ManageEngine

CIEM O SIEM

Diego Montenegro
Technical Account Manager

ManageEngine

IAM en el ambiente Cloud

Information Technology

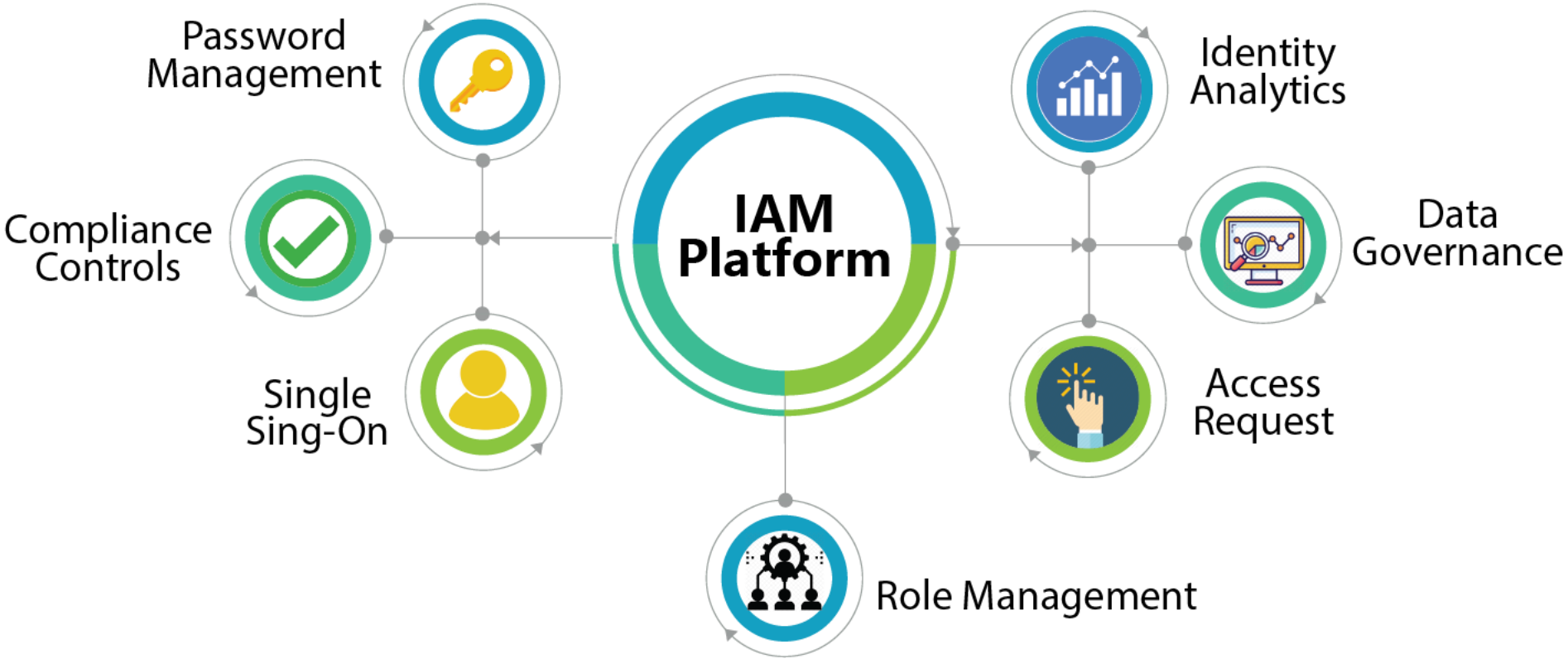
Gartner Glossary

Identity and Access Management (IAM)

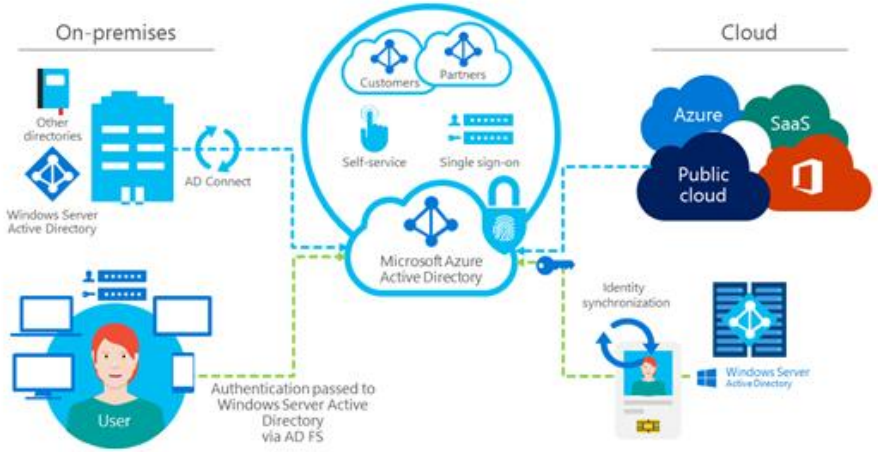
Identity and access management (IAM) is the discipline that enables the right individuals to access the right resources at the right times for the right reasons.

IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. IAM is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise.

Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives.


Password Management
Compliance Controls
Single Sing-On
IAM Platform
Identity Analytics
Data Governance
Access Request
Role Management

Nueva Tecnología, nuevos desafíos



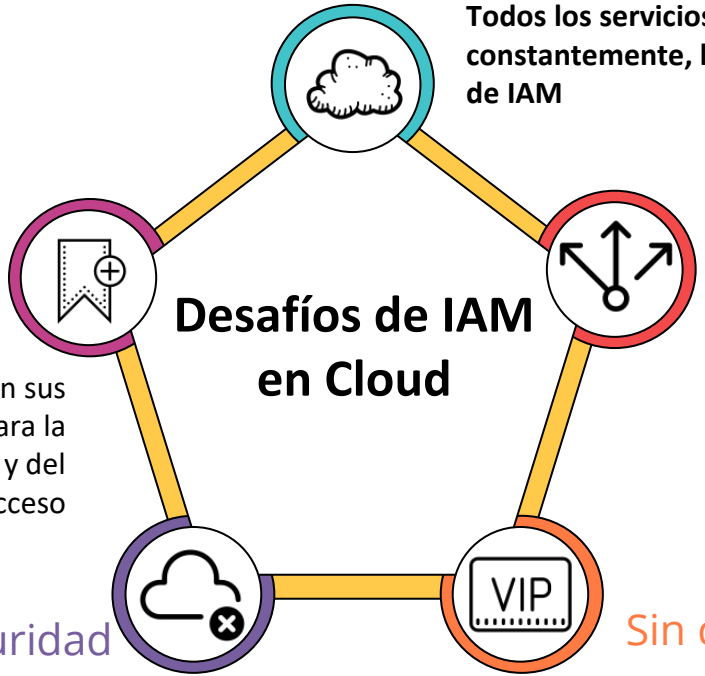
Lo dinámico de la nube

Todos los servicios de la nube cambian constantemente, lo que dificulta las tareas de IAM

Carencia de lógica y estándares

Cada proveedor cuenta con sus propias recomendaciones para la gestión de la identidad y del acceso

Desafíos de IAM en Cloud



Variedad de plataformas

Al existir una gran variedad de servicios, recursos y cuentas en Cloud, se dificulta la operación para el equipo de TI

Pobre seguridad

Un pobre manejo en la seguridad de las contraseñas y los accesos dentro de la organización

Sin control de privilegios

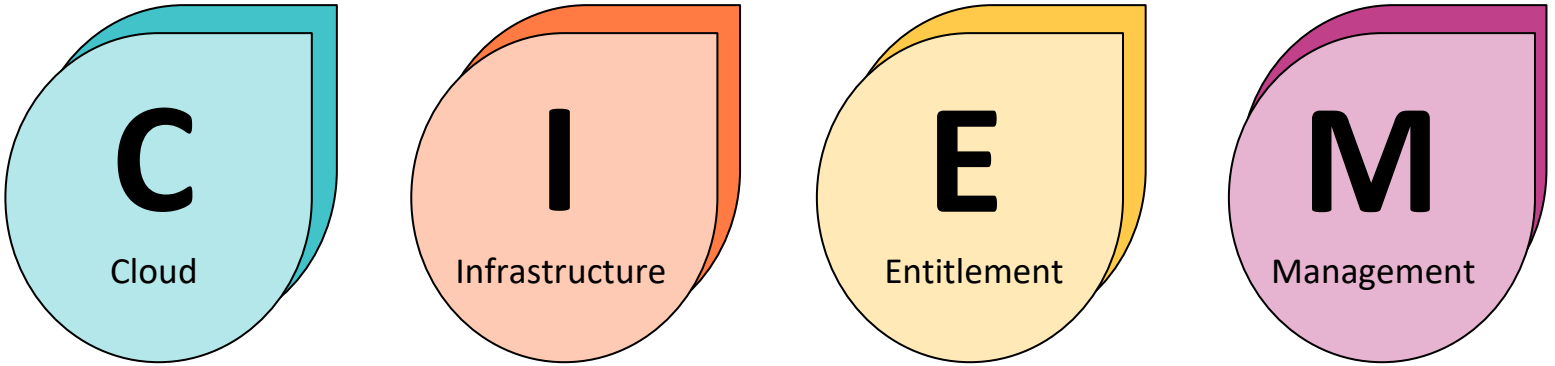
La carencia del control de privilegios provoca serias brechas de seguridad en la organización

ManageEngine

CIEM

Cloud Infrastructure Entitlement Management

CIEM



Es una solución que administra los derechos y permisos de los servicios en la nube, bien sean ambientes multinube, nube híbrida o nubes dinámicas

La IDENTIDAD es el NUEVO PERÍMETRO

Las **identidades** en la nube se extienden más allá de los usuarios/personas

5 **identidades de “máquina” para cada identidad de usuario (computadoras, almacenamiento, redes, memoria, etc.)**

34 mil **Tipos de accesos ofrecidos por los CSP**

Reporte 2020 “Managing Privileged Access in Cloud Infrastructure”

ManageEngine

66% de las organizaciones usan claves de acceso por más de 90 días (o sin caducidad)

99% de las identidades tienen permisos excesivos

75% Gartner los fallos de seguridad en la nube son consecuencia de una gestión inadecuada de identidades, accesos y privilegios

RIESGO de brecha de datos y escalamiento de privilegios

https://www.cleveroad.com/blog/cloud-security-risks/
https://www.gartner.com/en/documents/3986121

¿Qué debe contener una solución CIEM?

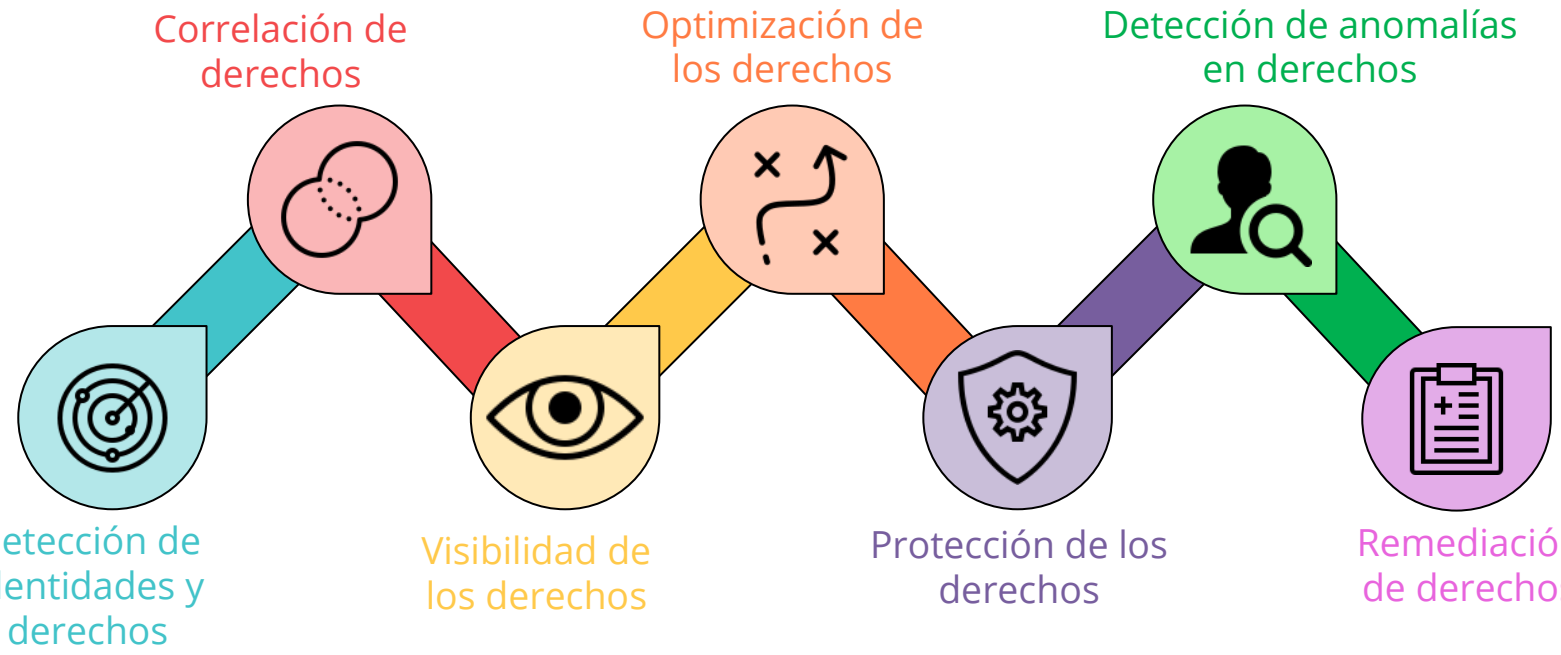
Panel de control centralizado para toda la nube

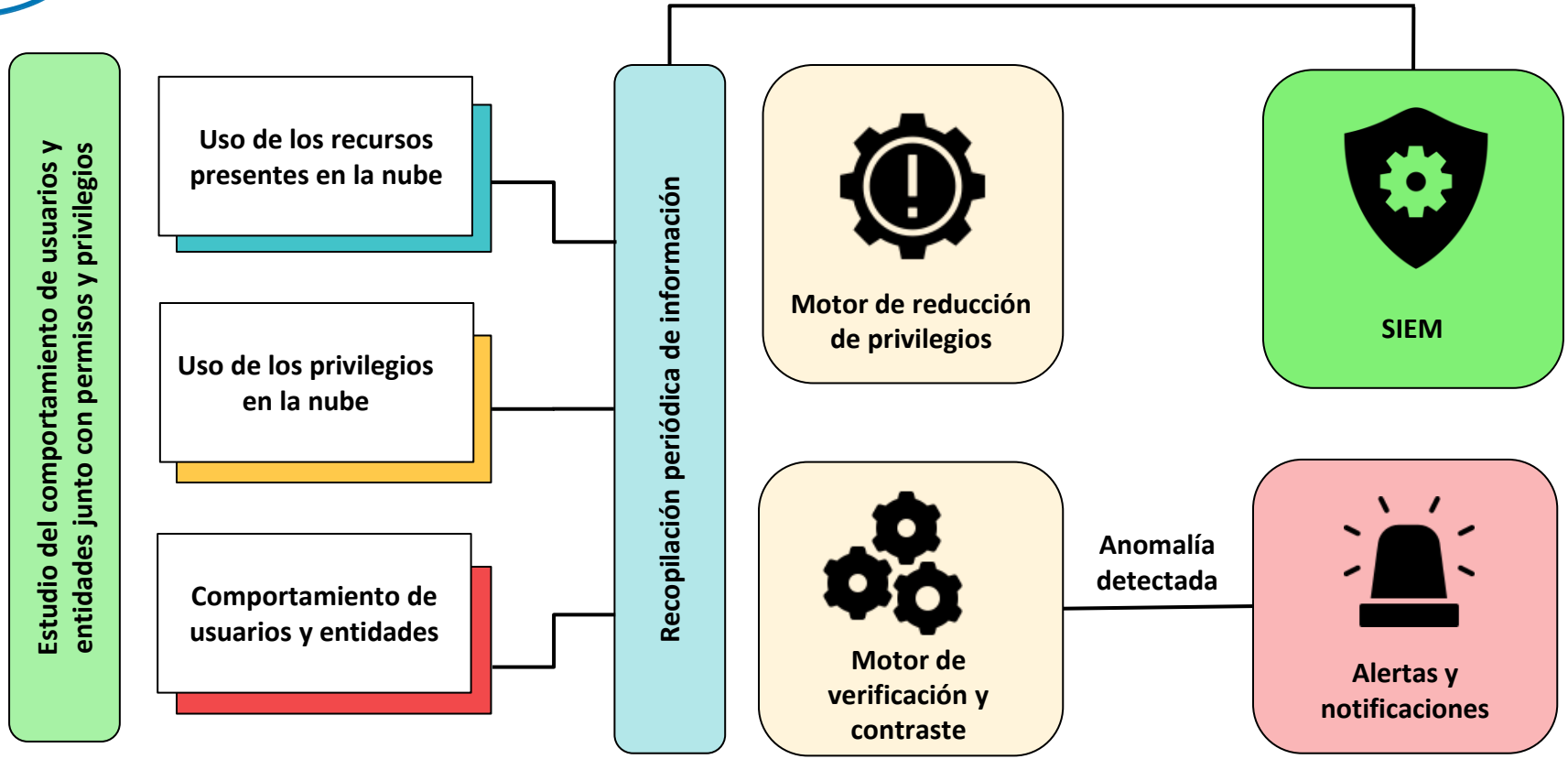
Aplicar el principio de acceso de mínimo privilegio

Involucrar soluciones de IA para identificar riesgos

Rastrear y controlar el acceso en toda la nube

Ciclo de vida de un CIEM




Estudio del comportamiento de usuarios y entidades junto con permisos y privilegios
Uso de los recursos presentes en la nube
Uso de los privilegios en la nube
Comportamiento de usuarios y entidades
Recopilación periódica de información
Motor de reducción de privilegios
SIEM
Motor de verificación y contraste
Anomalía detectada
Alertas y notificaciones

Cloud computing

Un aumento en la cantidad de empresas que empiezan a utilizar los servicios de la nube

Monitoreo

Revisión constante de lo que ocurre en todos los ambientes en la nube

IAM

Funcionamiento problemático para la gestión de las identidades y el acceso

Privilegios

Gestionar todos los accesos privilegiados en la infraestructura

Inteligencia Artificial

La implementación de la IA para el estudio de todo lo que ocurre en la nube

Visibilidad

Obtener información de todo lo que ocurre en la nube

ManageEngine

Como puede influir ManageEngine

ManageEngine

Cloud Security Plus

Administración de logs de Amazon Web Services (AWS)

Cloud Security Plus recupera y usa logs de AWS CloudTrail y logs de acceso del servidor S3 para detectar actividades maliciosas que suceden en el entorno de AWS.

Administración de logs de Microsoft Azure

Colecte, monitoree y analice datos de logs del entorno Azure.

Administración de logs de Salesforce

Cloud Secutiry Plus recupera logs de eventos de Salesforce desde el monitoreo de eventos de Salesforce por medio de llamadas REST API para monitorear inicios de sesión, informes, contenido y actividades de búsqueda. Esto puede ayudar a un monitoreo proactivo de eventos críticos en su entorno de Salesforce.

Administración de logs de la plataforma en la nube de Google

Obtenga insights detallados de la actividad del usuario, IAM, seguridad en la red, actividad VPC, servicios en la red, funciones en la nube, App Engine, almacenamiento de Google y administración de recursos GCP con una extensiva recuperación de logs usando llamadas gRPC.

Seguridad en la nube

Inteligencia de amenazas

Gestión de incidentes

ManageEngine

Log360 UEBA

Monitoreo de la seguridad en tiempo real

Análisis del comportamiento de usuarios y entidades

Detección de ataques

ManageEngine

PAM360

Elevación de privilegios a tiempo

Análisis de comportamiento del usuario privilegiado

Gobierno de cuentas privilegiadas

Controles de acceso remoto

Auditoría y cumplimiento

Correlación de eventos sensibles

ManageEngine

AD360

AD and Exchange Server management and reporting

Auditoría y alertas de cambios en tiempo real para AD on-premises y Azure AD

Autoservicio de gestión de contraseñas, para AD, Password Sync, e inicio de sesión único

Informes, auditorías y monitoreo para Exchange y Skype Empresarial Server

¡Muchas Gracias!

diego.montenegro@zohocorp.com


@ManageEngineLA


ManageEngine LATAM


@ManageEngineLA


manageenginelatam