



# Privilege Control for Cloud Entitlements

Aplique o privilégio mínimo permanente em nuvens públicas

A expansão das identidades humanas e de máquinas dispersas em várias nuvens públicas dificulta o monitoramento e o ajuste dos direitos pelas equipes de segurança da nuvem. Agentes mal-intencionados estão aproveitando a situação atual para atacar os recursos da nuvem. Eles colocam as identidades em perigo, passando-se por usuários legítimos para aproveitar os direitos existentes, aumentar os privilégios e obter acesso a sistemas e dados confidenciais.

Com muita frequência, os direitos de identidades privilegiadas na nuvem não são monitorados adequadamente, deixando contas obsoletas e órfãs e configurações incorretas de identidade que abrem brechas para invasores. Para proteger adequadamente seu ambiente multinuvem, você deve descobrir, monitorar e ajustar os direitos das identidades de nuvem. Isso inclui identidades humanas e de máquina, como contas de serviço e cargas de trabalho. As identidades de máquinas podem ser um ponto cego para muitas organizações, pois muitas vezes são provisionadas localmente, mas frequentemente esquecidas quando não são mais necessárias.

O Privilege Control for Cloud Entitlements fornece aos líderes de segurança um contexto profundo sobre o uso da nuvem e da identidade para descobrir privilégios excessivos e limitar a autorização em infraestruturas multinuvem a fim de reduzir riscos.

## COMO FUNCIONA

### ✓ **Descoberta contínua**

Localize com perfeição os direitos em nuvens públicas e provedores de identidade em ambientes de nuvem complexos e em constante mudança.

### ✓ **Ganho de visibilidade**

Veja rapidamente todas as identidades e seus caminhos de acesso na infraestrutura multinuvem pública em um único painel.

### ✓ **Identificação e remoção de configurações incorretas de identidade**

Reconheça automaticamente as configurações incorretas, como contas que não possuem autenticação multifator (MFA), e remova-as ou corrija-as.

### ✓ **Aplicação do privilégio mínimo**

Promova a definição correta dos direitos para limitar o risco e, ao mesmo tempo, permitir que os usuários tenham o acesso necessário para realizar seus trabalhos.

### ✓ **Unificação da administração**

Ofereça retorno rápido e menor custo total de propriedade com uma governança abrangente de privilégios na Delinea Platform nativa da nuvem.

## Benefícios do Privilege Control for Cloud Entitlement



### **POSTURA DE SEGURANÇA APRIMORADA**

Melhore a segurança com a visibilidade de todos os direitos de acesso e a capacidade de identificar permissões excessivas, bem como de aplicar práticas recomendadas de privilégio mínimo e confiança zero.



### **CONTEXTO DE IA/ML**

Utilize análises que criem contexto entre provedores de identidade e provedores de serviços em nuvem para normalizar quais direitos devem estar em vigor e avaliar outros para remoção.



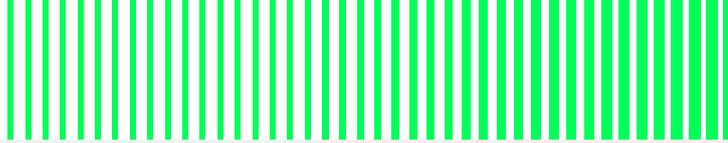
### **EFICIÊNCIA OPERACIONAL**

Automatize o gerenciamento de identidades e direitos, simplificando o acesso em ambientes de provedores de nuvem e acelerando a implantação de recursos.



### **REDUÇÃO DE RISCOS**

Monitore continuamente os direitos com privilégios excessivos e acesso incomum em identidades locais e federadas.

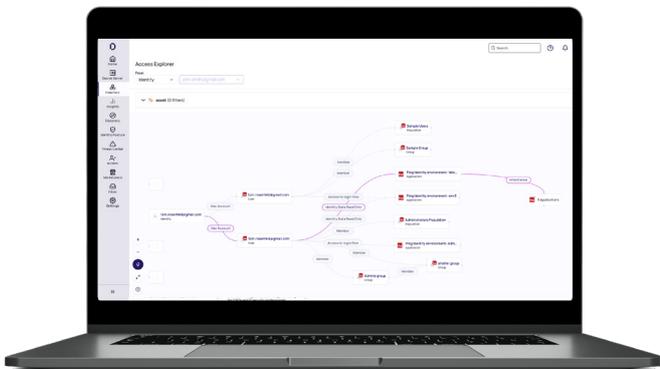


## O Privilege Control for Cloud Entitlement é fornecido na Delinea Platform nativa da nuvem, que impõe o privilégio mínimo permanente em nuvens públicas.

Integre os direitos de nuvem como parte de sua única fonte de verdade para autorização em todas as identidades. Economize tempo automatizando a descoberta e o desprovisionamento de contas locais e federadas obsoletas sem afetar as equipes de TI.

O Privilege Control for Cloud Entitlements fornece aos líderes de segurança um contexto profundo sobre o uso da nuvem e da identidade para descobrir privilégios excessivos e limitar a autorização em infraestruturas multinuvem a fim de reduzir riscos.

Usando o Delinea Privilege Control for Cloud Entitlements, os caminhos podem ser mapeados visualmente para determinar como o acesso foi obtido e o que mais pode ser feito por essa identidade.



### DESCOBERTA CONTÍNUA

Encontre identidades e seus direitos em ambientes de nuvem em constante mudança e cada vez mais complexos.

### APLICAÇÃO DO PRIVILÉGIO MÍNIMO

Defina rapidamente os direitos corretos para limitar os riscos e, ao mesmo tempo, aumentar a produtividade.

### RECONHECIMENTO DE IDENTIDADES DE RISCO

Encontre configurações incorretas e normalize o comportamento privilegiado em toda a infraestrutura de nuvem.

## Flexibilidade e agilidade para escalar os controles de segurança de PAM do seu jeito



### Essentials

Comece identificando, gerenciando e protegendo contas privilegiadas, com a capacidade de definir regras para solicitar acesso a credenciais e monitorar e auditar sessões de acesso remoto privilegiadas.



### Standard

Continue sua jornada de PAM protegendo-se contra ameaças de identidade, aplicando privilégios just-in-time e just-enough, bem como impondo MFA em profundidade.



### Enterprise

Aumente a automação e a inteligência em suas políticas de autorização para reduzir ainda mais os riscos relacionados à identidade e melhorar a produtividade.

Para obter mais informações, visite-nos em [Delinea.com](https://delinea.com)

## Delinea

A Delinea é pioneira na proteção de identidades por meio de autorização centralizada, tornando as organizações mais seguras ao controlar com perfeição suas interações em toda a empresa moderna. Ele aplica contexto e inteligência em todo o ciclo de vida da identidade, em infraestrutura tradicional e em nuvem, dados e aplicativos SaaS para eliminar ameaças relacionadas à identidade. Delinea fornece autorização inteligente para todas as identidades, permitindo identificação precisa do usuário, atribuição de acesso apropriada, monitoramento de interação e resposta rápida a irregularidades. A Plataforma Delinea acelera a adoção e aumenta a produtividade, sendo implementada em semanas, não em meses, exigindo apenas 10% dos recursos em comparação com os concorrentes. Descubra mais sobre Delinea em [delinea.com](https://delinea.com), [LinkedIn](#), [X](#), e [YouTube](#).