



# Esteban Azofeifa Soto

**Regional Cyber Security Architecture Manager.**

Lidera el área de arquitectura y diseño de soluciones y servicios de ciberseguridad a nivel regional.

Es responsable de diseñar arquitecturas holísticas de ciberseguridad para Costa Rica, Nicaragua, El Salvador, Guatemala, Panamá y República Dominicana, las cuales, responden a necesidades muy específicas de cada cliente.

Adicionalmente, es el responsable de diseñar los servicios de ciberseguridad administrados que son entregados desde el Cybersecurity Center de GBM.

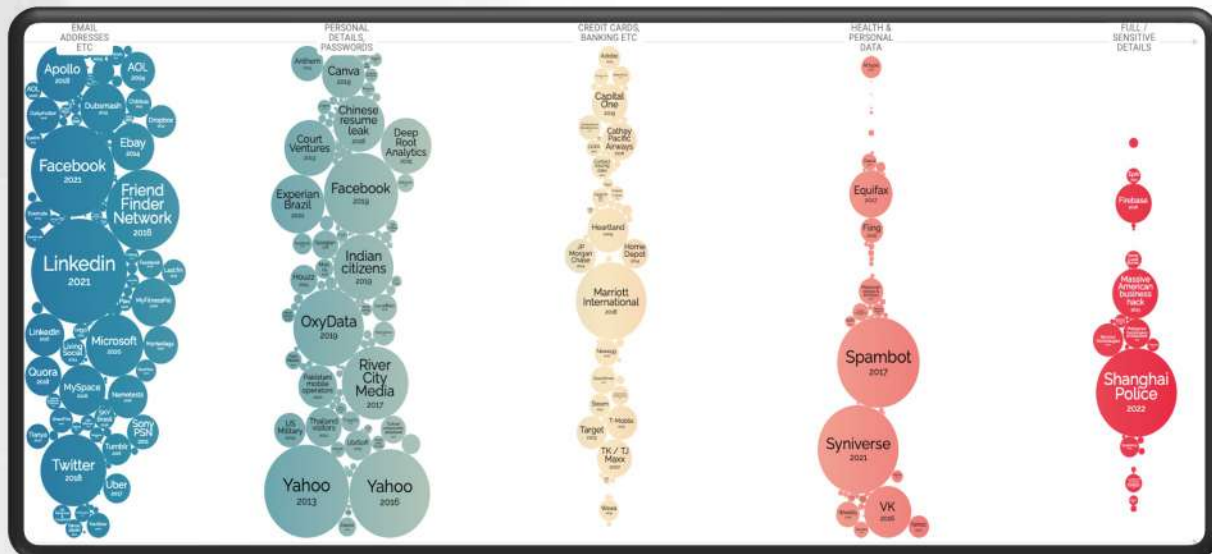




# Más Allá del Cumplimiento

Enfoque Integral de Seguridad de  
Datos en la Era Digital

# Las grandes fugas de datos siguen en aumento





# Data Security Challenges

Top Three



## Explosión de Datos en la Nube

**63%** de las organizaciones han expuesto datos sensibles en la nube



## Costo de una Brecha

**\$2.46M** es el costo promedio de una filtración de datos en Latinoamérica.



## Complejidad en el Cumplimiento

**1000** horas dedicadas al año por las organizaciones para facilitar las auditorías



# Navegar en la Oscuridad

Reto: Detectar amenazas de seguridad que puedan afectar los datos sensibles

# Data Security Framework

Contamos con un **enfoque integral** para abordar las necesidades de protección de datos de nuestros clientes



Extended  
Detection &  
Response



Identity &  
Access  
Management

Data  
Security  
Posture  
Management

Risk  
Management

Compliance  
Reporting

DSPM

Data  
Centric  
Protection

Discovery & Classification

Vulnerability Assessment

Activity Monitoring

Behavioral Analytics

Data  
Centric  
Enforcement

Data Obfuscation

Data Access Control

Data Loss Prevention

File Control

PROACTIVE

REACTIVE

Databases

Big Data

Data Lakes

Files

SaaS

DBaaS

IaaS

Consulting  
Services

Engineering  
Services

Managed  
Services



# Nuestro Enfoque

Zero Trust



Definir las políticas, metodología y criterios de clasificación

- ✓ Proveer el marco de referencia para clasificar la información empresarial



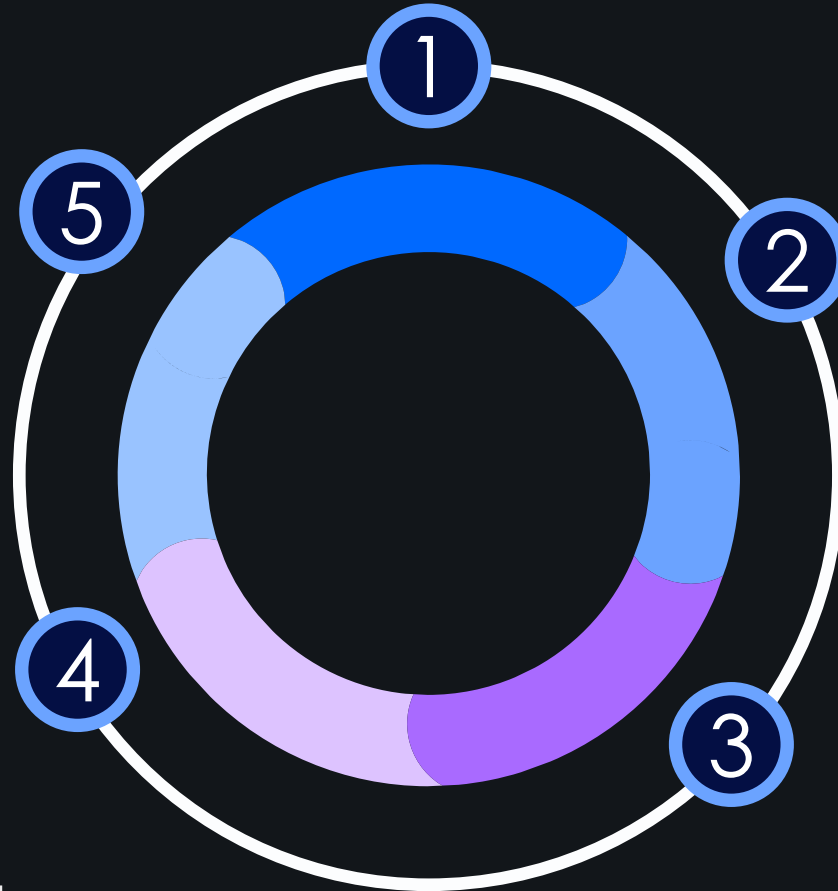
Detectar y Responder

- ✓ Monitorizar en tiempo real el acceso a los datos
- ✓ Evaluar el comportamiento de los usuarios en el acceso a los datos
- ✓ Responder de forma automatizada a amenazas de seguridad



Proteger la información sensible

- ✓ Cifrar
- ✓ Controlar el acceso granular
- ✓ Controlar los archivos compartidos
- ✓ Proteger los datos en la nube
- ✓ Prevenir la fuga de información



Clasificar la información y los activos

- ✓ Descubrir la información sensible
- ✓ Inventarios de activos e información
- ✓ Clasificar la información y los activos según su criticidad



Definir controles para cada nivel de clasificación

- ✓ Documentar y actualizar políticas



# Casos de Uso para Protección de Datos



Discovery & Classify

Data Encryption &  
Masking

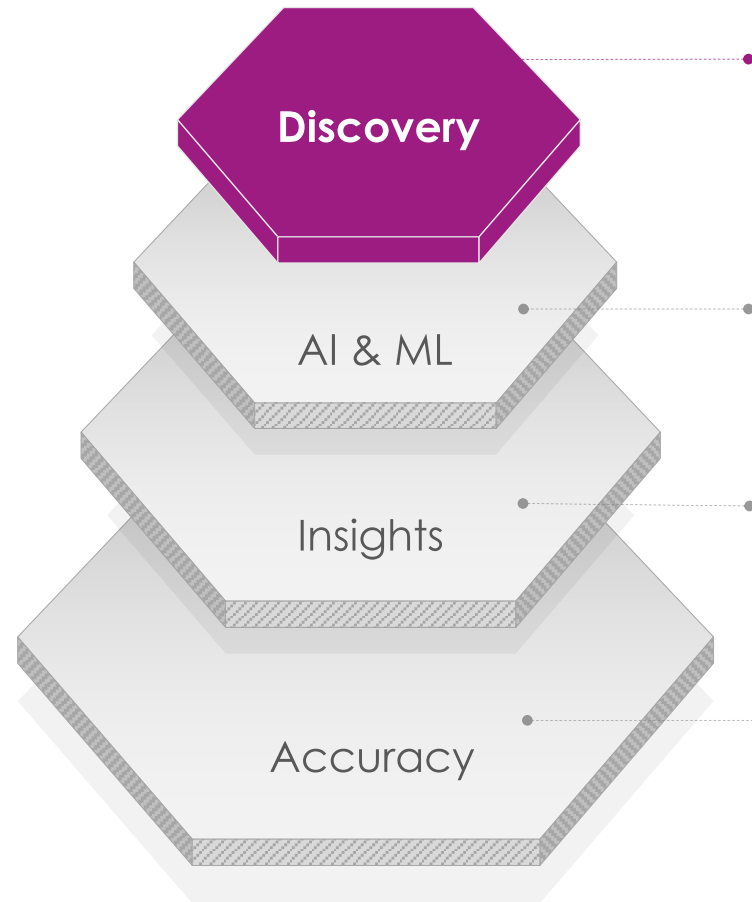
Cloud Data  
Security Posture  
Management

Data Protection,  
Detection &  
Response

Data Loss  
Prevention & Rights  
Management

# Discover & Classify

Los requisitos modernos exigen un nuevo enfoque para el descubrimiento y clasificación de datos



## Descubrir las fuentes de datos, donde quiera que se encuentren

Crear un inventario de fuentes de datos on-premise, en la nube, en mainframe o híbridas

## Utilizar modelos de IA y ML

Eliminar falsos positivos en la exploración y clasificación para aumentar la eficacia del catálogo de datos confidenciales

## Inteligencia Automatizada

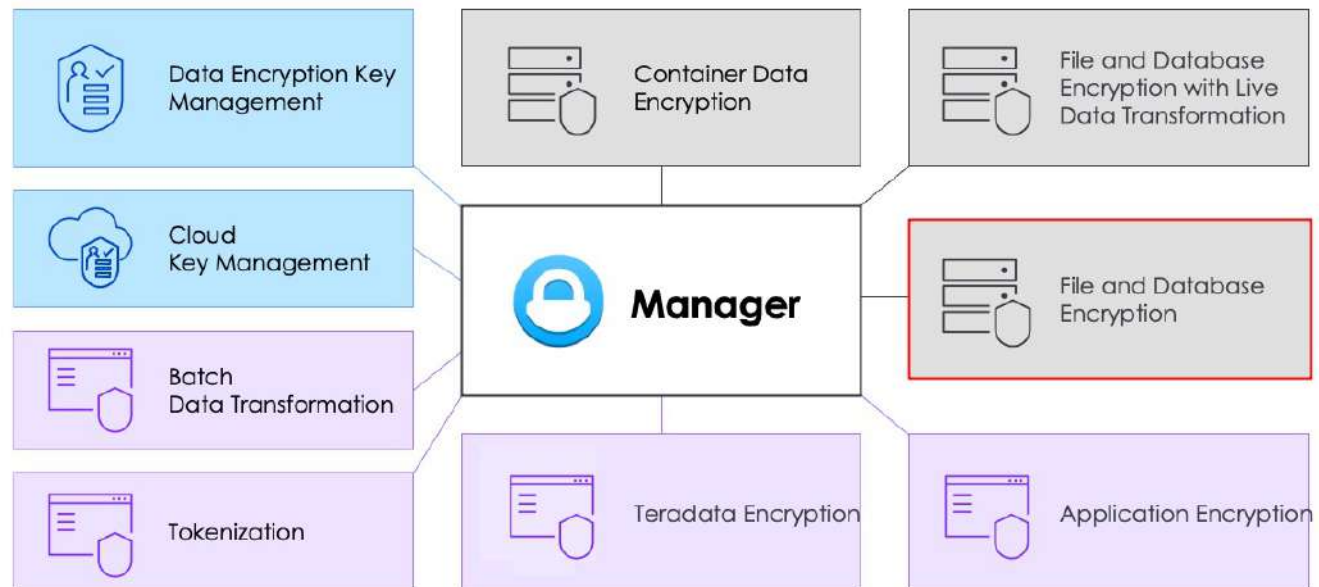
Comprenda los "Data Subjects", el linaje de los datos, las partes interesadas, los procesos y evalúe el riesgo

## Precisión en el inventario

Inventario preciso de datos a nivel de elemento de datos o repositorio

# Data Encryption & Masking

Defensa Proactiva frente a las amenazas.



# Data Security Posture Management

Seguimiento y protección de datos en la nube



## Visibilidad de Datos en la Nube

Descubrir los datos sin fricciones que se extienden dentro de los proveedores de la nube y las aplicaciones SaaS

## Protección de Datos en aplicaciones SaaS

Detener la fuga de datos entre cuentas en la nube y aplicaciones SaaS

## Movimiento de Datos en la Nube

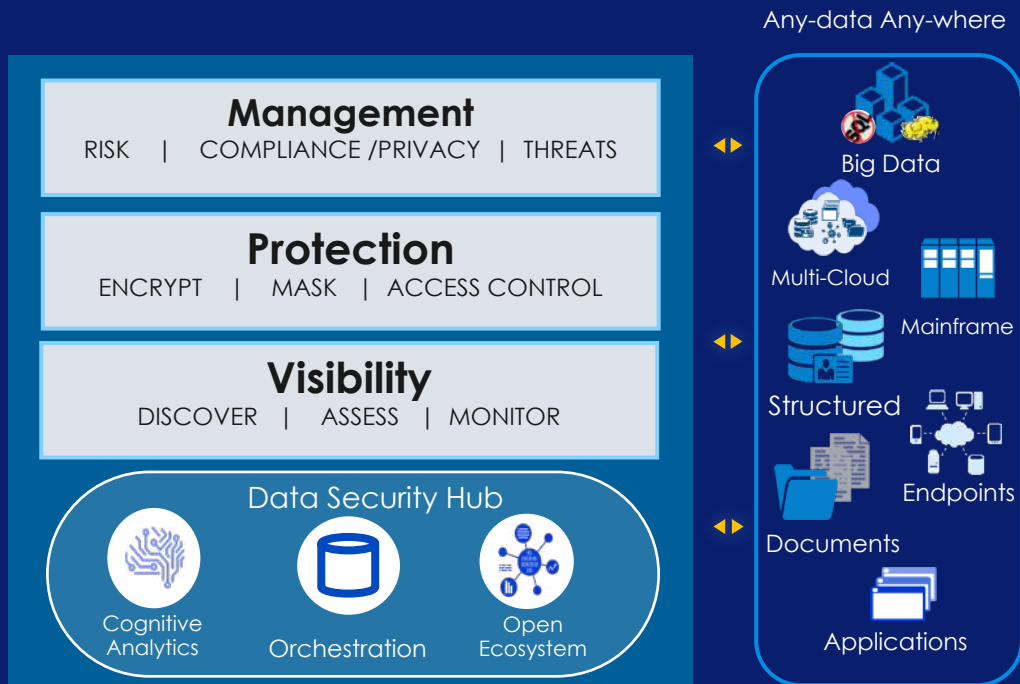
Analizar el flujo potencial y real de datos en y a través de la nube

## Protección de Datos en la Nube

Descubrir vulnerabilidades en los datos y en los controles y la postura de cumplimiento.



# Data Protection, Detection & Response



## Monitoreo y alertas en tiempo real

- Alertas de comportamiento
- Alertas por violación a políticas



## Control de Acceso

Políticas granulares para restringir el acceso:

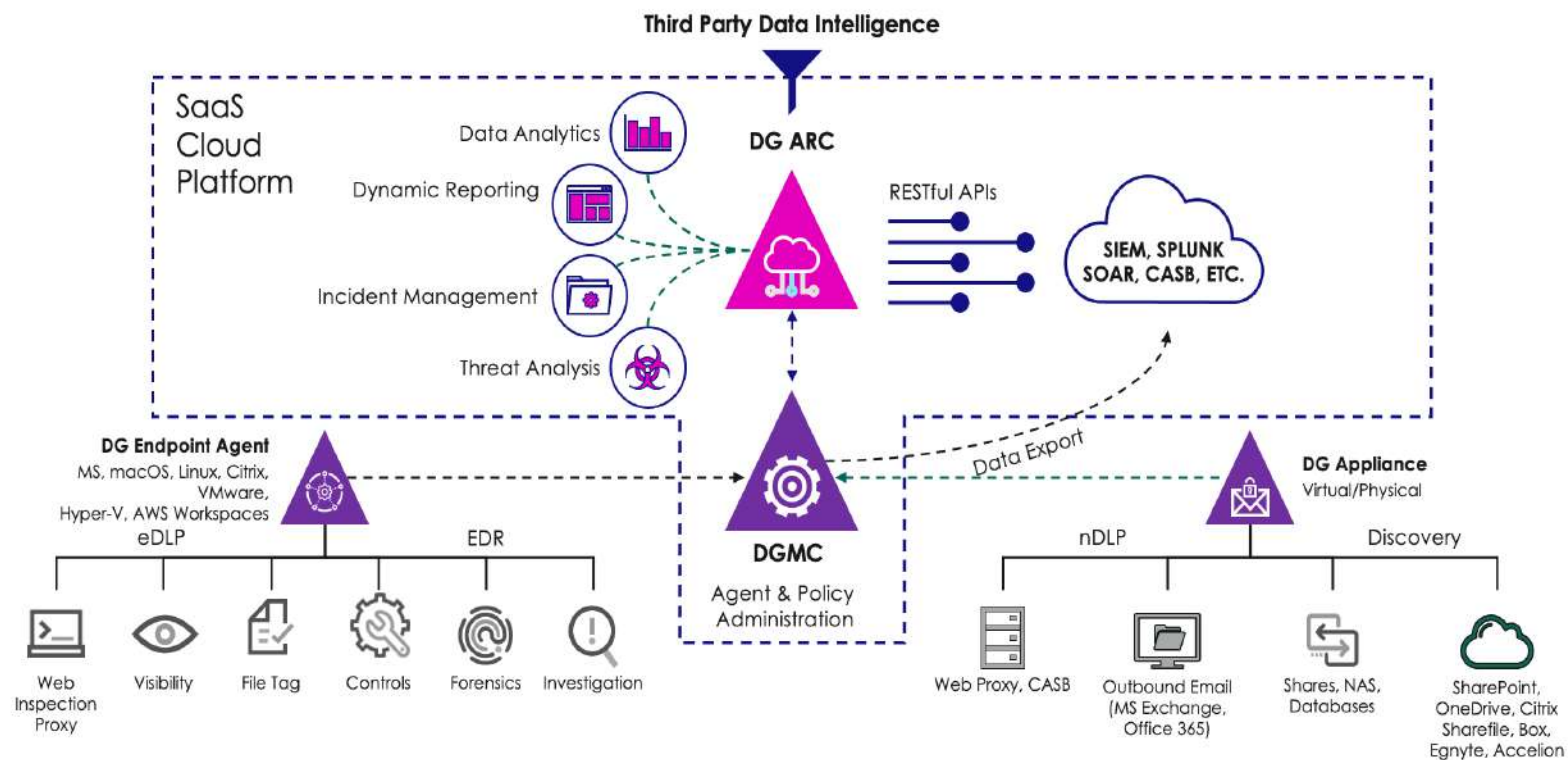
- Bloque de accesos y cuarentena de usuarios
- Enmascaramiento dinámico (data redaction)



## Evaluación de Vulnerabilidades

- Versiones obsoletas
- Privilegios incorrectamente asignados
- Falta de parches

## New DLP Architecture

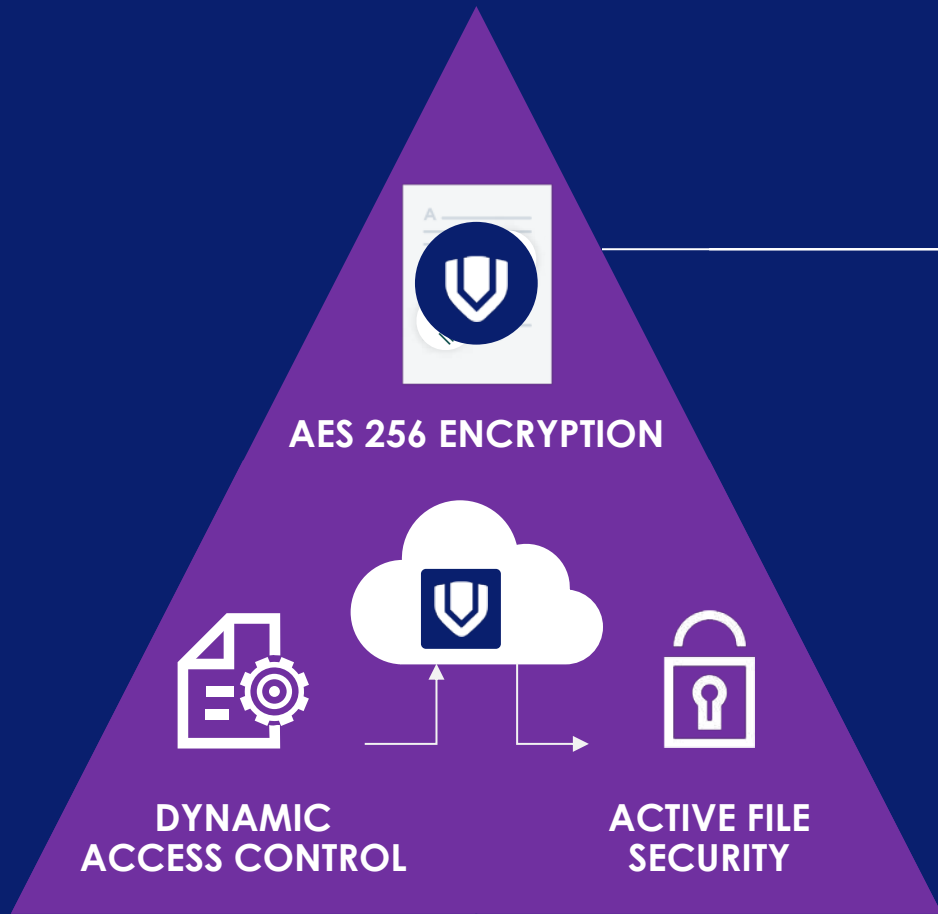


# New Generation DLP

## Más allá del DLP tradicional



# Zero Trust File Security



Proteger los datos sensibles



Requerido para la colaboración moderna



El cifrado sigue a los archivos a todo lugar



La seguridad viaja con cada archivo y copias



Soporta todo tipo de archivos



Documentos encriptados incluso después de descargarlos



Implantación SaaS para facilitar la gestión en tiempo real



Intuitive, low friction end-user experience

# MUCHAS GRACIAS

Para cualquier consulta, contactar a:

**Esteban Azofeifa**

Regional Cyber Security Architecture Manager

[eezofeifa@gbm.net](mailto:eezofeifa@gbm.net)

+(506) 8820-0392

**[www.gbm.net](http://www.gbm.net)**

[mercadeo@gbm.net](mailto:mercadeo@gbm.net) |    GBMCorp

