Delinea

Cloud Infrastructure Entitlement Management (CIEM)

Guía del comprador

Guía del comprador de Cloud Infrastructure Entitlement Management (CIEM)

Como resultado de la transformación de la nube, los datos confidenciales ahora se encuentran dispersos por toda la empresa. Los servicios en la nube se crean rápidamente, muchas veces fuera del control central de TI. Además, prácticamente todas las empresas cuentan con una combinación de recursos locales y en la nube, a menudo distribuidos en centros de datos y varios proveedores de servicios en la nube (CSP). Desafortunadamente, las configuraciones erróneas son comunes, lo que deja las identidades vulnerables comprometidas o brinda demasiado acceso, con la posibilidad de exponer información confidencial.

Los ciberdelincuentes están aprovechando la situación actual para atacar los recursos de la nube. Lo más común es que se hagan pasar por identidades autenticadas, aprovechen los permisos para obtener y elevar el acceso y lograr sus objetivos de ataque.

No puedes proteger tus recursos en la nube de ataques basados en identidad como estos utilizando las mismas estrategias que usarías en un mundo de archivos locales. Es increíblemente difícil rastrear la ruta de ataque real o potencial de una única identidad en un entorno tan distribuido, dinámico y poco uniforme. Las herramientas tradicionales (cortafuegos de red, servicios de directorio corporativo comunes y controles de acceso estáticos) no son efectivas en la realidad de la nube.

Por lo tanto, en respuesta a la escalada de ataques basados en identidad, las organizaciones están adoptando Cloud Identity Entitlement Management (CIEM) como solución de seguridad imprescindible. CIEM une los puntos a través de la capa de identidad para que comprendas y controles quién tiene acceso a qué, supervises su comportamiento y respondas rápidamente para contener las amenazas.

Si eres responsable de la seguridad de la nube, la arquitectura de la nube o la gestión de acceso e identidad (IAM) y estás considerando cómo las soluciones CIEM pueden encajar en tu hoja de ruta de seguridad, esta guía es para ti.

La información que contiene te ayudará a:

- Comprender los casos de uso de CIEM
- Ahorrar tiempo al prepararte para las conversaciones con los proveedores de CIEM proporcionándote una lista de verificación de preguntas que plantear mientras evalúas posibles soluciones.
- Ayudarte a comparar opciones y elegir la mejor solución CIEM para tus necesidades
- Considerar CIEM dentro del contexto de tu estrategia general de seguridad de identidad

Impacto de la nube en la seguridad de la identidad

En un entorno de nube, la seguridad de la identidad se vuelve mucho más compleja de administrar por varias razones:

Control distribuido: En lugar de un pequeño grupo de administración, numerosos usuarios y sistemas tienen acceso a datos y recursos e incluso pueden generar identidades.

Proliferación de roles: La cantidad de roles y permisos se ha disparado. Esto dificulta su gestión y comprensión sin herramientas especializadas.

Configuraciones erróneas: Los grupos mal configurados en los sistemas de gestión de identidades y/o recursos de la nube presentan riesgos sin que se detecten.

Brechas de visibilidad: Una combinación de diferentes proveedores de identidades, aplicaciones/servicios federados y usuarios de CSP locales restringe la monitorización de identidades y limita la comprensión del comportamiento en un entorno de nube.

Complejidad de los permisos de la nube: Los entornos de nube modernos cuentan con modelos de permisos complejos con miles de permisos posibles en numerosos servicios. Es fácil conceder permisos demasiado amplios por error, lo que genera permisos excesivos y de riesgo.

Pérdida de privilegios: Demasiadas identidades tienen más privilegios de los necesarios, lo que incumple las mejores prácticas de privilegios necesarios mínimos y confianza cero.

Cambio constante: Los entornos de nube experimentan cambios rápidos con nuevas identidades (especialmente identidades de máquinas) creadas constantemente y derechos aprovisionados y eliminados a velocidades vertiginosas. La naturaleza dinámica de los entornos de nube hace que la solución manual de problemas de permisos no sea escalable.

> CIEM une los puntos a través de la capa de identidad para que comprendas y controles quién tiene acceso a qué, supervises su comportamiento y respondas rápidamente para contener las amenazas.

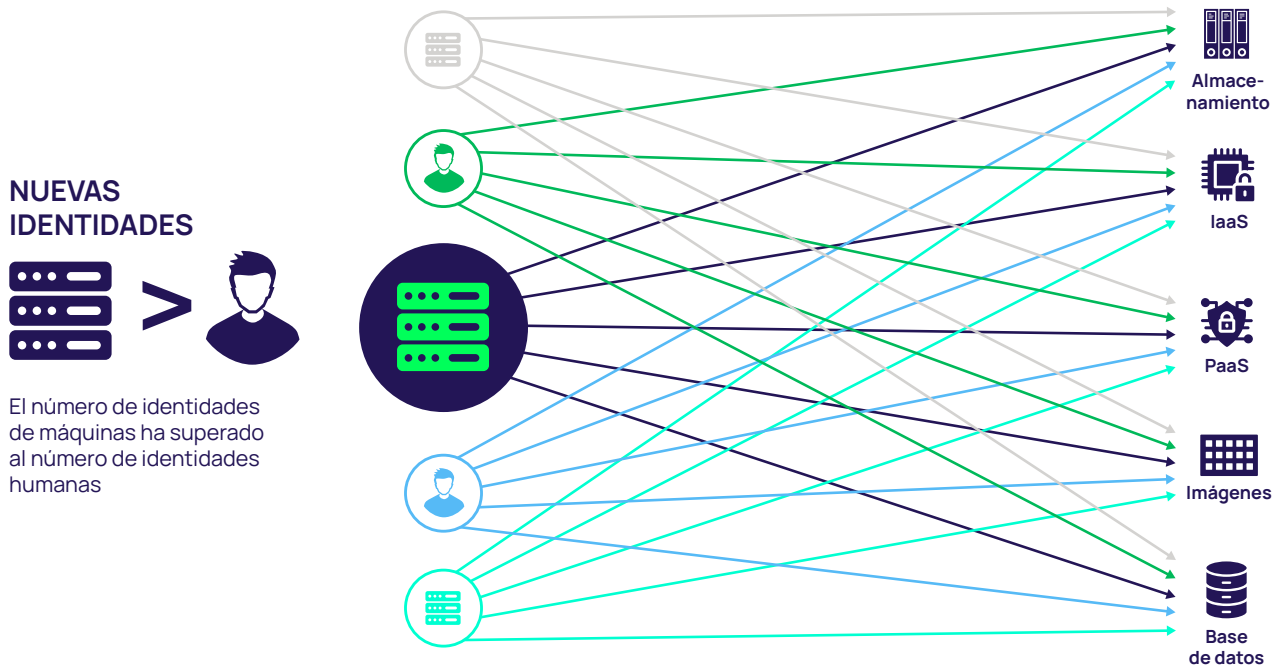
Cloud Infrastructure Entitlement Management (CIEM)

CIEM es el proceso de gestión de identidades y sus privilegios en entornos de nube. El propósito de CIEM es comprender qué derechos de acceso existen en entornos de nube y multinube, para luego identificar y mitigar los riesgos derivados de derechos que otorgan un nivel de acceso más alto del que deberían.

CIEM te ayuda a reducir estos riesgos de ataques basados en identidad mediante la aplicación de controles preventivos para la gobernanza de los derechos en identidad como servicio (IaaS) y plataforma como servicio (PaaS) híbridas y multinube. Mediante análisis y aprendizaje automático (ML), CIEM monitoriza continuamente identidades, permisos y actividades. Detecta anomalías en los derechos de las cuentas, como la acumulación de privilegios, permisos inactivos y cuentas o roles no utilizados. Al aplicar el principio de privilegio necesario mínimo, CIEM ayuda a garantizar que las identidades tengan acceso solo a lo que necesitan y minimiza tu superficie de ataque.

A diferencia de otras soluciones de seguridad en la nube, como las plataformas de protección de aplicaciones nativas de la nube (CNAPP), las soluciones CIEM se centran en el riesgo de identidad. Idealmente, las soluciones CIEM se integran en tu proceso de creación de identidad y gobernanza del ciclo de vida.

FIGURA 1 | La cantidad de identidades en una cuenta en la nube multiplicada por la cantidad de derechos que tiene cada identidad crea una superficie de ataque ingente.



Cuatro usos principales de las soluciones CIEM

1 Proporcionar visibilidad de los derechos de riesgo

CIEM proporciona visibilidad granular de identidades humanas y no humanas, activos confidenciales y derechos. Te muestra el «acceso efectivo» para cada identidad mediante el descubrimiento de posibles vías de acceso que pueden utilizar para navegar por tu entorno de TI. La detección de derechos inactivos y excesivos es una función central dentro de las soluciones CIEM (también conocida como gestión de permisos o auditoría de permisos).

2 Garantizar que los controles funcionen como se esperaba

CIEM te ayuda a garantizar que los controles de seguridad adecuados para la autenticación y autorización se apliquen y sean efectivos. Con CIEM, puedes reducir la posibilidad de que los ataques relacionados con la identidad obtengan un punto de apoyo inicial, mejoren el acceso o logren persistencia.

3 Detectar anomalías de comportamiento

CIEM te ayuda a reconocer cuándo se producen eventos contra la ciberseguridad. Recopila datos significativos mediante la monitorización continua de las identidades y su comportamiento, y proporciona el contexto esencial para comprender esa información. El aprendizaje automático enriquece el análisis de identidad histórico con datos de comportamiento, asegurando que los derechos otorgados se alineen con la necesidad y el uso genuinos.

4 Detectar y combatir amenazas relacionadas con la identidad

La corrección automática de riesgos es una característica esencial de una solución CIEM. Cuando se detecta un riesgo, CIEM recomienda un ajuste de política o activa un flujo de trabajo. Por ejemplo, CIEM puede abordar los derechos excesivos eliminando privilegios inactivos, corregir el incumplimiento de políticas reduciendo los privilegios y desencadenar acciones para solucionar configuraciones erróneas.

En la siguiente sección, encontrarás preguntas para hacerle a cualquier proveedor de soluciones CIEM sobre cada uno de estos casos de uso como parte de tu evaluación de proveedor.

Preguntas para proveedores de soluciones CIEM

1. Proporcionar visibilidad de los derechos de riesgo

Tu proveedor de identidad (IdP) no comprende realmente los derechos de tus CSP. La distribución normal de privilegios, los usuarios creados fuera de tu IdP (es decir, por administradores locales o identidades externas), los privilegios otorgados a través de membresías de grupos invisibles y otros factores crean puntos ciegos. CIEM completa la información que falta sobre el estado de facto y el uso de privilegios.

Estas capacidades CIEM sientan las bases para tus acciones de ciberseguridad al brindar visibilidad de extremo a extremo de tu superficie de ataque de identidad.

Capacidad CIEM	Preguntas para plantear a un proveedor de CIEM
Descubrir identidades humanas	¿Admites varios IdP (Okta, Azure Active Directory, PingOne, etc.)? ¿Puedes conectarte a sistemas de recursos humanos para realizar un seguimiento de los cambios de incorporaciones, traslados y bajas (JML) y las bajas parciales?
Descubrir identidades de máquinas	¿Puedes descubrir identidades de máquinas, como API y cargas de trabajo?
Descubrir identidades federadas	¿Puedes descubrir identidades federadas que se generan externamente y se unen a tu IdP mediante intercambio de tokens? ¿Puedes vincular la actividad en AWS a los usuarios federados para poder realizar un seguimiento de ellos?
Descubrir todos los servicios y aplicaciones críticos en la nube y su estado actual	¿Tu cobertura incluye IaaS y PaaS? ¿Qué CSP admites? ¿Puedes detectar carpetas confidenciales a las que se pueda acceder públicamente? ¿Qué hay de nuestros sistemas locales?
Descubrir permisos y privilegios para todo tipo de identidades	¿Puedes mostrar qué permisos se otorgan a quién y cómo en una vista centralizada? ¿Puedes proporcionar visibilidad granular a nivel de archivo de los permisos de acceso? ¿Puedes detectar identidades humanas y de máquinas con privilegios excesivos? ¿Cómo se descubren los privilegios ocultos otorgados a través de grupos, rutas de escalada de privilegios y configuraciones erróneas? ¿Puedes mostrarme contratistas que conserven acceso a activos con sus propias identidades?
Fusionar identidades	¿Se pueden fusionar identidades, incluidas aquellas que no están en nuestro IdP pero que tienen acceso a nuestros activos?
Descubrimiento continuo	¿Cómo descubre el sistema nuevas identidades y activos a medida que se crean para que puedan gestionarse rápidamente?
Descubrir identidades latentes y privilegios permanentes	¿Cómo se determina cuándo ya no se requiere una identidad o un acceso privilegiado? ¿Puedes mostrar el uso de privilegios de acceso, detectando privilegios no utilizados durante períodos específicos?

Capacidad CIEM	Preguntas para plantear a un proveedor de CIEM
Descubrir el acceso efectivo entre entornos	¿Cómo se rastrean las rutas de acceso y los permisos de derechos en todos los sistemas y entornos (locales y multinube)? ¿Ofreces visibilidad de extremo a extremo desde el IdP hasta el activo? ¿Puedes mostrarme rutas de escalada de privilegios, como el encadenamiento de roles y la concesión de acceso temporal a recursos, en Amazon Web Services? ¿Cómo creas visualizaciones de rutas de acceso para que sean fáciles de entender de inmediato?
Puntuación del riesgo	¿Puedes identificar identidades de alto riesgo en función del acceso efectivo? ¿Puedes proporcionar puntuaciones de riesgo para los usuarios en función de la totalidad del acceso? ¿Puedes agregar parámetros de riesgo e inteligencia sobre amenazas en una puntuación del riesgo de identidad dinámica y unificada?

2. Garantizar que los controles funcionen como se esperaba

La protección de tu superficie de amenazas de identidad contra ataques comienza con la reducción de los riesgos antes de que un atacante pueda aprovecharlos. Lo más probable es que tu organización ya cuente con algunos controles de identidad. Sin embargo, ¿estás seguro de que funcionan como se esperaba y que nada ha pasado desapercibido?

Estas capacidades CIEM te ayudan a garantizar que los controles de seguridad preventivos funcionen de manera efectiva para contener el posible radio de acción de un ataque basado en identidad. Las principales áreas de interés son imponer privilegios necesarios mínimos y contener rutas de escalada de privilegios porque niegan a un atacante que ha comprometido una identidad los privilegios que necesita para alcanzar sus objetivos.

Capacidad CIEM	Preguntas para plantear a un proveedor de CIEM
Soporte de autenticación	¿Puedes mostrarme qué identidades privilegiadas tienen habilitada la autenticación multifactor (MFA) y en qué nivel? ¿Puedes descubrir y corregir errores de configuración de IAM? ¿Puedes detectar configuraciones erróneas de riesgo que nos expondrían a la filtración de contraseñas en texto sin cifrado o a la suplantación de usuarios?
Soporte de autorización	¿Puedes mostrarme cómo los usuarios obtienen acceso a los activos a través de la pertenencia a un grupo (por ejemplo, grupos anidados, grupos públicos)? ¿Cómo limitas el acceso privilegiado? ¿Cómo eliminas las rutas de escalada de privilegios para contener los ataques?

3. Detectar anomalías de comportamiento

Detectar rutas y eventos de escalada de privilegios puede resultar extremadamente complicado en la nube debido a la complejidad y la falta de visibilidad. CIEM te ayuda a descubrir ataques basados en identidades en curso, incluidos intentos de obtener acceso inicial con credenciales comprometidas o escalar privilegios si los atacantes ya están dentro.

Capacidad CIEM	Preguntas para plantear a un proveedor de CIEM
Detección de tácticas, técnicas y procedimientos (TTP)	¿Puedes detectar bombardeos/ataques de fatiga de MFA? ¿Puedes detectar ataques de fuerza bruta? ¿Puedes detectar intentos fallidos de inicio de sesión mediante la introducción de credenciales robadas en múltiples aplicaciones que pueden indicar ataques relacionados a una identidad? ¿Puedes detectar el secuestro de sesión?
Actividades sospechosas	¿Puedes detectar cuándo se crean nuevas identidades privilegiadas? ¿Puedes detectar la reactivación de cuentas inactivas? ¿Puedes detectar una elevación o escalada de privilegios inesperada o no deseada? ¿Puedes detectar la conexión de nuevas fuentes de datos de identidad ascendentes, como IdP adicionales o aplicaciones de recursos humanos? ¿Puedes detectar configuraciones erróneas maliciosas recién creadas a nivel de IdP? ¿Puedes detectar cambios que los usuarios realizan en los registros de nuestro IdP que puedan indicar que están ocultando su actividad?
Monitorización del uso	¿Puedes proporcionar una línea de base de actividad para determinar el uso normal de los derechos de un usuario, de modo que sepamos cuándo se produce un comportamiento fuera de la norma? ¿La monitorización es continua?
Flexibilidad	¿Cómo me puedes ayudar a ampliar mis capacidades de detección existentes para nuevos IdP y aplicaciones en mis próximas fusiones y adquisiciones? Descríbeme tu flexibilidad para cambiar el alcance o agregar políticas de detección para la empresa recién adquirida o sus usuarios.

4. Reducción de riesgos y reparación

Debido al impacto potencial que pueden tener los cambios en los privilegios de acceso en el negocio, la reparación puede ser una tarea difícil de realizar. CIEM proporciona información práctica y recomendaciones sobre cómo reducir los riesgos con el contexto, basándose en factores como el acceso efectivo a una identidad, el comportamiento privilegiado y el posible radio de acción de un ataque.

Capacidad CIEM	Preguntas para plantear a un proveedor de CIEM
Tamaño correcto	¿Puedes proporcionar recomendaciones para ajustar el tamaño de las identidades y los permisos? ¿Cómo proporcionas contexto para comprender cómo ajustar el tamaño correctamente?
Puntuación del riesgo	¿Puedes identificar identidades de alto riesgo en función del acceso efectivo? ¿Puedes proporcionar puntuaciones de riesgo para los usuarios en función de la totalidad del acceso? ¿Puedes agregar parámetros de riesgo e inteligencia sobre amenazas en una puntuación del riesgo de identidad dinámica y unificada? ¿Puedo ajustar las fórmulas de puntuación de riesgo de las alertas que proporcionas?
Alertas	¿Cómo te integras con mis herramientas de seguridad para monitorización, análisis y alertas, como mi SIEM? ¿Puedes enviar webhooks o abrir tickets en sistemas de flujo de trabajo de TI como JIRA o ServiceNow?
Creación de políticas	¿Puedes crear nuevas políticas para permisos o roles?
Refactorización	¿Puedes refactorizar automáticamente los permisos de AWS/Azure/GCP para que sean más seguros en función del uso real?
Acciones de mitigación	¿Puedes automatizar las alertas a los usuarios para que cambien las contraseñas cuando se vean comprometidas sus credenciales? ¿Puedes cerrar automáticamente la sesión de los usuarios en las sesiones actuales para evitar ataques de secuestro mediante el robo de tokens? ¿Puedes desafiar al usuario mediante MFA adicional cuando realiza una actividad sospechosa o privilegiada? ¿O en función de su nivel de riesgo de identidad en constante cambio? ¿Puedes eliminar el acceso de terceros? ¿Puedes ajustar dinámicamente el acceso condicional según el nivel de riesgo? ¿Puedes automatizar los flujos de trabajo de reparación?

Las partnerships también importan

Un aspecto clave a la hora de seleccionar el proveedor adecuado es tener la confianza de que se desarrollará una relación a largo plazo. Un verdadero socio debe comprender su estrategia de seguridad de identidad y ayudarte a alcanzar tus objetivos, no solo venderte una herramienta CIEM.

El hecho es que una herramienta CIEM por sí sola no puede hacer mucho para mejorar tu postura de seguridad de identidad. Incorporar CIEM en el proceso de gobernanza de identidades de extremo a extremo significa que los sistemas se comunican entre sí, al igual que las personas. CIEM reúne a los equipos de seguridad, IAM y operaciones de TI porque tienen una imagen completa y precisa de la identidad y el acceso en la nube, una comprensión compartida del riesgo y pasos claros para la reparación.

Busca un proveedor que comprenda todas tus necesidades de identidad y pueda ofrecerte los resultados que esperas de manera oportuna. Para evitar sorpresas desagradables, haz estas preguntas a los proveedores desde el principio.

Capacidad del proveedor	Preguntas para plantear a un proveedor de CIEM
Es hora de valorar	¿Cuánto tiempo lleva la implementación? ¿Puedo ver resultados funcionales en 1 o 2 días? ¿Cómo me ayudarás a reducir el tiempo de respuesta ante incidentes?
Seguridad práctica	¿Qué conectores nativos tienes? ¿Tienes una API abierta? ¿Existe alguna necesidad de escribir scripts para operar tu solución? ¿Qué necesitas de mi parte para la implementación o integración? ¿Puedo ajustar las políticas de seguridad para rastrear y alertar sobre cuentas de riesgo sin necesidad de servicios profesionales o desarrollo de nuevas funciones? ¿Ofreces tu solución a través de una plataforma SaaS, junto con otros servicios privilegiados y de identidad, que podamos utilizar a medida que desarrollamos nuestro programa?
Apoyo estratégico	¿Cómo crees que CIEM encaja en mi estrategia general de seguridad de identidad? ¿Cómo puedes ayudarme a crear una convergencia entre los equipos?
Respuesta	¿Vas a atenderme cuando tenga preguntas o solicitudes de funciones? ¿Cómo de fácil es acceder a tu documentación técnica? ¿Tendré un administrador de éxito exclusivo? ¿Puedo obtener información sobre tu hoja de ruta?

Acerca de Delinea Privilege Control for Cloud Entitlements

Privilege Control for Cloud Entitlements proporciona a los responsables de seguridad en la nube un contexto profundo sobre el uso de la identidad y la nube para descubrir el exceso de privilegios y limitar la autorización en la infraestructura multinube para reducir el riesgo.

Descubre y visualiza continuamente todas las identidades, cuentas y su acceso en las nubes de Google, Amazon y Microsoft para identificar comportamientos anómalos y refactorizar los privilegios. Gracias a Delinea Platform, nativa de la nube, puedes integrar los derechos en la nube como parte de tu única fuente de confianza para la autorización de todas las identidades. Ahorra tiempo automatizando el descubrimiento y el desaprovisionamiento de cuentas locales y federadas obsoletas sin afectar a los equipos de TI.

Para obtener más información, visita nuestro sitio web https://delinea.com/products/privilege-control-for-cloud-entitlements. Descubre una demostración interactiva de Delinea Privilege Control for Cloud Entitlements en acción.

Delinea

Securing identities at every interaction

Delinea es pionera en la protección de identidades a través de la autorización centralizada, haciendo que las organizaciones actuales sean más seguras al gobernar sin problemas sus interacciones en entornos complejos. Delinea permite a las organizaciones aplicar el contexto y la inteligencia en todo el ciclo de vida de la identidad a través de la nube y la infraestructura tradicional, los datos y las aplicaciones SaaS para eliminar las amenazas relacionadas con la identidad. Con la autorización inteligente, Delinea proporciona la única plataforma que permite descubrir todas las identidades, asignar niveles de acceso adecuados, detectar irregularidades y responder inmediatamente a las amenazas de identidad en tiempo real. Delinea acelera la adopción por parte de sus equipos al desplegarse en semanas, no en meses, y los hace más productivos al requerir un 90% menos de recursos para su gestión que el competidor más cercano. Con un tiempo de actividad garantizado del 99,99%, Delinea Platform es la solución de seguridad de identidad más fiable disponible. Más información sobre Delinea en **LinkedIn**, **Twitter** y **YouTube**.