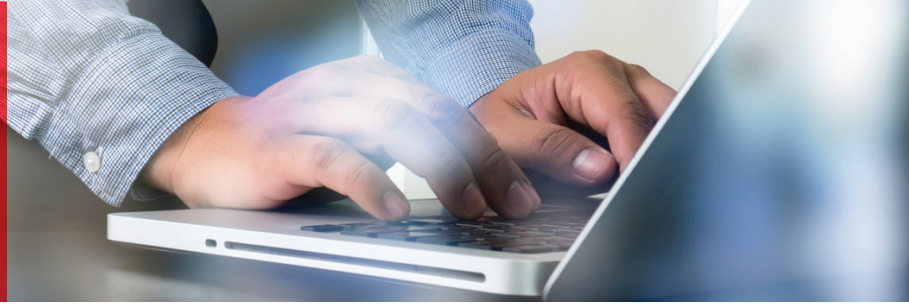

Centrify Authentication Service

Consolide Identidades para Reduzir a Superfície de Ataque

O cenário de ameaças atual difere drasticamente do passado, onde pessoas acediam à infraestrutura, às bases de dados e aos dispositivos de rede de uma organização, residindo todos dentro de uma fronteira bem definida. Hoje em dia, a gestão de acesso privilegiado (PAM) tem de lidar com solicitantes não humanos como máquinas, serviços e APIs. Ainda haverá contas partilhadas, mas, para maior garantia, as melhores práticas agora recomendam identidades individuais, não contas partilhadas, onde privilégios mínimos podem ser aplicados. Seja para mitigar o risco de ameaças internas e ameaças persistentes avançadas (APTs) ou para atender às exigências do PCI DSS, SOX ou outras do setor e regulamentações governamentais num ambiente cada vez mais heterogéneo e distribuído, as organizações de TI necessitam de uma solução Zero Trust Privilege pronta para a nuvem, que permite visibilidade e controlo centralizados sobre identidades, a gestão de acesso privilegiado e as atividade de utilizadores com privilégios.

PAM Legada Não é Suficiente para o Cenário de Ameaças Atual

PAM legada já existe há décadas e foi projetada numa época em que todo o acesso privilegiado estava restrito a sistemas e recursos dentro da rede de uma organização. O ambiente consistia em Administradores de Sistemas com uma conta "root" partilhada que faziam "check-out" num cofre de palavras-passe, geralmente para aceder a um servidor, uma base de dados ou um dispositivo de rede. PAM legada cumpriu o seu objetivo.

No entanto, não apenas o ambiente atual é diferente, os ciberadversários também estão a tirar proveito das credenciais privilegiadas comprometidas para executar os seus ataques. As organizações devem, portanto, eliminar contas locais e partilhadas com credenciais estáticas em sistemas e, em vez disso, utilizar contas individuais federadas com tokens de acesso temporários de forma a reduzir a respetiva superfície de ataque e, em última análise, fortalecer a sua postura de segurança. Por sua vez, muitas normas regulamentares e do setor, como NIST 800-63 e PCI DSS, estão a começar a exigir controlos de segurança que requerem níveis de garantia mais altos do que aqueles que podem ser fornecidos por cofres.

Ir Além da Descoberta e do Armazenamento Seguro de Palavras-Passe

O Centrify Authentication Service fornece aos clientes as capacidades necessárias para irem além do cofre, permitindo verificar adequadamente quem solicita acesso privilegiado. Isto pode ser conseguido aproveitando as identidades do diretório da empresa, eliminando contas locais e baixando o número total de contas e palavras-passe, reduzindo assim a superfície de ataque.

BROKER MULTIDIRETÓRIO

Simplifique a autenticação de utilizadores a servidores a partir de qualquer serviço de diretório, incluindo Active Directory, LDAP e diretórios na nuvem. As organizações podem aproveitar as vantagens da nuvem sem terem de criar novos repositórios de identidades fragmentados ou mecanismos de sincronização complexos.

BRIDGING DO ACTIVE DIRECTORY

Proteja sistemas Linux e UNIX com os mesmos serviços de identidade atualmente utilizados para proteger o acesso aos sistemas Windows. Centralize a gestão de políticas e a administração de utilizadores para sistemas Linux e UNIX a fim de permitir uma rápida consolidação de identidades para o Active Directory. Fornece integração profunda do Active Directory, mesmo para as arquiteturas mais complexas do Active Directory.

GESTÃO DE IDENTIDADES E CREDENCIAIS DE MÁQUINA

Administre centralmente as identidades de máquinas e respetivas credenciais no Active Directory ou nos Centrify Zero Trust Privilege Services para estabelecer uma raiz corporativa de confiança para autenticação computador a computador com base num modelo de confiança centralizado.

MFA NO LOGIN AO SISTEMA

O login em sistemas com privilégios é, geralmente, a principal interface de ataque que deve ser protegida contra ciberadversários que desejam roubar informações ou causar danos no ambiente. A autenticação multifator (MFA) no login para servidores Linux, UNIX e Windows minimiza o risco de exposição e satisfaz exigências regulamentares rigorosas como PCI DSS e NIST 800-63A. Com Centrify, pode ir além da MFA no login ao servidor e aplicar a MFA em toda a parte.

TECNOLOGIA CENTRIFY ZONE

Com a tecnologia patenteada do Centrify Zone consolide rapidamente, no Active Directory, identidades de utilizadores de sistemas UNIX e Linux complexas e díspares – sem ter de racionalizar previamente todas as identidades de utilizador. Centrify Zones permite gerir utilizadores, computadores, funções e direitos num modelo hierárquico que pode se moldar às suas necessidades.

GESTÃO DE CONTAS LOCAIS E GRUPOS

Faça a gestão de contas de sistema da mesma maneira que faria a gestão de contas de utilizador no Active Directory. Poupe tempo e dinheiro ao mesmo tempo que aumenta a produtividade da sua equipa de TI.

GESTÃO DE POLÍTICAS DE GRUPO

Faça a gestão de autenticação, controlo de acesso e política de grupo para sistemas não Windows da mesma forma que em sistemas Windows. Utilize a política de grupo do Active Directory para automatizar a configuração da firewall e de SSH, decidir quais utilizadores podem conectar-se a cada sistema, remover sessões inativas e atuar como uma autenticação baseada na rede.

Simplifique a Movimentação de Cargas de Trabalho para a Nuvem com Broker Multidiretórios

Simplifique a autenticação de utilizadores a servidores a partir de qualquer serviço de diretório, incluindo Active Directory, LDAP ou diretórios na nuvem como os da Google. As organizações podem aproveitar as vantagens da nuvem sem terem de criar novos silos de identidade, duplicarem repositórios de identidade ou comprometerem o nível de segurança do acesso privilegiado e do acesso empresarial de que atualmente dispõem on-premise. Além disso, os gestores de TI poupam tempo fazendo a gestão de um ambiente de TI heterogéneo, obtendo drásticas reduções de custos para a organização.

- Autentique-se em recursos privilegiados com qualquer serviço de diretório – on-premise e na nuvem.
- Ative a autenticação centralizada e os controlos de acesso a infraestruturas geograficamente dispersas, aproveitando identidades de um ou mais ambientes Active Directory, diretórios LDAP ou diretórios na nuvem, como Centrify Directory ou Google Directory.

Gestão e Consolidação de Identidades para Linux e Unix com Bridging do Active Directory

Centrify Authentication Service permite que os clientes unifiquem a sua infraestrutura de TI consolidando a gestão de identidades, autenticações e acessos para Linux e UNIX no âmbito do Microsoft Active Directory. Nesse contexto, a Centrify foi o primeiro fornecedor a integrar UNIX e Linux no Active Directory, suportando identidades múltiplas para um único utilizador. No Magic Quadrant for Privileged Access Management de 2018, a Gartner destaca especificamente o poder único do Centrify nesta área, que é uma capacidade popular entre clientes e potenciais interessados devido ao seu potencial para aumentar a produtividade e reduzir os custos de manutenção de TI, para além de reduzir a superfície de ataque.

- Associe nativamente os sistemas Linux e UNIX ao Active Directory, fazendo do sistema host um cliente do Active Directory. Proteja sistemas utilizando os mesmos serviços de autenticação e política de grupo atualmente implementados nos sistemas Windows.
- Consolide perfis de utilizadores e imponha a separação de deveres.
- Amplie a gestão de políticas de grupo a sistemas não Windows. Trata-se da única solução que fornece políticas de utilizador e de computador com funcionalidades avançadas, como filtragem de grupos e processamento de loopbacks. As definições de configuração da política de grupo são perfeitamente integradas no Centrify UNIX Agent por forma a gerir a configuração tanto da configuração do sistema como do ambiente do utilizador.
- Embora muitos fornecedores afirmem ter suporte para Kerberos, apenas a Centrify fornece suporte nativo para toda a complexidade e as nuances do Active Directory.
- A automação que economiza tempo é facilitada com amplas opções de CLI e de scripting, suportando a Gestão de Palavras-passe de Aplicativo para Aplicativo (AAPM).

Faça a Gestão de Contas e Grupos Locais Com Eficácia

Com o Centrify Authentication Service, os clientes podem otimizar a gestão de contas e grupos locais em toda a sua infraestrutura heterogénea. Centrify automatiza o ciclo de vida de contas locais e integra-se, sempre que necessário, com cofres de palavras-passe para serviços ou aplicações a fim de centralizar toda a gestão de contas e grupos numa única plataforma de gestão.

- Administre centralmente o ciclo de vida de contas de aplicação e de serviço, e proteja automaticamente credenciais e acesso.
- Integre a gestão de palavras-passe de contas locais com cofres de palavras-passe existentes, automatizando o registo de contas e o armazenamento seguro de palavras-passe para contas recém-criadas.
- Centralize a gestão de grupos locais.

Centralize Rapidamente a Gestão de Servidores Windows, Linux e Unix

A tecnologia Centrify Zone permite-lhe gerir o seu ambiente heterogéneo, vinculando os direitos que um utilizador possui num sistema Windows, Linux ou UNIX a uma única identidade, armazenada e gerida no Active Directory.

- Estabeleça hierarquia e herança.
- Permita a migração rápida de identidades UNIX para o Active Directory.
- Aproveite as Funções de Computador Centrify para obter vantagens exclusivas de gestão e segurança.

Imponha Políticas de Grupo para Utilizadores e Sistemas Heterogéneos

Centrify proporciona suporte abrangente a ampliação da gestão de políticas de grupo a sistemas não Windows. Trata-se da única solução que fornece políticas de utilizador e de computador com funcionalidades avançadas, como filtragem de grupos e processamento de loopbacks.

- Imponha políticas de grupo do Active Directory em todas as plataformas não Windows.
- Faça a gestão de autenticação, controlo de acesso e política de grupo para sistemas não Windows.

Assegure-se de Que Apenas Pessoas Autorizadas Estão a Aceder à Sua Infraestrutura Crítica com MFA no Login ao Sistema

O login em sistemas com privilégios é, geralmente, a principal interface de ataque que deve ser protegida contra ciberadversários que desejam roubar informações ou causar danos no ambiente. Para assegurar que apenas pessoas autorizadas acederão aos seus sistemas confidenciais, é preciso impor autenticação forte por meio da MFA. Centrify fornece tecnologia baseada no host que não pode ser contornada para impor MFA no login ao sistema para servidores Linux, UNIX e Windows, bem como estações de trabalho.

- Reforce os princípios de Zero Trust através da imposição da MFA baseada no host, que não pode ser contornada ou ignorada, em cada computador.
- Integração centralizada do serviço MFA.
- Capacidades de MFA locais para UNIX e Linux.
- MFA Windows nativamente integrada no processo de login.

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