Virginia Information Technologies Agency

Cloud Services and Security Spotlight

Demetrias Rodgers, CCSP, CISSP
Enterprise Services Director

Commonwealth Security Conference
April 12, 2019

Cloud Security

Cloud Security – Introduction

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.

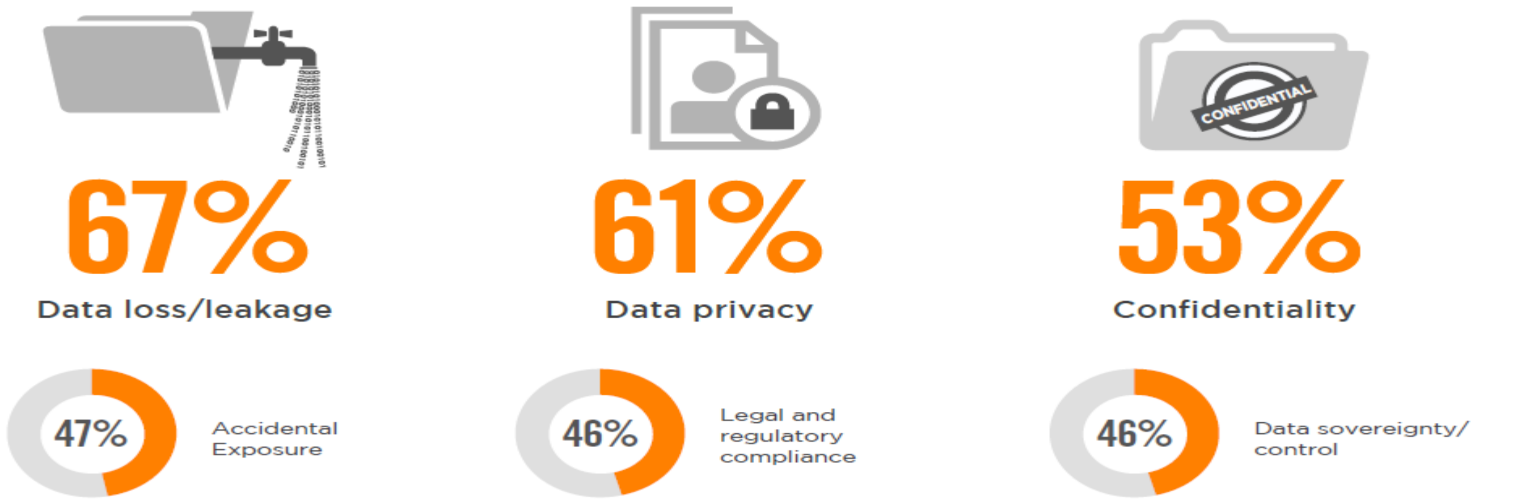
Cloud Passage Cloud Security Survey

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)

What are your biggest cloud security concerns?

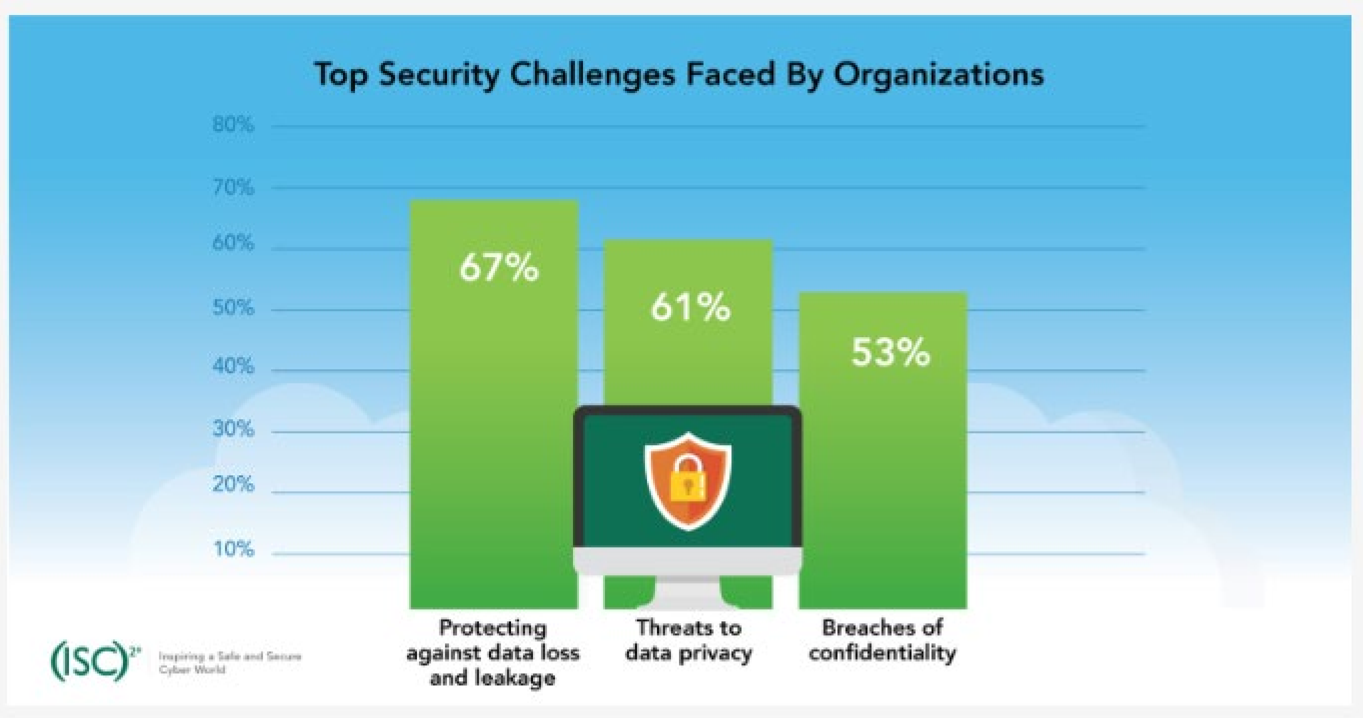


Lack of forensic data 37% | Incident response 35% | Visibility & transparency 34% | Fraud (e.g., theft of SSN records) 27% | Liability 25% | Availability of services, systems and data 21% | Business continuity 18% | Disaster recovery 18% | Performance 16% | Other 7%

2018 cloud security Report

Biggest Cloud Security Threats

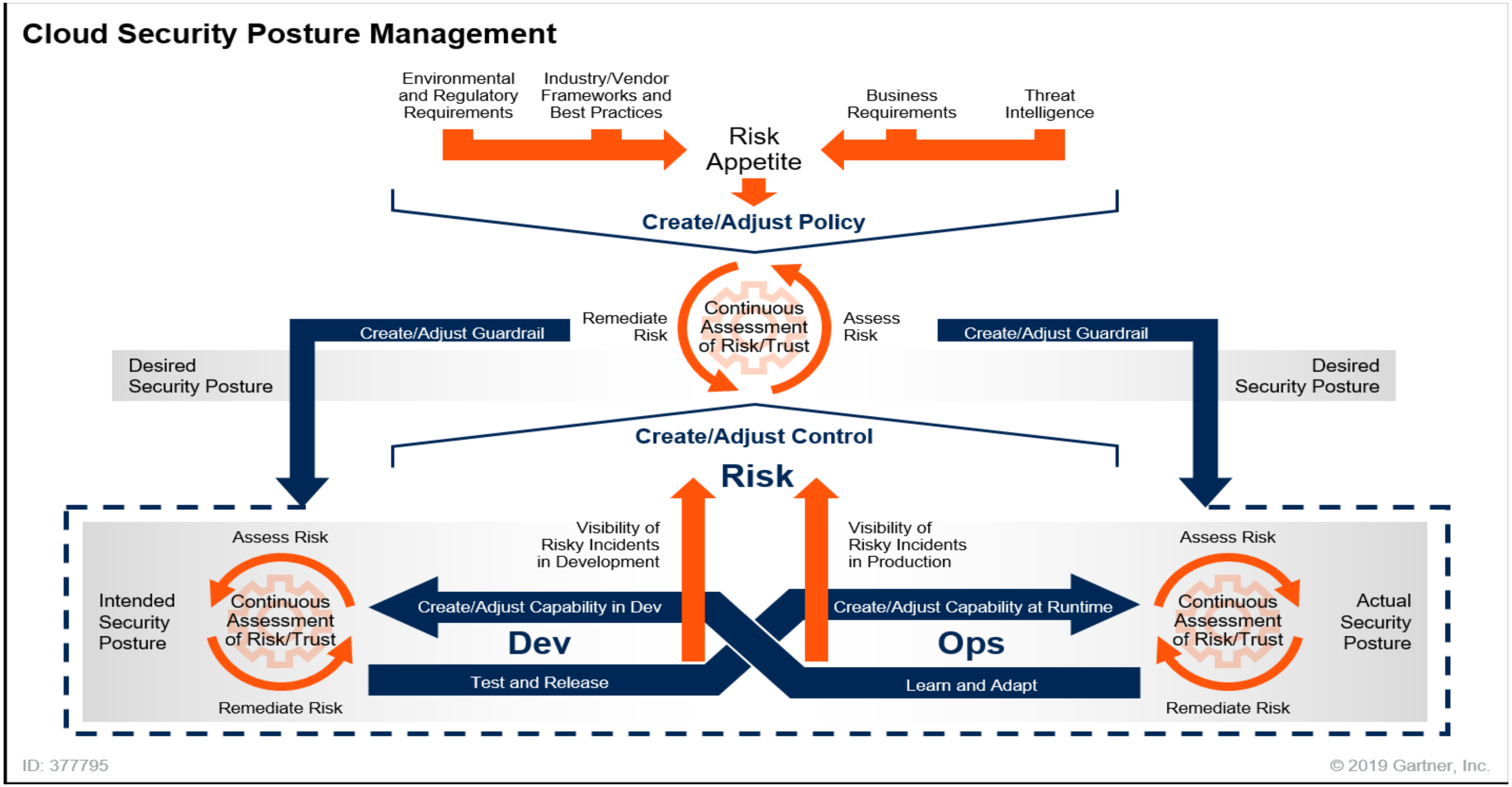
- Misconfiguration of the cloud platform is the number one threat to cloud security as of the 2018 cloud survey.
- The second item is unauthorized access via misuse of credentials and improper access controls (55 percent), and insecure interfaces/API's (50 percent).



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.
- Its 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.

Cloud Security Posture Management


Cloud Security Posture Management
Environmental and Regulatory Requirements
Industry/Vendor Frameworks and Best Practices
Business Requirements
Threat Intelligence
Risk Appetite
Create/Adjust Policy
Remediate Risk
Continuous Assessment of Risk/Trust
Assess Risk
Create/Adjust Guardrail
Create/Adjust Guardrail
Desired Security Posture
Desired Security Posture
Create/Adjust Control
Risk
Assess Risk
Visibility of Risky Incidents in Development
Visibility of Risky Incidents in Production
Assess Risk
Intended Security Posture
Continuous Assessment of Risk/Trust
Create/Adjust Capability in Dev
Dev
Test and Release
Create/Adjust Capability at Runtime
Ops
Learn and Adapt
Continuous Assessment of Risk/Trust
Actual Security Posture
Remediate Risk
Remediate Risk
ID: 377795
© 2019 Gartner, Inc.

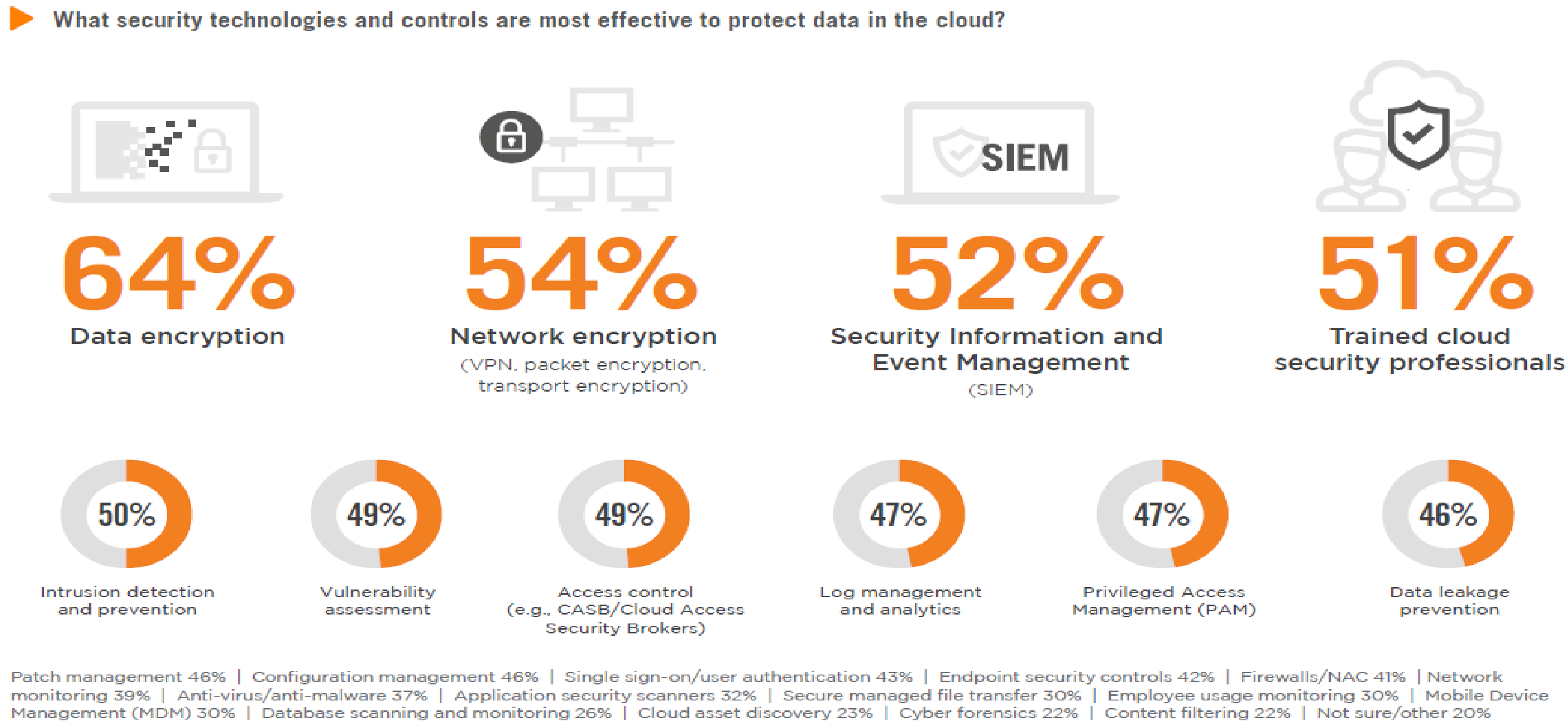
Source: Gartner (January 2019)

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)

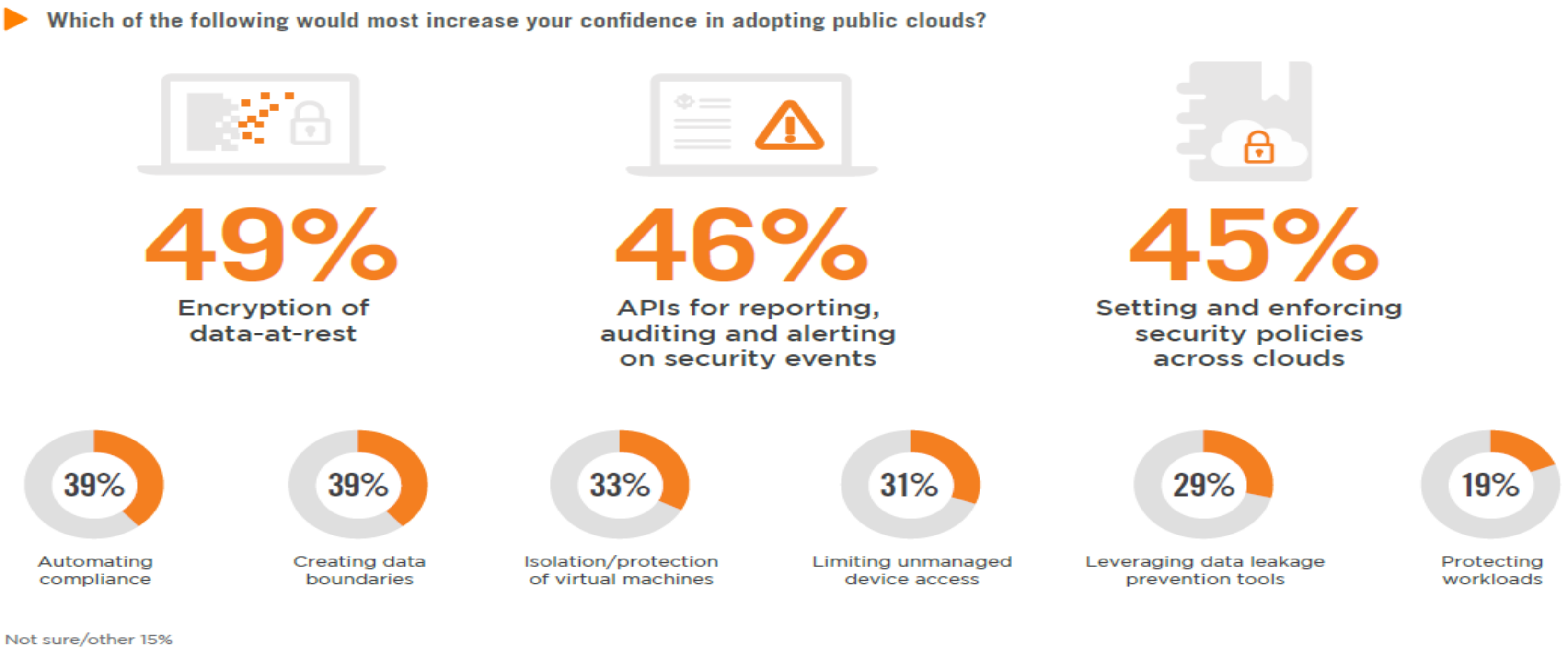
46% Data leakage prevention

Patch management 46% | Configuration management 46% | Single sign-on/user authentication 43% | Endpoint security controls 42% | Firewalls/NAC 41% | Network monitoring 39% | Anti-virus/anti-malware 37% | Application security scanners 32% | Secure managed file transfer 30% | Employee usage monitoring 30% | Mobile Device Management (MDM) 30% | Database scanning and monitoring 26% | Cloud asset discovery 23% | Cyber forensics 22% | Content filtering 22% | Not sure/other 20%

2018 cloud security Report

Cloud Confidence Builders

- 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?

49% Encryption of data-at-rest

46% APIs for reporting, auditing and alerting on security events

45% Setting and enforcing security policies across clouds

39% Automating compliance

39% Creating data boundaries

33% Isolation/protection of virtual machines

31% Limiting unmanaged device access

29% Leveraging data leakage prevention tools

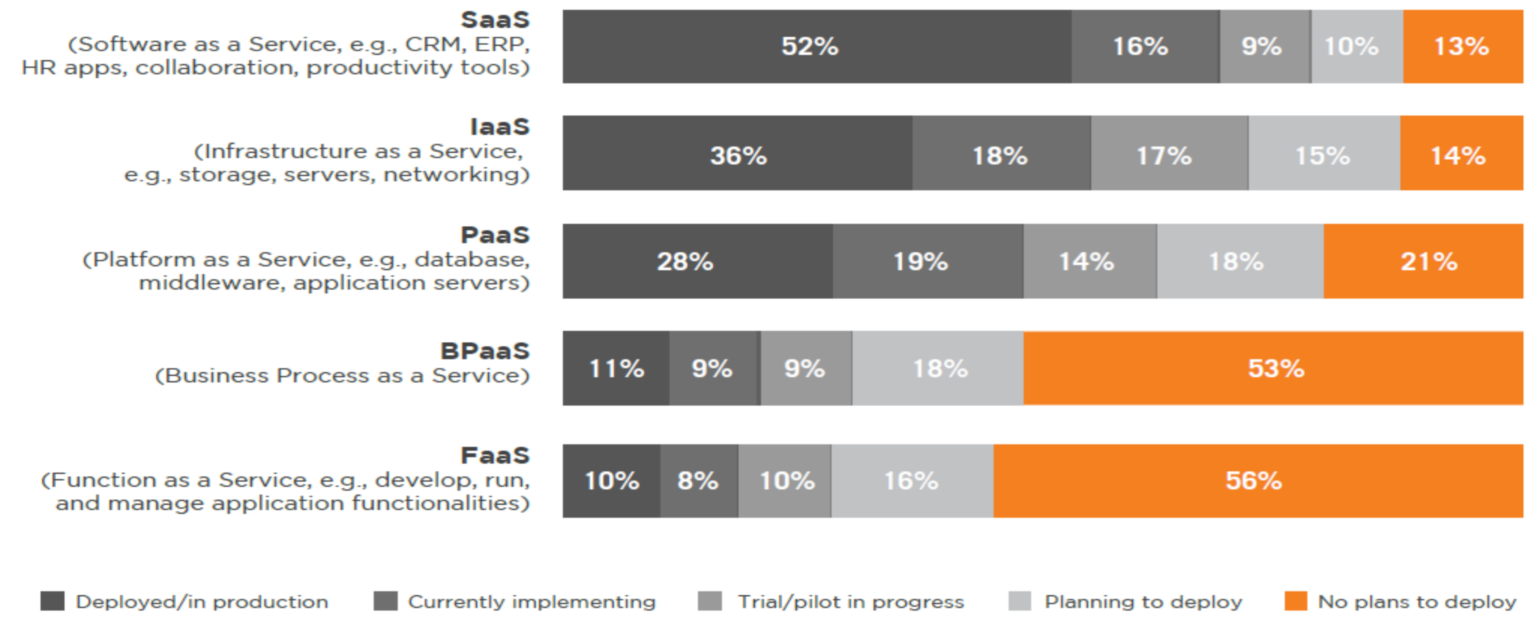
19% Protecting workloads

Not sure/other 15%

2018 cloud security Report

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.



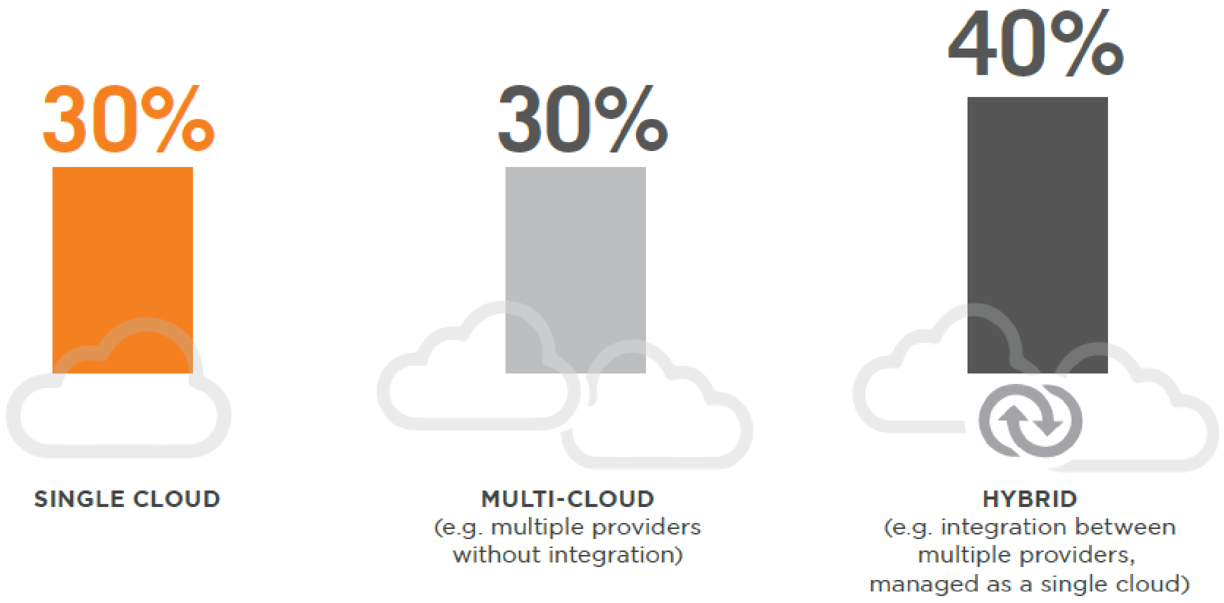
What is your organization's adoption of cloud computing?

2018 cloud security Report

Cloud Strategy

- Over forty percent of organizations say their primary cloud deployment strategy is a hybrid cloud.

What is your primary cloud deployment strategy?

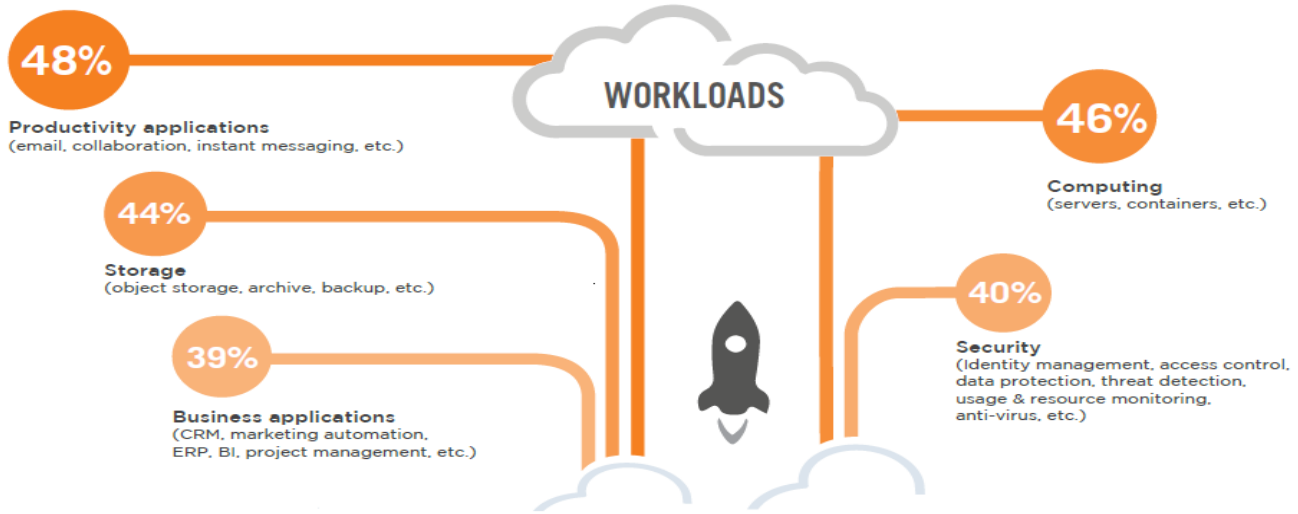


2018 cloud security Report

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.)

46%
Computing
(servers, containers, etc.)

44%
Storage
(object storage, archive, backup, etc.)

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

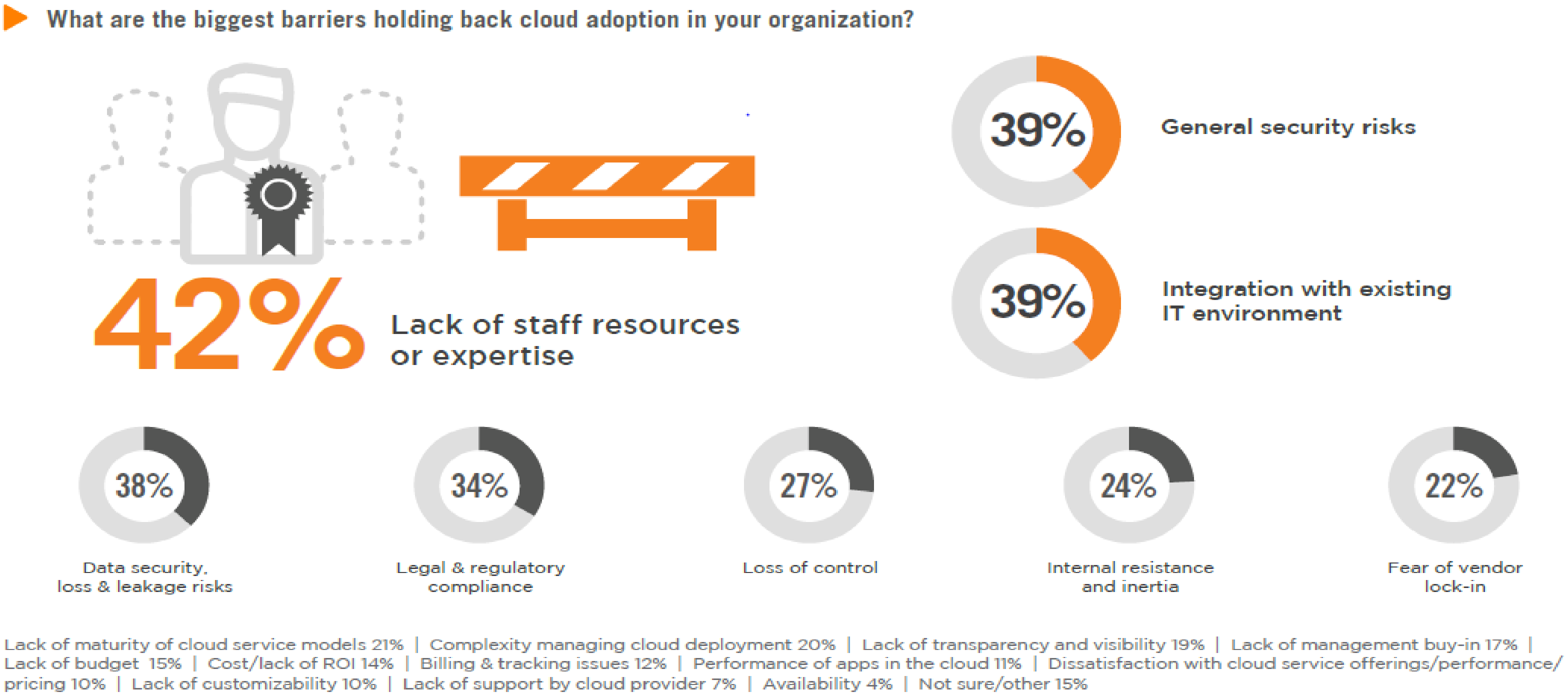
39%
Business applications
(CRM, marketing automation, ERP, BI, project management, etc.)

Database (relational, NoSQL, caching, etc.) 37% | Virtualization 37% | Developer/Testing Applications 37% | Networking (virtual private cloud, DNS, etc.) 34% | IT Operations Applications (administration, backup, provisioning monitoring, etc.) 31% | Operating System 29% | Middleware 17% | Runtime 10% | Not sure/other 22%

2018 cloud security Report

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 maturity of cloud service models 21% | Complexity managing cloud deployment 20% | Lack of transparency and visibility 19% | Lack of management buy-in 17% | Lack of budget 15% | Cost/lack of ROI 14% | Billing & tracking issues 12% | Performance of apps in the cloud 11% | Dissatisfaction with cloud service offerings/performance/ pricing 10% | Lack of customizability 10% | Lack of support by cloud provider 7% | Availability 4% | Not sure/other 15%

2018 cloud security Report

Questions

Contact: Demetrias Rodgers

Demetrias.Rodgers@vita.virginia.gov