Cloud Services and Security Spotlight

Demetrias Rodgers, CCSP, CISSP
Enterprise Services Director
Commonwealth Security Conference
April 12, 2019
Organizations of all sizes are continuing to adopt cloud computing at a rapid pace in order to benefit from increased efficiency, better scalability, and faster deployments.

This increasing shift to the cloud has not decreased the concerns about security, data, systems, and services. Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes; making it critical that organizations are focused on cloud security posture management processes and tools to proactively and reactively identify and remediate mistakes.
Cloud Passage Cloud Security Survey

1. **Cloud security concerns** – While adoption of cloud computing continues to surge, security concerns are showing no signs of abating. Reversing a multi-year downward trend, nine out of ten cybersecurity professionals confirm they are concerned about cloud security, up 11 percentage points from last year’s cloud security survey. The top three cloud security challenges include protecting against data loss and leakage (67 percent), threats to data privacy (61 percent), and breaches of confidentiality (53 percent).

2. **Biggest threats to cloud security** – Misconfiguration of cloud platforms jumped to the number one spot in this year’s survey as the single biggest threat to cloud security (62 percent). This is followed by unauthorized access through misuse of employee credentials and improper access controls (55 percent), and insecure interfaces/APIs (50 percent).

3. **Cloud security headaches** - The top three security control challenges SOCs are struggling with are visibility into infrastructure security (43 percent), compliance (38 percent), and setting consistent security policies across cloud and on-premises environments (35 percent).

4. **Legacy security tools limited in the cloud** - Only 16 percent of organizations report that the capabilities of traditional security tools are sufficient to manage security across the cloud, a 6 percentage point drop from our previous survey. Eighty four percent say traditional security solutions either don’t work at all in cloud environments or have only limited functionality.

5. **Paths to stronger cloud security** – For the second year in a row, personnel training and certification of IT staff (57 %) ranks as the most popular path to meet evolving security needs. 50 percent of respondents use their cloud provider’s security tools and 35 percent deploy third-party security software to ensure the proper controls are implemented.

6. **Cloud security budget increase** – Close to half of organizations (49 percent) expect cloud security budgets to go up, with a median increase of 28 percent.
Cloud Security Concerns

- While cloud providers offer many security measures, customer organizations are ultimately responsible for securing their own workloads in the cloud. The top three cloud security challenges highlighted by cybersecurity professionals in our survey are protecting against data loss and leakage (67 percent), threats to data privacy (61 percent), and breaches of confidentiality (53 percent).
Biggest Cloud Security Threats

- Misconfiguration of the cloud platform is the number one threat to cloud security as of the 2018 cloud survey.
- The second item is unauthorized access via misuse of credentials and improper access controls (55 percent), and insecure interfaces/API’s (50 percent).
Cloud Security Continued

- High levels of automation and user self service capabilities in public cloud IaaS and PaaS service has magnified the importance of correct cloud configuration and compliance. A single mistake can immediately expose thousands of systems or large amounts of sensitive data.

- The lack of comprehensive visibility into programmatic cloud infrastructure also contributes to the issues because incorrect and non-compliant configurations may go undetected for extended periods of time.

- What does this mean? While cloud provider infrastructure in itself is secure, enterprises do not usually have the processes, tools, and maturity levels to use the cloud securely.

- It's recommended that organizations look to adopt a Cloud security posture management framework (CSPM) strategy that embraces a continuous Risk and Trust assessment (CARTA) approach.

- This approach should be extended into development to identify and remediate risks prior to production.

www.vita.virginia.gov
Cloud Security Posture Management

Source: Gartner (January 2019)
Cloud Services Security - Challenges

- As enterprises place more services in the public cloud and as the public cloud providers introduce more infrastructure and platform services directly into the hands of developers, it is becoming increasingly complex and time-consuming to answer the seemingly straightforward question;

- How can you determine if the services are being used securely? Does the configuration of my cloud services add additional risk?

- CSP’s have multiple services, i.e. AWS has more than 160 different services.
  - Simple misconfiguration issues (such as AWS S3 buckets) represent significant risk and occur frequently as seen in some of the public disclosures for publicly exposed S3 buckets.

- The adoption of serverless PaaS (such as AWS Lambda and Azure functions) further complicate security. With serverless PaaS, there is no traditional OS or VM for IT to use as a control point and the problem of correct configuration becomes even more critical.

- IaaS and PaaS capabilities are built to be “self-service” for developers, removing IT and information security from the planning and deployments.

- Developers aren’t security experts, yet they are being asked to make security and risk decisions (such as the use of encryption, key management, service authorization, the use of API gateways, and so on). Without additional visibility and control, mistakes and misconfigurations are inevitable.

- Making it more critical for security to be integrated into the development pipeline.
Cloud Security – Effective Technologies

• As always Data and Network encryption technologies top the list as the most effective security technologies.

What security technologies and controls are most effective to protect data in the cloud?

64% Data encryption
54% Network encryption (VPN, packet encryption, transport encryption)
52% Security Information and Event Management (SIEM)
51% Trained cloud security professionals

50% Intrusion detection and prevention
49% Vulnerability assessment
49% Access control (e.g., CASB/Cloud Access Security Brokers)
47% Log management and analytics
47% Privileged Access Management (PAM)
46% Data leakage prevention

2018 cloud security Report
www.vita.virginia.gov
Here are the five key confidence boosters organizations stated that would alleviate their security concerns.

1. Encrypting data at rest (49 percent)
2. API’s for reporting, auditing and alerting on security events (46 percent)
3. Setting and enforcing security policies across clouds?

Which of the following would most increase your confidence in adopting public clouds?

- Encryption of data-at-rest: 49%
- APIs for reporting, auditing and alerting on security events: 46%
- Setting and enforcing security policies across clouds: 45%
- Automating compliance: 39%
- Creating data boundaries: 39%
- Isolation/protection of virtual machines: 33%
- Limiting unmanaged device access: 31%
- Leveraging data leakage prevention tools: 29%
- Protecting workloads: 19%

Not sure/other 15%
Cloud Adoption

- SaaS remains the most deployed cloud model (52 percent) as software stacks are maturing, followed by IaaS (36 percent) and PaaS (28 percent), both showing strong adoption by organizations.

What is your organization’s adoption of cloud computing?

- **SaaS** (Software as a Service, e.g., CRM, ERP, HR apps, collaboration, productivity tools): 52% Deployed/in production, 16% Currently implementing, 9% Trial/pilot in progress, 10% Planning to deploy, 13% No plans to deploy
- **IaaS** (Infrastructure as a Service, e.g., storage, servers, networking): 36% Deployed/in production, 18% Currently implementing, 17% Trial/pilot in progress, 15% Planning to deploy, 14% No plans to deploy
- **PaaS** (Platform as a Service, e.g., database, middleware, application servers): 28% Deployed/in production, 19% Currently implementing, 14% Trial/pilot in progress, 18% Planning to deploy, 21% No plans to deploy
- **BPaaS** (Business Process as a Service): 11% Deployed/in production, 9% Currently implementing, 9% Trial/pilot in progress, 18% Planning to deploy, 53% No plans to deploy
- **FaaS** (Function as a Service, e.g., develop, run, and manage application functionalities): 10% Deployed/in production, 8% Currently implementing, 10% Trial/pilot in progress, 16% Planning to deploy, 56% No plans to deploy
Over forty percent of organizations say their primary cloud deployment strategy is a hybrid cloud.

What is your primary cloud deployment strategy?

- **30%** Single Cloud
- **30%** Multi-Cloud (e.g., multiple providers without integration)
- **40%** Hybrid (e.g., integration between multiple providers, managed as a single cloud)
Most Common Workloads

- As organizations become more comfortable using cloud services, more are considering cloud for broader categories of services.
  - The top 3 are productivity applications, computing, and storage as illustrated below.

  What services & workloads is your organization deploying in the cloud?

- 48% Productivity applications
  - Email, collaboration, instant messaging, etc.

- 44% Storage
  - Object storage, archive, backup, etc.

- 40% Security
  - Identity management, access control, data protection, threat detection, usage & resource monitoring, anti-virus, etc.

- 39% Business applications
  - CRM, marketing automation, ERP, BI, project management, etc.

- 46% Computing
  - Servers, containers, etc.

2018 cloud security Report

www.vita.virginia.gov
Cloud Adoption Barriers

- The number one barrier to cloud is lack of qualified staff or expertise. Tied for second place are general security risks and integration with existing IT environments at 39 percent.

What are the biggest barriers holding back cloud adoption in your organization?

- Lack of staff resources or expertise: 42%
- General security risks: 39%
- Integration with existing IT environment: 39%
- Data security, loss & leakage risks: 38%
- Legal & regulatory compliance: 34%
- Loss of control: 27%
- Internal resistance and inertia: 24%
- Fear of vendor lock-in: 22%

2018 cloud security Report

www.vita.virginia.gov
Questions

Contact: Demetrias Rodgers
Demetrias.Rodgers@vita.virginia.gov