Introduction

As enterprises continue to seek scalability, flexibility and efficiency in their technology stack, utilization of cloud platforms in their various models becomes very attractive. For many organizations, the CIO’s strategy for information technology is to adopt cloud-based services first and seek on-premise implementation as an alternative if cloud options do not meet business needs. While in some cases a cloud service may be more secure than a similar service hosted internally, this is not an assumption that can be applied universally. It is critical for information security professionals to attain a baseline understanding of cloud computing, the various consumption models and services as well as the associated risks. Additionally, information security professionals must develop strategies that empower the business’ consumption of critical cloud services while adopting the necessary and prudent security measures, balancing the risk versus reward of cloud computing.

According to research from Netskope’s Cloud Report for January 2015, the typical enterprise has on average 613 cloud applications in use, with 88.1 percent of those not considered enterprise ready. Even more staggering is the fact that over 20 percent of enterprises have 1,000 or more cloud applications in use by their organization. These figures clearly demonstrate the necessity for effectively understanding and managing the security of enterprise cloud adoption.

The goal of this primer is to educate security professionals on the various cloud computing services available to the enterprise, their most common use-cases, and to identify key risks in these areas. Additionally, we will identify a series of leading practices and recommended activities that should be undertaken by information security professionals to proactively support the move of systems, data and critical business processes to the cloud.

Meeting Business Needs

The adoption of cloud computing is a clear reaction to the business’ need for agility, elasticity and cost-effective IT solutions. In addressing business needs, security professionals are in a rare position to address security early on in adoption cycles or even propose more secure alternatives to existing insecure practices before they become the norm in the organization. It is important, however, to first understand the most commonly utilized cloud services.

Commonly Consumed Cloud Services and Associated Risks

Storage

One of the most common and underestimated uses of cloud services in the enterprise is cloud storage. Examples include Dropbox, Box, Google Drive, Microsoft’s OneDrive and many other similar services. Popular due to their cross-platform utility, these cloud storage services offer varying levels of security to both enterprise users and consumers.
One example of this is Dropbox, which offers a consumer-level cloud storage (dubbed “freemium”), but also offers an enterprise product with security controls such as remote wipe, audit logging and single sign-on functionality in addition to disallowing users from having multiple accounts per device [2].

A key risk commonly overlooked by even security professionals is when cloud storage services are used for data exfiltration by an attacker. This is because it is very difficult to distinguish between an employee who is legitimately using a cloud storage service or malware copying sensitive files out to be stolen. This type of covert use is being utilized by criminals with little risk of being caught. Additionally, developers are likely to adopt cloud storage on Amazon S3 or Microsoft’s Azure platforms in order to address dynamic storage needs within their applications. While this may be speed development and testing cycles, it may also increase risk if not addressed appropriately. For example, it is not uncommon for developers to leverage production data for testing purposes.

**Collaboration**

Employees commonly utilize cloud collaboration platforms such as Yammer, Jive, Basecamp and Evernote to chat, share information and collaborate on ideas from across the office or across the globe without even a second thought that these are cloud services. The potential for increased productivity has created a rush of adoption faster than IT and information security can provide vetted solutions.

Two key risks with collaboration platforms are ownership of data placed in the cloud service and the potential of bypassing corporate governance and data security mechanisms. Employees seeking productivity gains may unintentionally expose sensitive corporate data outside the controlled environment into cloud services platforms that provide little to no protection for access control, audit trail, or even property ownership rights in some cases.

**Enterprise Applications**

Many enterprises are finding scale, efficiency, and cost-effectiveness in pushing enterprise applications to cloud providers. Whether through an office platform like Microsoft’s Office365 suite, CRM such as NetSuite or Salesforce, or other enterprise applications for internal consumption, the CISO must understand the implications of moving these essential tools hosting sensitive information into a multi-tenant environment and outside the corporate perimeter. Key risks include data ownership, governance, and fundamental security controls. Focus on addressing confidentiality, integrity, and availability concerns of back-end processes including access to data and systems by administrators, sufficient logging, multi-tenant segmentation, forensics/incident response and of course liability.
Cloud Security Defined

While cloud security has been described in many different ways, Accuvant defines Cloud Security as:

Cloud Security n. - 1. The security and risk management mechanisms and operational processes supporting the cloud computing IT model. (As defined by NIST SP800-145[1].)

Components of Cloud Security Marketplace

The cloud security marketplace can be broken down into three categories, as follows:

- Service discovery – Tools and platforms which core features provide the capabilities to discover and understand the cloud services and tools that are currently being utilized.

- Data security – Tools that provide direct security value, such as authentication, encryption, data loss prevention, and logging to the data being pushed out to cloud services and platforms.

- Service governance – Tools designed to limit or otherwise control the consumption of cloud services or platforms.

Operationalizing Cloud Security

Fundamentals

As a consumer of a cloud platform, application or service, it is the customer’s responsibility to understand the inner-workings of the cloud model and inherent risks with applicable available controls. This includes understanding not only the services being provided but the back-end processes including governance, physical security, network security and other critical controls. The Cloud Security Alliance (CSA) maintains an active body of work titled the Cloud Controls Matrix, or CCM, currently in version 3.0.1 (here: https://cloudsecurityalliance.org/research/ccm/), which provides an excellent way to understand common available security controls for cloud services.

As of January 2015, 88.1 percent of cloud apps aren’t enterprise-ready, per Netskope research.
Leveraging Cloud Security

A cloud security program strategy extends existing security capabilities into cloud services and provides additional abilities to detect and respond to security threats, while meeting the business need for flexibility and agility in IT services. It is critical that the security organization have reasonably developed and operationalized security fundamentals that can be extended to cover cloud services. There are three key security capabilities that become more pronounced when addressing cloud services:

- **Security Validation and Testing** – The ability to effectively test and validate the security of the infrastructure, platform or application is critical to security. This includes but is not limited to auditing, vulnerability scanning, software security testing, patching and penetration testing. Effectively extending existing security capabilities into the cloud often requires additional specialized skills and an understanding of the cloud consumption model, risks, and architectures.

- **Logging and e-Discovery** – Incorporating the ability to extract, consume and analyze logging information and data artifacts from cloud services into an existing platform must be done to provide a complete security picture of the organization. Also, the extension of existing e-discovery capabilities into cloud services are required to comply with applicable regulations.

**IaaS – Infrastructure as a Service**

Infrastructure as a service (IaaS) is a standardized, highly automated offering, where compute resources, complemented by storage and networking capabilities are owned and hosted by a service provider and offered to customers on-demand. Customers are able to self-provision this infrastructure, using a Web-based graphical user interface that serves as an IT operations management console for the overall environment. API access to the infrastructure may also be offered as an option. [1]

**PaaS – Platform as a Service**

Platform as a service (PaaS), usually depicted in all-cloud diagrams between the SaaS layer above it and the IaaS layer below, is a broad collection of application infrastructure (middleware) services, including application platform, integration, business process management and database services. [2]

**SaaS – Software as a Service**

Software as a service (SaaS) is defined as software that is owned, delivered and managed remotely by one or more providers. The provider delivers software based on one set of common code and data definitions that is consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on use metrics. [3]
• Forensics and Incident Response – Extending forensics and incident response operations into cloud services requires additional skill sets, tools and methodologies, and means addressing alerting, triage and incident management. These capabilities should already be operationalized within the enterprise to then be extended into cloud services effectively.

Developing a Program Strategy Approach

With a foundational understanding of cloud services and their associated risks, it is important for security organizations to develop a program strategy approach for cloud adoption. By first developing a strategy and operationalizing it into the existing security program, cloud security will become a component of security, rather than an outlier activity. Adopting a program strategy approach acts as a forcing function to perform due-diligence to discover, assess, understand and act upon business needs, depending if these are current or future requirements which warrant security consideration.

Phase 1 – Due Diligence and Discovery of Existing Services

Drivers
The critical initial step to addressing cloud security concerns is to assess existing business needs and current utilization of cloud services within the organization. Performing due-diligence through business needs analysis, and discovery through manual and automated means gives insight into how the organization is leveraging cloud services, and where the greatest risks that need to be immediately addressed lie.

Components

• Service discovery tools (network or endpoint-based) identify cloud services currently in use across enterprise assets and networks.

• Cross-functional needs analysis team representing departments including legal, procurement, human resources, audit and finance, privacy.

Capabilities

• Identify cloud services currently in use across the organization on corporate assets or data.

• Identify business needs and requirements for consumption of cloud services.

*Statistics courtesy of Netskope for January 2015
Operational Advice

• When performing discovery across an organization, start with high-risk assets or endpoints as this provides a risk-based analysis and doesn’t attempt to understand the entire organization at once, which can be overwhelming.

• Leverage tools wherever possible to address this issue at scale for speed and efficiency. Many existing network security platforms have the built-in ability to identify cloud services.

• When working through business due-diligence and requirements gathering, look for opportunities to provide the greatest gains in scalability, availability and efficiency together with cost management and security gains.

Phase 2 – Triage Existing Service Consumption

Drivers

Once the existing use of cloud services has been identified and requirements have been gathered from the business, the immediate next step is to triage and begin addressing pending needs. Taking a risk-based security approach must address highest-risk cloud services (based on data value, criticality to business support and privacy) in a phased manner. This includes providing stop-gap support in the immediate term tactically and developing a phased approach to strategically addressing the identified concerns and needs in the long-term. This allows the business to continue to function and meet its goals, while addressing security concerns in an organized and meaningful fashion.

Components

• Define high risk cloud services based on input and guidance from the cross-functional team.

• Use data security tools to address, where possible, data currently being deployed across cloud services to lessen the potential negative impact of an incident while maintaining usability and benefits of cloud services.

• Service governance tools control use of non-sanctioned cloud services through alerting, and increased visibility.

• Develop updated policies and procedures to address the additional operating models and risks of cloud services.

• Update the services catalog, which should include addressing business requirements on cloud services in a secure manner, providing necessary functionality while addressing risk.
Capabilities

• Provide security to address the immediate risks posed through discovered in-use and high risk cloud services.

• Discontinue the use of non-sanctioned cloud services, especially where the risk is considered inappropriate by the cross-functional team. Where possible, offer viable alternatives that meet business requirements.

• Update policies and procedures which address the additional risks and opportunities, providing guidelines and requirements for adding new cloud services.

Operational Advice

• Focus on adding security to address immediate critical risks posed through existing high-risk cloud services. Set up monitoring for all moderate and low-risk services while investigating more secure alternatives, and update policies and operating guidelines.

Phase 3 –Develop Strategy and Address Future Needs

Drivers

Once the initial critical risks have been addressed, security must shift from tactical to strategic operation and focus on long-term gains. Creating a strategy which includes methods for onboarding additional necessary cloud services and vetting by security allows security to begin to lead innovation and help drive business value rather than continually operating in crisis and triage mode.

Components

• Update program strategy to address the unique needs of cloud service platforms in conjunction with existing security requirements on internal systems, applications and procedures.

• Update technical architecture, including budget impacts, to address security services such as user authentication, account provisioning, data loss prevention, vulnerability and application scanning, security monitoring, etc.

• Define policy and operational practices across the life-cycle from contracts, validation, incident response, data retention and decommissioning across all known and unknown cloud services.
Capabilities

- Address cloud security concerns across the utility life-cycle.
- Provide streamlined procedures for onboarding, utilization, modification and retirement of cloud services.
- Integrate technical architecture and appropriate budget identified to address on-premise and cloud security requirements.

Operational Advice

- Key focus should be given to developing a strategy, which can be readily operationalized and modified as needed to create frictionless support for business needs.
- Work to anticipate business needs and have options ready for when requirements and needs arise, decreasing the need to fire-drill on demand.
- It is critical to address security concerns across all points from requirements to retirement throughout the system life-cycle.

Phase 4 – Operationalize Program Strategy

Drivers

Implementing and operationalizing program strategy allows the security organization to get away from being tactical and reactionary and move to a strategic and innovative mode of operation. This decreases the internal friction and minimizes the possibility for security incidents due to predictable errors.

Components

- Perform service discovery to address “unsanctioned cloud service usage” as it may appear across the enterprise.
- Data security tools and procedures should be in place to facilitate “safe” cloud service consumption where appropriate and necessary.
- Service governance capabilities are required to work in conjunction with discovery tools not only for identification of unauthorized usage but also to ensure compliance with licensing and legal policies and compliance regulations.
- Implement testing, validation and audit procedures to ensure that policy and strategy are being properly implemented and followed.
Capabilities

- Operationalized cloud security strategy addresses needs and requirements along the system life-cycle.
- Ability to detect, isolate and effectively address unsanctioned cloud services usage.
- Ability to test, validate and audit cloud security strategy in practice.

Operational Advice

- Test the strategy and operational implementation extensively, both in terms of addressing business needs and addressing potential incidents.
- Ensure internal procedures are updated for cloud service utilization, including non-technical functions such as call lists, compliance procedures, audit policies and service level agreements (SLAs).
- Revisit the strategy on an ongoing basis and at least annually with key stakeholders given the rapidly evolving nature of cloud services and information risk management practices.

Next Steps

As companies and business units are increasingly looking to the cloud to leverage services and platforms that enable their business to operate with greater agility, it is essential that information security professionals are viewed as enablers. Through measured steps and collaboration with key stakeholders, leveraging cloud services will be less disruptive to the information security organization and more rewarding for the company.

As the business continues to push services into the cloud, security is no doubt following suit. This creates an opportunity for security professionals to not only create a “secure by design” condition for enabling the business through technology, but to also lay the foundation for additional cloud-based security services if risks can be reduced while increasing productivity and agility. Taking a systematic, strategic approach to cloud adoption and security is essential to creating a strong business-aligned security program, which ultimately benefits security organizations as well.
Contribution to this document from:

Michael St. Vincent
Paul Hershberger
Jason White
Robb Reck

References


Thank you to Netskope for supplying the data referenced within this paper. www.netskope.com
Accuvant, a Blackstone (NYSE: BX) portfolio company, is the leading provider of information security services and solutions serving enterprise-class organizations across North America. The company offers a full suite of service capabilities to help businesses, governments and educational institutions define their security strategies, identify and remediate threats and risks, select and deploy the right technology, and achieve operational readiness to protect their organizations from malicious attack. Founded in 2002, Accuvant has been named to the Inc. 500|5000 list of fastest growing companies for the last eight consecutive years. The company is headquartered in Denver, Colo., with offices across the United States and Canada. Further information is available at www.accuvant.com.

© 2015 Accuvant, Inc. All Rights Reserved. “Accuvant” is a registered trademark of Accuvant, Inc.