tools that will help prevent or minimize risks due to poorly provisioned identities. Operate under the assumption that the principal risk to your hybrid cloud environment is a trusted identity with too much privilege. Risk can be greatly reduced by minimizing identities that are either provisioned incorrectly or have too many permissions associated with them.



#### Know Your Responsibilities

Do you understand what security you are responsible for, and what the cloud provider is responsible for? Which security and privacy standards must your organization meet? Do you keep a signed audit trail of which identities performed which actions and when through their UIs and APIs? What access do you provide to logs? Which tools can provide insight into the behaviors that will help identify more sophisticated attacks?



#### Keep Velocity in Mind

The cloud introduces a rate of change very different from that of traditional data centers, and its velocity presents a challenge for monitoring security threats. Many traditional tools either have not kept up because they are not API-enabled or they cannot manage data over time. The cloud's volatility means static inventory tools are less useful. Are you able and willing to trade security for speed and velocity?



#### Visibility

Many companies rely primarily on native security tools from their cloud providers. This may leave gaps in visibility – particularly at the application and data processing levels. Organizations should have the ability to observe anomalous behaviors at all layers of their cloud architecture. In addition, traditional solutions like role-based access control (RBAC) do not provide good visibility in hybrid (enterprise + cloud) environments.

# Cloud Security Monitoring

Cloud Security Monitoring provides incident detection, analysis and reporting capabilities in the cloud. This service assimilates information of interest, including security events, data/network flows, vulnerability data, asset models and identities from cloud-based log sources.



**SaaS**

- CSP Native Security Enablement
- Security and Audit Logging
- Asset Management
- Data Protection, Encryption & Key Management
- IAM
- Configuration Management
- Risk-Based Authentication



**PaaS & IaaS**

- CSP Native Security Enablement
- Network Security
- Host Security
- Security and Audit Logging
- Vulnerability Management
- Cloud Access Federation and SSO
- User Behavior Analytics



**SecOps**


- Configuration and Vulnerability Management
- Metrics and Reporting
- Security Analytics
- SIEM
- Incident Response
- Threat Intelligence




**Governance, Risk and Compliance**

- Cloud Governance Model
- Risk Assessments
- Security Awareness and Training
- Standards, Processes and Procedures
- Compliance Validation and Reporting


## Business Outcomes




Protection of SaaS, PaaS, and IaaS cloud services




Monitor and access anomalies and use of unauthorized cloud services



Data security through data-centric policies



Threat protection through content and context-based policies




CASB/SWG integration



SIEM integration

Schedule a Technology Assessment today by contacting us at [TechnologyConsulting@Protiviti.com](mailto:TechnologyConsulting@Protiviti.com).

 [Protiviti.com/TechnologyConsulting](https://Protiviti.com/TechnologyConsulting)

 [TechnologyConsulting@Protiviti.com](mailto:TechnologyConsulting@Protiviti.com)

 [TCblog.Protiviti.com](https://TCblog.Protiviti.com)

Robert Half is the world's first and largest specialized staffing firm. Robert Half Technology, a division of Robert Half, offers project, contract-to-hire and full-time technology staffing, as well as managed IT services worldwide.

Protiviti, a wholly owned subsidiary of Robert Half, is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independently owned member firms provide consulting solutions through a network of more than 80 offices in over 25 countries.

© 2022 Robert Half International Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

 **Robert Half**<sup>®</sup>  
Talent Solutions

**protiviti**<sup>®</sup>  
Global Business Consulting