DISRUPTEC

BeyondTrust

Como Ver, Gerenciar e Proteger os Caminhos para os Privilégios

Caminhos Para os Privilégios™

A segurança é uma jornada, não um destino. E essa máxima é verdadeira especialmente quando se trata de proteger identidades e seus privilégios.

BeyondTrust

ÍNDICE

Introdução

O princípio do menor privilégio e a disciplina da Gestão de Acessos Privilegiados (PAM) há muito tempo são pilares da segurança de TI. Sabemos que os privilégios são fortes alvo de ataques e, por isso, é essencial protegê-los. No entanto, a tecnologia moderna e os cenários de ameaças evoluíram significativamente, e a maioria das organizações está abordando o desafio da segurança de identidades e dos privilégios de forma incompleta porque estão ignorando os caminhos para os privilégios. **Mas os invasores não.**

> Para proteger identidades de forma eficaz, você precisa ir além da gestão direta de contas privilegiadas, e saber como as identidades humanas e não humanas acessam os privilégios.

Isso significa que você precisa observar a infraestrutura de identidades que concede privilégios, as políticas e os grupos usados para gerenciar privilégios e as conexões entre identidades e contas que abrem caminhos em diferentes domínios (por exemplo, fornecendo caminhos do ambiente on-premise para a nuvem). Todos estes são caminhos para privilégios que, se não forem contabilizados e protegidos, podem minar a segurança das identidades da sua empresa – incluindo a própria infraestrutura de identidades.

Nesse documento, você saberá quais são os caminhos para os privilégios, como e por que os invasores os procuram, e como observar seu ambiente pela lente de um invasor para entender e defender melhor seu cenário de identidades. Saiba também como a Plataforma BeyondTrust aborda muito mais que o PAM a fim de descobrir, gerenciar e proteger os caminhos para os privilégios.

O que é privilégio?

Antes de definir caminhos para os privilégios, precisamos definir o que é privilégio no contexto da segurança de identidades.

Privilégio é um direito concedido a uma identidade para poder ser usada na realização de operações relevantes de segurança.

Embora muitas vezes pensemos em privilégios em termos de identidades humanas com contas de usuários administradores e não administradores, é importante destacar que o privilégio não é binário e nem todo privilégio é administrativo.

Existem vários planos de privilégios que concedem às identidades acesso a sistemas, recursos e dados por meio de modelos tradicionais de privilégios on-premise ou por meio de funções e direitos em ambientes de nuvem e SaaS.

Enquanto as organizações geralmente se concentram em privilégios administrativos, os privilégios atribuídos a um usuário comum, não administrador, podem causar danos significativos.

Existem vários planos de privilégios que concedem às identidades acesso a sistemas, recursos e dados.

Um usuário aparentemente com poucos privilégios tem a capacidade de executar código e acessar dados – que podem ser explorados por ameaças, como ransomware, caso sua credencial seja comprometida. Na pior das hipóteses, um usuário pode receber involuntariamente um nível muito alto de privilégio como resultado de participação em grupos, configurações incorretas ou confusão sobre qual privilégio uma função permite. Esses cenários podem possibilitar que esse usuário (ou um invasor que o tenha comprometido) assuma facilmente uma função altamente privilegiada.

Além das identidades humanas, há outro tipo importante de identidade: as não humanas (INHs). Estas podem superar muitas vezes o número de identidades humanas em alguns ambientes de TI. As INHs (às vezes chamadas de identidades de máquina) podem ser contas de serviço, de sistema, de máquina ou de aplicações. Em geral, são usadas para permitir que aplicações e serviços interajam entre si.

Embora as INHs possam receber privilégios significativos, elas muitas vezes não possuem camadas adicionais de proteção (MFA, por exemplo) usadas para identidades humanas. Além das credenciais normais de nome de usuário e senha, as identidades não humanas podem ter chaves API, chaves SSH e certificados usados para autenticação. Elas podem ter diferentes níveis de controles aplicados a elas ao acessar o privilégio.

> As credenciais representaram quase 90% dos ativos em nuvem à venda na dark web. E o uso de credenciais válidas foi o vetor de acesso inicial mais comum em incidentes de segurança na nuvem.

IBM Security, Relatório de cenário de ameaças à nuvem do IBM Security X-Force de 2023. Setembro. 2023.

Ao pensar em segurança e privilégios das identidades, precisamos considerar todas as identidades, contas e privilégios. Isso se aplica a contas humanas, não humanas/máquinas, colaboradores, fornecedores e demais terceiros.

A maioria das organizações se vê gerenciando sistemas díspares e isolados e tendo que usar soluções pontuais focadas em casos de uso específicos em toda a estrutura de identidades. Esses desafios são ainda agravados por estruturas organizacionais onde o gerenciamento de acessos de identidades (IAM) e as equipes de segurança são completamente separados.

As lacunas entre esses silos de identidades criam pontos cegos que impedem a capacidade de ver holisticamente identidades e privilégios. Como a segurança de identidades atravessa todos os domínios, precisamos visualizá-las através de uma lente de domínio cruzado para ter uma visão completa.

Quais são os caminhos para os privilégios?

A importância dos privilégios e dos acessos privilegiados para a segurança está bem estabelecida, mas a proteção das identidades modernas exige ir além dessas noções básicas de privilégio para encontrar e proteger os caminhos até eles.

Os caminhos para os privilégios podem ser indiretos ou bem ocultos na análise de ferramentas de segurança. No entanto, se forem encontrados e explorados por agentes de ameaças, esses caminhos poderão acelerar o comprometimento das identidades, minar a integridade da infraestrutura de identidades e deixar uma empresa muito vulnerável.

Caminhos para os privilégios são qualquer coisa que possa ser aproveitada para obter acesso a um privilégio – uma conta privilegiada que possa ser comprometida, um segredo que possa ser usado para autenticação, uma configuração incorreta que permita a elevação de privilégios, uma VPN vulnerável a um ataque de senha que fornece acesso a toda a rede ou infraestrutura de identidades que é explorada para conceder privilégios.

> Para evitar o uso indevido de privilégios em um ambiente, você precisa entender todos os caminhos que um invasor pode explorar.

Depois de ter visibilidade dos caminhos para os privilégios, você pode começar a aplicar o princípio do menor privilégio para remover caminhos que não são absolutamente necessários e, em seguida, aplicar controles e proteções para os que são necessários. Dada a natureza dinâmica dos ambientes de TI modernos, este precisa ser um processo contínuo. Ao focar nos caminhos para obter privilégios à medida que identidades, aplicações e sistemas são integrados, desativados e atualizados, você pode garantir melhor que sua postura de segurança de identidades permaneça reforçada, mesmo que seu ambiente mude.

Por que é Importante Entender o Contexto

Ao pensar nos caminhos para os privilégios e nos riscos, é importante estar ciente do contexto de negócios. Por exemplo, ter o privilégio de acessar dados em um determinado sistema de uma organização pode representar um altíssimo risco para o negócio em virtude da alta sensibilidade desses dados. Em contrapartida, para outra empresa, esse mesmo privilégio pode representar pouco ou nenhum risco. Da mesma forma, uma conta em um ambiente de teste pode ser considerada de baixo risco, enquanto um administrador de domínio no ambiente corporativo é de alto risco.

Mas o que acontece quando existe uma relação de confiança entre os dois ambientes?

Nesse caso, há um caminho para o privilégio da conta no ambiente de teste que se extende para o ambiente corporativo. Isso permite que uma conta de teste comprometida autentique e acesse recursos no ambiente corporativo. Essas conexões e relações de confiança tornaram-se muito comuns à medida que as organizações buscam maneiras fáceis de testar novos sistemas e migrá-los para ambientes de produção.

Essas conexões destacam como os invasores vencem: procurando caminhos para obter privilégios, em vez de apenas observar os limites do sistema. É essencial considerar todos os caminhos possíveis para obter privilégios da perspectiva de um invasor, para que se possa proteger adequadamente as identidades privilegiadas em seu ambiente contra rotas complexas de ataque entre domínios.

Indo além do PAM para Proteger Privilégios

Quando pensamos em proteger nossas organizações, a gestão de acessos privilegiados (PAM) e a proteção de contas privilegiadas tradicionais é frequentemente a prioridade. PAM é uma base essencial de qualquer programa de segurança. As organizações normalmente começam concentrando-se no gerenciamento direto de identidades humanas privilegiadas.

No entanto, em qualquer ecossistema de identidades moderno, há muitas maneiras diferentes de atribuir, acessar e autorizar privilégios, e isso apresenta uma grande superfície de ataque de identidades.

> Para proteger os privilégios, você precisa ir além da gestão de identidades privilegiadas. É preciso saber também como elas podem acessar os privilégios elevados.

Considere contas de administrador de domínio. Em um ambiente tradicional, você poderia seguir as práticas recomendadas: limitar o número de contas, implementar MFA e usar uma solução PAM para fornecer acesso just-in-time e automatizar a rotação de credenciais.

Atualmente, precisamos pensar como um invasor no que se refere a caminhos alternativos para acesso de admin de domínio. Por exemplo:

Modelos de certificado mal configurados no Active Directory Certificate Services (AD CS) podem fornecer ao invasor um caminho para se autenticar como administrador de domínio a partir de qualquer conta de domínio válida.

Permissões fracas em grupos AD podem fornecer ao invasor um caminho para se adicionar a um grupo de administrador ou a um grupo com privilégios equivalentes a administrador.

Contas de serviço podem ter altos níveis de privilégio e serem vulneráveis à exploração, fornecendo um caminho para criar uma nova conta de administrador de domínio.

Contas de agente de sincronização do AD (Entra ID) em ambiente Azure herdado com privilégios de administrador global podem permitir que um usuário com acesso ao sistema do agente de sincronização capture credenciais altamente privilegiadas e migre para a nuvem ou altere associações do AD.

Esses caminhos para o privilégio são todos exemplos de técnicas de ataque comuns que os atores de ameaças utilizam para movimento lateral e escalação de privilégios. Embora essas técnicas sejam comumente usadas porque exploram caminhos indiretos para obter privilégios, muitas empresas lutam para encontrar, gerenciar e proteger esses caminhos em virtude da complexidade de seus ambientes e da natureza isolada de sistemas e ferramentas.

Caminhos Comuns para o Privilégio

Contas Humanas e Não Humanas

Comprometer uma identidade humana é um dos pontos de entrada mais conhecidos para encontrar e explorar acessos privilegiados e caminhos para privilégios. Um invasor pode usar credenciais comprometidas para autenticar a identidade e explorar os privilégios que a conta possui diretamente ou indiretamente. Eles também podem usar phishing, ou explorar software ou malware para executar código como uma conta para acessar os privilégios. Em alguns casos, um invasor pode até usar malware em um endpoint que permite capturar um token de sessão após o usuário ter se autenticado usando MFA. Conseguir tal exploração dá ao invasor acesso a privilégios sem precisar saber qual é a senha da conta ou ter que passar pelo MFA.

Quando uma identidade tem privilégios de administrador local, abre-se uma variedade de caminhos para acessar os privilégios. Se uma conta de administrador local for comprometida, um invasor poderá usar os privilégios da conta para capturar as credenciais de outros usuários logados no sistema usando ferramentas comuns, como Mimikatz. Essas credenciais poderiam então ser usadas para movimentação lateral, criação de novas contas localmente, acesso aos dados de outros usuários locais, adulteração de controles de segurança de endpoint e elevação para o nível de SISTEMA. É por isso que a remoção do privilégio de administrador local é uma mitigação crítica. Identidades não humanas, como contas de serviço, apresentam alvos de alto valor porque geralmente são altamente privilegiadas, mas ainda não possuem os controles de MFA aplicados em contas humanas. Usando uma conta de domínio comprometida, um invasor pode utilizar técnicas, como Kerberoasting, para capturar as credenciais de uma conta de serviço e acessar novos caminhos para movimentação lateral.

Essas identidades não humanas também podem ser expostas em código ou arquivos de configuração, onde as credenciais da conta são armazenadas em texto simples. Novamente, é provável que sejam contas altamente privilegiadas usadas para executar tarefas importantes, por isso é fundamental gerenciar e proteger os caminhos para esses privilégios.

A capacidade de entender quais privilégios as contas podem acessar, a exposição ao risco quando as contas estão inativas e quais contas têm falta de higiene de senha ou não possuem controles adequados (como MFA ou políticas de acesso condicional) podem ajudá-lo a ver caminhos para privilégios e os riscos que um invasor pode encontrar e explorar. Este é um recurso crítico para fortalecer proativamente a postura de segurança das identidades, bem como para detectar e responder com eficácia a ataques.

Segredos Expostos

Muitas violações começam com um invasor ganhando uma posição de baixo privilégio em uma rede e, em seguida, investigando o ambiente em busca de segredos que possam abrir novos caminhos para os privilégios. Esses caminhos podem ser credenciais armazenadas em texto simples, chaves de API salvas localmente em scripts, ou certificados armazenados em recursos compartilhados de rede. Os segredos expostos podem fornecer uma variedade de caminhos de privilégio entre domínios, permitindo que um invasor passe de um ambiente on-premise para a nuvem e escale privilégios.

Por exemplo, armazenar credenciais para uma conta de serviço privilegiado não gerenciado em um script ou arquivo de configuração representa um caminho que é fácil de ser explorado por um invasor, especialmente quando as credenciais não estão sendo alternadas. Mesmo que inicialmente os invasores obtenham acesso apenas a uma identidade de baixo privilégio, esse acesso pode permitir que eles realizem reconhecimento no ambiente e encontrem segredos expostos que abrem novos caminhos para privilégios.

Nos últimos anos, o grupo internacional de extorsão cibernética LAPSUS$ comprometeu grandes empresas, incluindo Microsoft, Nvidia, Ubisoft, Okta e Samsung (entre outras), sem flexibilizar quaisquer conjuntos de habilidades técnicas significativas. Eles simplesmente exploraram identidades e caminhos para obter privilégios, aproveitando ferramentas disponíveis no mercado para reconhecimento e acesso remoto.

Aqui estão algumas técnicas observadas durante violações do LAPSUS$:

- Acesso e extração de sites corporativos do Microsoft SharePoint para identificar segredos armazenados em documentação técnica.
- Acesso a armazenamentos de senhas e bancos de dados locais para obter mais segredos.
- Clonagem de repositórios Git para extrair chaves API.
- Uso de credenciais comprometidas para acessar VPNs corporativas.

Os invasores também podem utilizar segredos expostos em violações de terceiros. Por exemplo, os segredos comprometidos podem ser usados em um ataque direcionado ou em ataques mais amplos de pulverização de senhas e de preenchimento de credenciais (onde as credenciais comprometidas são testadas em uma variedade de serviços de nuvem).

As empresas Cisco e Duo Labs emitiram avisos de um número crescente de ataques de pulverização de senhas em grande escala, aproveitando credenciais comumente usadas ou comprometidas. Embora essas técnicas de ataque não sejam novas, a escala e a sofisticação aumentaram. O número cada vez maior de caminhos para obter privilégios oferece aos invasores uma gama de opções que eles podem aproveitar caso consigam comprometer uma identidade.

Infraestrutura de Identidades

A infraestrutura de identidades fornece autenticação e autorização para caminhos aos privilégios, tornando-a um alvo muito desejável para os agentes de ameaças. Apesar desse alto nível de risco, o monitoramento e a proteção da infraestrutura de identidades em si são muitas vezes inadequados e caracterizados por perigosos pontos cegos e lacunas de segurança.

Configurações incorretas da infraestrutura de identidades podem fornecer aos invasores caminhos aos privilégios. Por exemplo, configurações incorretas nos Serviços de Certificados do Active Directory podem fornecer um caminho para qualquer usuário de domínio válido se autenticar como administrador de domínio. Da mesma forma, uma conta de sincronização Entra privilegiada pode não ter uma política de acesso condicional aplicada, tornando possível a autenticação na nuvem fora de locais confiáveis e sistemas gerenciados.

A infraestrutura de identidades pode também ser explorada diretamente. Por exemplo, o grupo Scattered Spider e outros têm como alvo contas de superadministrador do Okta por meio de engenharia social no suporte técnico para redefinir senhas e controles de MFA. Depois que os invasores fazem login no Okta como superadministrador, eles conseguem adicionar seu próprio IdP não autorizado ao ambiente, permitindo-se acessar aplicações na organização comprometida.

Os caminhos da infraestrutura de identidades para privilégios geralmente ficam ocultos. Os diferentes sistemas de identidade podem pertencer a equipes diferentes, e podem exigir conhecimento especializado para serem compreendidos. E os eventos dos sistemas podem não ser consumidos ou compreendidos pelo SIEM ou pelas ferramentas de segurança.

Ter a capacidade de entender quando existem configurações incorretas de alto risco e quando são feitas alterações de alto risco na infraestrutura de identidades é fundamental para encontrar, gerenciar e proteger caminhos aos privilégios.

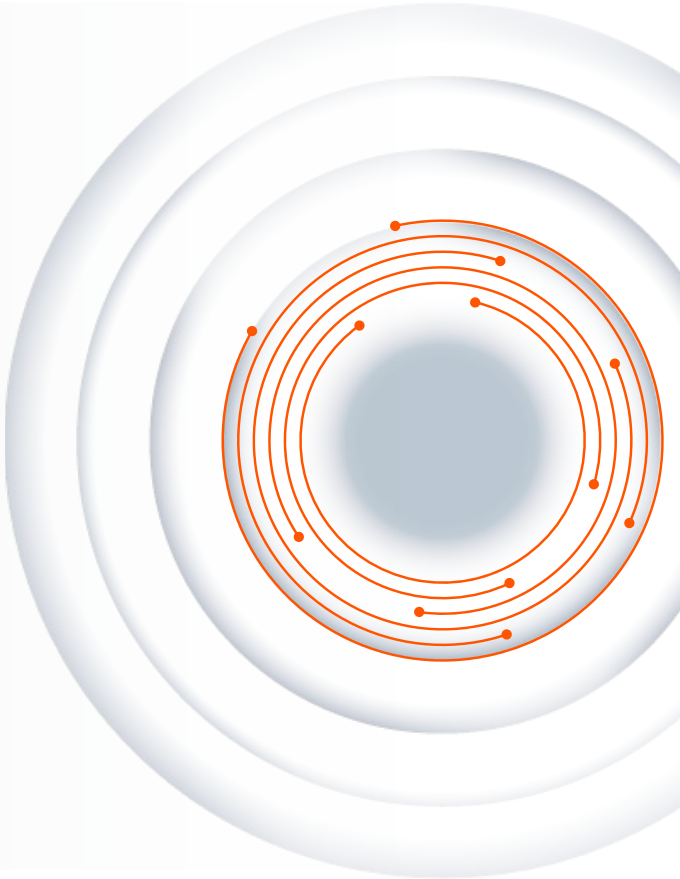
Acesso Remoto

Soluções de acesso remoto comumente usadas, como VPNs e RDPs, podem levar a muitos caminhos aos privilégios porque podem abrir o acesso a uma rede inteira, pois o usuário só precisa acessar um sistema ou endpoint. Isso é particularmente verdadeiro para identidades privilegiadas, onde as mesmas credenciais usadas para autenticação na VPN também podem ser usadas para autenticação em sistemas dentro da rede e para executar ações administrativas.

Isso foi o caso na violação da Cisco em 2022, onde o grupo de ransomware Yanluowang comprometeu credenciais corporativas no armazenamento de senhas pessoais do Chrome de um usuário e as usou não apenas para se conectar à VPN, mas também para acessar sistemas dentro da rede, criar novos grupos de administradores locais e instalar outro software de acesso remoto.

Ao pensar nos caminhos para os privilégios de acesso remoto, priorize controles de acesso com menos privilégios e just-in-time (JIT).

Fornecendo a quantidade certa de acesso e privilégios necessários, e apenas em momentos finitos necessários, você pode reduzir o privilégio de permanência, reduzindo assim o **"raio de explosão"** de um possível comprometimento.



Atores de ameaças, como o LAPSUS$, prometem pagamentos aos colaboradores que entregam credenciais para soluções de acesso remoto, para que possam obter acesso aos sistemas e à rede. Isso mostra o quão valiosos esses caminhos aos privilégios são para um invasor.

Mesmo que as identidades comprometidas tenham apenas privilégios limitados, o amplo acesso fornecido por uma VPN oferece aos agentes da ameaça a capacidade de descobrir sistemas potencialmente vulneráveis, segredos armazenados em recursos compartilhados de rede, além de encontrar mais privilégios e caminhos que eles possam explorar para atingir seus objetivos.

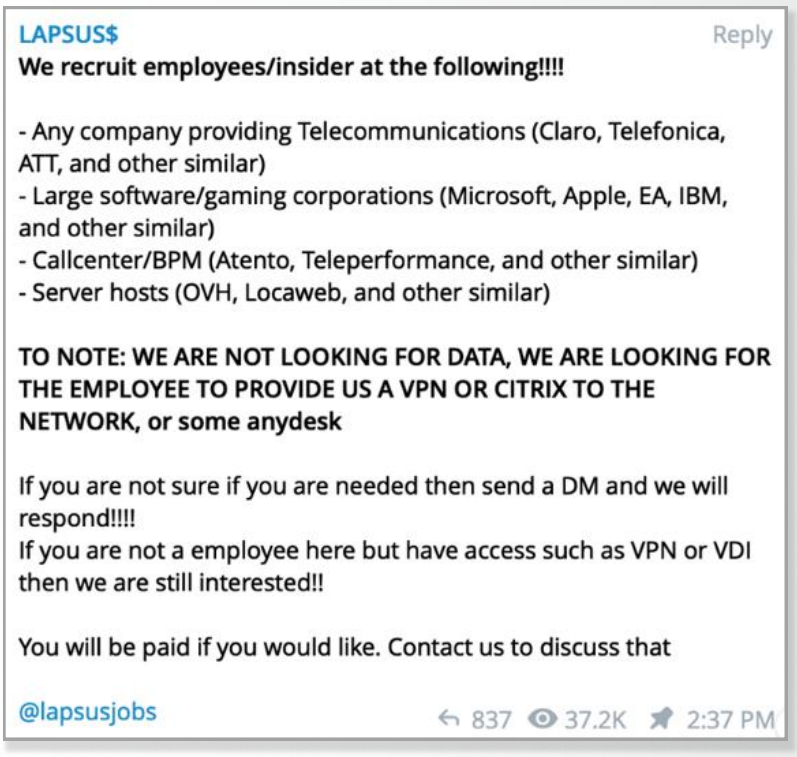


FIGURA 1
Post da LAPSUS$ no Telegram recrutando colaboradores

Privilégios Excessivos

O excesso de privilégios é muito comum. Os privilégios são frequentemente concedidos de forma permanente (privilégios permanentes), mesmo que sejam necessários apenas uma vez. À medida que os usuários mudam de função ou assumem novos projetos, suas identidades podem continuar a coletar privilégios que nunca serão removidos. Em casos extremos, as identidades altamente privilegiadas de ex-funcionários podem existir num estado inativo. Eles não oferecem valor para o negócio porque não são mais usados (legitimamente), mas criam muitos riscos em caso de comprometimento.

Na corrida para a nuvem, vemos uma abundância de privilégios concedidos através de funções e direitos, muitas vezes com pouco conhecimento ou consideração da extensão do seu alcance. Esse problema é ainda mais complicado pelos milhares de privilégios diferentes e granulares que podem ser concedidos nas principais plataformas de nuvem.

Número de permissões de IAM e ações por plataforma de nuvem

*Os dados da AWS, Azure e Google Cloud são atualizados regularmente. Esses números são de 31 de julho de 2024.

A adoção de mais aplicações em nuvem foi o **fator#1 que impulsionou o aumento** no número de identidades.

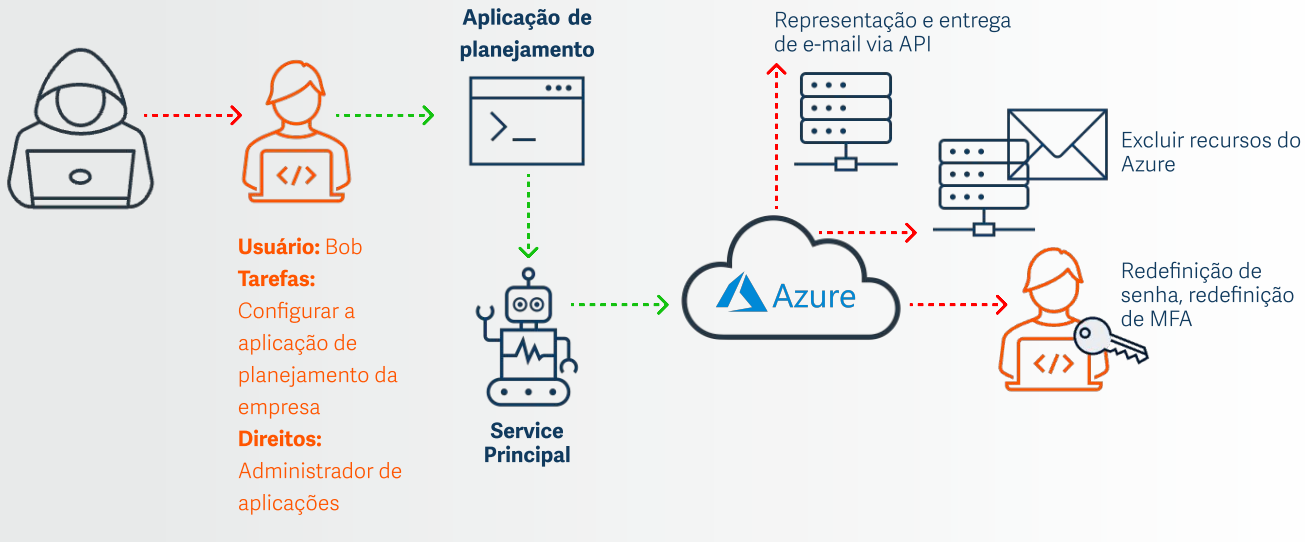
- IDSA. 2023 Trends in Securing Digital Identities. Junho de 2023.

1. https://aws.permissions.cloud
2. https://azure.permissions.cloud
3. https://gcp.permissions.cloud/

Vários ataques de alto perfil, incluindo o infame Midnight Blizzard contra a Microsoft foram bem-sucedidos em função das conexões ocultas e aos caminhos excessivos para obter privilégios que surgem da criação e da gestão de identidades humanas e não humanas na nuvem.

Um exemplo comum de caminhos para privilégios no Entra é uma identidade com controle sobre uma aplicação OAuth. Mesmo que a identidade não seja diretamente privilegiada, ela possui um caminho para os privilégios concedidos à aplicação que controla. Em muitos casos, as aplicações recebem altos níveis de privilégio na nuvem, apresentando um caminho aparentemente com poucos privilégios até o administrador global na nuvem por meio de uma aplicação ou serviço.

Caminhos para o privilégio no Entra



Em muitos casos, essas aplicações foram configuradas para projetos legados de migração para a nuvem, que exigiam altos níveis de privilégio na época, mas não são mais necessários. Em outros casos, eles foram simplesmente superprivilegiados em virtude da falta de compreensão do que era necessário. De qualquer forma, esses privilégios constituem um alvo tentador para invasores que desejam migrar para a nuvem. Em ambientes de nuvem, os invasores podem usar esses caminhos para elevar seus privilégios de acesso a caixas de correio, armazenamentos de dados e outras identidades por meio do Entra ID.

Por que encontrar caminhos para os privilégios é a chave para a segurança das identidades modernas

Os sistemas de TI modernos são complexos e contêm um número cada vez maior de sistemas, aplicações e identidades díspares, os quais potencialmente criam novos caminhos para privilégios — **caminhos que estão sendo ativamente explorados por invasores.**

90%

No ano passado, 90% das empresas sofreram pelo menos um incidente de segurança relacionado à identidades.

IDSA. 2024 Trends in Identity Security. Maio de 2024

John Lambert, do Microsoft Threat Intelligence Center, resumiu o desafio na segurança de identidades que atualmente está favorecendo muito os invasores.

Sua declaração adequada deu origem à seguinte expressão:

"...os defensores pensam em listas. Os invasores, em gráficos. Se isso for verdade, os invasores vencem."

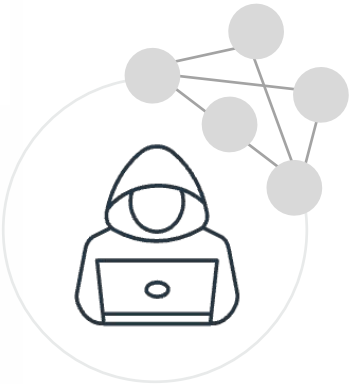
– John Lambert

Quando falamos sobre invasores que pensam em gráficos, não estamos descrevendo gráficos de pizza e de barras, mas sim aplicando os conceitos da teoria dos grafos, que examina as estruturas usadas na matemática para modelar relacionamentos entre objetos para criar um modelo de comportamento de ameaça às identidades. No caso das identidades, o gráfico contém nós (círculos) que representam endpoints (desktops, servidores, IoT/OT, outros dispositivos com capacidade de internet, etc.) e serviços, e arestas (linhas) que representam o caminho que conectam os nós - ou como os definimos, os caminhos para o privilégio. Pensando em gráficos, podemos conceituar como os invasores poderiam sair do comprometimento inicial de uma identidade e se mover pelo seu ambiente, explorando os privilégios em seus sistemas.

Comprometer uma identidade ou endpoint dá a você acesso a um ou mais nós, e o privilégio permite o controle deles. Quanto mais caminhos para privilégios no ambiente, mais oportunidades para um invasor acessar e controlar endpoints e serviços.

LISTAS VERSUS GRÁFICOS

Esquerda, defensor pensa em listas.
Direita, atacante pensa em gráficos.



Os invasores procuram os caminhos entre domínios que conectam os sistemas pensando em gráficos. No entanto, os silos organizacionais e as ferramentas muitas vezes deixam os defensores pensando em listas (ou seja: listas de verificação) isoladas de um sistema ou ambiente. Isto limita a capacidade de ver o que o atacante vê, dificultando assim a sua defesa.

> Por exemplo, um ataque pode começar explorando um servidor público vulnerável on-premise e, em seguida, mover-se lateralmente para um sistema que executa um agente de sincronização em nuvem. A partir daí, o invasor pode extrair do agente as credenciais da conta da nuvem altamente privilegiadas e usá-las (assim como os privilégios) para migrar para a nuvem e assumir o controle de todo o locatário da nuvem. **O invasor poderia então usar todos os caminhos aos privilégios** que descobriu para excluir sistemas e dados, tanto na nuvem quanto on-premise, em um golpe de knock-out (ou "game over").

Este exemplo não é ficção de ameaça, é apenas um entre muitos exemplos do mundo real de como os invasores pensam em gráficos e exploram caminhos para obter privilégios e se mover com fluidez entre diferentes domínios. Quanto mais caminhos para privilégios em seu ambiente, mais oportunidades um invasor terá de se mover lateralmente, escalar privilégios e cruzar domínios.

Do lado dos defensores, muitas vezes pensamos em listas e silos. Isso significa que podemos ter uma equipe do Active Directory (AD), uma de nuvem, uma de endpoints e uma de servidores. Ou podemos pensar em termos de listas de verificação de conformidade para sistemas e controles individuais. Silos e listas são muitas vezes o resultado de uma infraestrutura de identidades díspar, ferramentas de nicho e diferentes estruturas de equipe. O resultado: brechas na visibilidade à medida que você cruza domínios, equipes e ferramentas, deixando o IAM e a segurança cegos quanto aos caminhos aos privilégios entre sistemas que os invasores podem explorar prontamente.

Pensar em gráficos e focar nos caminhos aos privilégios permite que você veja sua superfície de ataque da perspectiva de um invasor para que você possa proteger proativamente seu ambiente. Dessa maneira, você entende o raio da explosão no caso de uma violação, para que possa detectar rapidamente e responder adequadamente a um ataque. É por isso que compreender os caminhos para os privilégios não é apenas o ponto crucial da segurança das identidades modernas, mas também é essencial para a segurança geral.

E as ferramentas de segurança já existentes?

Muitas soluções disponíveis hoje concentram-se fortemente na detecção de malware, explorações conhecidas e códigos maliciosos. Embora sejam defesas valiosas, **elas não são eficazes contra ameaças de identidade modernas**.

Considerando que atualmente é mais fácil para um invasor fazer login do que hackear, é vital poder ver, gerenciar e proteger os caminhos para os privilégios em seu ambiente.

Como a maioria das ferramentas de detecção atuais geralmente são reativas a eventos e não possuem o contexto de identidade e caminhos para os privilégios, é um desafio reduzir proativamente a superfície de ataque e o risco. Sem uma compreensão clara dos caminhos para os privilégios, é impossível entender quais identidades apresentam o maior risco em seu ambiente ou quais controles terão o maior impacto na redução da superfície de ataque das identidades para proteção contra ataques futuros. Por exemplo, um EDR ou SIEM pode detectar que um endpoint foi comprometido por malware e que uma identidade foi exposta a riscos. No entanto, sem o contexto de qual privilégio essa identidade possui – não apenas naquele endpoint, mas também em todo o ambiente – você não saberá quais caminhos estão disponíveis para o invasor.

> Existe uma maneira do invasor passar a administrador de domínio a partir desse endpoint comprometido? Ele poderiam usar a identidade para acessar dados na AWS? Ele tem controle sobre as aplicações OAuth no Azure que poderiam ser usadas para migrar para a infraestrutura em nuvem? **Sem um contexto mais amplo, torna-se difícil (se não impossível) responder adequadamente e evitar novos compromissos.**

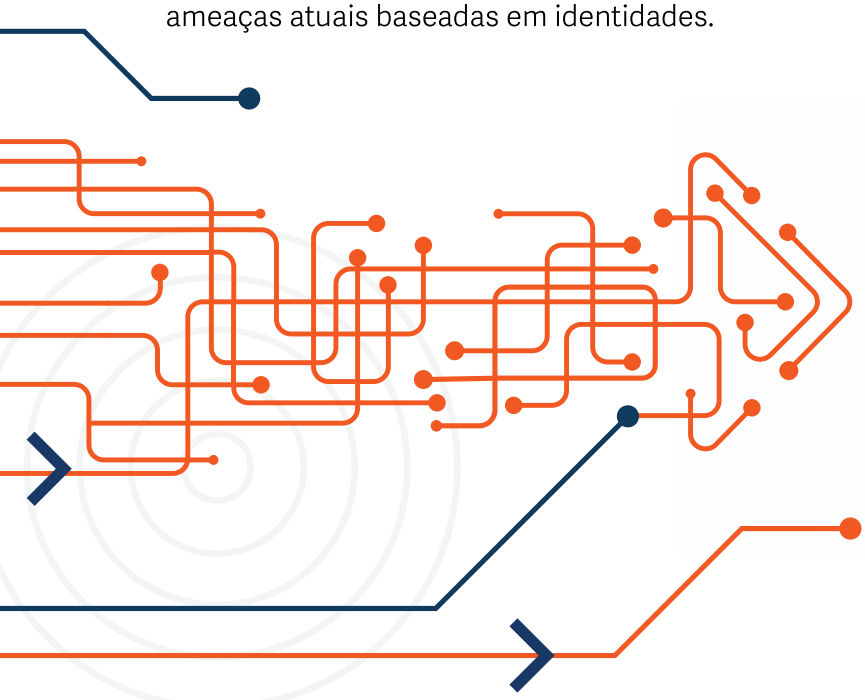
Embora exista uma série de controles centrados nas identidades (por exemplo, MFA, acesso condicional e SSO), eles não são suficientes. Os invasores podem aproveitar da engenharia social para que os usuários forneçam códigos MFA, os kits de ferramentas de phishing podem capturar credenciais e solicitações de proxy MFA, os dispositivos comprometidos podem ser usados para sequestrar sessões, as redes proxy podem escapar das restrições de acesso e, uma vez que o invasor tenha esse acesso inicial, o SSO pode conceder acesso a uma série de aplicações e dados em nuvem.

Ao compreender o raio potencial de explosão de uma identidade comprometida, você pode priorizar, responder e mitigar melhor os riscos. Esse conhecimento permite que você adote uma abordagem proativa para reduzir sua superfície de ataque de identidades e remova, gerencie e monitore efetivamente caminhos para os privilégios. Eliminar os caminhos fáceis que um invasor pode usar para acessar sistemas ou desativar controles de segurança também ajudará a garantir que suas ferramentas de segurança funcionem de maneira eficaz.

Como a BeyondTrust Protege os Caminhos para os Privilégios

A BeyondTrust, empresa líder reconhecida por analistas na gestão de acessos privilegiados (PAM) e detecção e resposta a ameaças de identidades (ITDR), **está preparada para proteger as empresas contra ameaças de identidades, minimizar sua superfície de ameaça e reduzir o raio de explosão de ataques.**

Contamos com anos de experiência no gerenciamento de privilégios, além de um conhecimento sólido do cenário de segurança cibernética em constante mudança e uma plataforma avançada de soluções comprovadas de segurança de identidades para proteger nossos clientes das ameaças atuais baseadas em identidades.



A plataforma BeyondTrust oferece a cobertura mais ampla e profunda para encontrar, gerenciar e proteger os caminhos aos privilégios.

A plataforma BeyondTrust

Os produtos BeyondTrust integram-se entre si para oferecer mais proteção e eficiência. Integrações avançadas com conjuntos de ferramentas de terceiros ajudam sua organização a maximizar ainda mais os investimentos existentes em segurança.

Para obter mais informações sobre a plataforma BeyondTrust, visite nosso website.
www.beyondtrust.com/pt

A BeyondTrust protege seus caminhos para os privilégios e melhora sua postura de segurança de identidades.

Visibilidade Holística

Tenha visibilidade de seus caminhos para os privilégios

Gestão Simplificada

Implemente os privilégios mínimos e ganhe eficiência

Proteção inteligente

Aprimore usando insights de IA e ML

Identity Security Insights

BeyondTrust Identity Security Insights oferece avaliação unificada e contínua de riscos e caminhos para privilégios em todo o seu panorama de identidades, desempenhando um papel fundamental na prevenção e interrupção de ataques sofisticados de identidade. Os clientes confiam no Identity Security Insights para avaliar e melhorar de forma holística a segurança de suas identidades com pouco esforço, independentemente de onde estejam.

A solução aproveita a IA/ML para analisar grandes quantidades de dados de identidades de diversas fontes, incluindo Active Directory, Entra ID, Ping e Okta, bem como produtos BeyondTrust. Isso permite que você identifique e resolva proativamente seus problemas críticos de segurança de identidades com profunda visibilidade e contexto em um único lugar.

Caminhos para a Proteção dos Privilégios:

Descubra Caminhos Diretos e Indiretos para os Privilégios

Descubra caminhos para os privilégios e caminhos de risco de identidades em ambientes de TI interconectados, como os decorrentes de associações a grupos aninhados, identidades com privilégios excessivos, contas inativas, configurações incorretas, caminhos desconhecidos de acesso entre ambientes de produção e não produção, vulnerabilidades nos Serviços de Certificados do Active Directory (ADCS), contas privilegiadas não gerenciadas, contas vulneráveis ao Kerberoasting, etc.

Fortaleça Proativamente sua Postura de Segurança de Identidades

Fique à frente dos invasores. Melhore a higiene da segurança da suas identidades com avaliações de risco contínuas que fornecem informações detalhadas sobre direitos, combinados com recomendações. Aproveite a solução PAM da BeyondTrust e outras integrações para resolver rapidamente as descobertas e eliminar ou proteger privilégios e caminhos para privilégios.

Operacionalize Detecção e Resposta a Ameaças de Identidades (ITDR)

Detecte quando privilégios ou caminhos para privilégios estão sob ataque. Receba alertas sobre anomalias como sprays de senha, login de IP mal-intencionado, excessos de tentativas de leitura de senha, alterações de infraestrutura após eventos de MFA suspeitos, alterações incomuns nas entidades de serviço do Azure e acesso de intervalos de IP maliciosos. Aproveite recomendações prescritivas e controles de PAM da BeyondTrust para prevenir e remediar prontamente tentativas de explorar caminhos para privilégios. Integre-se às suas plataformas conhecidas de SIEM, SOAR, ITSM e ChatOps para acelerar a resposta e a mitigação.

O Identity Security Insights foi crucial para detectar a violação do suporte da Okta em outubro de 2023, identificando atividades críticas (como sequestro de sessão e ações administrativas baseadas em proxy) semanas antes do reconhecimento público do ataque à Okta. Um de nossos clientes disse que quando a violação da Okta foi detectada pela BeyondTrust, o CIOs e o CISO ficaram aliviados ao saber sobre os **recursos proativos do Identity Security Insights**. Isso lhes permitiu garantir à liderança da empresa que não foram afetados pela violação.

Ao mapear interconexões complexas entre identidades, contas, privilégios e configurações humanas e não humanas em toda a estrutura de identidades – incluindo endpoints, servidores, provedores de identidade, ferramentas IaaS, PaaS, SaaS e DevOps – o Identity Security Insights revela exclusivamente caminhos ocultos para os privilégios que outras soluções não conseguem identificar. Com as recomendações e detecções prescritivas do produto, você pode fortalecer sua postura de segurança de identidades, corrigir problemas e interromper caminhos para privilégios de forma mais proativa e eficaz.

Password Safe

O Password Safe da BeyondTrust fornece visibilidade e controle abrangentes de contas, sessões, credenciais e segredos privilegiados. O produto simplifica os recursos de gerenciamento de contas e sessões privilegiadas (PASM) e gestão de segredos em uma solução coesa.

O Password Safe é fundamental para proteger alguns caminhos mais utilizados até os privilégios. O produto ajuda as organizações a minimizar os riscos associados ao comprometimento de credenciais privilegiadas, integrando contas e credenciais privilegiadas e protegendo o acesso a senhas de contas e segredos de DevOps, bem como certificados, chaves de API, tokens e chaves SSH.

Caminhos para a Proteção dos Privilégios:

Descubra, Integre e Gerencie Contas e Credenciais Privilegiadas

Aproveite os recursos avançados de descoberta do Password Safe para agilizar o processo de gerenciamento de contas privilegiadas. Tenha visibilidade e controle total sobre contas privilegiadas para mitigar riscos associados ao acesso não monitorado.

Automatize a Rotação de Credenciais

Proteja os caminhos para os privilégios por meio da rotação automática de credenciais, minimizando assim riscos como reutilização de senhas e comprometimento de contas, o que pode provocar a pontos de apoio ou movimentos laterais em sua rede.

Habilite o Acesso Just-in-Time

Forneça acesso just-in-time a caminhos para privilégios em recursos críticos para eliminar privilégios permanentes e reduzir a superfície de ataque.

Gerencie Segredos

Proteja os caminhos para os privilégios em DevOps e outros ambientes dinâmicos, gerenciando e protegendo segredos com eficiência e eliminando credenciais codificadas que os agentes de ameaças procuram.

Utilize a Ferramenta Workforce Passwords

Elimine credenciais de aplicações não gerenciadas e compartilhadas, implementando práticas robustas de gestão de senhas, garantindo a segurança das identidades.

Ao implementar esses recursos, o Password Safe pode evitar muitos ataques, como ameaças de reutilização de senhas e ataques Pass-the-Hash (PtH), em que os agentes de ameaças utilizam credenciais com hash roubadas para acessar outros sistemas em rede. Ao rotacionar automaticamente as credenciais e remover privilégios permanentes, o Password Safe garante que, mesmo que uma identidade e suas credenciais sejam comprometidas, elas não poderão ser reutilizadas, reduzindo significativamente o risco de movimentos laterais. Ao estender a segurança corporativa até mesmo para senhas de colaboradores, o Password Safe expande ainda mais o caminho para a proteção de privilégios além das contas tradicionalmente tratadas como privilegiadas.

Endpoint Privilege Management

A solução BeyondTrust Endpoint Privilege Management ajuda as empresas a impor o privilégio mínimo e obter conformidade, controlando direitos de administrador local e acesso root em desktops e servidores Windows, macOS e Linux.

O Endpoint Privilege Management desempenha um papel vital na defesa dos caminhos para os privilégios, oferecendo controle e visibilidade abrangentes sobre privilégios de administrador local e acesso a aplicações em endpoints. O produto garante que as políticas de segurança de endpoints sejam aplicadas de forma consistente em todos os dispositivos, reduzindo o risco de acesso não autorizado e a escalação de privilégios.

Caminhos para a Proteção dos Privilégios:

Remova Caminhos para os Privilégios de Administrador Local em Endpoints
Elimine direitos desnecessários de administrador local, reduzindo o risco de exploração por agentes mal-intencionados caso o endpoint seja comprometido.

Desbloqueie a Produtividade com Modelos de Início Rápido Prontos para Uso
Permita que os usuários acessem facilmente os privilégios necessários para sua função, por meio de políticas e controles granulares.

Previna o Uso Indevido com Mecanismos Avançados de Anti-Tamper
Bloqueie o uso indevido de privilégios, como a criação de novas contas de administrador local e elevação de privilégios não autorizados.

Proteja os endpoints
Direitos de administrador local e acesso root são caminhos comumente explorados, que os invasores usam para desativar controles de segurança, capturar credenciais e mover-se lateralmente. O Enpoint Privilege Management mitiga esses riscos e fornece uma base sobre a qual se permite construir a segurança de seus endpoints.

Ao proteger os caminhos para os privilégios em endpoints, o Endpoint Privilege Management pode mitigar a escalação de privilégios. Ao eliminar os privilégios desnecessários de admin local e usar mecanismos anti-tamper avançados, esta solução reduz significativamente a superfície de ataques e mitiga o risco de movimentos laterais e uso indevido de privilégios. Mesmo que um endpoint seja comprometido, os controles de segurança do Endpoint Privilege Management ajudam a minimizar o raio de explosão e o risco.

Entitle

A solução BeyondTrust Entitle automatiza o gerenciamento de permissões na nuvem, permitindo que as empresas implementem o acesso just-in-time para reduzir a superfície de ataque de ativos críticos da nuvem.

O Entitle é uma solução poderosa para obter controle sobre os caminhos para os privilégios na nuvem. O produto fornece uma abordagem descomplicada para controles de acesso robustos e políticas de segurança para proteger identidades, dados confidenciais e sistemas. Com o Entitle, é possível conceder acesso privilegiado apenas nos momentos necessários e sob estrita supervisão.

Caminhos para a Proteção dos Privilégios:

Orquestre o Acesso Just-in-Time à nuvem
Controle o acesso aos recursos da nuvem concedendo privilégios somente quando necessário, reduzindo a necessidade de privilégios permanentes e minimizando as janelas de ameaça durante as quais os privilégios podem ser explorados.

Habilite o Acesso de Autoatendimento
Permita que os usuários solicitem e aprovem acesso por meio de fluxos de trabalho automatizados que aplicam políticas de segurança, garantindo que os caminhos para os privilégios estejam protegidos.

Ofereça Acesso Emergencial
Forneça acesso emergencial em situações críticas, com auditoria e controle completos. Garanta que esse acesso seja seguro e rastreável.

Ofereça Acesso SSH Just-in-Time para Identidades não Federadas e Ambientes Legados
Ofereça acesso SSH seguro e oportuno para usuários em sistemas legados e não federados, mantendo a segurança em diversos ambientes.

Ao proteger os caminhos para os privilégios em ambientes de nuvem, o Entitle pode mitigar ataques de escalação de privilégios e uso indevido de permissões para acessar dados e sistemas confidenciais. A solução fornece acesso just-in-time garantindo que, mesmo que as credenciais sejam comprometidas, elas não podem ser usadas para obter acesso não autorizado. Além disso, o suporte do Entitle para cenários emergenciais garante que o acesso seja concedido com segurança e totalmente auditável, reduzindo o risco de uso indevido durante momentos críticos. Essa abordagem abrangente protege caminhos para privilégios em ambientes de nuvem e aplicações SaaS.

Privileged Remote Access

O Privileged Remote Access permite que as organizações criem acesso just-in-time com identidades seguras para todos os ambientes de nuvem, on-premise e OT.

O produto fornece segurança de identidade essencial e controle sobre conexões remotas, eliminando a necessidade de VPNs tradicionais, além de remover e proteger os caminhos para os privilégios. O Privileged Remote Access garante que o acesso remoto seja seguro e gerenciável para colaboradores e fornecedores, com visibilidade e controle abrangentes sobre todas as atividades privilegiadas.

Caminhos para a Proteção dos Privilégios:

Controle e Proteja os Caminhos para os Privilégios de Fornecedores e Terceiros
Elimine a necessidade de VPNs e credenciais privilegiadas conhecidas. Obtenha total controle e visibilidade sobre o acesso de fornecedores, garantindo conexões remotas seguras e monitoradas.

Implemente o Acesso Remoto Seguro Just-in-Time para Colaboradores
Crie acesso remoto seguro e com privilégios mínimos somente quando necessário. Injete credenciais gerenciadas diretamente nas sessões e elimine privilégios permanentes para funcionários.

Tenha Visibilidade e Controle Total de Todas as Ações e Privilégios em Cada Sessão
Monitore, gerencie e audite todas as ações e privilégios em cada sessão remota, garantindo que as atividades sejam rastreadas e controladas.

Proteja mais Caminhos para os Privilégios com Suporte para Vários Protocolos
Gerencie com segurança o acesso remoto através de vários protocolos, incluindo RDP, VNC, HTTPS, SSH, e SQL, para garantir ampla proteção dos caminhos para os privilégios.

Ao implementar esses recursos, o Privileged Remote Access pode impedir acesso não autorizado e ataques de escalação de privilégios. O produto fornece apenas o acesso necessário e injeta credenciais diretamente na sessão a partir de um cofre seguro, sem expô-las ao usuário. Isso reduz o risco de que credenciais comprometidas sejam usadas para obter acesso não autorizado.

Além disso, os recursos de gerenciamento e auditoria de sessões garantem que todas as ações sejam monitoradas e controladas, evitando o uso indevido de privilégios. Essa abordagem robusta mantém um alto nível de segurança em conexões remotas, ao mesmo tempo que protege caminhos para os privilégios que um agente de ameaça poderia aproveitar para ganhar uma posição ou expandir um ataque.

Remote Support

O BeyondTrust Remote Support permite que as organizações acessem e forneçam suporte a qualquer dispositivo ou sistema no mundo. O produto é crucial para proteger caminhos de acesso remoto para privilégios de centrais de atendimento.

O Remote Support elimina a necessidade de VPNs tradicionais e privilégios permanentes, garantindo que o acesso seja concedido somente quando necessário e sob monitoramento rigoroso. Aproveite também os controles robustos e a auditoria do produto para garantir a segurança e a supervisão de sessões remotas.

Caminhos para a Proteção dos Privilégios:

Proteja e Controle os Caminhos de Acesso Remoto para Privilégios

Forneça acesso remoto seguro e sem VPN para reduzir o risco de conexões comprometidas e garanta que todos os caminhos de acesso remoto sejam rigorosamente controlados. Defina e aplique políticas diferentes para sessões de suporte remoto assistidas e não assistidas.

Implemente o Acesso Just-in-Time para Sessões de Suporte

Conceda permissões e acesso granulares somente quando necessário, eliminando caminhos permanentes para privilégios e reduzindo o potencial de acesso não autorizado.

Integre a Segurança de Senhas

Permita que os técnicos armazenem, compartilhem e rastreiem com segurança o uso de credenciais privilegiadas no service desk.

Audite As Sessões

Monitore e audite cada sessão remota para garantir que as identidades não sejam mal utilizadas, alcançando total responsabilidade e visibilidade de todas as atividades remotas.

Ao implementar esses recursos, o Remote Support pode impedir o acesso não autorizado e o uso indevido de identidades. Por exemplo, ao remover caminhos permanentes para os privilégios e implementar o acesso just-in-time, você pode garantir que, mesmo que as credenciais sejam comprometidas, elas não poderão ser usadas para obter acesso indesejado. Além disso, a auditoria de cada sessão garante que todas as atividades sejam monitoradas, evitando o uso indevido de identidades e mantendo um alto nível de segurança e responsabilidade em cenários de suporte remoto.

Active Directory Bridge

O Active Directory Bridge (AD Bridge) estende a autenticação do Microsoft AD, os recursos de SSO e o gerenciamento de configuração de Políticas de Grupo para sistemas Unix e Linux. O produto simplifica a política e a administração, otimiza a segurança e reduz o potencial de erros.

Ao integrar sistemas não Windows ao Active Directory, o AD Bridge garante a aplicação consistente de políticas e acelera o caminho para segurança Zero Trust.

Caminhos para a Proteção dos Privilégios:

Simplifique as Políticas e a Gestão
Unifique o gerenciamento estendendo os recursos do AD para sistemas não Windows, reduzindo a complexidade administrativa e possíveis erros que poderiam criar caminhos para os privilégios.

Simplifique a Segurança
Aproveite o controle centralizado sobre políticas de identidades e acessos, garantindo padrões de segurança uniformes em todas as plataformas.

Reduza o Potencial de Erros
Automatize a aplicação e conformidade de políticas, minimizando o risco de configurações incorretas e erros humanos.

Acelere seu Caminho para o Zero Trust
Monitore e audite cada sessão remota para garantir que as identidades não sejam mal utilizadas, alcançando total responsabilidade e visibilidade de todas as atividades remotas.

Ao utilizar o Active Directory Bridge, as organizações podem evitar desvios de configuração e inconsistências de segurança, que podem abrir ou expor caminhos para os privilégios. O produto centraliza e automatiza o gerenciamento de políticas para garantir que as políticas de segurança sejam aplicadas uniformemente em infraestruturas heterogêneas, reduzindo a probabilidade de erros que poderiam ser explorados por invasores. Esta abordagem está alinhada com o Zero Trust, onde a verificação contínua é fundamental para manter um ambiente seguro.

Próximos Passos

Proteger identidades e seus caminhos para obter privilégios é uma jornada essencial e contínua que requer uma abordagem estratégica e o conjunto certo de ferramentas de segurança de identidades.

Este White Paper ressaltou a importância de compreender e proteger os caminhos para os privilégios. Ao considerar a infraestrutura de identidades, as políticas, os grupos e as interconexões mais amplas, as organizações podem aprimorar sua postura de segurança e mitigar riscos de maneira eficaz.

Interessado em descobrir os caminhos para os privilégios em seu próprio ambiente e ter recomendações claras sobre como fortalecer proativamente sua postura de segurança?

Aproveite nossa **avaliação de segurança de identidade gratuita e 30 dias de monitoramento contínuo de ameaças,** com tecnologia do Identity Security Insights.

SAIBA MAIS

beyondtrust.com ou entre em contato conosco

Recursos Adicionais

WHITEPAPER

Buyer's Guide for Complete Privileged Access Management (PAM)

WHITEPAPER

Advancing Zero Trust with Privileged Access Management (PAM)

PODCAST

The Midnight Blizzard Breach on Microsoft and Other Identity Attacks

BLOG

AD CS 101: Introduction to Active Directory Certificate Services & How to Detect and Mitigate ESC1 Attacks

BLOG

Identity Attack & Defense: Lessons in Okta Security

Sobre a BeyondTrust

A BeyondTrust é líder em segurança cibernética, protegendo os caminhos para os privilégios com uma abordagem centrada nas identidades. Estamos liderando a transformação da segurança de identidades e contamos com mais de 20.000 clientes, incluindo os 75 maiores da Fortune 100, além de nosso ecossistema global de parceiros.

Saiba mais em **www.beyondtrust.com/pt**

https://disruptec.com.br/acesso-remoto-privilegiado/