IBM Managed Cloud Security Best Practices and Compliance Monitoring for AWS

Your trusted advisor with global reach

Modern security, coupled with the move to cloud infrastructure, requires dramatic changes to responsibilities, processes, and technologies. Yet, many organizations managing their own security lack the specialized skills and competencies needed to cost-effectively protect against the rising range, volume and severity of threats.

For organizations that need to reduce the cost and complexity of securing workloads on AWS, IBM Managed Security Services helps to optimize the value of existing security investments while delivering continuous near real-time asset visibility, monitoring of security best practices and compliance, and analysis and management of cloud resource configurations.

As your trusted security partner, IBM Managed Security Services simplifies security and risk with continuous, value-driven monitoring, management and intelligence backed by global expertise, local delivery, and an integrated security portfolio to secure AWS cloud supported by a matrix of thoroughly tested and industry leading ISV technologies to provide:

- AWS resource inventory visibility with powerful visualization of cloud assets, including network topology.

Highlights

- Not your traditional Managed Security Services
- Faster, more relevant detection and response
- Global scale, local delivery and security program impact
- Security confidence enabled by deep AWS skills and insights
- Trusted advisors deliver forward-looking cloud security strategy

- Comprehensive compliance management including automated continuous compliance to help assess, monitor and enforce AWS Security best practices.
- Manage the compliance lifecycle for standards such as HIPAA, HITRUST and PCI DSS from automated data aggregation and assessment to remediation and reporting for the configuration.

Key drivers for Managed Cloud Security Best Practices and Compliance Monitoring

- Brings deep AWS experience and partners with organizations at a global scale with local delivery capabilities to secure hybrid cloud environments and assist organizations in managing compliance with complex regulatory requirements.
- Enriched context and insights for faster and more relevant detection and response. With hundreds of investigation experts at IBM Managed Security Services combined with proprietary and partner-driven AI and automation technologies, alert fatigue is minimized, context drives prioritization and rapid response is delivered.
- Accelerated detection via near real-time, high-fidelity monitoring, analysis and 24x7 investigation across the threat lifecycle, supporting your compliance and security best practice requirements with near instant views of security posture.
- On average, managed services require less cost, time and resources compared to building, operating and maintaining your own Security Operations Center with guaranteed service levels.

Cloud resources inventory visibility

For securing workloads, organizations need to see what they are running on cloud. Most security teams do not know the full extent of the deployment on cloud since the move of applications to cloud is more business-led and DevOps-driven. Enabling visibility into all the resources utilized within cloud environments is critical to securing workloads.

IBM Security can provide agentless native integration of AWS resources and services as well as optimize usage of near real-time monitoring services, such as AWS Config, CloudTrail and VPC Flow Logs, Amazon GuardDuty, AWS Lambda and AWS Inspector for continuous visibility and monitoring.

Key features provided with the managed security services include:

- A single glass of pane for cloud resource inventory information by type of service, region, account and other relevant attributes.
- Maintaining resource configuration and audit details.
- Enriching visibility by correlating data from external sources – e.g. vulnerability scanners, threat intelligence tools and security information and event management (SIEM).
- Reporting of performance and audit metrics including resource inventory dashboard and reports.
- Customized support hours e.g., 8/5, 24/7,16/5
- Health monitoring, log correlation and retention via a robust portal for client visibility of security status and interactions.

Cloud security best practices and compliance monitoring

With DevOps taking over the setting up of workloads on cloud with standard easy-setup configurations, the focus is on ensuring quick turnaround times and fast delivery of compute and services. Security oversight enables organizations to continuously monitor cloud resources for configuration drift allowing users to create, modify and destroy resources on-demand within guiderails baselined against security best practices.

IBM Security can help organizations quickly assess security posture against best practices, identify risks and gaps, actively enforce gold standards and provide near real-time recommendations for AWS accounts not configured with security best practices.

Key features provided with the managed security services include:

- Management, monitoring, alerting, governance and reporting of AWS best practices, native cloud security controls and policies.
- Manage: Manage and troubleshoot security controls and policies for ongoing protection of your AWS environment.
- Governance: Gain confidence in the security maturity through relevant reporting, insights and recommendations.
- Alert Management and Burndown: Monitor policy violations and recommendations for manual and auto-remediation.
- Reporting of performance and compliance metrics including compliance dashboard and reports.
- Customized support hours e.g., 8/5, 24/7,16/5
- Health monitoring, log correlation and retention via a robust portal for client visibility of security status and interactions.

AWS compliance monitoring support

Adherence to compliance standards including assessments and maintaining audit evidence across changing workloads, accounts and regions is a key ask. The risk and compliance guidance helps define and enforce standard policies to measure against industry standards and compliance frameworks, including CIS, NIST, HITRUST and PCI

IBM Security can provide real time monitoring against the configuration of AWS accounts and service against multiple compliance standards including CIS AWS, HIPAA, ISO 27001:2013 and PCI DSS, including the ability to craft enterprise-specific policies to capture and record baseline drift and maintain a historical record of the compliance posture.

Key features provided with the managed security services include:

Services include:

- Management, monitoring, alerting, governance, and reporting of industry standards and compliance frameworks.
- Manage: Manage and troubleshoot security controls and policies for ongoing protection of the AWS environment.
- Governance: Gain confidence in the security maturity through relevant reporting, insights, and recommendations.
- Alert Management and Burndown: Monitor policy violation and recommendation for manual and auto-remediation.
- Reporting of performance and compliance metrics including compliance dashboard and reports.
- Customized support hours e.g., 8/5, 24/7,16/5
- Health monitoring, log correlation and retention via a robust portal for client visibility of security status and interactions.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 10,000 security patents. To learn more, visit ibm.com/security.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM Managed Security Services, please contact your IBM representative or IBM Business Partner, or visit the following website: https://www.ibm.com/security/services/managed-security-services

Read the MSS Buyer’s Guide: https://www.ibm.com/downloads/cas/KPEG6J8Q?cm_sp=CTO-_-en_US-_-BVWMRDGY