Mandiant

DATASHEET

Cloud Architecture and Security Assessment

Benefits

- **Understand** threats to your specific cloud environment architecture
- **Mitigate** commonly exploited cloud architecture misconfigurations
- **Reduce** your attack surface from common exploitation techniques
- **Gain visibility** of top security risks related to existing configurations
- **Enhance** monitoring, visibility, and detection in the cloud
- **Prioritize** the right security enhancements to your cloud environment

Improve cyber defenses through better cloud architecture and configurations

Why Mandiant

Mandiant has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders are on the frontlines of the most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques and procedures.

Overview

To reduce costs and improve scalability, organizations are increasingly migrating their on-premise assets to the cloud. In response, attackers are realigning their tactics and techniques, including social engineering and exploiting misconfigurations, to target cloud environments.

The Mandiant Cloud Architecture and Security Assessment evaluates your current security state and recommends hardening priorities for assets on the most popular cloud platforms: Microsoft Azure, Amazon Web Services and Google Cloud Platform.

This assessment helps your organization understand the threats and security controls unique to your specific cloud environment, hardens the environment against targeted threats, and improves your ability to detect, investigate and respond to attacker activity across all phases of the attack lifecycle.

These services are designed for organizations using cloud service providers that support an infrastructure as a service (IaaS) or platform as a service (PaaS) model. These models rely on shared responsibilities between the cloud service provider and the customer to protect against cyber incidents. Our assessment focuses on the customer responsibilities that will strengthen their security posture.

Our approach

The assessment consists of four phases, during which Mandiant experts map your existing cloud environment and determine how your current security program works to protect it:

Week 1. Initial Document Review of migration strategies, architecture diagrams, hardening documentation, access management policies and standards, SOPs/playbooks and logging standards, conducted offsite in collaboration with client stakeholders.

Week 2. Onsite Workshops to explore your cloud environment, the current security model in place, and potential security concepts and controls to implement in the future in order to meet your business needs.

Weeks 3-4. Configuration Review from the cloud platform to ensure security controls are implemented effectively, identify potential weaknesses and confirm learnings from the onsite workshops to identify potential weaknesses that could be exploited by attackers.

Week 5. Reporting that details practical technical recommendations to harden the cloud environment, enhance visibility and detection and improve processes to reduce the risk of compromise.

Deliverables

The post-assessment report provided by Mandiant includes:

- A snapshot of your current cloud environment, detailing existing architecture and security controls.
- Security for specific cloud services aligned with your current configurations and operational processes.
- Practical recommendations for enhancing visibility and detection.
- Prioritized and detailed recommendations for further hardening your cloud infrastructure.

Technical- and executive-level briefs are available upon request.

TABLE 1. Core focus areas for evaluation during assessment.

Governance, risk and compliance	Security architecture and networking	Identity and access management
• Cloud governance and services • Cloud policies and standards • Threat risk assessments • Vulnerability management • Regulatory compliance requirements	• Cloud architecture and security controls • Network segmentation and on-premise integration • Remote system connectivity and management • Disaster recovery • Containers, configurations and security controls	• Cloud authentication infrastructure, including on-premise connectivity (e.g., ADFS) • Identity management • Privilege access management • Role-based access controls
Secrets and data protection	**DevOps**	**Threat detection and response**
• Data protection and loss prevention • Database security • Certificates and keys management • Encryption	• Pipeline configurations • System and application deployment • Secure software development life cycle • Code repository security controls	• System, database, and application logging • Security logging and centralization • Endpoint and network security controls • Cloud incident response processes