OPTIV

CLOUD SECURITY

Solution Primer

Rafal Los
Director, Solutions Research
Office of the CISO, Optiv

Renee Guttmann
Vice President, Information Risk, Optiv

Jason Clark
Chief Strategy and Security Officer, Optiv

Introduction

Enterprises are moving to cloud to provide scalability, flexibility and efficiency across their technology stack. In many cases, a CIO's information technology strategy has shifted to adopting a **cloud-first** strategy with migration to an on-premise implementation as an alternative.

While some cloud services and applications may be more secure than on-premise solutions, this is not an assumption that can be universally applied. Information security professionals must attain a baseline understanding of cloud computing to implement security measures and strategies that empower business users – balancing risk versus reward of cloud computing.

Complicating the landscape, users are adopting a variety of cloud offerings more rapidly than IT organizations can sanction (and secure) them. According to Netskope's January 2015 Cloud Report, the typical enterprise has *on average* 613 cloud applications in use, with 88.1 percent not considered enterprise-ready, in other words, lacking robust enterprise security features. Further, more than 20 percent of enterprises have at least 1,000 cloud applications in use. These figures clearly demonstrate the need for strategically managing and securing enterprise cloud services.

The goal of this primer is to educate security professionals on the various cloud computing services available to enterprises, the most common cloud use-cases, and to identify key risks in these areas. Finally, the primer will identify a series of recommended activities to tactically and strategically support the move of systems, data and critical business processes to the cloud.

Cloud Security Defined

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

"...The security and risk management mechanisms and operational processes supporting the cloud computing IT model, as defined by NIST SP800-145[1]."

Meeting Business Needs

The adoption of cloud computing is a clear reaction to enterprises' need for agility, elasticity and cost-effective IT solutions. **In mature organizations, security professionals are in a rare position to address security early on in**

adoption cycles or even propose more secure alternatives that enable the adoption of innovative IT delivery.

Security professionals should first understand what is motivating the CIO and senior management to pursue cloud options and how the current cloud landscape can transform their enterprise's IT risk posture for better, or worse.

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, Google Docs 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 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.

According to Netskope's January 2015 Cloud Report, the typical enterprise has on average 613 cloud applications in use, with 88.1 percent not considered enterprise-ready. Further, more than 20 percent of enterprises have at least 1,000 cloud applications in use.

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, these applications offload non-core functions such as application delivery, achieve better uptime and provide increased cost-effectiveness and better security.

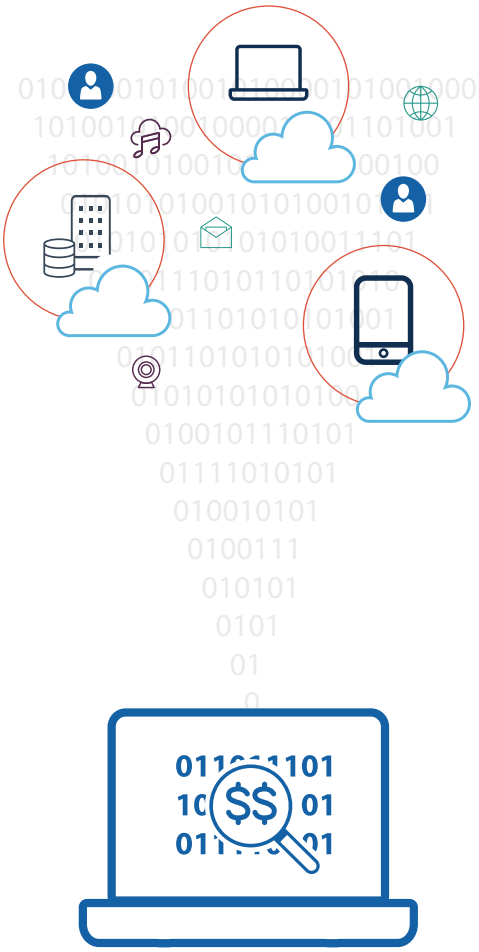
The CISO must understand the implications of moving these essential tools hosting sensitive information into a multi-tenant environment and outside the corporate perimeter. Key risks include data ownership, governance and fundamental security controls. Focus on addressing confidentiality, integrity and 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.

Components of the Cloud Security Marketplace

The cloud security marketplace can be broken down into three categories. These categories vary depending on whether services are consumed in the form of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), or in the form of Software as a Service (SaaS).

- Service discovery – Tools and platforms providing core capabilities to discover and understand the cloud services currently in use.
- Service governance – Tools designed to identify, limit or otherwise control the consumption of cloud services or platforms.
- Data security – Tools providing direct operational security value, such as: authentication, encryption, data loss prevention or logging of data being pushed out to cloud services and platforms.

Of these three categories of services, the first two—service discovery and governance—are often packaged together in CASB solutions to help secure current cloud application (SaaS) use. IaaS and PaaS still see a heavy reliance upon traditional security such as firewalls and endpoint tools but adapted to the cloud computing model of scale and rapid entropy. Beyond these three services are a number of functional elements of overall cloud security

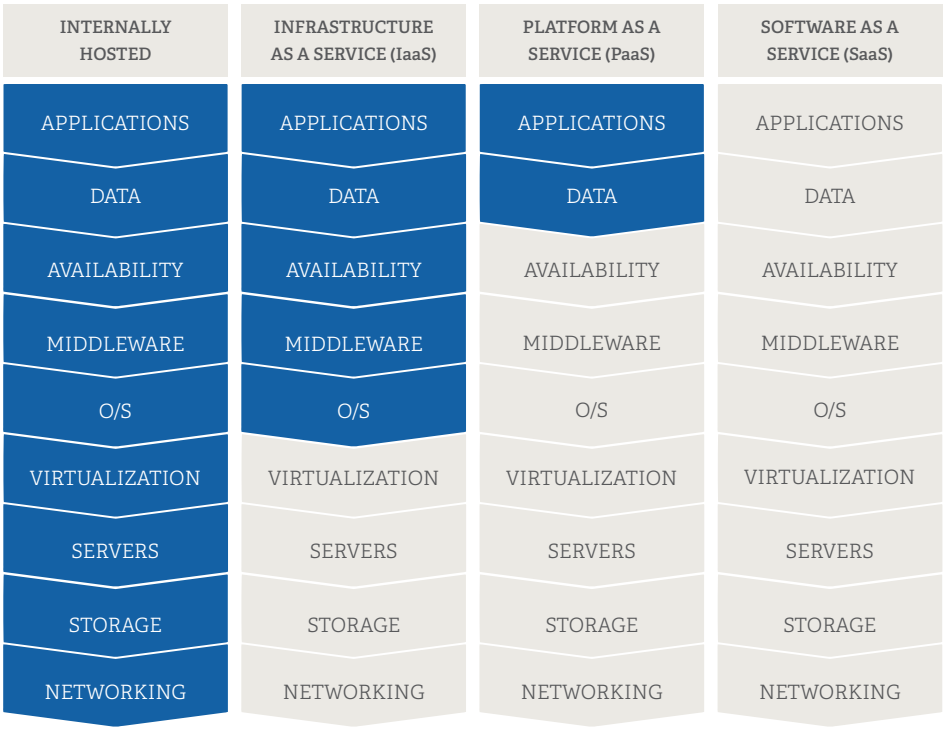


programs that we have aligned to the three models (SaaS, IaaS and PaaS) and across the various levels of organizational maturity.

Operationalizing Cloud Security

Fundamentals

As a consumer of a cloud platform, application or service, it is the customer's responsibility to understand the attributes of the cloud model and inherent risks, applying controls to the extent possible given the model, and managing SLAs always. This understanding includes not only the services being provided, but the back-end processes such as: 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.



BLUE is customer responsibility, while GRAY is provider responsibility.

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]

Leveraging Cloud Security

A cloud security program strategy extends existing security capabilities into cloud services to meet business needs for flexible and agile IT by providing additional abilities to detect and respond to security threats. It is critical that the security organization have reasonably developed and operationalized security fundamentals that can be extended to cover cloud services. Here are three of the most common security capabilities that must evolve the most when consuming cloud services-

- Logging and E-Discovery – Demand the ability to at least extract logging information and data artifacts from cloud services into an existing platform for analysis to provide a true security picture of the organization. Also, the extension of existing e-discovery capabilities into cloud services are required to comply with applicable regulations. These eDiscovery requirements should be addressed up front and tested if possible.

- 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.

- Forensics and Incident Response – Extending forensics and incident response operations into cloud services requires additional skillsets, 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. The cloud will make activities like (x, y and z) more difficult, while activities like (a, b and c) will be easier.

Developing a Program Strategy Approach

With the fundamentals of cloud security more firmly understood, security managers can move on to creating a program strategy for cloud adoption. Cloud control becomes an inherent part of security through a well thought out plan of which core security functions need to be enhanced, developed or torn down.

Create a program strategy with multiple and distinct phases to naturally lead teams to perform due-diligence to discover, assess, understand and act upon business needs

Phase 1 – Due Diligence and Discovery of Existing Services

Drivers

The critical initial step to addressing cloud security concerns is to assess 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, endpoint or proxy-based) identify cloud services currently in use across enterprise assets and networks.
- Cross-functional business needs analysis team representing departments including legal, procurement, human resources, audit and finance and privacy.

Capabilities

- Identification of cloud services currently in use across the organization on corporate assets or data.
- Identify business needs and requirements for consumption of cloud services.

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 ability to identify built-in 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 these 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 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

- Provision of security controls to address the immediate risks posed through discovered in-use and high risk cloud services, such as blacklisting and encryption of high risk data.
- Ability to selectively allow or disallow specific cloud services and/or functions within those services.
- Policy creation function that can rapidly update policies and procedures which address the additional risks and opportunities related to managing

Once the initial critical risks have been addressed, security must shift from tactical to strategic operation and focus on long-term gains.

cloud services. Also needed is a process for creating guidelines and requirements that help implement objectives in policy.

Operational Advice

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

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 them 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 protection, vulnerability and application scanning, security monitoring, etc.
- Define policy and operational practices across the lifecycle from contracts, validation, incident response, data retention and decommissioning across all known and unknown cloud services.

Capabilities

- Ability to address cloud security concerns across the utility lifecycle.
- Provision of streamlined procedures for onboarding, utilization, modification and retirement of cloud services.

- Ability to create technical architecture requirements that address on-premise and cloud security risks while also staying within the identified budget.

Operational Advice

- Develop a strategy which can be readily operationalized and modified as needed to create frictionless support for business needs.
- Anticipate business needs and have options ready for when requirements and needs arise, decreasing the need to fire-drill on demand.
- Address security concerns across the entire system lifecycle, from requirements to retirement.

Phase 4 – Operationalize Program Strategy

Drivers

The requirement to move from a reactionary mode of operation to a technical one is met by implementing and operationalizing program strategy. This results in a more fluid and seamless internal cloud security function. This decreases the internal friction and minimizes the possibility for security incidents due to predictable errors.

Components

- Continuous service discovery capabilities 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 rogue 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 lifecycle.
- Ability to detect, isolate and effectively address rogue 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

It is essential that security professionals are viewed as enablers as companies and business units are increasingly looking to leverage cloud. Through measured steps and collaboration with key stakeholders, cloud services can provide disruptive innovation, without exposing the enterprise to unnecessary risks.

There is an opportunity for security professionals to not only create a "secure by design" condition, **but to also lay the foundation for additional cloud-based security services.**

There is an opportunity for security professionals to not only create a "secure by design" condition, but to also lay the foundation for additional cloud-based security services.

References

1. The NIST definition of cloud computing - http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
2. Dropbox Support – "How do I allow only one Dropbox per computer?" - https://www.dropbox.com/help/4236
3. Cloud Security Alliance Guide, V3, "Security Guidance for Critical Areas of Focus in the Cloud." - https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

7.15 | F1