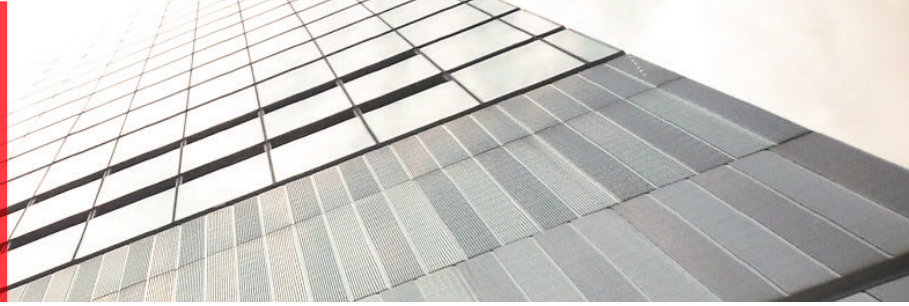

Centrify Privilege Elevation Service

Estabelecer Acesso com Privilégios Mínimos para Reduzir a Superfície de Ataque

Ao longo dos últimos anos, tornou-se evidente que os atacantes já não estão mais a "hackear" para provocar falhas de segurança de dados: estão simplesmente a fazer login utilizando credenciais privilegiadas fracas, furtadas ou de outra forma comprometidas. Uma vez lá dentro, tiram partido do facto de muitas organizações atribuírem privilégios a mais aos seus utilizadores administrativos. Isto permite aos hackers espalharem-se e deslocarem-se lateralmente por toda a rede, procurando furtivamente mais contas e credenciais privilegiadas que os ajudem a obter acesso privilegiado à infraestrutura mais crítica e aos dados confidenciais de uma organização. Zero Trust Privilege exige a concessão de privilégios "just enough" e "just-in-time" para limitar o movimento lateral em toda a rede.

Zona de Perigo: Privilégios A Mais

Privilégios mínimos como conceito é mais comum do que imagina. Pense no controlo de acesso físico no seu escritório: diferentes níveis de utilizadores têm direitos de acesso diferentes e, para obter acesso a determinadas áreas, deve solicitá-lo e ser aprovado. Isto tudo não é nada de novo no espaço da segurança física e a mesma lógica aplica-se à segurança lógica. Aplica-se ao conceder acesso granular baseado em funções a recursos privilegiados.

Outro objetivo da concessão de privilégios mínimos é limitar o movimento lateral em toda a rede. Trata-se da via principal através da qual atacantes obtêm acesso a dados confidenciais: começam num local e movem-se lateralmente até encontrarem o que estão a procurar. Se vedarmos aquilo a que têm acesso, podemos parar o movimento lateral. Do mesmo modo que ninguém deve ter um(a) só chave/crachá que permite acesso a tudo, não vai realmente querer utilizar a conta root num servidor, visto que dá maior acesso e não tem qualquer atribuição ao utilizador real, que chamaremos "Bob". Em vez disso, Bob deve fazer login diretamente no sistema de destino com os seus próprios direitos de administrador que lhe dão acesso para reiniciar apenas um conjunto específico de servidores. Se precisar de alterar a configuração ou aceder a um sistema de destino diferente, então deverá solicitar acesso por um período especificado. O acesso pode ser proporcionado automaticamente ou através de algo como ServiceNow® ou SailPoint Technologies®. Além disso, poderá ser solicitado a fornecer autenticação multifator (MFA). Uma vez concluído, os direitos de Bob serão reduzidos ao que é necessário.

Estabelecer Acesso com Privilégios Mínimos para Reduzir a Superfície de Ataque

O Centrify Privilege Elevation Service minimiza a exposição ao risco de ciberataques devido a indivíduos com privilégios a mais. O serviço permite que os clientes implementem as melhores práticas de acesso privilegiado "just enough", "just-in-time", limitando, por sua vez, potenciais danos provocados por falhas de segurança.

ELEVAÇÃO DE PRIVILÉGIOS

Proteja e faça a gestão de privilégios detalhados em todos os sistemas Windows, Linux e UNIX, limitando potenciais danos devido a falhas de segurança. Faça com que os utilizadores iniciem sessão como a sua própria identidade para responsabilização e eleve privilégios com base nas suas funções internas dentro de uma organização.

GESTÃO DE POLÍTICAS E DE FUNÇÕES DE PRIVILÉGIO DELEGADAS

Políticas centralizadas de funções, de direitos e de privilégios simplificam a gestão em ambientes heterogéneos (UNIX, Linux e Windows). As políticas são armazenadas no Active Directory, separadas de outros objetos comuns, de forma a dar suporte à delegação a administradores de servidor e à separação de deveres dos administradores do Active Directory, impedindo que os administradores de servidor façam a gestão de objetos do Active Directory que não deveriam. Tudo isto é feito sem modificações ao esquema do Active Directory.

ATRIBUIÇÃO DE FUNÇÕES BASEADA NO TEMPO

Minimize os riscos de segurança, ao permitir que os administradores solicitem sistematicamente uma nova função para obter os direitos necessários à realização das suas tarefas. A solicitação de acesso para funções privilegiadas permite que as organizações concedam privilégios e funções de longa duração ou temporários através de um modelo "just-in-time" flexível que acomoda as necessidades flutuantes do negócio.

MFA NA ELEVAÇÃO DE PRIVILÉGIOS

MFA no login é uma excelente melhor prática – especialmente para administradores. No entanto, ela deve ser aumentada com MFA na elevação de privilégios para proteger contra agentes mal-intencionados ao garantir que apenas pessoas autorizadas estejam a iniciar comandos privilegiados através da validação por MFA antes da execução de comandos privilegiados.

Conceder Privilégios Apenas Suficientes Em Windows, Linux e Unix

Reduza o risco de ataque por indivíduos com privilégios a mais e a utilização rotineira de contas privilegiadas partilhadas. A implementação de acesso com privilégios mínimos limita potenciais danos devido a falhas de segurança. Assim, o Centrify Privilege Elevation Service flexível e detalhado permite que os utilizadores realizem o trabalho, reduz os riscos e facilita a implementação de um modelo de privilégios mínimos "just-in-time", com controlos de acesso baseados em funções.

- Controlos de acesso baseados em funções facilitam a concessão de privilégios mínimos. A tecnologia patenteada do Centrify Zones fornece controlos de acesso altamente granulares e baseados em funções que simplificam a implementação de um modelo de privilégios mínimos nos sistemas Windows, Linux e UNIX.
- Proteja os seus sistemas Windows, Linux e UNIX ao controlar exatamente quem pode aceder o quê e quando. Ao contrário das ferramentas descentralizadas de utilização única, como sudo, Centrify permite a configuração de privilégios dinâmicos, para que os utilizadores possam elevar privilégios apenas a horas específicas, por um espaço de tempo e em determinados servidores. Também pode isolar servidores com base em tempo e relações de confiança para proteger ainda mais os dados confidenciais. Isto ajuda a limitar ainda mais o movimento lateral.
- Centrify fornece um poderoso conjunto de ferramentas para simplificar a adoção e a gestão de um modelo de acesso com privilégios mínimos.

Simplificar a Gestão de Ambientes Heterogéneos

Políticas centralizadas de funções, de direitos e de privilégios simplificam a gestão em ambientes heterogéneos (UNIX, Linux e Windows). As políticas dos Centrify Zero Trust Privilege Services são armazenadas no Active Directory, separadas de outros objetos comuns, de forma a dar suporte à delegação a administradores de servidor e à separação de deveres dos administradores do Active Directory, impedindo que os administradores de servidor façam a gestão de objetos AD que não deveriam. Centrify fornece, além disso, um modelo hierárquico de políticas projetado para oferecer suporte a modelos comuns de gestão empresarial para controlo centralizado descendente, com funções e direitos comuns geridos centralmente, além de oferecer suporte à delegação departamental, baseada em funções e em computadores a equipas administrativas subordinadas para atribuições de direitos a sistemas.

- O modelo de políticas consistente e estruturado, tanto para Windows como para Linux e UNIX, permite conformidade e menor custo de manutenção.
- A gestão de políticas Windows, Linux e UNIX no Active Directory impõe uma abordagem consistente no sentido da segurança de acesso privilegiado e, além disso, cria a separação adequada de deveres entre proprietários de políticas e administradores de sistema. Esta abordagem homogénea a ambientes heterogéneos assegura auditorias mais curtas e facilita a conformidade.

Solicitações Personalizadas de Funções para Privilégio "Just-In-Time"

Minimize os riscos de segurança, ao permitir que os administradores solicitem sistematicamente uma nova função para obter os direitos necessários à realização das suas tarefas. A solicitação de acesso para funções privilegiadas permite que as organizações concedam privilégios e funções temporários através de um modelo "just-in-time" flexível que acomoda as necessidades flutuantes do negócio.

- Permita que os administradores iniciem sessão como a sua própria identidade e eleve o privilégio ao solicitarem sistematicamente uma nova atribuição de função para obter os direitos necessários à realização das suas tarefas. Um sistema de solicitações personalizadas facilita a solicitação para a função e o período especificados e, se aprovado, revogará automaticamente esse direito após a expiração.
- Minimize a superfície de ataque ao permitir acesso temporário e limitado no tempo a contas e funções privilegiadas para obter privilégio "just-in-time". Conceda aos administradores de TI acesso a credenciais de contas privilegiadas, sessões de gestão remota ou quando precisarem modificar temporariamente a sua atribuição de funções para executarem tarefas administrativas adicionais.
- Reduza o risco de falhas de segurança de dados ao exigir aprovação para utilizadores de TI que precisam de aceder a sistemas com funções privilegiadas. Os utilizadores de TI da base de dados de gestão de ativos e de configurações (CMDB) da ServiceNow® ou das soluções de governança e administração de identidades da SailPoint Technologies® podem solicitar a utilização de uma função com privilégios para aceder a servidores específicos durante um período determinado. As aprovações são concedidas ou negadas através de um processo de gestão baseado em fluxo de trabalho.

Valide se o Utilizador com Privilégios Correto está a Utilizar Comandos Privilegiados

A execução de um comando privilegiado deve ser sempre protegida contra agentes mal-intencionados ao assegurar que apenas pessoas autorizadas ou apenas aplicações e serviços com direitos apropriados possam executar atividades privilegiadas. Centrify fornece tecnologia baseada no host que não pode ser contornada para impor MFA quando da execução privilegiada em servidores Linux, UNIX e Windows.

- Aplique MFA no login ao sistema ou ao cofre, ou durante a elevação de privilégio, a integração com Centrify Privileged Access Service permite um serviço MFA consistente e de fácil manutenção para todos os acessos privilegiados. Com a mais ampla variedade de autenticadores e suporte pronto para os Níveis 2 e 3 dos Níveis de Garantia NIST.
- Uma abordagem Zero Trust Privilege exige sempre que se verifique quem está a solicitar acesso privilegiado. O login de administradores do UNIX/Linux para verificação do sistema não é considerado como arriscado e não deve exigir MFA; no entanto, a execução de quaisquer comandos privilegiados deve ser configurada de modo a exigir MFA antes da execução, aproveitando os serviços MFA centralizados do Centrify.
- Uma abordagem Zero Trust Privilege exige sempre que se verifique quem está a solicitar acesso privilegiado. Os administradores Windows que precisam executar comandos privilegiados podem ser desafiados pela MFA, obrigados a efetuar a reautenticação com a sua palavra-passe do AD ou a validarem a sua identidade com um smart card.

A nossa missão é eliminar a principal causa de falhas de segurança: o abuso de acesso privilegiado. Com uma abordagem Zero Trust Privilege pronto para a nuvem, Centrify habilita os nossos clientes a protegerem o acesso à infraestrutura, a DevOps, à nuvem, aos containers, a Big Data e a outras superfícies de ataque de empresas modernas. Para saber mais, visite www.centrify.com.

EUA Sede +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Ásia Pacífico +61 1300 795 789
Brasil +55 11 3958 4876
América Latina +1 305 900 5354
sales@centrify.com

www.centrify.com