BeyondTrust

Esclarecendo os 6 mitos do PAM

Gerenciamento de Acessos Privilegiados:
Fatos e Mitos

ÍNDICE

INTRODUÇÃO 1

A CRESCENTE AMEAÇA DE UMA VIOLAÇÃO DE DADOS 2

Estudo Ponemon: Custo de uma violação de dados em 2019

A ALEGRIA DOS HACKERS: MAIS FÁCIL DO QUE NUNCA 3

GESTÃO DE SEGURANÇA RESTRITIVA VS OBSERVADA 4

Segurança Restritiva

Segurança Observada

PAM: O PROJETO DE SEGURANÇA NÚMERO UM PARA 2019 5

MITO 1: O MODELO ZERO TRUST É POSSÍVEL 6

MITO 2: CONTAS COMPARTILHADAS SÃO NECESSÁRIAS PARA ATIVAR O PAM 7

MITO 3: SOMENTE CONTAS PRIVILEGIADAS SÃO GERENCIADAS PELO PAM 8

MITO 4: PAM AJUDA A GERENCIAR E CONTROLAR O ACTIVE DIRECTORY 9

MITO 5: O ACESSO DE TERCEIROS PODE SER GARANTIDO USANDO OS RECURSOS DA VPN 10

MITO 6: UMA GRANDE EQUIPE DE TI É NECESSÁRIA PARA IMPLEMENTAÇÃO E GERENCIAMENTO DO PAM 11

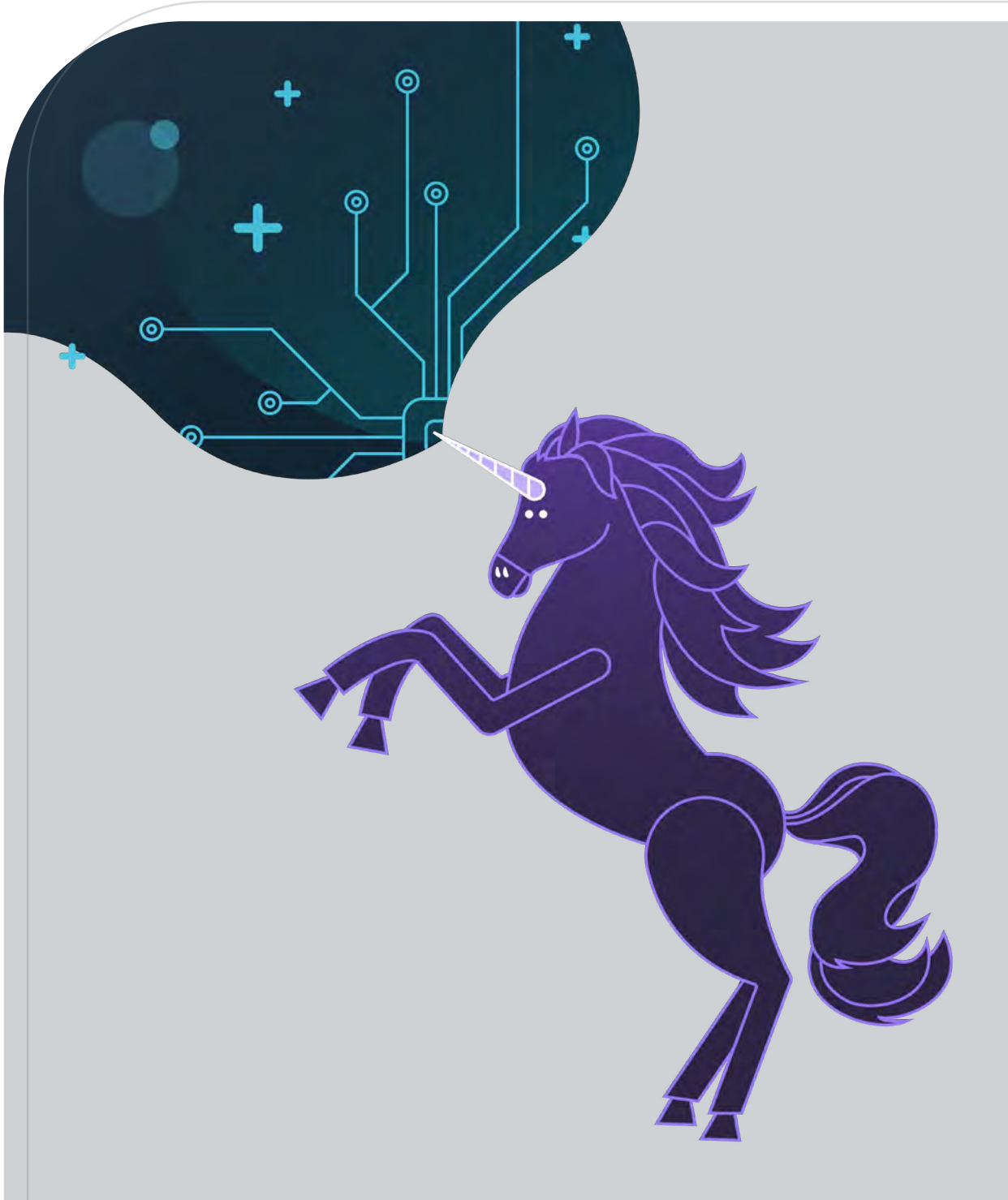
CONCLUSÃO 12

A PLATAFORMA DA BEYONDTRUST 13

INTRODUÇÃO

Mitos são curiosos, não? Amplamente defendidos, eles podem ganhar espaço, crescer e viralizar rapidamente. A linha entre o que é mito e o que é verdade é tênue - e muitos decidem acreditar no mito porque geralmente é uma realidade 'mais agradável' ou mais atraente, ou simplesmente porque é mais popular.

Neste whitepaper, vamos comentar seis crenças sobre o Gerenciamento de Acessos Privilegiados (PAM) que estão, de fato, erradas. Explicaremos o porquê, esclareceremos qual a verdade e forneceremos dicas práticas para você desenvolver sua jornada para uma organização mais segura e livre de achismos.



A CRESCENTE AMEAÇA DE UMA VIOLAÇÃO DE DADOS

Antes de chegar aos mitos, vamos começar com alguns fatos. As violações de dados só crescem. A impressão é que a cada mês que passa, as notícias comentam novos casos de ataques, além das centenas que não são divulgadas na imprensa. Já não se trata mais de "se", e sim de "quando" a segurança será comprometida - e por isso é tão importante ter uma estratégia para lidar com esses riscos. Confira algumas estatísticas de relatórios recentes publicados sobre violações de dados.

Estudo Ponemon: Custo de uma violação de dados em 2019

O recente relatório Cost of a Data Breach conduzido pelo Instituto Ponemon e patrocinado pela IBM Security revela algumas estatísticas impactantes sobre o que as vítimas de violação cibernética enfrentam.

Atualmente, o custo total médio global de uma violação de dados fica a em torno de US$ 4 milhões, sendo 25.575 o número médio de registros comprometidos em uma violação. Como o tempo médio para identificar e conter uma violação é de quase 10 meses, , é óbvio que uma solução é necessária, e rápido.

Fontes: 1. 2019 Cost of a Data Breach Report, Ponemon Institute;
2. 2019 MidYear QuickView Data Breach Report, Cyber Analystic, Aug

A ALEGRIA DOS HACKERS: MAIS FÁCIL DO QUE NUNCA

Uma das principais razões pelas quais tantas violações estão ocorrendo é simplesmente porque a superfície de ataque cresceu exponencialmente nos últimos 20 anos. Enquanto as redes de TI consistem principalmente em ativos locais, o número de contas e endpoints explodiu. As equipes de TI precisam aprender a gerenciar identidades de usuários, bem como contas de administrador compartilhadas, servidores, desktops, IoT e credenciais de máquina em diversos ambientes: local, na nuvem, ambiente híbrido e DevOps. Os ataques cibernéticos e os golpes que alavancam a IA também são cada vez mais percebidos como um salto da ficção científica para a realidade atual.

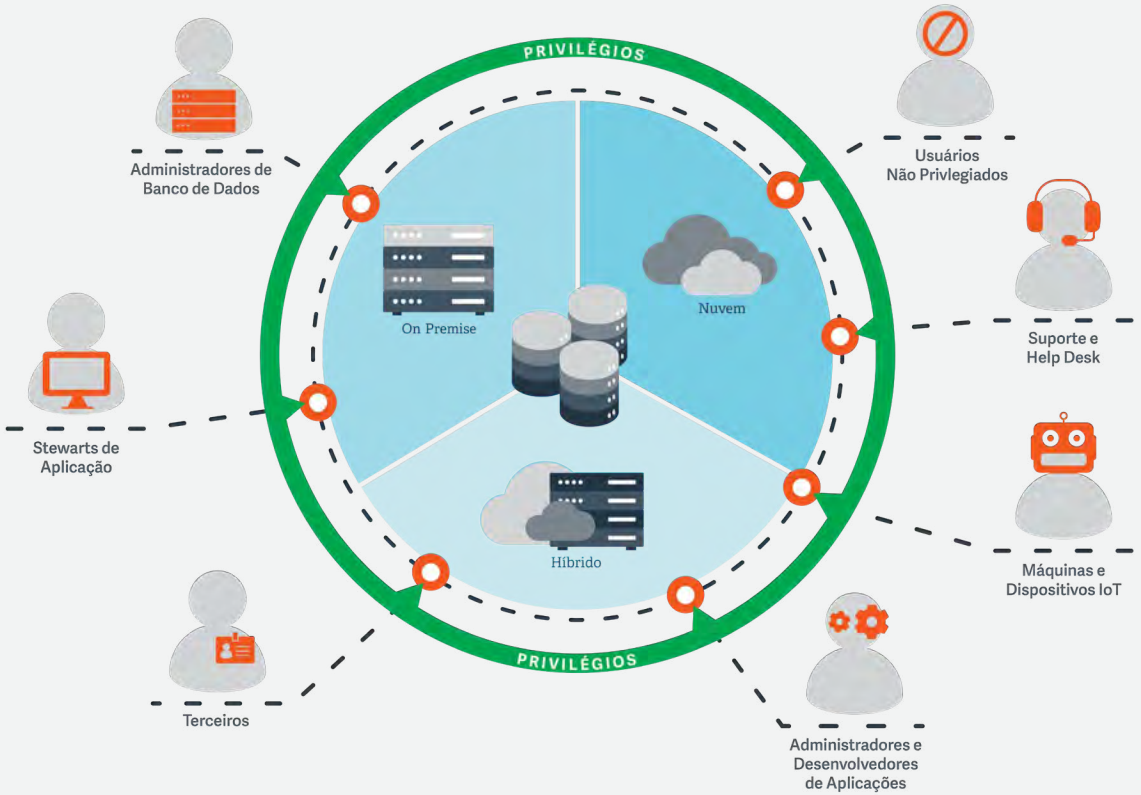
Todas essas variáveis tornam o problema complexo e potencialmente difícil de resolver. Manter-se atualizado pode significar novos investimentos em segurança e uma evolução de suas estratégias, mas não fazer nada pode ser catastrófico para o seu negócio.

Um problema relacionado ao aumento de ataques é a necessidade de produtividade. À medida que aumenta o número de aplicativos, sistemas e novas tecnologias, aumenta também a necessidade de acesso privilegiado.

Os funcionários de empresas modernas necessitam acessar ativos críticos de TI e dados valiosos da companhia. E dependendo do cargo, local ou sistema operacional, dar a eles o acesso necessário sem criar riscos, muitas vezes parece impossível.

Como muitas equipes de TI têm medo de afetar negativamente a produtividade, elas concedem direitos de administrador e privilégios em excesso, sem considerar o risco relacionado à segurança.

Como Suas Redes Estão Sendo Acessadas?



GESTÃO DE SEGURANÇA RESTRITIVA VS OBSERVADA

Segurança Restritiva

A segurança restritiva é um conceito no qual os sistemas de TI são gerenciados a partir de dispositivos de 'pouca confiança' que correm um risco maior de serem comprometidos, como um computador pessoal em casa. Infelizmente, este é o cenário típico atual, provando que a prática comum nem sempre é uma boa prática. O equipamento de um usuário final usado pelo administrador pode ser um dos caminhos mais fáceis para o sistema alvo.

Em computadores em que a integridade dos dados é importante (como serviços de armazenamento em nuvem, que lidam com dados ou pagamentos pessoais, ou sistemas de controle industrial), se você não confia nos dispositivos que estão sendo usados para administrar ou operar um sistema, não pode confiar nele.

Segurança Observada

Do outro lado do espectro, a segurança observada é a melhor prática para mitigar riscos em seu ambiente. A segurança observada consiste em ter estações de trabalho dedicadas para administração remota que residem em uma rede segregada com sistema operacional, email e navegador bloqueados.

A idéia é que, se uma estação de trabalho/ambiente menos confiável for comprometido, ele não estará diretamente abaixo do ambiente "limpo", e será difícil para um hacker ter acesso ao ambiente "limpo", pois ele está separado.

No entanto, essa abordagem vem com várias desvantagens. Embora muito seguro, é impraticável. Imagine um colaborador remoto - eles normalmente têm acesso a um sistema secundário em uma VPN isolada?

Uma alternativa muito melhor é o Gerenciamento de Acesso Privilegiado (PAM).

Conforme declarado pelo National Cyber Security Center (NCSC, parte do GCHQ), "Segurança Restritiva é um modelo ruim, embora muito usado, pois facilita o gerenciamento da equipe.

O Gerenciamento de Acessos Privilegiados (PAM) ajuda a mitigar alguns desses riscos. Segurança observada é uma melhor prática e, com o Gerenciamento de Acessos Privilegiados, pode realmente ajudá-lo a ganhar confiança em suas interfaces de gerenciamento.

Gestão de Segurança Restritiva por si só não é escalável e não diminui o risco

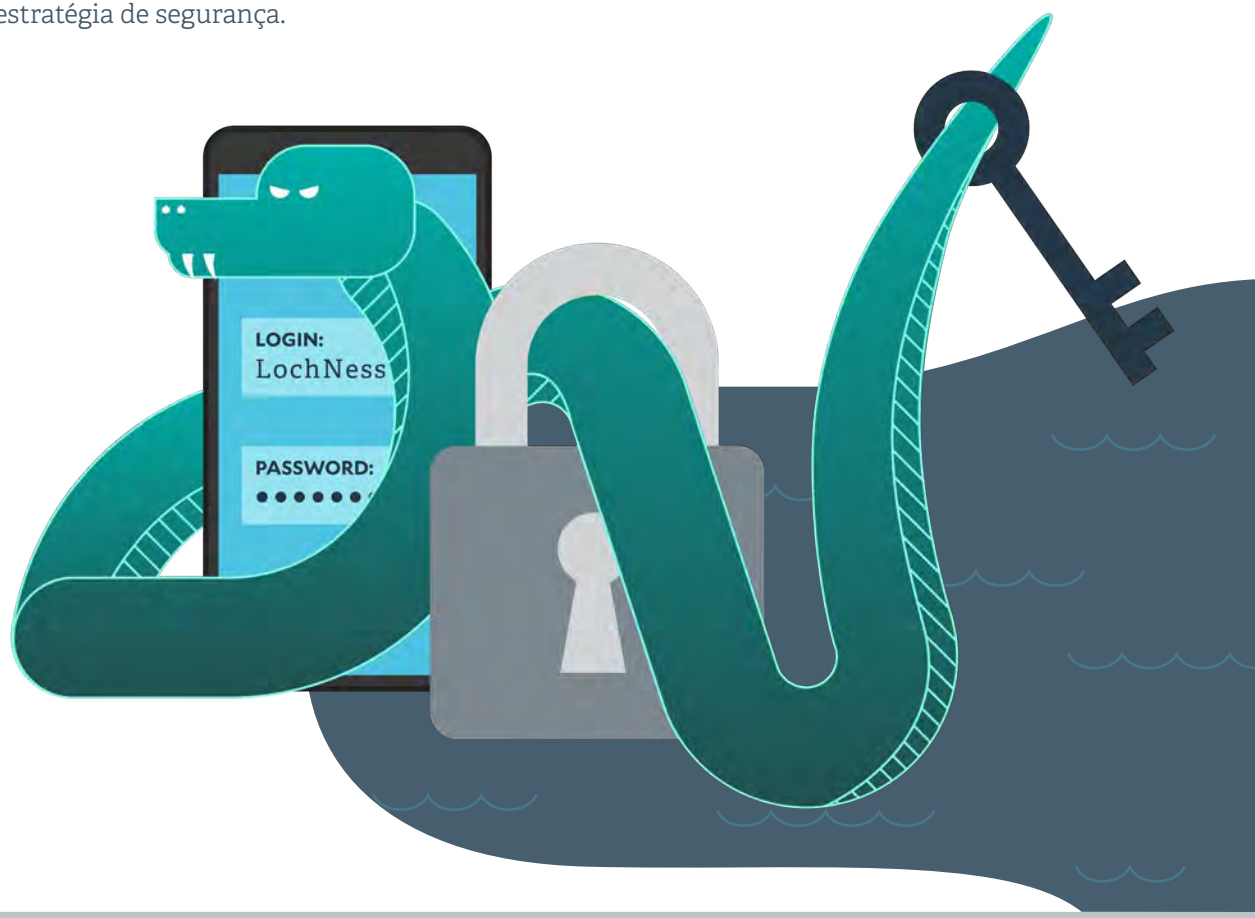
PAM: O PROJETO DE SEGURANÇA NÚMERO UM PARA 2019

Por que o Gartner nomeou o PAM como projeto de segurança número um no ano? Porque a implementação do PAM não apenas tem um forte impacto nos negócios (positivo), mas também reduz significativamente o risco de violação de dados.

O gerenciamento de acessos privilegiados ajuda as organizações a gerenciar e controlar o acessos privilegiados sem comprometer a produtividade. O PAM pode garantir um alto nível de segurança gerenciando credenciais privilegiadas por meio de um armazenamento centralizado de senhas, controlando atividades e acessos privilegiados, e monitorando qualquer atividade suspeita.

No final de 2018, o Gartner lançou seu primeiro quadrante mágico para PAM. O relatório avalia o cenário de ameaças privilegiadas, fornece uma análise completa de 14 fornecedores de PAM e destaca quais recursos de gerenciamento de acessos privilegiados são indispensáveis.

No entanto, mal-entendidos sobre PAM ainda ocorrem. Por isso, a BeyondTrust identificou seis dos maiores mitos sobre o Gerenciamento de Acessos Privilegiados e os detalhou para facilitar sua vida quando se trata de planejar sua estratégia de segurança.



“Até 2022, 90% das empresas reconhecerão que a mitigação de riscos de PAM é um controle de segurança fundamental, que significa um aumento de 70% em relação à hoje.

— Gartner, “Melhores Práticas para Gerenciamento de Acessos Privilegiados” 28 de janeiro de 2019

MITO 1: O MODELO ZERO TRUST É POSSÍVEL

O que é o Modelo Zero Trust?

Criado pela primeira vez em 2010 por John Kindervag, Analista Chefe da Forrester Research, tornou-se um conceito muito popular entre muitas organizações que buscavam reduzir o risco de violação de dados.

O princípio por trás do Zero Trust é que ele exige medidas rigorosas de verificação para todos os dispositivos e pessoas que acessam recursos em uma rede privada, independentemente de estarem dentro do perímetro da rede. Não há uma tecnologia específica associada ao Zero Trust. Pelo contrário, várias tecnologias (com autenticação multifatorial, ou MFA, sendo um princípio básico) são utilizadas para atingir o estado ideal de segurança. Portanto, é considerada uma abordagem holística e ideal que muitas empresas buscam.

Três razões pelas quais Zero Trust é um Modelo Utópico

Embora tenha se tornado um slogan da moda na TI, na prática, esse modelo geralmente é impraticável e utópico. A Forrester apresentou um roteiro de cinco etapas para alcançar o Zero Trust e, embora muitas das abordagens recomendadas mereçam crédito e pareçam lógicas, várias suposições irreais são feitas em virtude dos seguintes desafios enfrentados por quase todas as empresas:

1 Défict Técnico

Se a empresa desenvolver seu próprio software para uso e as aplicações forem antigas, você terá um défict técnico. Redesenhar, recodificar e reimplementar aplicações internas pode ser caro e complexo. É necessário que haja uma razão importante para seguir com esse tipo de iniciativas. Adicionar parâmetros de segurança a aplicações existentes para torná-los Zero Trust nem sempre é possível. É muito provável que sua organização utilize aplicações existentes que não podem acomodar este modelo.

2 Sistemas Legados

É muito provável que aplicações, infraestrutura e sistemas operacionais herdados não reconheçam o modelo Zero Trust. Eles podem não reconhecer os conceitos de restrição de privilégios e movimento lateral, e podem não possuir modelos de autenticação que permitam dinamicamente modificações com base no uso contextual. Qualquer implementação Zero Trust requer uma abordagem em camadas para habilitar esses sistemas. No entanto, tal abordagem implica envolver o acesso externo ao recurso e raramente pode interagir com o próprio sistema. Isso derruba a premissa do Zero Trust.

3 Transformação Digital

Mesmo para as organizações que estão em fase de construção de um novo data center, implementar um modelo de acesso baseado em funções e adotar 100% do modelo Zero Trust, as considerações sobre transformação digital podem dificultar a adoção da teoria. A transformação digital conduzida pelos conceitos de nuvem, DevOps e IoT não suporta o modelo Zero Trust, pois requer tecnologia adicional para segmentar e aplicar o conceito. Para grandes implementações, isso pode ser proibitivo em termos de custo e pode até impactar a capacidade das soluções interagirem corretamente com o acesso para vários usuários.

"Realidade"

Um modelo que pode ajudar a resolver o problema é o Gerenciamento de Acessos Privilegiados Just-in-Time (PAM JIT). O conceito JIT vem da indústria de manufatura e é uma estratégia que minimiza custos, reduzindo o nível de estoque em processo. Trata-se de uma série de alertas que informam a linha de produção para fabricar um próximo produto apena quando necessário.

O PAM JIT pode ajudar a condensar drasticamente a superfície de ameaças privilegiadas e reduzir os riscos em toda a empresa, garantindo que as identidades tenham apenas os privilégios apropriados quando necessário e pelo menor tempo possível. Esse processo pode ser totalmente automatizado e por isso não é notado pelo usuário final.

De acordo com o Gartner, em seu Quadrante Mágico de 2018 para PAM , "até 2022, mais da metade das empresas que utilizam ferramentas de gerenciamento de acessos privilegiados (PAM) irão considerar o acesso privilegiado just in time no longo prazo. Hoje, esse número representa pouco mais de 25% ".

Conheça mais sobre o Gerenciamento de Acessos Privilegiados Just-in-Time.

MITO 2: CONTAS COMPARTILHADAS SÃO NECESSÁRIAS PARA ATIVAR O PAM

Muitas equipes de TI usam contas compartilhadas para usuários privilegiados, administradores ou aplicações, para que eles possam ter o acesso necessário para realizar seus trabalhos. Se gerenciada incorretamente, essa prática apresenta riscos significativos de segurança e conformidade decorrentes do uso intencional, acidental ou indireto de privilégios compartilhados.

Mesmo para as equipes de TI mais experientes, a tarefa de gerenciar contas compartilhadas apresenta complexidades e riscos.

Contas Compartilhadas São Difíceis de Auditar

De acordo com o recente relatório Monitor Report by ICS-CERT, as contas compartilhadas "dificultam a identificação do usuário e permitem que terceiros maliciosos as usem anonimamente. As contas usadas por um grupo compartilhado de usuários geralmente têm senhas ruins que atores mal-intencionados podem adivinhar com facilidade e que os usuários não mudam frequentemente, nem quando um membro do grupo sai."

É Difícil Mudar Hábitos de Funcionários Engajados

Mesmo um extenso treinamento e conscientização sobre segurança nem sempre são suficientes, e os hackers atacam nossa natureza humana. A engenharia social continua a ser uma técnica popular e bem-sucedida quando se trata de obter acesso a sistemas e dados importantes. Basta um funcionário clicar em um link de phishing ou visitar um site não seguro para abrir uma porta para hackers. O funcionário pode até ser conhecedor desses tipos de ataques, mas se for pego em um momento agitado ou for alvo de um phishing sofisticado, poderá se tornar uma vítima. E se uma conta de superusuário for comprometida, o hacker pode ter acesso instantâneo às jóias da coroa.

"Realidade"

Se uma conta privilegiada compartilhada for comprometida, ela acarreta riscos devastadores, pois é frequentemente usada em várias aplicações e recursos. Se ocorrer uma violação, o invasor poderá acessar várias contas de funcionários da empresa. Torna-se mais difícil identificar quem foi comprometido e geralmente exigem-se muitos sistemas que precisam ser usados para "corrigir" o problema.

Uma conta compartilhada comprometida é um prato cheio para um hacker. A boa notícia é que você não precisa mudar para contas compartilhadas para ativar o PAM.

MITO 3: SOMENTE CONTAS PRIVILEGIADAS SÃO GERENCIADAS PELO PAM

O PAM Faz Mais Do Que Gerenciar Suas Contas Privilegiadas

Gerenciar Contas Privilegiadas é a ponta do iceberg do processo de PAM. O Gerenciamento de Acessos Privilegiados é composto por vários componentes, cada um servindo a um objetivo para alcançar o equilíbrio ideal entre segurança e produtividade. O objetivo principal é a imposição de privilégios mínimos, definida como a restrição de direitos e permissões de acesso para usuários, contas, aplicativos, sistemas, dispositivos (como IoT) e processos ao mínimo necessário para executar atividades autorizadas de rotina.

Também conhecido como Gerenciamento de Identidades Privilegiadas (PIM) ou apenas gerenciamento de privilégios, o PAM é considerado por muitos analistas e tecnólogos como um dos projetos de segurança mais importantes para reduzir o risco cibernético e alcançar o ROI de alta segurança.

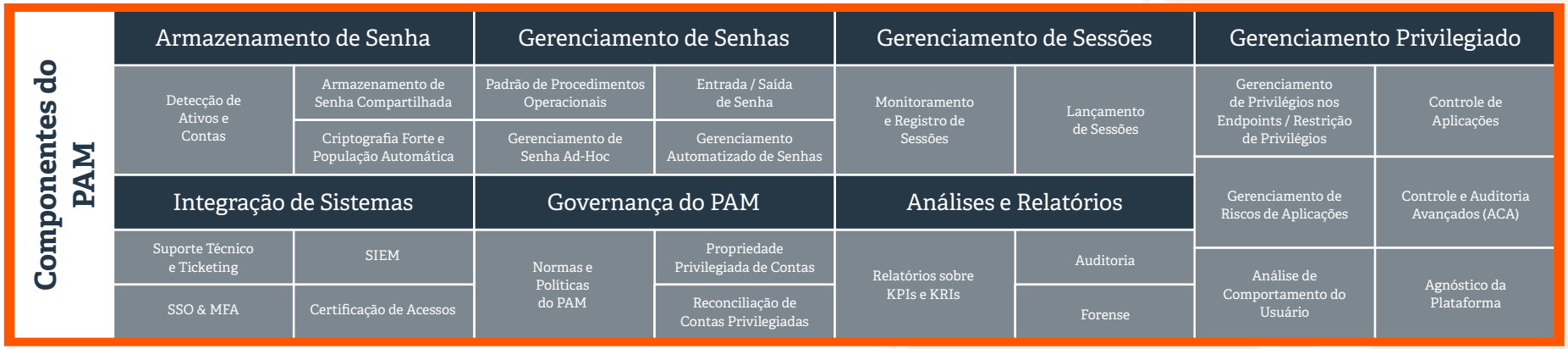
"Realidade"

Uma plataforma PAM abrangente inclui muito mais do que apenas gerenciamento privilegiado de contas e sessões (PASM), embora esse continue sendo um componente essencial. O PAM também consiste na elevação e delegação de privilégios (PEDM) - também conhecido como gerenciamento de privilégios nos endpoints, acesso remoto seguro (para fornecedores e funcionários) e muito mais. Alguns dos principais recursos do PAM incluem:

- Descoberta de contas / credenciais privilegiadas em sistemas, dispositivos e aplicações, além da integração para gerenciamento contínuo.
- Randomização e armazenamento automáticos de senhas para identidades privilegiadas humanas e não pessoais.
- Eliminação de privilégios de administrador e raiz, e simplificação da imposição de políticas de menos privilégios
- Acesso remoto seguro para fornecedores e funcionários
- Integração de dados de vulnerabilidade para tomar decisões privilegiadas de elevação e delegação com base em risco em tempo real
- Registro de acessos privilegiados para auditoria e relatórios
- Compartilhamento privilegiado de usuário e análise de ameaças
- Integração com soluções de governança de identidade para visibilidade e gerenciamento contínuos de identidades privilegiadas e não privilegiadas em toda a empresa.

Resumindo: o PAM cobre uma área muito maior de controles de segurança e mitigação de ameaças do que as pessoas imaginam.

- MITRE ATT&CK
- Os 20 Principais Controles Críticos



MITO 4: PAM AJUDA A GERENCIAR E CONTROLAR O ACTIVE DIRECTORY

O Gerenciamento de Acessos Privilegiados trata muito mais do que as contas do Active Directory (AD), que é um serviço de diretório desenvolvido pela Microsoft para redes de domínio Windows. Autentica e autoriza todos os usuários e computadores Windows - atribuindo e aplicando políticas de segurança para todos os computadores e instalando ou atualizando software.

"Realidade"

Em 2018, 52,2% do tráfego da Internet veio de dispositivos móveis e deverá aumentar para 63,4% até o final de 2019. Os desafios crescentes de BYOD e expansão de serviços em nuvem fazem parte do movimento multi-plataformas para o qual os ambientes de TI estão migrando. Também é importante notar que as empresas que utilizam redes DMZ (que geralmente ficam fora do ambiente AD) apresentam riscos adicionais à segurança que o PAM também pode ajudar a mitigar.

Outro alvo de alto valor para os invasores são os sistemas Unix e Linux, pois eles hospedam dados e aplicações mais críticos. Sem proteção e controle completos de credenciais privilegiadas e responsabilidade sobre as ações dos usuários, as organizações poderiam ser expostas a lacunas de risco.

Uma solução abrangente de PAM para Unix e Linux mitiga todos esses riscos, protegendo, auditando e monitorando todas as contas e atividades privilegiadas nos seus sistemas mais críticos. O Active Directory é apenas uma das muitas considerações que as organizações devem ter em sua estratégia de segurança.

Além disso, o PAM também ajuda outras áreas de risco menos convencionais em sua organização, como contas corporativas de mídias sociais. As senhas para suas contas corporativas do Facebook, Twitter ou LinkedIn devem ser consideradas privilegiadas; se as credenciais caírem em mãos erradas, o uso indevido pode levar a danos significativos à marca e à reputação a longo prazo.

MITO 5: O ACESSO DE TERCEIROS PODE SER GARANTIDO USANDO OS RECURSOS DA VPN

A Função Dos Gerenciadores de Senhas

Os gerenciadores de senhas são ferramentas úteis para os usuários que possuem um grande volume de senhas, e precisam acessar uma infinidade de sistemas, portais e demais aplicações existentes na organização. Portanto, a ideia de ter um cofre digital criptografado que possa armazenar todas essas informações para você, além de gerar senhas únicas e fortes para diferentes serviços, geralmente é uma ferramenta essencial (e às vezes gratuita) que muitas pessoas utilizam.

Porém, alguns gerenciadores de senhas, como LastPass, 1Password e Dashlane, têm limitações significativas. Muitos acreditam que esses tipos de gerenciadores oferecem recursos de gerenciamento de sessões que podem proteger o acesso do fornecedor. Esse não é o caso.

As Limitações da VPN

O acesso à VPN não é o mesmo que o monitoramento de sessão. Saber que uma sessão de VPN foi iniciada não ajuda a dizer se as ações na sessão são apropriadas. Por questões de segurança e auditabilidade, as equipes de TI precisam ir além dos recursos de gerenciamento da VPN, o que significa monitoramento de sessão com registro de pressionamento de tecla, indexação e filtragem de comandos para sessões remotas verdadeiramente seguras.

"Realidade"

O gerenciamento de sessões por si só não protege os protocolos usados para o acesso a terceiros. Um gateway, proxy, host ou jump point são necessários como middleware para garantir que a sessão não seja usada como ponte para atividades maliciosas.

Soluções como o Privilege Remote Access não apenas protegem, gerenciam e auditam os acessos de terceiros sem precisar de VPN, mas também funcionam em ambientes híbridos e permitem que você atenda a requisitos de conformidade mais complexos por meio de trilhas abrangentes de auditoria e análise forense de sessões.

É importante ressaltar que ferramentas gratuitas (como RDP) não são suficientemente robustas - para uma análise aprofundada, leia o White Paper: The True Cost of Free Remote Support Software.

MITO 6: UMA GRANDE EQUIPE DE TI É NECESSÁRIA PARA IMPLEMENTAÇÃO E GERENCIAMENTO DO PAM

Implementar o gerenciamento de acessos privilegiados pode ser assustador para muitos - especialmente se o seu ambiente é composto por uma variedade de sistemas operacionais, softwares legados e geografias distantes. Ou talvez você tenha uma pequena equipe de TI que já esteja no limite. No entanto, uma boa solução PAM será simples de implantar e manter ao longo do tempo. A implementação do PAM é mais fácil do que você imagina.

"Realidade"

O PAM é composto por três componentes principais, com diferentes esforços necessários para cada um, listados abaixo do menor para o maior esforço e manutenção:

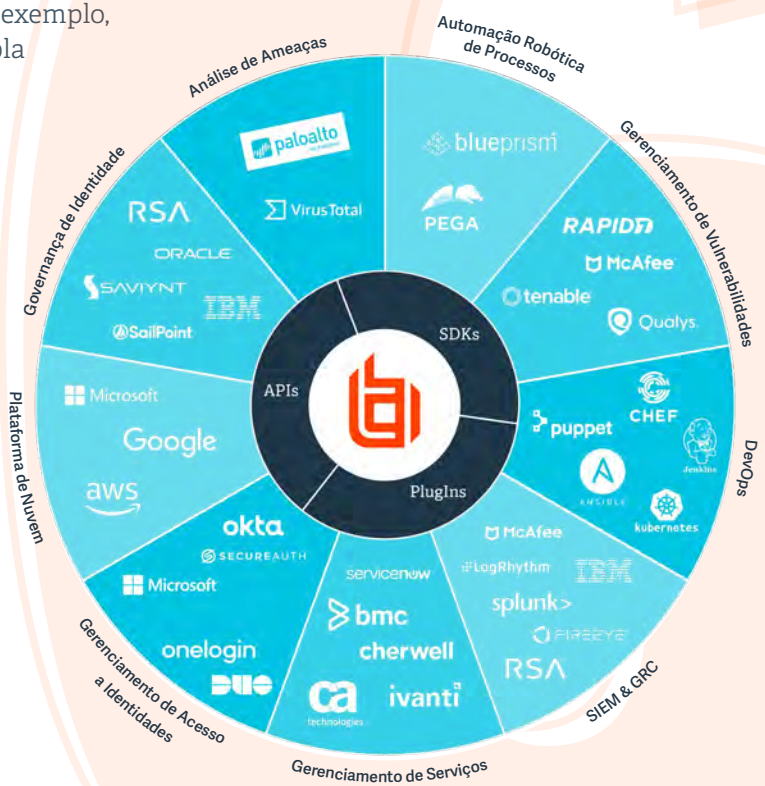
- **Acesso Remoto Seguro (SRA):** Proteja, gerencie e audite terceiros e acessos privilegiados remotos internos sem precisar de uma VPN. Necessita de pouca ou nenhuma manutenção.
- **Gerenciamento de Privilégios no Endpoint (EPM):** Elimine privilégios desnecessários e eleve direitos a Windows, Mac, Unix, Linux e dispositivos de rede sem prejudicar a produtividade. Manutenção limitada necessária quando ocorrem alterações ambientais ou de aplicação.
- **Gerenciamento Privilegiado de Contas e Sessões (PASM):** Descubra, gerencie, audite e monitore contas privilegiadas de todos os tipos. Manutenção de nível médio necessária, quando ocorrem alterações nos procedimentos, ambiente ou pessoal.

Depois que o ambiente é instalado para cada componente, a automação interna (incluindo manutenção do banco de dados) é fornecida em uma boa solução de PAM.

Implementação Facilitada por Meio de Integrações

Em termos de implementação, você deve consultar os especialistas de parceiros, fornecedores e integradores de sistemas. Os principais fabricantes de PAM oferecerão um amplo conjunto de integrações, o que significa que você pode se beneficiar de tecnologias que trabalham juntas para uso imediato, maximizando seus investimentos em TI existentes e tornando todo o processo ainda mais uniforme e eficiente. Por exemplo, a BeyondTrust se integra a uma ampla variedade de soluções de terceiros. Veja a figura abaixo para uma visão geral do ecossistema de nossos parceiros.

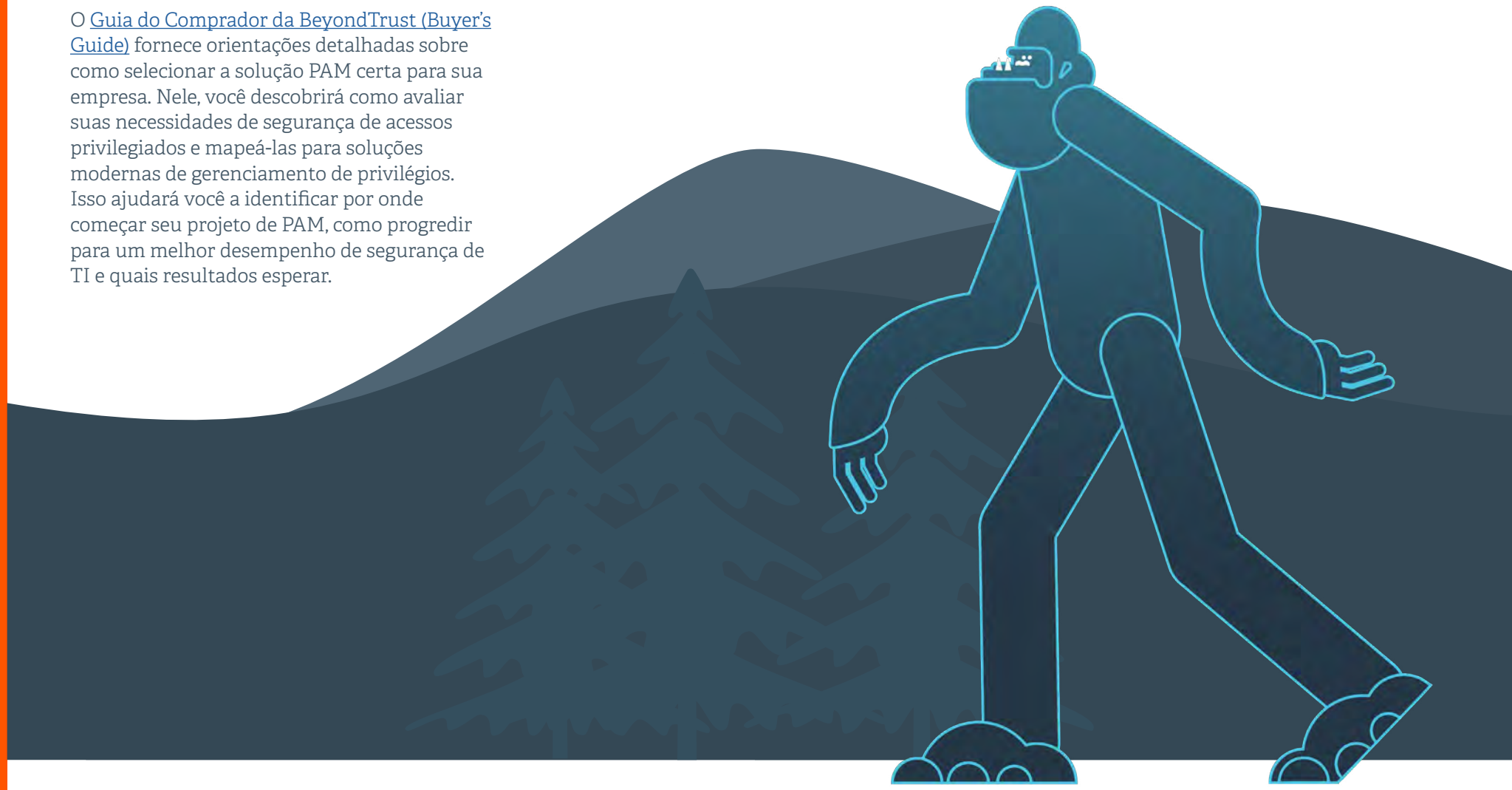
Para menos requisitos de sobrecarga e infraestrutura, as soluções PAM podem ser implantadas na nuvem usando SaaS (software como serviço) ou uma solução hospedada como AWS ou Azure. O gerenciamento de credenciais na nuvem pode tornar o gerenciamento de acessos privilegiados mais fácil e econômico. Para organizações que buscam reduzir riscos de acessos privilegiados, enquanto enfrentam falta contínua de pessoal e recursos, as soluções em nuvem do PAM fornecem encargos administrativos reduzidos, além de rápida implantação.



CONCLUSÃO

É importante distinguir os mitos e verdades ao eleger a abordagem para mitigar os riscos de uma violação cibernética em sua empresa. Compreender os verdadeiros benefícios e os casos de uso do gerenciamento de acessos privilegiados é uma etapa importante que você pode executar para aprimorar significativamente a estratégia de segurança da sua organização.

O Guia do Comprador da BeyondTrust (Buyer's Guide) fornece orientações detalhadas sobre como selecionar a solução PAM certa para sua empresa. Nele, você descobrirá como avaliar suas necessidades de segurança de acessos privilegiados e mapeá-las para soluções modernas de gerenciamento de privilégios. Isso ajudará você a identificar por onde começar seu projeto de PAM, como progredir para um melhor desempenho de segurança de TI e quais resultados esperar.



A PLATAFORMA DA BEYONDTRUST

A plataforma de Gerenciamento de Acessos Privilegiados da BeyondTrust é uma solução integrada que fornece controle e visibilidade sobre todas as contas e usuários privilegiados em todas as plataformas corporativas. Ao unir os melhores recursos em uma só solução, a plataforma BeyondTrust simplifica implantações, reduz custos, melhora a segurança do sistema e elimina as brechas de segurança para reduzir riscos.

Sobre BeyondTrust

A BeyondTrust é líder mundial no gerenciamento de acessos privilegiados, oferecendo uma abordagem direta para evitar violações relacionadas a privilégios. Nossa plataforma permite que as organizações dimensionem facilmente a segurança de privilégios à medida que as ameaças evoluem nos ambientes de endpoints, servidores, nuvem, DevOps e dispositivos de rede. Mais de 20.000 clientes confiam nas soluções da BeyondTrust.

Sobre o Gerenciamento de Privilégios nos Endpoints

As soluções de gerenciamento de privilégios de endpoint da BeyondTrust oferecem a você o poder de restringir privilégios e eliminar os direitos de administrador local. Remova privilégios excessivos de usuários finais e controle aplicativos em Windows, Mac, Unix, Linux e dispositivos de rede - tudo sem prejudicar a produtividade do usuário final.

Sobre o Gerenciamento de Senhas

O BeyondTrust Password Safe unifica o gerenciamento de senhas e sessões privilegiadas, fornecendo descoberta, gerenciamento, auditoria e monitoramento seguros para qualquer credencial privilegiada. O Password Safe permite que as organizações obtenham controle e responsabilidade completos sobre contas privilegiadas.

Sobre o Privilege Remote Access

O Privileged Remote Access fornece visibilidade e controle sobre o acesso de terceiros, bem como acesso remoto interno, permitindo que as organizações estendam o acesso a ativos importantes, mas sem comprometer a segurança.

beyondtrust.com/pt

V2019_09_ENG