McAfee
Together is power.

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

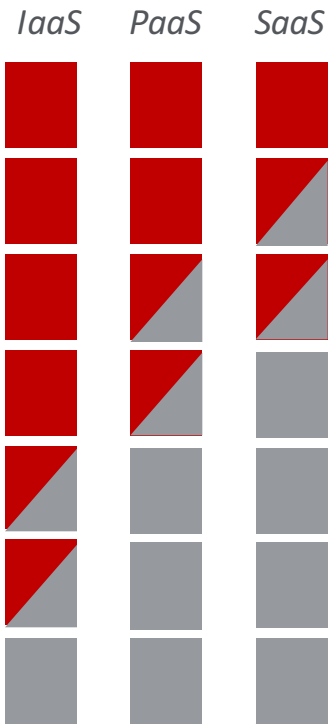
Platform-as-a-Service sits nicely in between the other Cloud Service models.
Typically it's used to develop Applications and Services that you cant buy as a SaaS and are either too expensive or to complex to run in IaaS

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.

The Cloud (First) Enterprise Challenges

Shared Responsibility



Customer Responsibility

Service Provider Responsibility

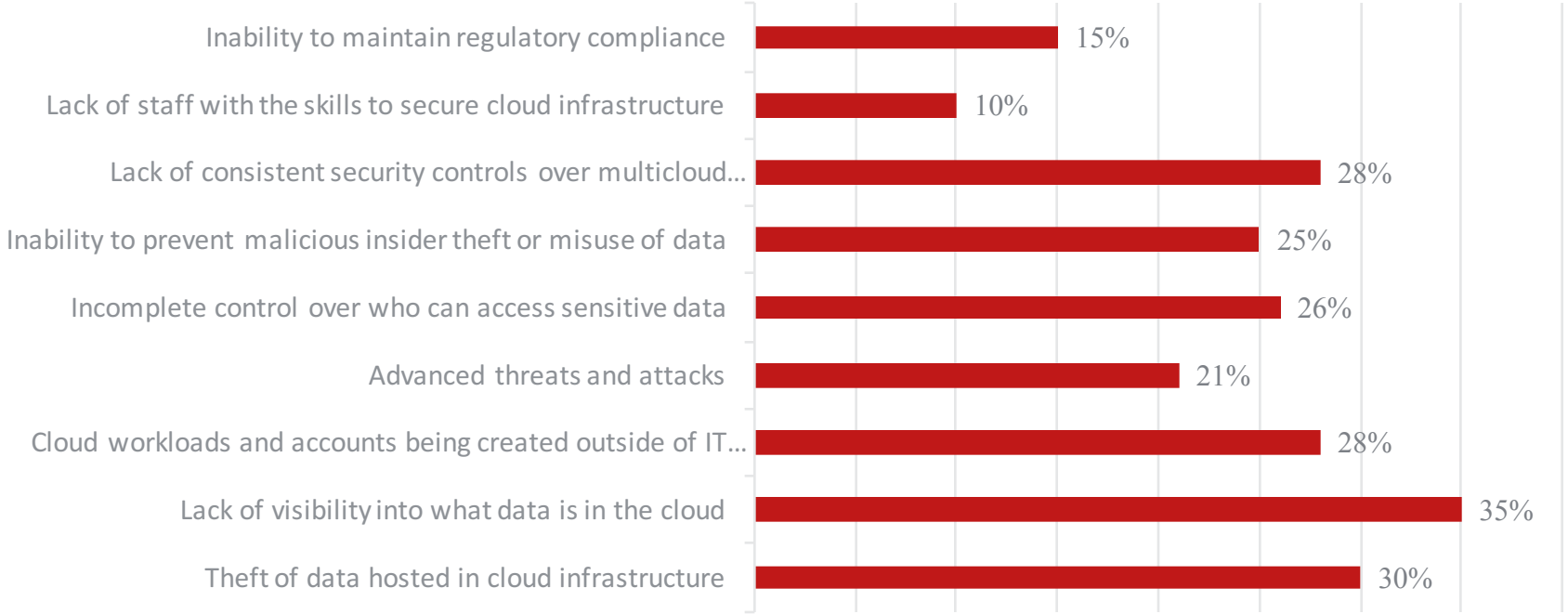
Network security fails to protect data in the cloud & mobile era

Data created natively in cloud is invisible to network security

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

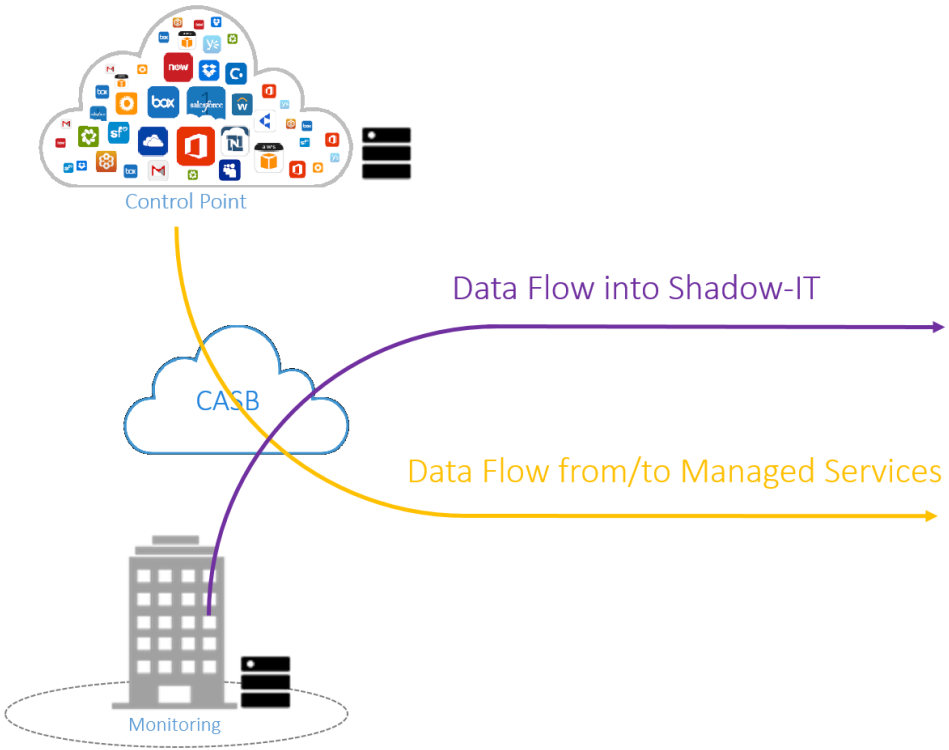
Data uploaded to cloud from mobile is invisible to network security

What do customers say?



Fuente: McAfee

Gartner's four areas of CASB security



Gartner

Visibility: 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.

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

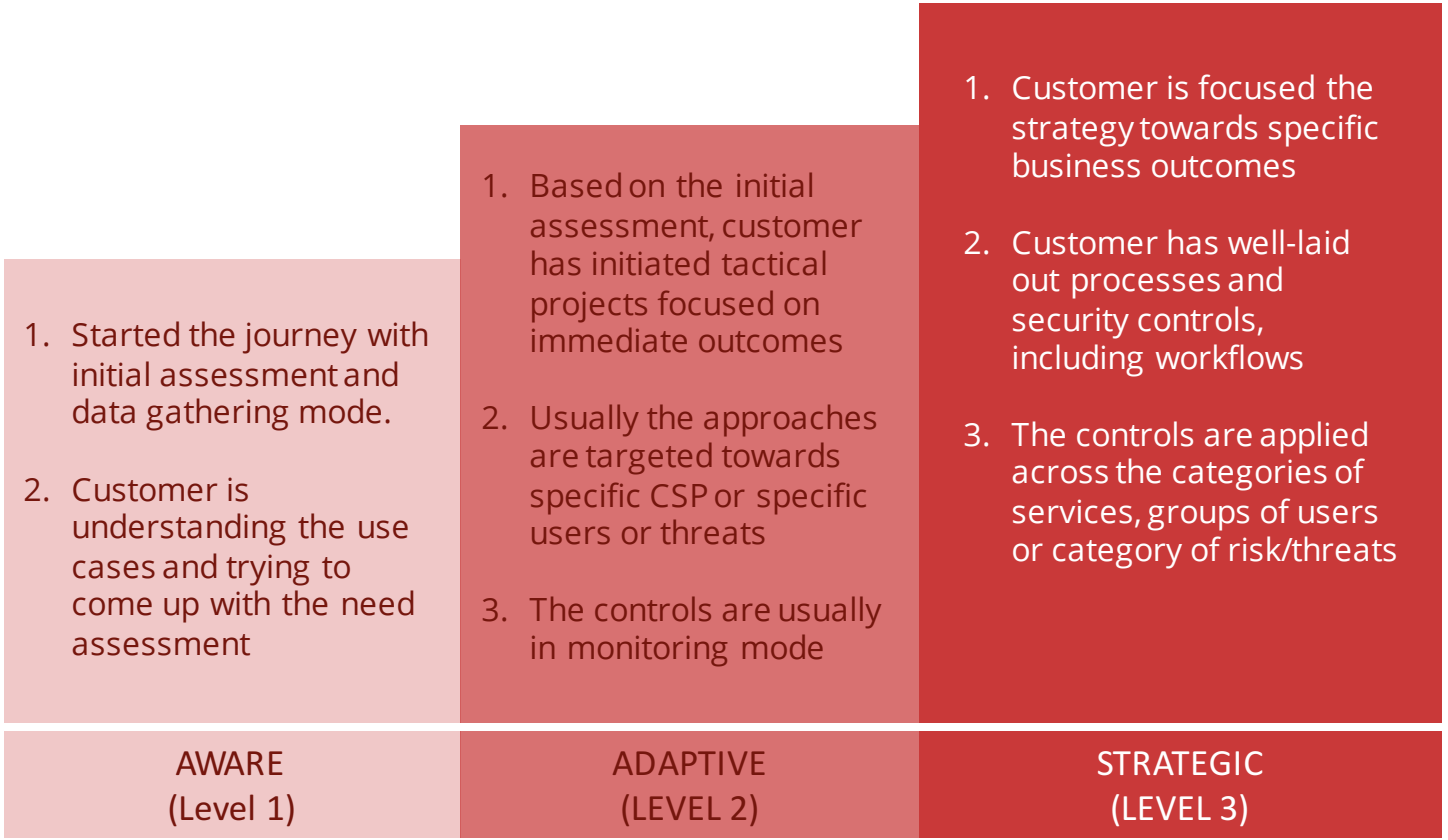
Data Security: CASBs provide the ability to enforce data-centric security policies to prevent unwanted activity based on data classification, discovery and user activity monitoring of access to sensitive data or privilege escalation. Policies are applied through controls, such as audit, alert, block, 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**

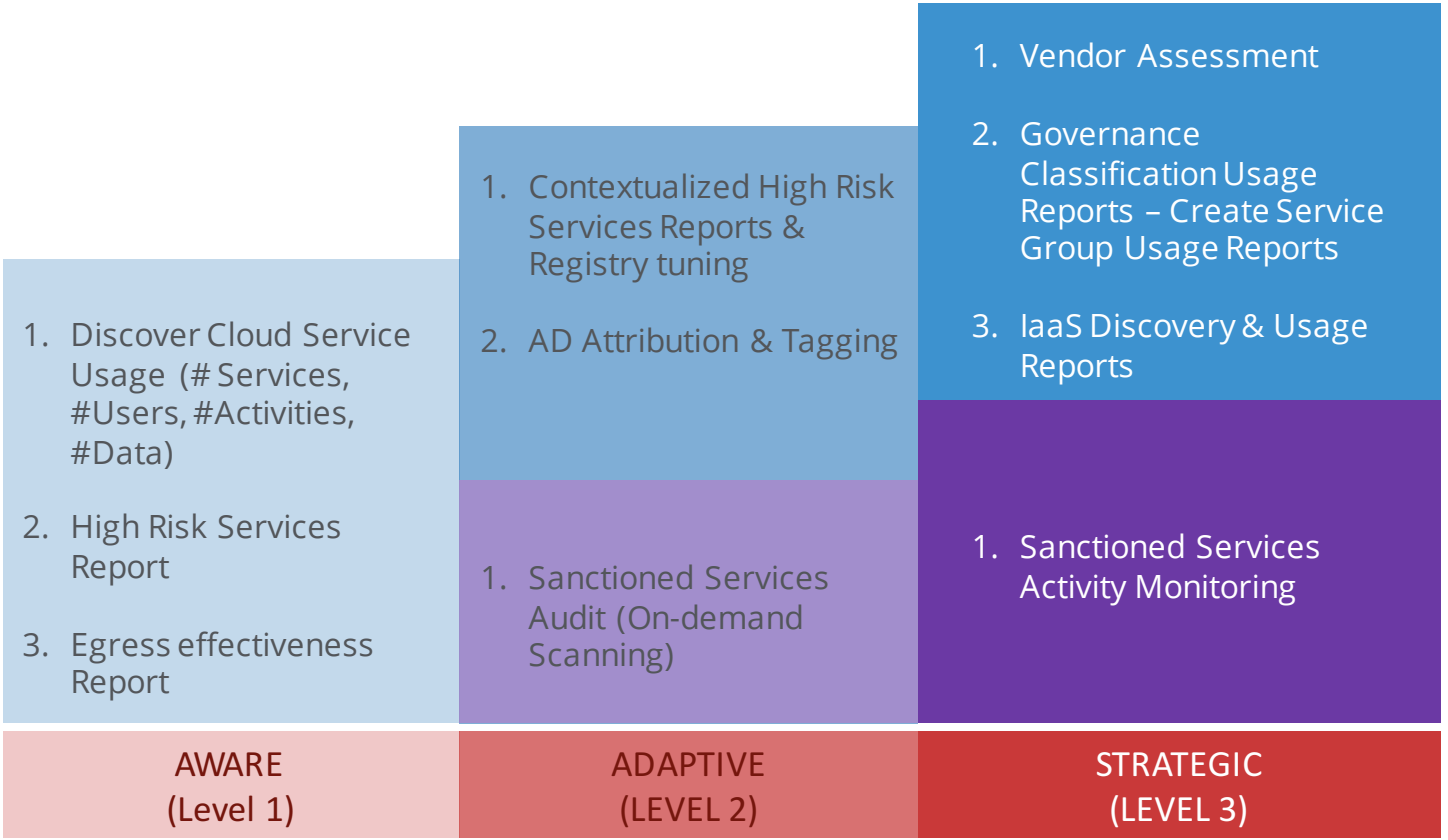
	VISIBILITY (Level 1)	THREAT PROTECTION (LEVEL 2)	COMPLIANCE (LEVEL 3)	DATA SECURITY (LEVEL 4)
Shadow IT	1. **Discover Cloud Services & High Risk Services Usage** 2. **Contextualized High Risk Services Report** 3. **Egress Leakage Report** 4. **Vendor Assessment** 5. **AD Attribution & Governance** 6. **IaaS Discovery**	1. **High Severity Anomalies** • **Repeat Offender** • **Robotic Activity** • **Data Exfiltration** 2. **SIEM Integration & IR workflow** 3. **Insider Threats and Advanced Threat protection (with SSL inspection)**	1. Coaching and Blocking High Risk Services 2. Ensuring Data Handling Policies and Endpoint DLP policies are in line with organization's cloud initiatives	1. 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**	1. **Threat Protection & Analytics** • **Compromised Accounts** • **Insider Threats** • **Privilege User Monitoring** • **Security Config Audit** 2. **SIEM integration & IR workflow** 3. **Targeted threat hunting & contextual investigations**	1. Content-aware (and AD) Secure Collaboration Policy 2. DLP policy violation workflow [Skyhigh or Enterprise DLP] 3. Advanced DLP (Skyhigh + Enterprise DLP)	1. Contextual Access Control • GEO, Activity, Device • Service, User, Group 2. Structured Encryption [field level) – SSE/OPE/LOE 3. Unstructured Encryption (file level) – SSE/AES 4. KMS & Key brokering 5. DRM

Skyhigh Cloud Security Maturity Levels Definitions



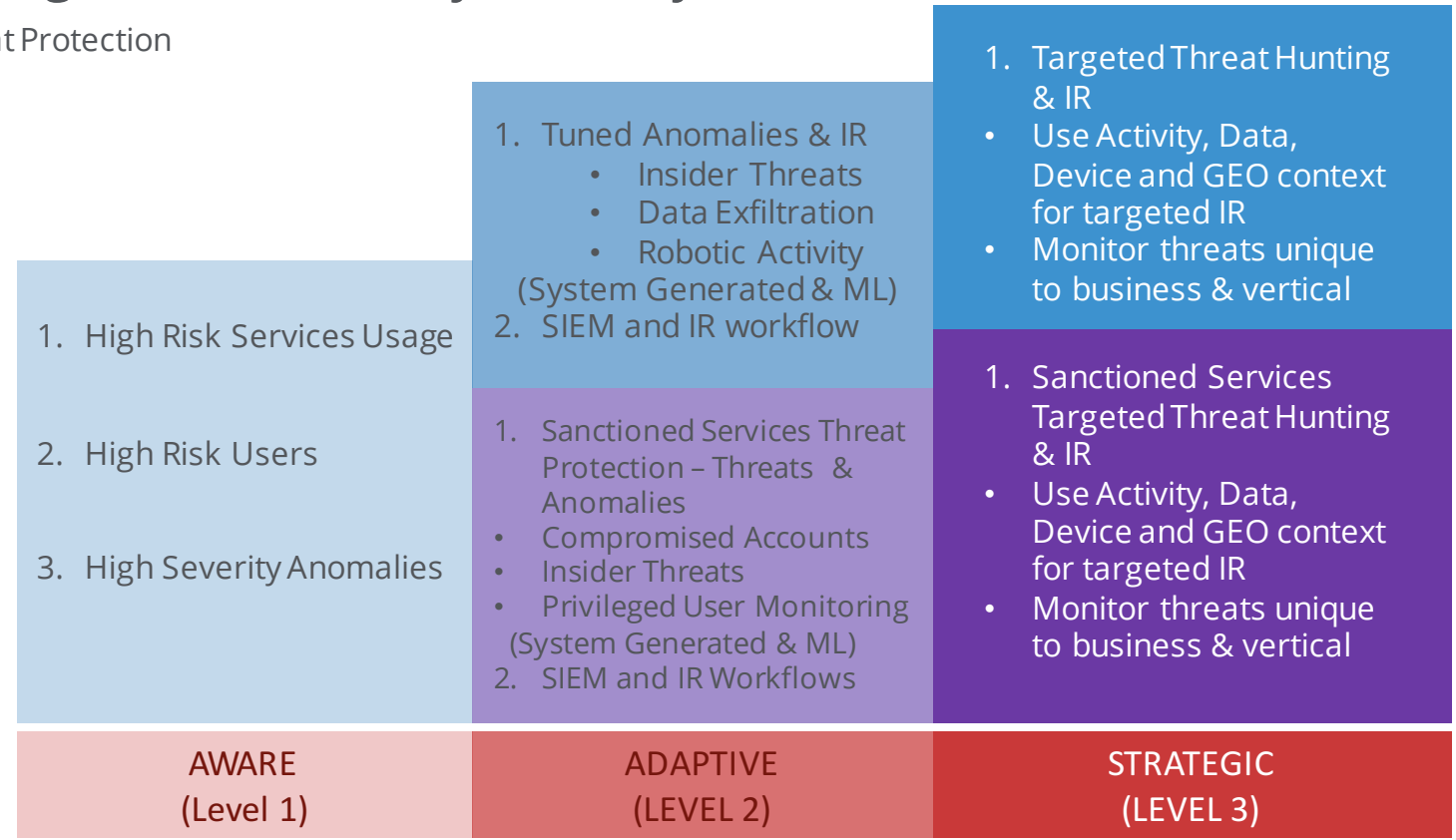
Skyhigh Cloud Security Maturity Framework:

Visibility



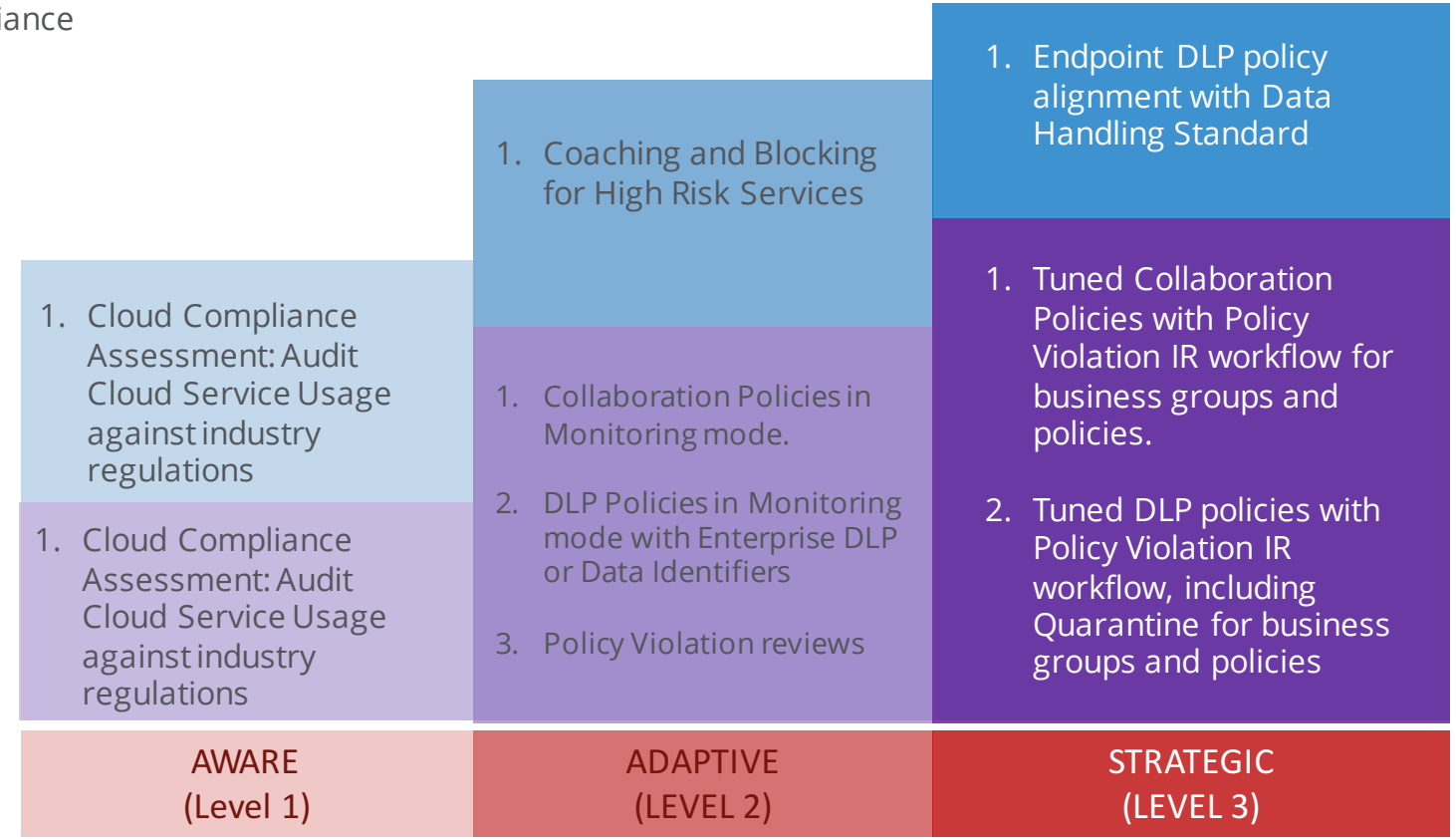
Skyhigh Cloud Security Maturity Framework:

Threat Protection



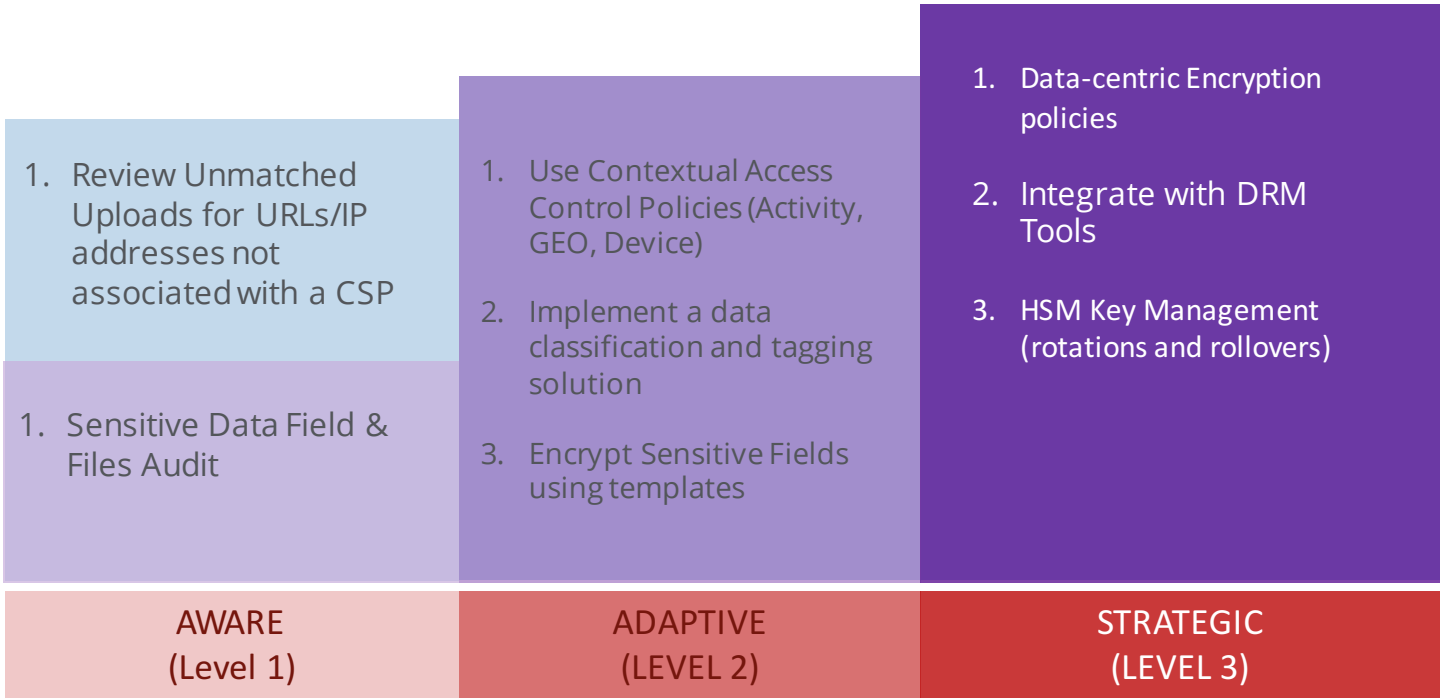
Skyhigh Cloud Security Maturity Framework:

Compliance

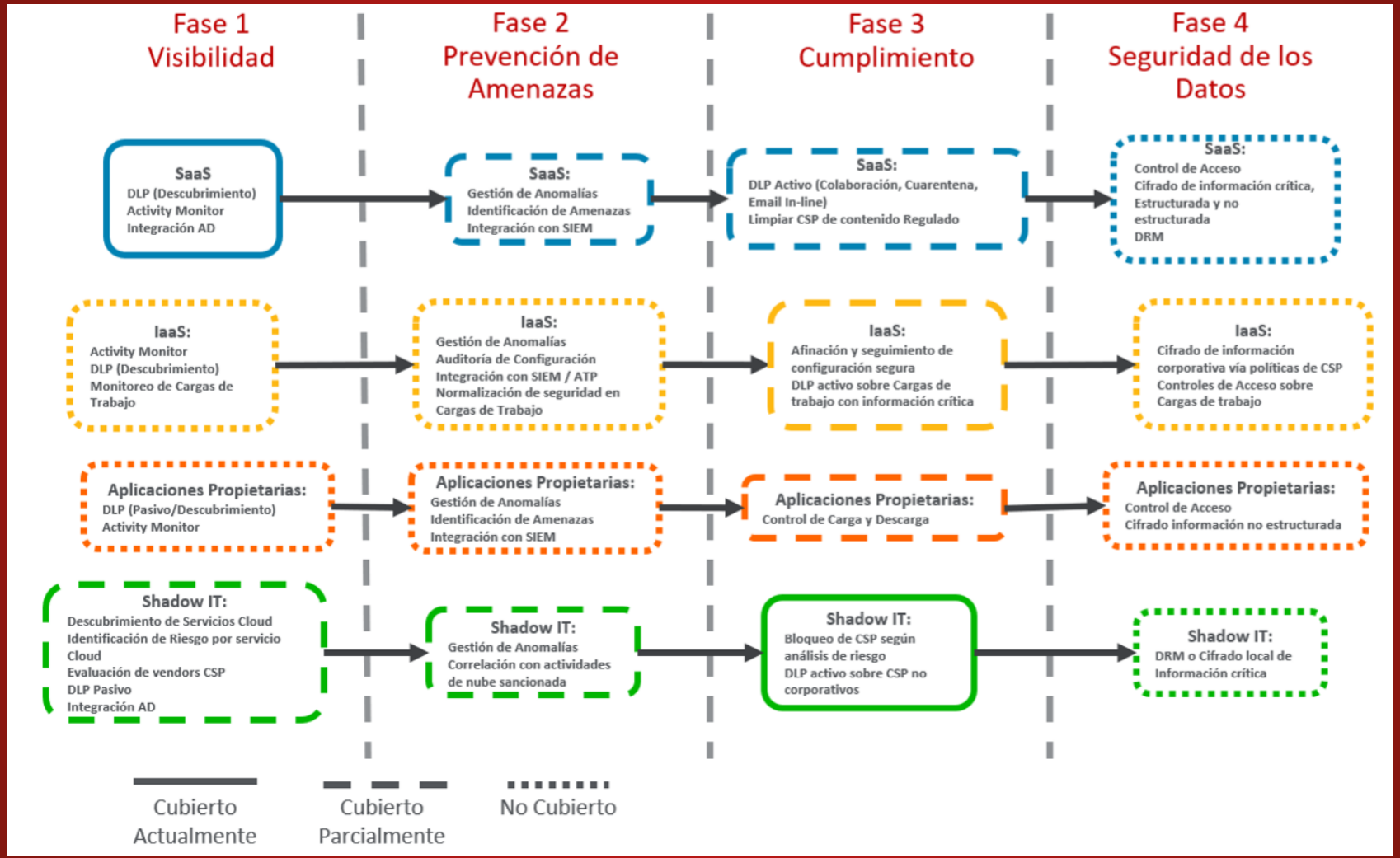


Skyhigh Cloud Security Maturity Framework:

Data Security



Helping Customers Focus on What is Important


Fase 1
Visibilidad
Fase 2
Prevención de Amenazas
Fase 3
Cumplimiento
Fase 4
Seguridad de los Datos
SaaS
DLP (Descubrimiento)
Activity Monitor
Integración AD
SaaS:
Gestión de Anomalías
Identificación de Amenazas
Integración con SIEM
SaaS:
DLP Activo (Colaboración, Cuarentena, Email In-line)
Limpiar CSP de contenido Regulado
SaaS:
Control de Acceso
Cifrado de información crítica, Estructurada y no estructurada
DRM
IaaS:
Activity Monitor
DLP (Descubrimiento)
Monitoreo de Cargas de Trabajo
IaaS:
Gestión de Anomalías
Auditoría de Configuración
Integración con SIEM / ATP
Normalización de seguridad en Cargas de Trabajo
IaaS:
Afinación y seguimiento de configuración segura
DLP activo sobre Cargas de trabajo con información crítica
IaaS:
Cifrado de información corporativa vía políticas de CSP
Controles de Acceso sobre Cargas de trabajo
Aplicaciones Propietarias:
DLP (Pasivo/Descubrimiento)
Activity Monitor
Aplicaciones Propietarias:
Gestión de Anomalías
Identificación de Amenazas
Integración con SIEM
Aplicaciones Propietarias:
Control de Carga y Descarga
Aplicaciones Propietarias:
Control de Acceso
Cifrado información no estructurada
Shadow IT:
Descubrimiento de Servicios Cloud
Identificación de Riesgo por servicio Cloud
Evaluación de vendors CSP
DLP Pasivo
Integración AD
Shadow IT:
Gestión de Anomalías
Correlación con actividades de nube sancionada
Shadow IT:
Bloqueo de CSP según análisis de riesgo
DLP activo sobre CSP no corporativos
Shadow IT:
DRM o Cifrado local de Información crítica
Cubierto Actualmente
Cubierto Parcialmente
No Cubierto

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

Definición de Información Crítica/Sensible

HDLP en modo observación

Integración vía syslog con solución de Proxy actual

Integración vía API entre servicios Cloud IaaS y solución de CASB

Definición de método de ingreso

Integración vía Reverse Proxy con aplicaciones desarrolladas in-house

Mapeo de Actividades a monitorear