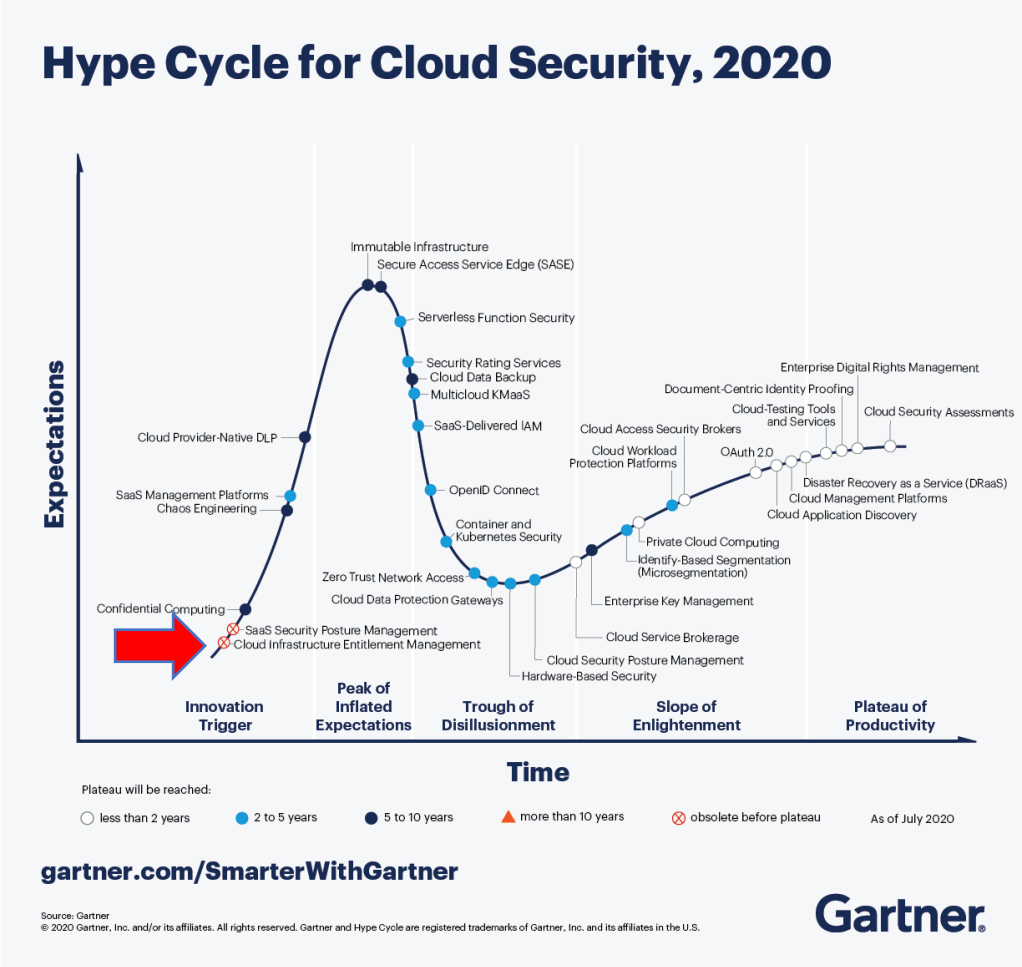
Título: Entenda o papel do Cloud Infrastructure Entitlement Management na jornada gestão de identidades, permissões, redução de risco e otimização de tempo

Data: 07/02/2023

Autor: Diego Oliveira

Cargo: Security Global Black Belt

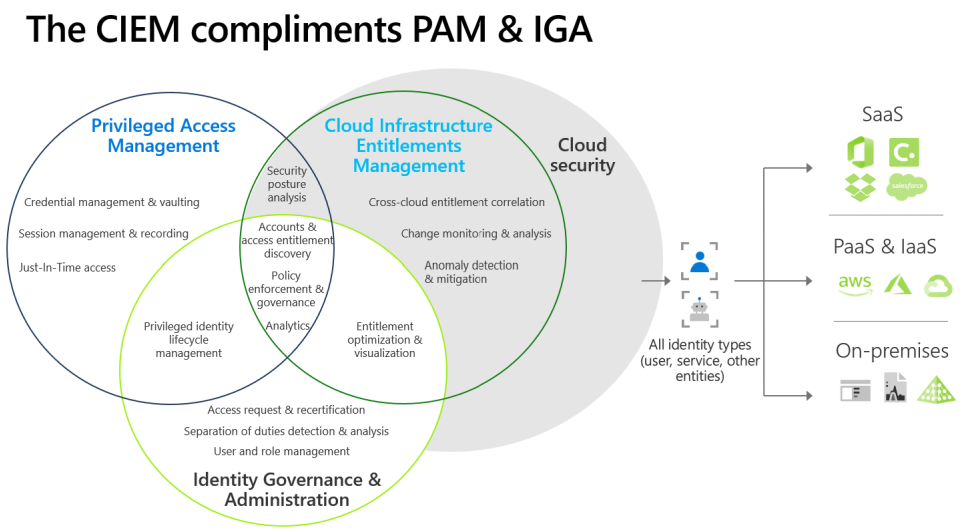
A abordagem Zero Trust é uma estratégia de segurança que se baseia no princípio de que nenhuma entidade, seja ela interna ou externa, deve ser automaticamente confiavel. Tal afirmativa inclui identidades humanas ou nao humanas, tais como: Workloads, aplicações, grupos ou recurso do tipo *functionless*. O Cloud Infrastructure Entitlement Management (CIEM), ou "*Kyn*" como é pronunciado globalmente, é uma nova categoria de ferramenta de segurança anunciado no relatório anual do Gartner de 2020 chamado **Cloud Security Hype Cycle.**



Fonte: [Top Actions From Gartner Hype Cycle for Cloud Security, 2020]

O CIEM estende o conceito de princípio de menor privilégio, conhecido pela sigla POLP (Principle of Least Privilege) para o ambiente de cloud pública ou CSP (Cloud Service Provider) de maneira muito efetiva e simples. POLP também está alinhado com outros capítulos de gestão de identidade representadas pelas categorias de Governança de Identidade de Acesso (IGA) e Gerenciamento de Acesso Privelegiado (PAM). Desta maneira, o CIEM potencializa e expande a visão das identidades em outra superficie, que até então era predominantemente mantida pelas ferramentas de IAM nativas de CSP.

CIEM, IGA e PAM, cada uma destas ferramentas tem um proposito diferente dentro da jornada de identidade o que nao gera conflito no posicionamento, pelo contrário agrega de maneira substancial valor na jornada gestão de identidades e permissões; vale ressaltar, que o cenário atual de multicloud incrementa significativamente a complexidade nesta jornada tendo cada CSP atuando com conceitos despojadamente distintos. E, exatamente neste ponto que CIEM vem apresentando um dos seus grandes beneficios, criar uma harmonia entre as diferentes categorias de ferramentas frente a árdua tarefa de manter todos os CSP's na mesma página no critério controle de permissões. Vejam aqui uma referência de como as ferramentas co-existem em prol do processo de gestão de identidades:



Enfoque: O CIEM se concentra na gestão de acesso a recursos de infraestrutura de nuvem, enquanto o PAM se concentra na gestão de acesso privilegiado a recursos críticos, o IGA se concentra na governança e administração de identidades.

Funcionalidade: O CIEM fornece um controle centralizado sobre o acesso a recursos de infraestrutura de nuvem, o PAM fornece uma abordagem segura para a gestão de acessos privilegiados, incluindo o monitoramento, o registro e a rotina de revogação, e o IGA fornece

uma visão geral da gestão de identidades, incluindo a criação, modificação e exclusão de contas.

Integração: O CIEM, o PAM e o IGA podem ser integrados entre si para fornecerem uma abordagem abrangente e integrada para a gestão de identidade e acesso.

Focando nos casos de uso mapeados com CIEM, compartilho aqui uma lista dos mais explorados atualmente e que tem elevado a qualidade das entregas das equipes de segurança a patamares superiores:

Governança de identidade: Permitir que somente identidades autorizadas tenham acesso a recursos críticos no CSP. Isso inclui também a gestão das próprias ferramentas nativas de segurança e gestão do CSP.

Multi-cloud: O CIEM cria uma camada centralizada de gerenciamento de acesso para vários CSP's traduzindo a complexidade de cada um em uma linguagem agnóstica, ajudando a garantir a conformidade e a segurança em ambientes multicloud de maneira simples.

Redução de risco: O CIEM evidência o risco dos ambientes com base no histórico de uso efetivo da identidade vs o alcance sob os recursos ativos, ajudando o time responsável a minimizar o risco ao aplicar limites a identidades que não estão consumindo todas as permissões outrora cedidas.

Otimização de tempo e recursos: O CIEM permite que as organizações otimizem o tempo dos times de segurança ao identificar, mitigar e monitorar de maneira automática os riscos latentes atrelados a identidade durante a sua jornada dentro do ambiente.

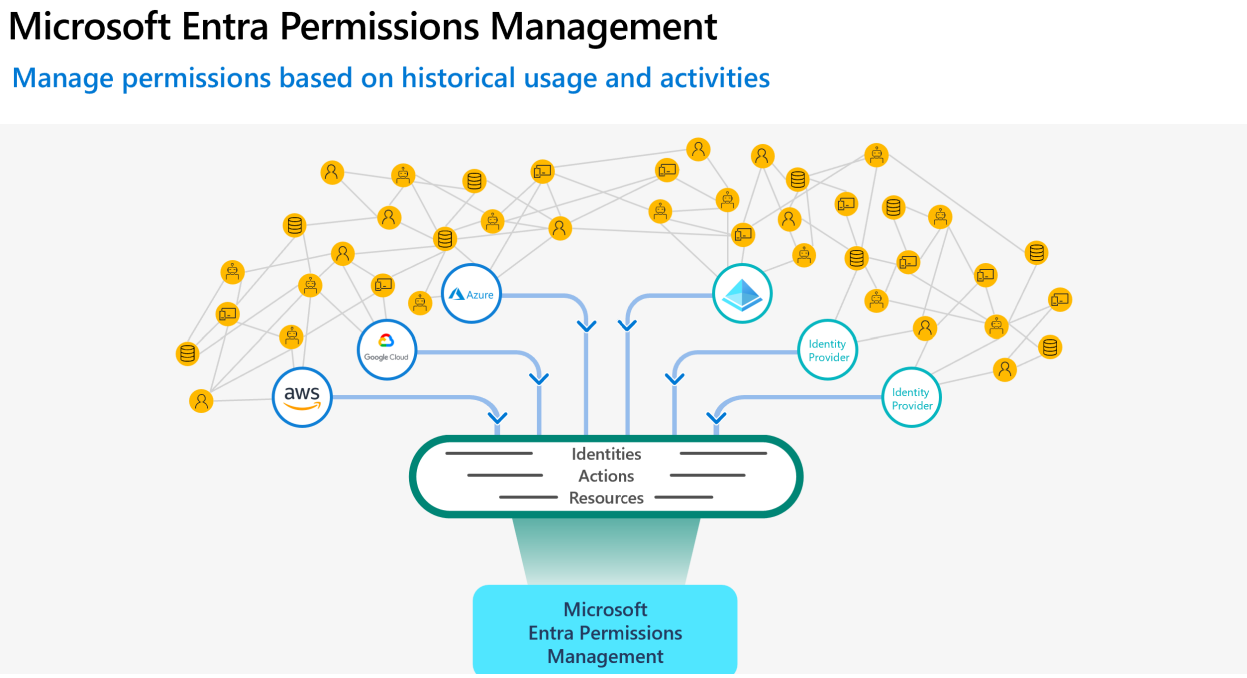
Break the Glass: Famoso conceito conhecido pelos times de ciberguranca para mitigar problemas em ativos de grande importância, o Break the Glass também faz parte do CIEM permitindo a aplicação de ações imediatas de controle situações de emergência.

Escalabilidade: O CIEM permite que as organizações gerenciem seus recursos na nuvem de forma escalável e prático acompanhando a evolução orgânica do ambiente, sem a necessidade de nenhum novo agente na arquitetura. Toda integração é realizada apenas uma vez por conector, fácil de plugar ou desplugar.

Análise de acesso: O CIEM fornece relatórios detalhados sobre acessos, incluindo quem acessou os recursos e quais ações granulares foram realizadas neste acesso, o que é útil para auditorias e outros processos de segurança.

Centralização de informações: O CIEM centraliza as informações sobre as identidade e seus relacionamentos com outras entidades dentro do ambiente nuvem passando por cenários de cross-account, tornando-as mais fáceis de gerenciar e monitorar.

Todos estes casos de uso compartilhados neste artigo são replicados na integra pelo **Microsoft Entra Permissions Management** (**MEPM**), a nossa solução de categoria CIEM. O **MEPM** suporta atualmente os 3 maiores CPS's, sendo eles Azure, AWS e GCP criando está camada agnóstica na gestão de permissão.



Em resumo, o **MEPM** é uma ferramenta valiosa para as organizações que buscam garantir a segurança, a conformidade e a eficiência na gestão de identidade e acesso em ambientes de nuvem. O **MEPM** permite que as organizações implementem políticas de segurança rigorosas, monitorar acessos e integrar-se com outras ferramentas de segurança para proteger seus recursos críticos.