

The Challenges of Cloud Security

Javier Said Olivo

Regional Cloud Sales Specialist

The Cloud has Arrived!





IAAS

Infrastructure-as-a-Service allows you to deploy a variety of workloads and Services across someone else's hosting platform.

You have no access to the physical component of the environment, such as Compute, Storage or Network



PAAS

Platform-as-a-Service sits nicely in between the other Cloud Service models.

Typically it's used to develop Applications and Services that you cant buy as a SaaS and are either too expensive or to complex to run in laaS













SAAS

Software-as-a-Service simply allow you access to consume a particular Software Application running as a Service you connect to via the Internet.

You interact with the Application in it's native form typically with no ability to modify the Application itself.

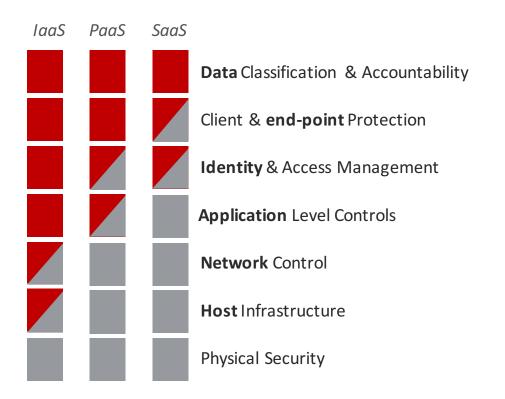
McAfee Confidential - Shared Under NDA McAfee | 2

The Cloud (First) Enterprise Challenges

Shared Responsibility

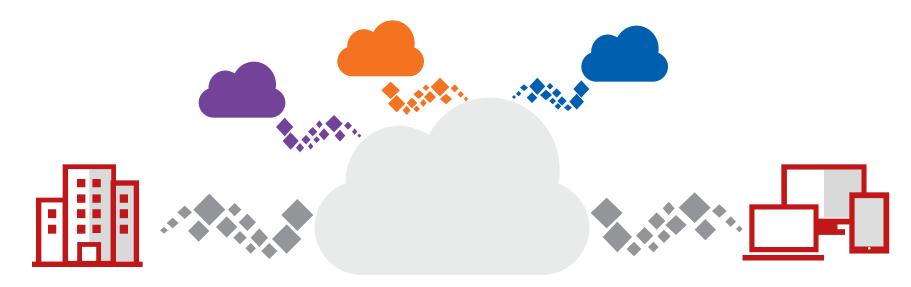


Service Provider Responsibility



McAfee Confidential - Shared Under NDA McAfee | 3

Network security fails to protect data in the cloud & mobile era

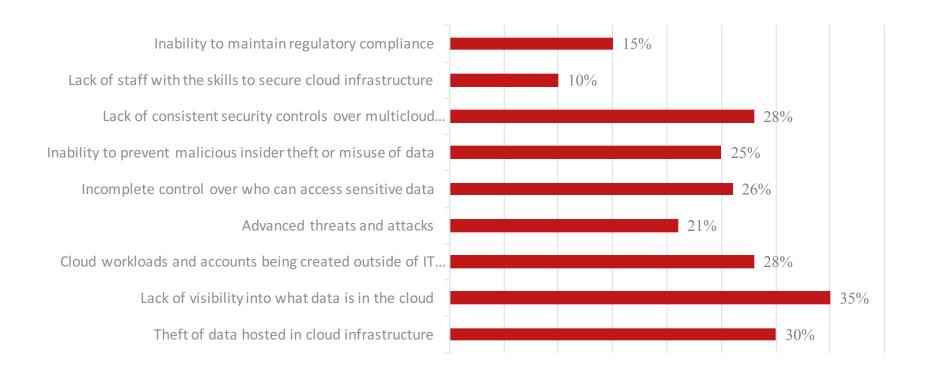


Data created natively in cloud is invisible to network security

50% of cloud traffic is cloud-tocloud and invisible to network security

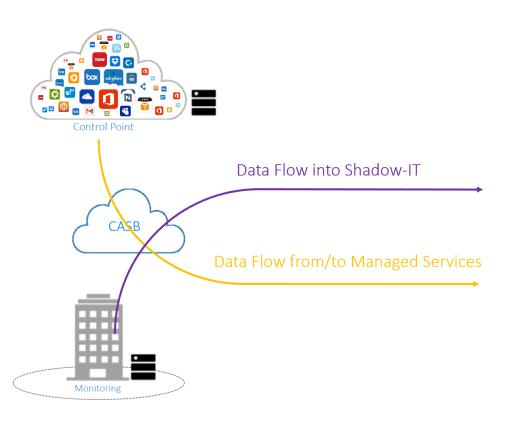
Data uploaded to cloud from mobile is invisible to network security

What do customers say?



Fuente: McAfee

Gartner's four areas of CASB security



Gartner

<u>Visibility:</u> CASBs provide shadow IT discovery and sanctioned application control, as well as a consolidated view of an organization's cloud service usage and the users who access data from any device or location.

Threat Protection: CASBs prevent unwanted devices, users and versions of applications from accessing cloud services. Other examples in this category are user and entity behavior analytics (UEBA), the use of threat intelligence and malware identification.

<u>Compliance:</u> CASBs assist with data residency and compliance with regulations and standards, as well as identify cloud usage and the risks of specific cloud services.

<u>Data Security:</u> CASBs provide the ability to enforce datacentric security policies to prevent unwanted activity based on data classification, discovery and user activity monitoring of access to sensitive data or privilege escalation. Policies are applied through controls, such as audit, alert, block, quarantine, delete and encrypt/tokenize, at the field and file level in cloud services.

Cloud Governance Maturity Model

Skyhigh Cloud Security and Governance Maturity Model: Business Outcomes

	VISIBILITY (Level 1)	THREAT PROTECTION (LEVEL 2)	COMPLIANCE (LEVEL 3)	DATA SECURITY (LEVEL 4)		
Shadow IT	 Discover Cloud Services & High Risk Services Usage Contextualized High Risk Services Report Egress Leakage Report Vendor Assessment AD Attribution & Governance laaS Discovery 	 High Severity Anomalies Repeat Offender Robotic Activity Data Exfiltration SIEM Integration & IR workflow Insider Threats and Advanced Threat protection (with SSL inspection) 	 Coaching and Blocking High Risk Services Ensuring Data Handling Policies and Endpoint DLP policies are in line with organization's cloud initiatives 	Investigate Unmatched Uploads for URLs/IP addresses not associated with a Cloud Service Provider (CSP)		
Sanctioned IT	1. Cloud Service Risk Audit (On-demand scanning) • Personal Sharing • PII/PCI/Custom DLP Audit • Password Files • Proprietary Encryption 2. Activity Monitoring	 Threat Protection & Analytics Compromised Accounts Insider Threats Privilege User	 Content-aware (and AD) Secure Collaboration Policy DLP policy violation workflow [Skyhigh or Enterprise DLP] Advanced DLP (Skyhigh + Enterprise DLP) 	 Contextual Access Control GEO, Activity, Device Service, User, Group Structured Encryption [field level) - SSE/OPE/LOE Unstructured Encryption (file level) - SSE/AES KMS & Key brokering DRM 		

Skyhigh Cloud Security Maturity Levels Definitions

1. Customer is focused the strategy towards specific business outcomes 1. Based on the initial assessment, customer 2. Customer has well-laid has initiated tactical out processes and projects focused on security controls, 1. Started the journey with immediate outcomes including workflows initial assessment and data gathering mode. 2. Usually the approaches 3. The controls are applied are targeted towards across the categories of 2. Customer is specific CSP or specific services, groups of users understanding the use users or threats or category of risk/threats cases and trying to come up with the need 3. The controls are usually assessment in monitoring mode **AWARF ADAPTIVE STRATEGIC** (Level 1) (LEVEL 2) (LEVEL 3)

McAfee Confidential − Shared Under NDA McAfee | 9

Visibility

		1. Vendor Assessment
	Contextualized High Risk Services Reports & Registry tuning	 Governance Classification Usage Reports – Create Service Group Usage Reports
Discover Cloud Service Usage (# Services,	2. AD Attribution & Tagging	IaaS Discovery & Usage Reports
#Users, #Activities, #Data)		
2. High Risk Services Report	Sanctioned Services	Sanctioned Services Activity Monitoring
3. Egress effectiveness Report	Audit (On-demand Scanning)	
AWARE (Level 1)	ADAPTIVE (LEVEL 2)	STRATEGIC (LEVEL 3)

McAfee Confidential − Shared Under NDA 10 McAfee

McAfee Confidential − Shared Under NDA

Threat Protection	Targeted Threat Hunting	
	 Tuned Anomalies & IR Insider Threats Data Exfiltration Robotic Activity (System Generated & ML) SIEM and IR workflow 	 & IR Use Activity, Data, Device and GEO context for targeted IR Monitor threats unique to business & vertical
 High Risk Services Usag 		1. Sanctioned Services
2. High Risk Users	 1. Sanctioned Services Threat Protection – Threats & Anomalies Compromised Accounts 	Targeted Threat Hunting & IR Use Activity, Data, Device and GEO context
3. High Severity Anomalies		for targeted IR Monitor threats unique to business & vertical
AWARE	ADAPTIVE	STRATEGIC
(Level 1)	(LEVEL 2)	(LEVEL 3)

McAfee Confidential − Shared Under NDA

Compliance 1. Endpoint DLP policy alignment with Data Handling Standard 1. Coaching and Blocking for High Risk Services 1. Tuned Collaboration 1. Cloud Compliance Policies with Policy Assessment: Audit Violation IR workflow for Cloud Service Usage Collaboration Policies in business groups and against industry Monitoring mode. policies. regulations 2. DLP Policies in Monitoring 2. Tuned DLP policies with mode with Enterprise DLP 1. Cloud Compliance Policy Violation IR or Data Identifiers Assessment: Audit workflow, including Cloud Service Usage Ouarantine for business 3. Policy Violation reviews against industry groups and policies regulations **AWARF ADAPTIVE STRATEGIC** (Level 1) (LEVEL 2) (LEVEL 3)

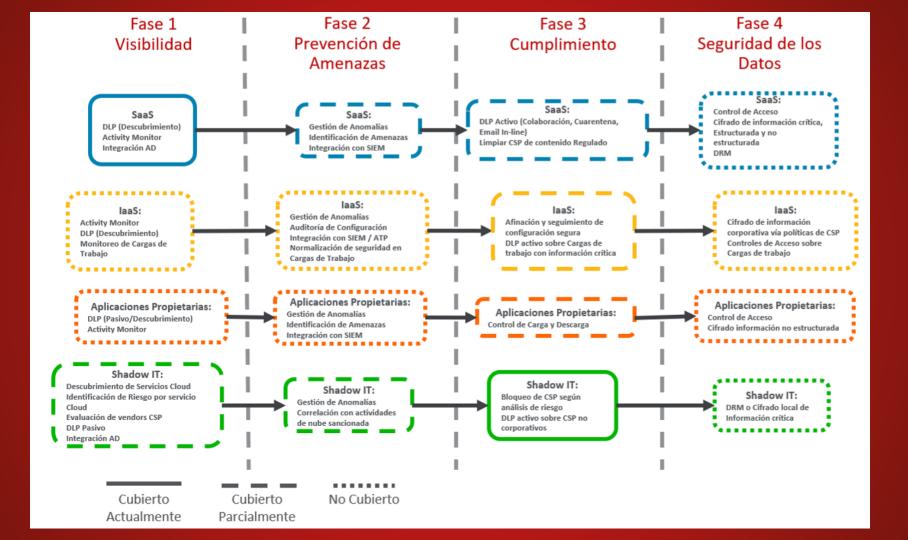
McAfee Confidential - Shared Under NDA

Data Security

Review Unmatched Uploads for URLs/IP addresses not	Use Contextual Access Control Policies (Activity, GEO, Device)	 Data-centric Encryption policies Integrate with DRM Tools
associated with a CSP 1. Sensitive Data Field & Files Audit	 Implement a data classification and tagging solution Encrypt Sensitive Fields using templates 	3. HSM Key Management (rotations and rollovers)
AWARE (Level 1)	ADAPTIVE (LEVEL 2)	STRATEGIC (LEVEL 3)

McAfee Confidential - Shared Under NDA

Helping Customers Focus on What is Important



Soluciones Involucradas:

Fase1:



Definición de Información Crítica/Sensible

Integración vía API entre servicios Cloud SaaS y solución de CASB

Integración entre Active Directory y CASB

laaS:
Activity Monitor
DLP (Descubrimiento)
Monitoreo de Cargas de
Trabajo

Integración vía API entre servicios Cloud IaaS y solución de CASB

Shadow IT: Descubrimiento de Servicios Cloud Identificación de Riesgo por servicio Cloud Evaluación de vendors CSP DLP Pasivo Integración AD

Definición de Información Crítica/Sensible

HDLP en modo observación

Integración vía syslog con solución de Proxy actual

Aplicaciones Propietarias: DLP (Pasivo/Descubrimiento) Activity Monitor Definición de método de ingreso

Integración vía Reverse Proxy con aplicaciones desarrolladas in-house

Mapeo de Actividades a monitorear



McAfee, the McAfee logo and Skyhigh Security Cloud are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the U.S. and/or other countries. Other names and brands may be claimed as the property of others. Copyright © 2018 McAfee, LLC.