2017 Cloud Security Trends

Dome9 SECURITY

Cloud adoption continues to grow rapidly as organizations are looking to reduce IT cost, increase agility and better support business functions. The 2017 Cloud Security Report, conducted in partnership with the 350,000 member Information Security Community on LinkedIn, reveals that security of critical data and systems in the cloud remains a key barrier to adoption of cloud services. The following preview highlights key findings from the 2017 Cloud Security Survey, reveals the key drivers and risk factors of migrating to the cloud, and how organizations are responding to new security threats in their move to the cloud.

BIGGEST CLOUD SECURITY THREATS

- **61%** Unauthorized access
- **52%** Hijacking of accounts, services or traffic
- **43%** Insecure interfaces / APIs

BARRIERS TO CLOUD ADOPTION

- **33%** General Security Risks
- **28%** Lack of staff resources or expertise
- **27%** Integration with existing IT environment

CLOUD SECURITY HEADACHES

- **37%** Visibility into infrastructure security
- **36%** Compliance
- **33%** Setting consistent security policies

TRADITIONAL SECURITY TOOLS DON'T WORK IN THE CLOUD

- Our traditional network security tools don't work in the cloud **20%**
- All capabilities work in the cloud **22%**
- **58%** Limited functionality

Get the NEW 2017 Cloud Security Spotlight Report

This report reveals the latest data points and trends in cloud security, shares how your peers are approaching security, and provides valuable benchmark data that will help guage how your own organization stacks up compared with others.

Download the Report:
http://go.dome9.com/cloud-security-spotlight-report-2017.html

#1 Barrier to Cloud Adoption: Security

Security concerns continue to top the list of barriers to cloud adoption, unchanged from last year's survey. This is followed by lack of expertise and qualified staff, jumping to the second highest ranking issue from the number five spot in the previous survey. The third ranking barrier to cloud adoption today is integration of cloud with existing IT environments, up one spot compared to last year's ranking.

The risk of data loss, and concerns about data privacy and regulatory compliance keeps CISOs up at night, making security risks the single biggest factor holding back faster adoption of cloud computing. This is pushing organizations and their security teams to implement robust security controls that help unlock the full potential of the cloud.

Biggest Cloud Security Threats

Specifically, unauthorized access through misuse of employee credentials and improper access controls pose the single biggest threat to cloud security. This is followed by hijacking of accounts and insecure API interfaces - all virtually unchanged from last year's survey.

The good news: all these security risks can be addressed by robust cloud security controls to provide deep visibility, multi-factor authentication and policy automation for verifiable and comprehensive security management.

Mind the Gap: Traditional Security Tools Don't Work in the Cloud

Traditional security tools have not been designed for cloud environments and their unique challenges. The need to secure cloud access from anywhere across highly dynamic, virtual cloud environments simply breaks the traditional network perimeter defense approach designed to secure traditional datacenters. The survey results confirm that traditional tools are woefully inadequate in securing the cloud - unchanged from last year's survey. The gap is primarily in controlling and verifying security policies, and providing deep visibility into cloud infrastructure security.

Cloud Security Headaches

The result of this gap: Visibility into cloud infrastructure rises to the top as the biggest security management headache, moving up from being the #2 cloud management concern in the previous year. Compliance concerns comes in second, while setting consistent, verifiable security policies remains the third biggest cloud security headache.

ABOUT DOME9 SECURITY

Dome9 delivers verifiable cloud infrastructure security and compliance to all businesses at all times across all public clouds. The Dome9 Arc SaaS platform leverages cloud-native security capabilities and cloud-agnostic policy automation to bring comprehensive network security, advanced IAM protection, and continuous compliance to every public cloud environment. Dome9 offers technologies to assess security posture, detect misconfigurations, model gold standard policies, protect against attacks and insider threats, and conform to security best practices in the cloud. Enterprise organizations to SMBs use Dome9 Arc for faster and more effective cloud security operations, pain-free compliance and governance, and rugged DevOps practices. Learn more at **www.dome9.com.**