WHITE PAPER

GUIA PARA GERENCIAMENTO DE PRIVILÉGIOS MULTICLOUD

Proteja, Gerencie e Audite Todos os Acessos Privilegiados em um Mundo Híbrido e Multicloud

BeyondTrust

ÍNDICE

1 Introdução

As empresas não debatem mais se devem ou não ir para a nuvem; agora é uma questão de quanta tecnologia e ativos implementar na nuvem e com que rapidez. Quer a empresa aproveite ou não os modelos SaaS, IaaS ou PaaS e hospede suas próprias aplicações em uma nuvem pública ou privada, é quase certo que seus colaboradores estejam consumindo alguma forma de aplicações e serviços na nuvem.

A transição para os vários modelos de nuvem oferece muitos benefícios e tem sido fundamental para que as empresas mudem com flexibilidade para acesso remoto e trabalho em casa. Entretanto, a segurança que as empresas desfrutam em suas instalações geralmente não pode ser transferida para ambientes na nuvem. Ou seja, a segurança desfrutada em um ambiente de nuvem pode não ser adequada ou compatível para outro ambiente de nuvem.

Hoje, as organizações não estão se prendendo a apenas um ambiente de nuvem do tipo IaaS ou PaaS. De acordo com o relatório RightScale State of the Cloud, quase todas as empresas (84%) que usam nuvens de Infraestrutura como um serviço (IaaS) ou como Plataforma como um serviço (PaaS) usam mais de um provedor. E a maioria das organizações emprega três ou mais nuvens públicas de provedores líderes do mercado, como Amazon Internet Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).

> *"Multicloud, por definição, é a implementação de vários provedores de nuvem para dar suporte a ambientes públicos, privados ou híbridos para uma aplicação ou serviço, para atender um objetivo de negócio."*

Teoricamente, a multicloud oferece alguns benefícios adicionais além da implantação de um provedor IaaS/PaaS, como:

- Redundância e recuperação de desastres
- Aproveitamento da portabilidade da carga de trabalho para movê-la para ambientes de nuvem que oferecem o melhor caso de uso e custos operacionais
- Latência reduzida e conformidade da privacidade de dados fazendo hospedagem com provedores regionais, que pode ser importante para apoiar empresas multinacionais e governos locais
- Liberdade na nuvem (ou seja, sem depender de fidelidade ao fornecedor) para alterar a hospedagem com base nos negócios, tecnologia ou preocupações geopolíticas

Entretanto, também há desvantagens em ambientes multicloud. Por exemplo, cada plataforma de nuvem pública usa seu próprio sistema de identidade proprietário (por exemplo: Azure Active Directory). Além disso, a maioria das empresas não está 100% na nuvem - elas operam com um modelo híbrido que inclui uma infraestrutura nas instalações, baseada geralmente em tecnologia mais antiga.

Os benefícios de ambientes em nuvem, multicloud e híbridos podem ser facilmente prejudicados pela complexidade do ambiente, formação de silos de identidade e pela proliferação de ferramentas dependentes da plataforma que devem ser aprendidas e administradas. Isso se traduz em riscos mais elevados de brechas de segurança, descuidos e vulnerabilidades que podem (e levam) a violações e paradas ou outras interrupções operacionais. E a interoperação da segurança entre ambientes multicloud disseminado em multirregiões requer um novo paradigma de segurança e de privacidade de dados, para as quais muitas organizações estão mal preparadas.

À medida que os ambientes se tornam cada vez mais descentralizados, a identidade das pessoas se torna a base mais sólida para a segurança.

À medida que os ambientes se tornam cada vez mais descentralizados, a identidade das pessoas se torna a base mais sólida para a segurança. O desafio da identidade é o problema de segurança mais importante para as organizações resolverem em ambientes de nuvem e em suas instalações. Diferentes ambientes de provedores de nuvem exigem suas próprias identidades exclusivas e têm suas próprias estruturas de permissão e terminologias exclusivas.

Padronizar os controles de gerenciamento e segurança em todo o ecossistema de TI é fundamental para o sucesso da implementação de sua estratégia de segurança. Em particular, identidades e acessos privilegiados representam o maior risco e também a maior urgência e prioridade de segurança. Uma identidade comprometida e suas contas compartilhadas associadas são o vetor de ataque mais eficaz para um agente de ameaça comprometer todo um ambiente multicloud. Isto é especialmente verdadeiro para quaisquer contas privilegiadas que são compartilhadas em um ambiente multicloud para facilitar o gerenciamento ou a operação das soluções ou serviços.

MODELOS DE RESPONSABILIDADE COMPARTILHADA E O QUE ISSO SIGNIFICA PARA O PAM

Os principais fornecedores de IaaS e PaaS em nuvem colocam um grande foco na proteção de sua própria infraestrutura de nuvem, mas cada um reconhece que a segurança na nuvem é uma responsabilidade compartilhada com o cliente.

Os principais fornecedores de IaaS e PaaS em nuvem colocam um grande foco na proteção de sua própria infraestrutura de nuvem, mas cada um reconhece que a segurança na nuvem é uma responsabilidade compartilhada com o cliente – e o cliente é responsável por resolver as lacunas deixadas pelas responsabilidades do fornecedor. Obviamente, não há duas plataformas na nuvem iguais e cada Provedor de Serviços na Nuvem (CSP) difere em seu modelo de responsabilidade compartilhada. Da mesma forma, cada CSP difere na segurança nativa e em outros conjuntos de ferramentas que fornecem a seus clientes. A Forrester Research apelidou esse modelo de segurança compartilhado de "aperto de mão desigual". O Gartner Institute estima que, "Até 2022, pelo menos 95% das falhas de segurança na nuvem serão por culpa do cliente".

Figura 1: O Modelo de Responsabilidade Compartilhada da Azure e Onde a BeyondTrust Pode Ajudar

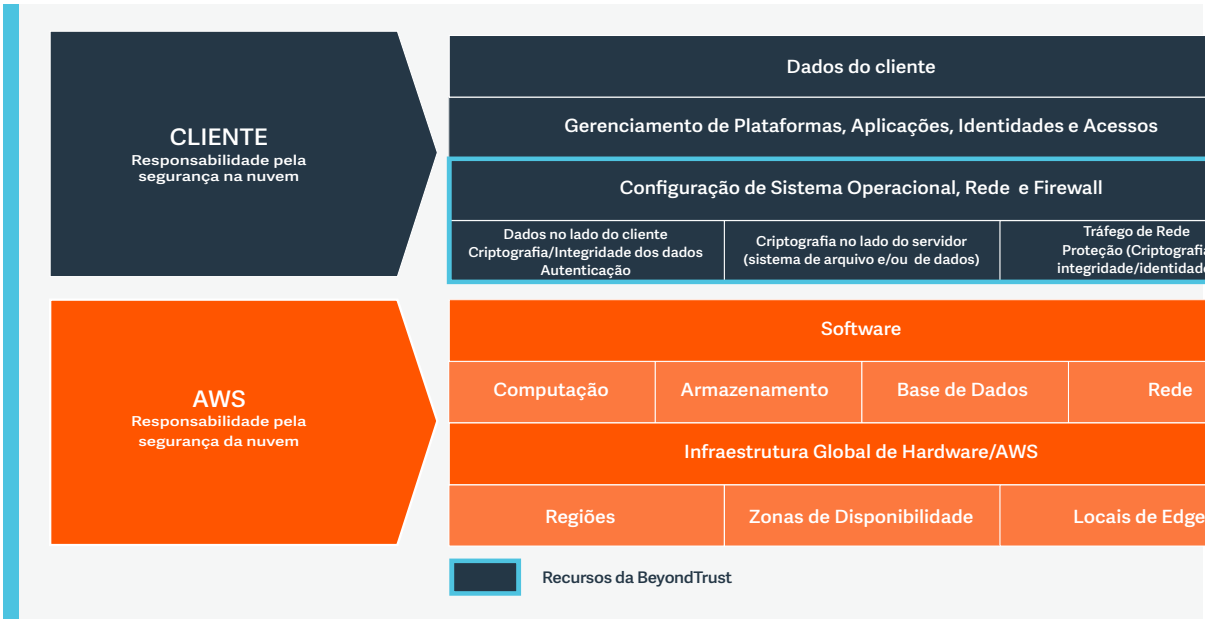
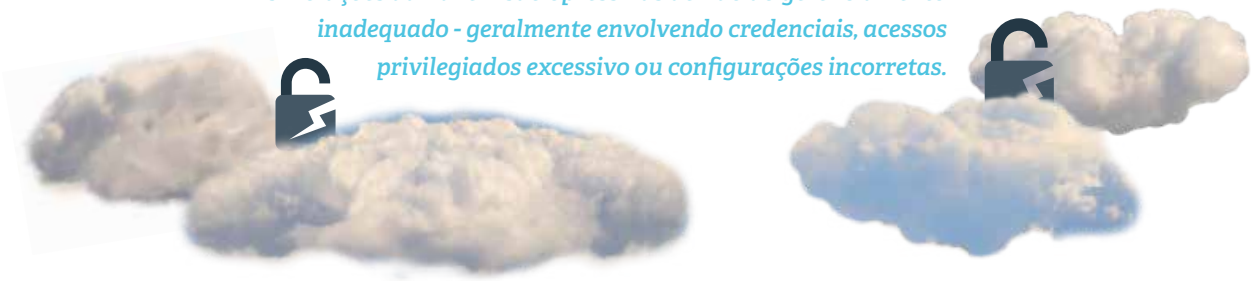


Figura 2: O Modelo de Responsabilidade Compartilhada da AWS e Onde a BeyondTrust Pode Ajudar

A maioria das plataformas de nuvem (AWS, Azure, Google, etc.) fornece apenas controles básicos de gerenciamento de identidades e acessos (IAM), e a lacuna nos controles de segurança de acessos privilegiados é deixada principalmente para os clientes. Algumas das plataformas de virtualização e nuvem mais comumente usadas oferecem suporte apenas para sua própria autenticação multifatorial (MFA) nativa e de alguns líderes do setor. Além disso, os recursos integrados de monitoramento de sessão estão totalmente ausentes na maioria das plataformas, e forneçam apenas funções rudimentares em outras. O gerenciamento e o monitoramento de sessões são essenciais para garantir a segurança, a capacidade de auditoria e a responsabilidade dos ambientes de nuvem.

E, é claro, essas ferramentas nativas não são aplicáveis a outros ambientes de nuvem ou locais onde as organizações podem ter soluções de segurança hospedadas. Essas inconsistências e deficiências de segurança criam oportunidades férteis para o uso indevido de contas e acesso, o que pode resultar no vazamento de dados confidenciais ou de recursos potencialmente sequestrados. Na prática, as violações da nuvem são opressivas devido ao gerenciamento inadequado - geralmente envolvendo credenciais, acessos privilegiados excessivo ou configurações incorretas.

As violações da nuvem são opressivas devido ao gerenciamento inadequado - geralmente envolvendo credenciais, acessos privilegiados excessivo ou configurações incorretas.



A ELASTICIDADE DA NUVEM

A elasticidade na nuvem significa que os recursos da nuvem e suas instâncias operacionais podem ser facilmente aumentados e diminuídos com base na carga de trabalho, teste ou demanda da tarefa. Ao fazer isso, novas contas - geralmente com privilégios administrativos - são criadas em grande escala. Os planos de controle de virtualização e nuvem baseados na internet vêm com contas altamente privilegiadas que dominam todo o ambiente de nuvem. Aplicações SaaS, consumidas pelos colaboradores, geralmente fornecem acesso a recursos confidenciais e normalmente operam abaixo do radar de recursos gerenciados. A elasticidade da nuvem permite que eles operem em um estado efêmero em comparação com suas contrapartes nas instalações da empresa. Isso torna o gerenciamento de acessos privilegiados ainda mais difícil, pois, a qualquer momento, a instância pode estar presente ou pode ter sido descartada.

A escala de gerenciamento do universo em crescimento dos privilégios requer uma abordagem integrada, em vez de depender de ferramentas de nicho, cada uma ajudando a gerenciar apenas uma parte do problema dos privilégios.

A escala de gerenciamento do universo em crescimento dos privilégios requer uma abordagem integrada e universal, em vez de depender de ferramentas de nicho, cada uma ajudando a gerenciar apenas uma parte do problema dos privilégios. Isso é especialmente verdadeiro quando a elasticidade da nuvem permite mudanças rápidas que mesmo as ferramentas tradicionais de gerenciamento e governança podem não ver.

Leia este white paper para entender:

- Lacunas de gerenciamento de acessos e riscos de privilégios em ambientes de nuvem
- Práticas recomendadas para proteger contas privilegiadas e acessos para IaaS, PaaS e SaaS
- Como as soluções BeyondTrust protegem uma variedade de ambientes de implantação em nuvem, híbrida e multicloud

Em última análise, sua estratégia de gerenciamento de acessos privilegiados deve garantir que cada conta, sessão e ativo privilegiado seja protegido, gerenciado e monitorado em toda a sua infraestrutura na nuvem.

2 Desafios da nuvem e ameaças à segurança

Muitas organizações já correm alto risco com administradores de TI e usuários avançados com privilégios excessivos. Conforme migram mais cargas de trabalho para a nuvem, a complexidade nas instalações da empresa não desaparece. Em vez disso, eles tendem a ficar com o desafio do gerenciamento híbrido e multicloud mostrado na figura abaixo:

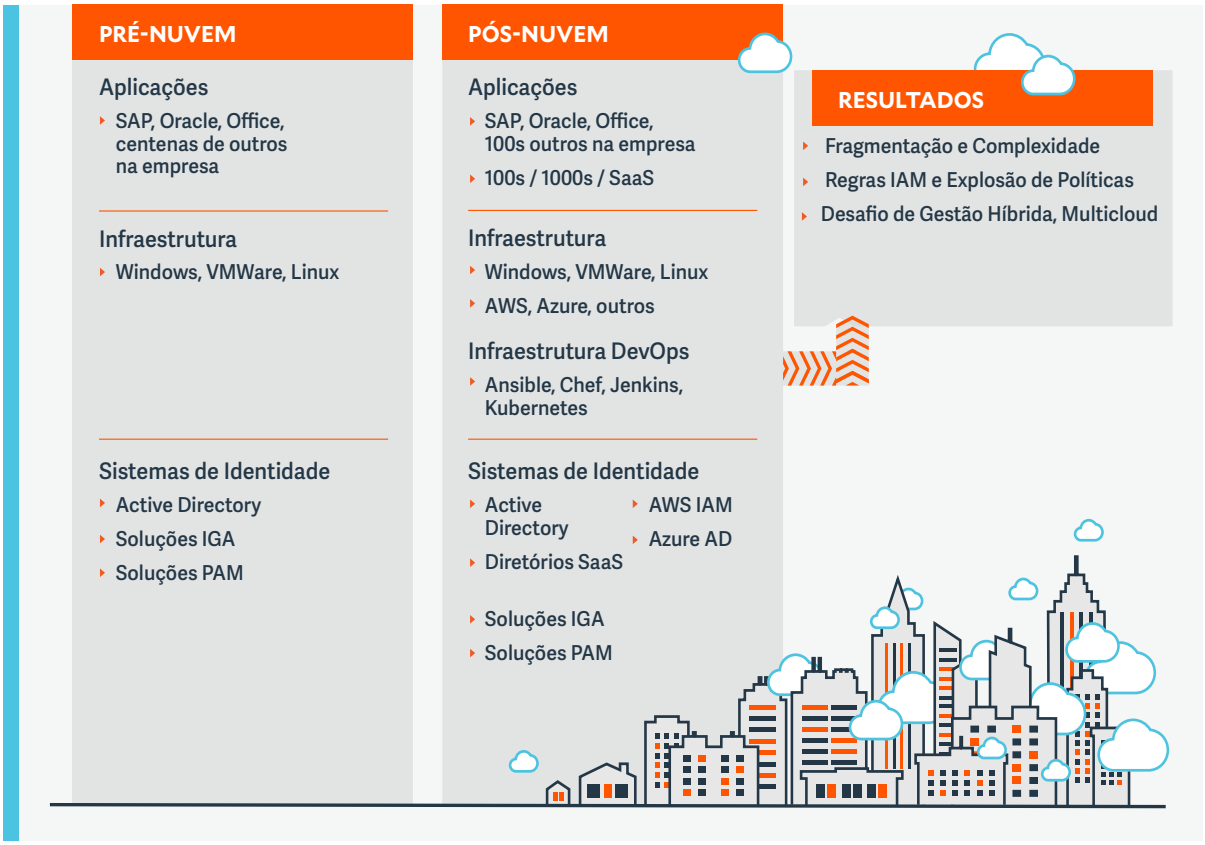


Figura 3: O Efeito da Migração para a Nuvem

No relatório de pesquisa das principais ameaças à computação na nuvem da Cloud Security Alliance, eles chamam sua lista das principais ameaças de ambiente na nuvem de "The Egregious 11". O gráfico na página a seguir mostra como as soluções BeyondTrust PAM tratam 10 das 11 ameaças:

	Principais Ameaças da CSA à Computação na Nuvem	Como a BeyondTrust Protege a Nuvem
1	**Falhas em dados**	Protege contra os principais vetores de ataque de incidentes de segurança na nuvem, incluindo roubo de credenciais, abuso de privilégios, acesso remoto comprometido e movimento lateral.
2	**Configuração incorreta e controle de mudanças inadequado**	Aplica o acesso apropriado e fluxos de trabalho estabelecidos para controle de mudanças. Também permite que a equipe de segurança descubra configurações incorretas em contas privilegiadas.
3	**Falta de arquitetura e estratégia de segurança na nuvem**	Fornece descoberta completa de ativos para garantir que todos os recursos ativos implantados sigam sua arquitetura, estratégia e governança de segurança na nuvem.
4	**Gerenciamento de identidade, credencial, acesso e chaves insuficientes**	Descobre, integra e gerencia com segurança todos os tipos de senhas humanas e não humanas, chaves, segredos e outras credenciais na nuvem. Insere credenciais com segurança em sessões sem revelar as senhas e monitora todas as sessões envolvidas em atividades privilegiadas. Alterna segredos automaticamente para gerenciar ameaças às credenciais.
5	**Roubo de conta**	Protege as credenciais de forma robusta e aplica as melhores práticas de segurança para senhas, como senhas complexas e rotação de senhas. Previne e minimiza ataques como "pass-the-hash", reutilização de senha e muitos outros. Além disso, aplica monitoramento e gerenciamento de sessão, com a capacidade de pausar ou encerrar sessões suspeitas.
6	**Ameaças internas**	Impõe restrição de privilégios para todos os usuários e implementa controle avançado de aplicações para limitar o movimento lateral e o aumento de privilégios. Esses controles restringem as atividades que um usuário pode realizar ou executar ao mínimo necessário, protegendo contra ações maliciosas e inadvertidas (erros). A filtragem de comandos e scripts e os recursos de monitoramento/gerenciamento de sessão fornecem proteção adicional contra atividades inadequadas.
7	**Interfaces e APIs inseguras**	Elimina credenciais incorporadas em código, protege centralmente todos os segredos usando uma API segura e rotacional para garantir que não se tornem obsoletas ou vulneráveis a ataques para reutilização.
8	**Plano de controle fraco**	A BeyondTrust aumenta significativamente a segurança do plano de controle de várias formas: ▸ Acesso de proxies ao plano de controle ▸ Elimina privilégios desnecessários e permite apenas o privilégio mínimo necessário para a administração ▸ Gerencia, monitora e audita sessões de plano de controle ▸ Aplica as melhores práticas de segurança para todas as contas que acessam o plano de controle
9	**Falhas na metaestrutura e na estrutura da aplicação**	A BeyondTrust não fornece uma solução para esse caso de uso.
10	**Visibilidade limitada do uso da nuvem**	Descobre e integra todos os ativos na nuvem. Além disso, monitora, gerencia e audita todas as sessões privilegiadas na nuvem, incluindo para automação de DevOps de CI/CD.
11	**Abuso e uso nefasto dos serviços na nuvem**	Protege contra uso indevido e abuso, pelo menos destas maneiras significativas: ▸ Impõe a restrição de privilégios para limitar as atividades apenas ao que é autorizado ▸ Previne o roubo de credencial privilegiada ▸ Impõe o controle avançado de aplicações para garantir que apenas as aprovadas estejam em execução e apenas com os privilégios mínimos necessários. Além disso, coloca visibilidade e segurança em torno de recursos de shadow IT ▸ A filtragem de comandos e de scripts garante que apenas os comandos certos possam ser executados, e apenas dentro do contexto adequado

Muitas das principais ameaças (violações, contas sequestradas, etc.) citadas no relatório CSA têm outras causas raízes que é importante entender. Vamos dar uma olhada mais detalhada nos contribuintes subjacentes significativos que causam incidentes, violações e interrupções de segurança na nuvem antes de mergulhar nas práticas recomendadas de segurança para a nuvem:

Falta de controle e múltiplos usuários

Alugar um serviço na nuvem pública significa que as organizações não têm propriedade do hardware, das aplicações ou do software no qual os serviços da nuvem são executados. Certifique-se de entender a abordagem do fornecedor de nuvem para esses ativos e o suporte oferecido para tecnologia proprietária.

Falta de visibilidade e shadow IT

As organizações usam, em média, cerca de 1.935 serviços na nuvem.
CLOUD ADOPTION AND RISK REPORT 2019, MCAFEE

A computação na nuvem facilita a criação de novas instâncias e ambientes, a assinatura de uma aplicação SaaS e a criação de novas contas e privilégios. Ambientes na nuvem desconhecidos ou mal gerenciados apresentam riscos de segurança significativos, incluindo violações, perda de dados, roubo de propriedade intelectual e problemas de conformidade regulatória. De acordo com um relatório da McAfee, as organizações usam, em média, cerca de 1.935 serviços na nuvem. Os usuários devem seguir políticas de uso aceitável rígidas para obter autorização e para assinar novos serviços na nuvem ou criar novas instâncias.

Proliferação descontrolada de privilégios

O crescente número de privilégios humanos e de máquina, e a natureza dinâmica dos privilégios apresentam um risco existencial para os ambientes na nuvem.

A exploração de privilégios é um componente de quase todos os ataques cibernéticos atualmente. O uso indevido, intencional, acidental ou indireto de privilégios prejudica a integridade do ambiente na nuvem. Uma catástrofe em potencial fica à espreita quando o uso indevido envolve uma conta de super usuário, como root ou um console administrativo na nuvem. O crescente número de privilégios humanos e de máquina, e a natureza dinâmica dos privilégios apresentam um risco existencial para os ambientes na nuvem.

As organizações tendem a super oferecer privilégios aos usuários - seja para evitar solicitações de elevação de privilégios para o service desk, seja devido à negligência no gerenciamento de privilégios padrão. Além disso, o modelo padrão para a maioria das organizações é de privilégios persistentes ou permanentes, o que significa que uma conta sempre pode executar os privilégios inerentes a ela.

Na nuvem, há muitos planos de privilégios para oferecer aos usuários, servidores, aplicações e cargas de trabalho. As máquinas virtuais podem ser instanciadas na ordem de milhares por meio de alguns cliques simples. Entretanto as muitas contas privilegiadas geradas com essas instâncias tendem a ser ignoradas.

Outra preocupação é que os planos de controle na nuvem (consoles de gerenciamento da nuvem) fornecem amplo acesso de super usuário. Porém, as ferramentas nativas são incapazes de gerenciar e auditar esse acesso de maneira granular. Se a integridade do plano de controle for prejudicada, pode comprometer todo o ambiente da nuvem. Tudo isso pode ser ainda mais agravado em ambientes DevOps, que, por sua natureza, são de carregamento rápido, dependem fortemente de automação e abrangem uma escala maciça.

Sem controles de acesso, o cenário privilegiado apresenta uma superfície de ataque massiva, deixando as organizações vulneráveis a tudo, desde ataques de sequestro à escalada de privilégios, movimento lateral, ransomware, malware, abuso de acesso interno e muito mais.

Gestão insuficiente de credenciais

O uso indevido de credenciais continua sendo a causa No. 1 de violações, de acordo com o Verizon Data Breach Investigations Report de 2020 e outras pesquisas importantes. A Verizon relatou que credenciais comprometidas estavam envolvidas em 77% das violações na nuvem em 2019. A Forrester Research citou especificamente as credenciais privilegiadas como implicadas em mais de 80% das violações.

As explorações de senha são assustadoras devido às práticas de gerenciamento de credenciais insuficientes. Reutilizar senhas em vários ativos e contas, compartilhar senhas com outras pessoas, falta de vencimento de senhas e aplicações na nuvem e código DevOps com credenciais padrão ou incorporadas são apenas algumas práticas descuidadas que deixam as organizações à mercê de roubo de credenciais e sequestro de contas.

Devido à escala de identidades e contas humanas e de máquina na nuvem, qualquer gerenciamento manual de senhas é simplesmente insustentável. Soluções de gerenciamento de credenciais e segredos de terceiros que automatizam as práticas recomendadas de segurança de senha são absolutamente essenciais.

Erros

Mudanças de configuração não intencionais, comandos incorretos e outros erros são algumas das principais causas de violações de dados na nuvem. Notícias dos últimos anos estão cheias de histórias de violação em torno de buckets AWS S3 configurados incorretamente e outros bancos de dados expostos inadvertidamente devido à falta de proteção por senha ou outros controles básicos de acesso. Com muita frequência, esses erros de configuração envolvem simplesmente negligenciar a atualização das configurações de segurança padrão.

Um estudo de segurança na nuvem da McAfee relatou que, em média, as organizações têm 14 instâncias IaaS mal configuradas em operação, resultando em uma média de 2.269 incidentes de configuração incorreta por mês. De todos os buckets AWS S3, 5,5% foram considerados configurados incorretamente. Muitos desses buckets mal configurados incluem permissões de gravação abertas que os tornam presas fáceis para invasores.

Comandos malformados também podem causar interrupções em larga escala na nuvem. Por exemplo, um comando digitado incorretamente (agora conhecido como "o erro de digitação de 150 milhões de USD") pela equipe S3 da Amazon durante a "depuração de rotina" resultou em uma interrupção de 5 horas em vários servidores e serviços dentro da AWS.

Proteger colaboradores e ativos com restrição de privilégios e controles de acessos privilegiados (ou seja, filtragem de comando), pode ajudar a prevenir ou reduzir muitos erros de nuvem e seu impacto.

APIs expostas e desprotegidas

As aplicações na nuvem geralmente se integram e fazem interface com outros serviços, bancos de dados e aplicações. Isso normalmente é obtido por meio de uma interface de programação de aplicação (API). Os CSPs expõem APIs para que os clientes possam aproveitar e gerenciar serviços na nuvem. Devido à natureza exposta rotineiramente das APIs, elas podem estar sob ataque constante.

O risco de API de uma organização pode aumentar em proporção ao número de sistemas e recursos que as conectam. As chaves de APIs geralmente permanecem inalteradas por meses ou anos. Quando uma API é quebrada, exposta ou hackeada, quaisquer dados protegidos pela aplicação podem ser facilmente acessíveis a indivíduos não autorizados, usando técnicas de programação que não são monitoradas por tecnologias tradicionais de gravação de sessão baseadas em usuários.

É vital conhecer as aplicações e as pessoas que têm acesso aos dados da API e criptografar todas as informações confidenciais. A exploração de uma API pode comprometer os serviços e os dados associados.

Incompatibilidades

As ferramentas de TI arquitetadas para ambientes nas instalações da empresa ou um tipo de nuvem são frequentemente incompatíveis com outros ambientes de nuvem. As incompatibilidades podem se traduzir em lacunas de visibilidade e controle que expõem as organizações ao risco desde complexidade administrativa, a configurações incorretas, vulnerabilidades, vazamentos de dados, acessos privilegiados excessivo e problemas de conformidade.

Colaboradores remotos e BYOD (traga seu próprio dispositivo)

Nos últimos anos, o teletrabalho tornou-se o novo padrão com base em uma ampla variedade de fatores ambientais e economia de custos. Cada vez mais, colaboradores e fornecedores estão se conectando remotamente por meio de roteadores sem patch, Wi-Fi inseguro e usando dispositivos pessoais que não foram protegidos. Alguns desses dispositivos podem até ser compartilhados entre membros da família.

VPN, RDP, SSH e outros protocolos não protegem suficientemente os caminhos de acesso remoto para muitos dos casos de uso da nuvem mais comuns. As soluções PAM que incluem proxies, bastion hosts de nuvem e/ou jump hosts são um ponto de partida para proteger os tipos mais confidenciais de acesso à nuvem. Essas soluções PAM também podem ajudar a proteger o acesso que ocorre entre endpoints ou ativos que podem não ser protegidos adequadamente ou têm status desconhecido.

Acesso de fornecedores

As organizações podem exigir que os fornecedores administrem os servidores na nuvem ou contribuam com aplicações SaaS. Mas lembre-se que VPNs, RDP, SSH e outras tecnologias de acesso remoto podem não ser capazes de impor restrições de privilégios no acesso de fornecedores ou sessões de monitoramento. O relatório BeyondTrust Privileged Access Threat descobriu que uma organização tem em média 182 fornecedores que se conectam a seus sistemas a cada semana, e 58% das organizações acreditam que sofreram uma violação relacionada a fornecedor.

É importante garantir que os endpoints do fornecedor sejam reforçados e protegidos de acordo com os padrões da empresa, além de restringir e monitorar o acesso a ativos confidenciais.

Paradas não planejadas na nuvem

Paradas na nuvem ocorrem - seja devido a um ataque distribuído de negação de serviço (DDoS), uma configuração incorreta ou outro problema. Dependendo de como se aproveita a nuvem, um problema operacional pode tirar de operação grande parte da sua empresa ou pode afetar apenas um ou alguns serviços.

Embora qualquer parada seja prejudicial, será muito mais grave se afetar sua segurança e permitir que invasores obtenham o controle de senhas ou de sistemas confidenciais. É por isso que é fundamental implementar processos de emergência para que o acesso de gestão especial possa ser concedido para permitir a solução de problemas e implementar medidas de proteção, como redefinições de senha para um sistema potencialmente comprometido.

3

Aplicação de 7 Práticas de Segurança Recomendadas na Nuvem, Utilizando o PAM da BeyondTrust

A plataforma de gerenciamento de acessos privilegiados da BeyondTrust oferece visibilidade e segurança robustas em todo o universo da nuvem (IaaS, PaaS, SaaS) e privilégios locais. Nossa abordagem holística, centralizada e elegantemente automatizada ao PAM garante que cada conta privilegiada (humana e máquina), sessão e ativo sejam contabilizados e gerenciados de forma adequada. Com a BeyondTrust, você pode descobrir, proteger e auditar instâncias, serviços, aplicações, ativos e identidades de forma consistente na nuvem.

Os clientes da BeyondTrust utilizam nossas soluções para alcançar boas práticas consistentes de PAM para seus ativos, usuários e cargas de trabalho, em uma infraestrutura heterogênea. Nossos clientes nos dizem que isso se traduz nestes benefícios:

- Maior produtividade e agilidade do usuário final
- Redução de erros humanos/configurações incorretas
- Menor superfície de ataque e menor taxa de contaminação por malware, violações e outros incidentes de segurança
- Melhor desempenho operacional
- Caminho simplificado para a conformidade

Abaixo estão descritas as 7 melhores práticas de segurança na nuvem habilitadas pela plataforma PAM da BeyondTrust.

1. DESCOBRIR E CATALOGAR INSTÂNCIAS E ATIVOS DA NUVEM

A primeira etapa para se obter controle sobre os ativos na nuvem é a descoberta. A plataforma de gestão e análise centralizada da BeyondTrust, a BeyondInsight, realiza descobertas e faz inventários contínuos de ativos em ambientes na nuvem, físicos e virtuais.

A descoberta na nuvem inclui todas as instâncias online e offline, dispositivos, servidores, máquinas virtuais, cargas de trabalho, objetos, usuários, contas e muito mais.

A BeyondInsight inclui inúmeros conectores de nuvem dedicados.

Figura 4: A BeyondTrust localiza e agrupa instâncias na nuvem para que possam ser gerenciadas adequadamente.

Esses conectores podem fazer um inventário preciso de todas as instâncias na nuvem, independentemente do estado e do tempo de execução. Assim que essas instâncias são encontradas, elas devem ser gerenciadas para limitar a exposição.

As organizações podem agrupar rapidamente as instâncias da nuvem e outros ativos em grupos inteligentes para gerenciamento de privilégios consistente. Grupos inteligentes e acesso baseado na função da pessoa permitem que as equipes avaliem e gerenciem instâncias de nuvem de acordo com as necessidades comerciais exclusivas de uma organização.

A BeyondInsight também verifica os riscos relacionados a privilégios, como senhas padrão.

2. INTEGRAR E GERENCIAR CONTAS E CREDENCIAIS PRIVILEGIADAS

O plano de controle da nuvem (Consoles e instâncias virtuais e de gerenciamento na nuvem)

Todos os principais provedores de nuvem pública e virtualização oferecem uma console de gerenciamento, que é usada para administrar os vários serviços na nuvem que esses fornecedores oferecem. Os planos de controle da nuvem e a virtualização são governados por contas privilegiadas poderosas, como root. Esses portais podem ser acessados por humanos, máquinas, APIs e muito mais.

As consoles de gerenciamento são normalmente usadas para:

- Instalação, implantação, resolução de problemas e administração
- Adicionar, modificar e excluir servidores
- Configuração de serviços
- Controles básicos de segurança, como autenticação e gerenciamento de acesso
- Monitorar e relatar o uso
- Integrações/APIs
- Faturamento e compras

Uma exploração no plano de controle pode facilmente minar a integridade de todo o ambiente de nuvem. Portanto, é absolutamente crítico que as contas administrativas privilegiadas do plano de controle sejam gerenciadas de acordo com as práticas recomendadas de segurança por uma solução PAM de terceiros.

Esses consoles de gerenciamento de nuvem baseados na internet oferecem um fator de escala enorme, o que tem implicações de segurança consideráveis. Por exemplo, cada uma dessas novas instâncias, não importa quão efêmeras, tem privilégios que precisam ser gerenciados e monitorados. O AWS Console, por exemplo, também é um sistema de compras que permite que os administradores solicitem instantaneamente sistemas adicionais, armazenamento e recursos de rede.

Assim como acontece com suas contrapartes IaaS e PaaS, as soluções SaaS fornecem um console de gerenciamento baseado na internet que é acessado por usuários e administradores. Isso se aplica a sistemas desde SalesForce, ServiceNow e GitHub a contas de mídia social, como Twitter, Facebook e LinkedIn. Frequentemente, essas contas de administrador são compartilhadas entre os usuários, o que multiplica a superfície de ataque e também confunde a trilha de auditoria de quem fez o quê.

Para abordar adequadamente a segurança e a conformidade da nuvem, os controles de acesso IaaS, PaaS e SaaS nativos precisam ser aumentados ou substituídos por uma solução PAM.

Contas privilegiadas

Administradores de TI, desenvolvedores, engenheiros de software e outros técnicos rotineiramente exigem acessos privilegiados, enquanto usuários que não são da TI podem ocasionalmente precisar de acesso elevado a aplicações em nuvem ou locais, ou para alterar as configurações em seus desktops.

Em ambientes IaaS, as contas não humanas - como máquinas, aplicações e scripts - que precisam de privilégios para funcionar corretamente podem, na verdade, superar as contas humanas.

As senhas, segredos, chaves (chaves SSH, chaves do Azure, etc.) e outras credenciais para todas essas contas humanas e não humanas precisam ser protegidas, gerenciadas e auditadas. As chaves de acesso API são classificadas como uma das credenciais mais confidenciais a serem protegidas. Essas chaves são frequentemente incorporadas em aplicações de nuvem ou outro código, onde são vulneráveis a exploração por invasores.

O BeyondTrust Password Safe unifica senhas privilegiadas e gerenciamento de sessão privilegiada, fornecendo descoberta, coordenação, auditoria e monitoramento abrangentes para qualquer conta/credencial privilegiada - humana, aplicação, máquina, etc.

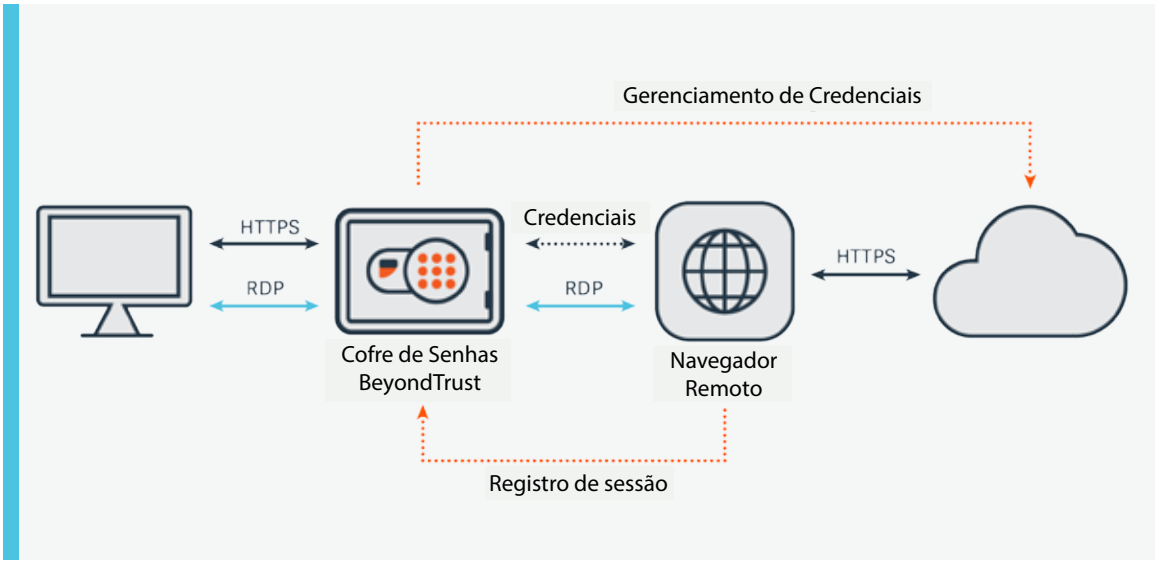


Figura 5: O Password Safe detecta, integra, monitora e gerencia o acesso às credenciais na nuvem.

O Password Safe da BeyondTrust:

- Incorpora automaticamente e guarda em cofre usuários privilegiados (Azure AD, AWS IAM, etc.), aplicações, contas de serviço, máquinas e outras credenciais humanas e não humanas (senhas, segredos, chaves SSH, etc.) na nuvem e na empresa.
- Impõe o uso de credenciais apropriado de acordo com sua política, como complexidade da senha, exclusividade (senhas diferentes por ativo, conta, etc.), vencimento da senha, rotação, check-in e check-out e outras regras.
- Identifica e elimina senhas padrão e codificadas em consoles de gerenciamento de nuvem, aplicações, scripts de construção e código e substitui por chamadas de API ou segredos dinâmicos.
- Permite um processo de fluxo de trabalho simples para verificação de senhas e injeta senhas nas sessões, nunca revelando estas ao usuário final.
- Fornece um fluxo de trabalho completo para plataforma de gerenciamento de nuvem e acesso a dispositivos, incluindo um processo de aprovação para quando o acesso administrativo for necessário; também permite que você aproveite seus clientes nativos (PuTTY, Microsoft MSTSC, etc.) para manter os fluxos de trabalho existentes.
- Gerencia e monitora todas as sessões privilegiadas e garante que todas as atividades privilegiadas estejam associadas a uma identidade única.
- Fornece gerenciamento seguro e auditado de contas de administrador para fins de emergência (break-glass).
- Integra-se com provedores de identidade existentes, com armazenamento de identidade na nuvem ou nas instalações da empresa e em plataformas MFA.

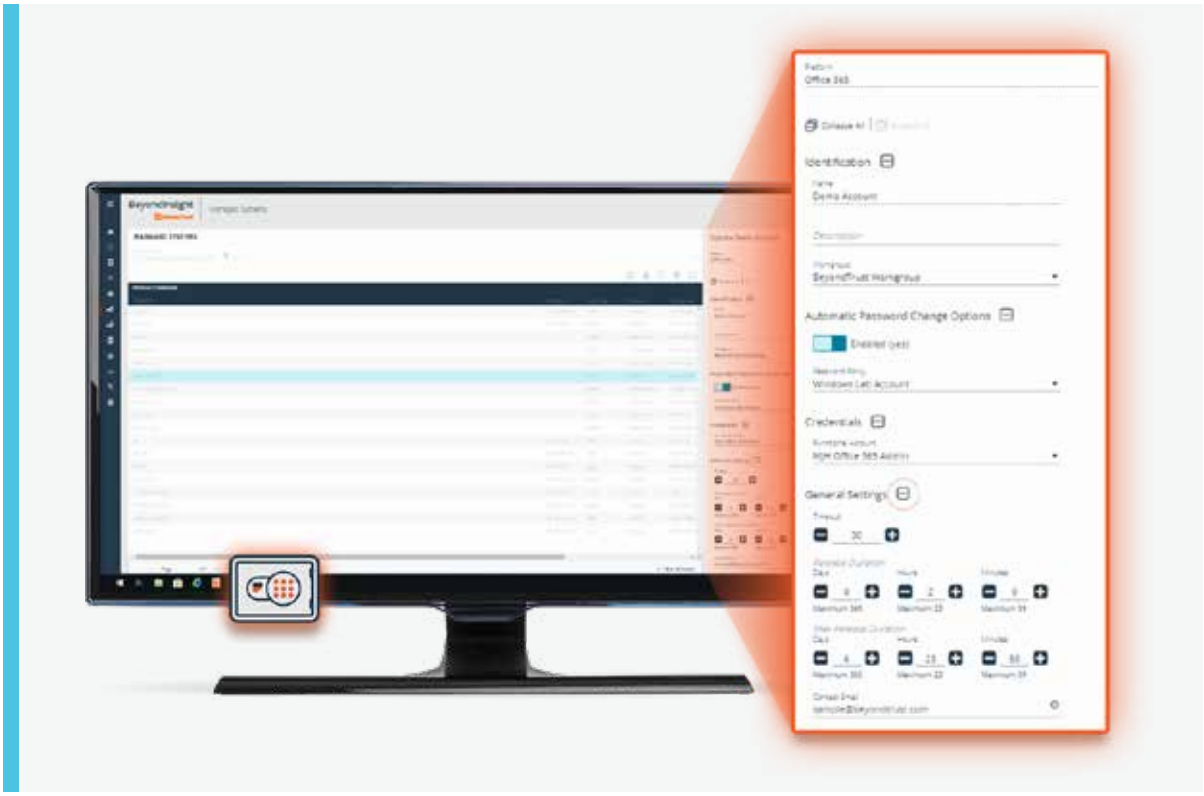


Figura 6: O Password Safe permite o armazenamento e o gerenciamento seguro de credenciais na nuvem.

3. PROTEGER, CORRIGIR E AUDITAR TODOS OS ACESSOS REMOTOS

Os administradores e outros usuários precisam de uma maneira segura para controlar e auditar os recursos na nuvem com eficácia. Como o plano de controle da nuvem é usado para gerenciar todo o ambiente da nuvem, proteger, controlar e monitorar todo o acesso é absolutamente crítico.

VPNs, RDP e SSH simplesmente não permitem controles de acesso granulares, visibilidade e auditoria, que são essenciais para os tipos mais confidenciais de nuvem e de acesso remoto. Os usuários domésticos, potencialmente usando dispositivos pessoais e acesso de fornecedores complicam ainda mais o quadro de segurança e apresentam riscos insustentáveis para esses tipos de protocolos de acesso remoto.

Nos últimos anos, os ataques BlueKeep e DejaBlue destacaram esse problema porque as máquinas virtuais baseadas na nuvem são os alvos mais convenientes para essas explorações. O BlueKeep e o DejaBlue permitem que os hackers invadam os sistemas via RDP e obtenham acesso no nível root, sem nenhuma credencial. E a autenticação por dois fatores não oferece proteção. Com os ataques "blue", o jogo acaba antes mesmo que o RDP sequer pense em verificar sua senha, quanto mais 2FA.

Embora agora se possa corrigir as vulnerabilidades exploradas pelo BlueKeep e DejaBlue, esses ataques forneceram uma confirmação séria de que muitos protocolos de administração remota amplamente usados são inadequados para exposição direta à Internet. O acesso remoto a instâncias de servidores hospedados no Azure, AWS e em outras nuvens deve ser disponibilizado sem expor uma porta de escuta RDP ou SSH para a Internet. O mesmo vale para o acesso remoto ao plano de controle da nuvem.

A solução ideal é criar um gateway seguro para instâncias de servidor na nuvem e planos de controle, restringindo o tráfego por meio de um servidor proxy reforçado, Jump Host ou Bastian Host. Isso essencialmente segmenta e isola o tráfego de acesso remoto para sua nuvem, para proteger sua infraestrutura geral. A segmentação é em si um princípio fundamental de implementações de restrição de privilégios e confiança zero.

Aproveitar uma abordagem de zona para isolar instâncias, contêineres, aplicações e sistemas completos uns dos outros protege os recursos e ajuda a prevenir ataques de movimento lateral, bem como o vazamento de um ambiente a outros adjacentes.

Ao colocar um proxy entre o usuário final e o sistema de destino, você pode impedir que a senha privilegiada, ou seu hash, chegue ao endpoint do usuário. As credenciais privilegiadas gerenciadas devem ser injetadas e auditadas de forma programada. Elas são usadas para abrir uma sessão entre o dispositivo e o sistema que está sendo administrado. A tecnologia de proxy também permite a gravação com total fidelidade de sessões privilegiadas para a captura de metadados e para torná-los pesquisáveis.

Embora a maioria dos provedores de nuvem exija que as portas de entrada sejam abertas para permitir o acesso remoto, você pode melhorar ainda mais a segurança aproveitando uma solução que requer apenas portas de saída para acesso remoto.

Como a BeyondTrust organiza e audita com segurança o acesso à nuvem/planos de controle de virtualização

Muitas organizações utilizam corretores de serviço de acesso à nuvem (CASBs) como um proxy para todo o tráfego da nuvem. Normalmente implementado usando proxy reverso (ou uma conexão VPN), todo o tráfego de rede vinculado à Internet é canalizado por meio desses proxies para centralizar o controle de acesso e a auditoria. A maioria dos CASBs, entretanto, fornece apenas políticas generalizadas.

A BeyondTrust oferece duas opções que melhoram a funcionalidade do CASB, que vamos explorar agora.

Aproveitando as soluções de acesso remoto seguro da BeyondTrust como um Bastian Host

A solução BeyondTrust Secure Remote Access permite que as organizações protejam, gerenciem e auditem fornecedores, usuários com privilégios internos e atividades de acesso remoto ao help desk, tanto no local quanto na nuvem, sem a necessidade de VPN ou outra tecnologia de túnel. A solução permite o gerenciamento seguro de sessão, com a capacidade de proxy de acesso a hosts RDP, SSH e Windows/Unix/Linux.

Nossa solução Secure Remote Access também pode ser aproveitada como um Bastian Host para acesso baseado na nuvem. O Internet Jump da solução ajuda a resolver brechas de segurança de acessos privilegiados na nuvem, inserindo uma camada segura para autenticação nesses sistemas com recursos completos de monitoramento de sessão. A solução fornece um navegador baseado no Chrome embutido em um Bastian Host (proxy) que pode acessar um recurso baseado na internet remotamente. A solução BeyondTrust pode injetar credenciais seguras automaticamente - completamente invisíveis para o usuário final e sem nunca revelar a senha - para acessar esses recursos de maneira controlada.

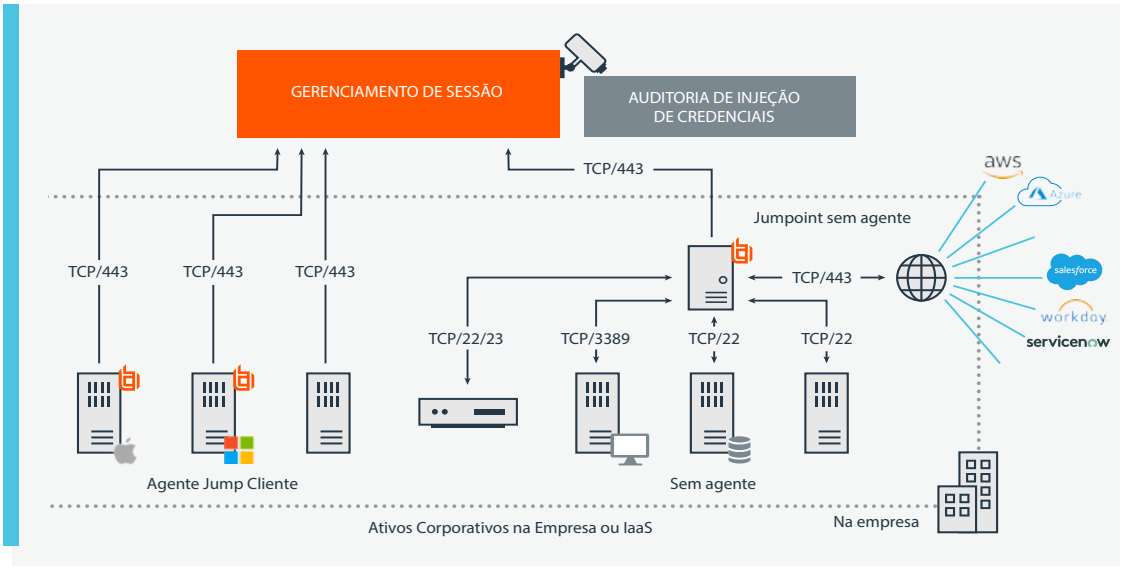


Figura 7: Arquitetura do Privileged Remote Access da BeyondTrust

O BeyondTrust Privileged Remote Access (parte do Secure Remote Access) oferece várias opções para acesso remoto em ambientes de nuvem:

1. Um agente nativo que permite que os protocolos de acesso antigos sejam totalmente desativados (por exemplo, RDP/SSH)
2. Uma abordagem sem agente que aproveita um Bastian Host e mantém todo o tráfego antigo localmente
3. A opção de um navegador Chrome incorporado para isolamento do navegador virtual — permitindo um navegador seguro/bloqueado com injeção de credencial e gravação de vídeo

Ao aplicar listas de controle de acesso (ACLs) e outras práticas recomendadas de segurança, as organizações podem garantir que a interface do Internet Jump seja a única fonte autorizada de recursos da nuvem. Isso evita que sessões de acesso remoto sejam iniciadas por fontes e usuários inadequados. Esta configuração bloqueia qualquer atividade invasora ou suspeita, enquanto força todas as atividades do usuário por meio de um navegador confiável.

A configuração do Bastian Host também evita a necessidade de um ambiente de área de trabalho virtual para atuar como servidor de terminal ou gateway apenas para hospedar um navegador para fazer essa conexão. O BeyondTrust Secure Remote Access também pode ser aproveitado para soluções de administração locais baseadas na internet para impor o zoneamento e segmentação de rede adequados na nuvem. Além disso, as organizações podem estender o acesso a ativos importantes na nuvem, ou dentro de uma organização, usando Jump Points e aderir às melhores práticas de segurança, limitando o tráfego de rede e portas a apenas fontes e aplicações autorizadas.

O BeyondTrust Secure Remote Access oferece os seguintes recursos:

- Protege a arquitetura da rede na qual todo o tráfego é criptografado via HTTPS. Nenhum encaminhamento de porta ou reconfiguração de firewall é necessário
- Fornece acesso a terceiros não confiáveis, dando-lhes apenas o nível certo de acesso ao seu ambiente, reduzindo a ameaça de propagação lateral de um sistema potencialmente infectado
- Integra-se com o BeyondTrust Password Safe para injetar com segurança credenciais gerenciadas em sessões de acesso remoto, aplicações e páginas da internet para adicionar camadas de abstração adicionais entre o usuário e segredos privilegiados
- Fornece acesso a páginas da internet, como o portal do Azure ou Office 365, por meio de um navegador Chrome bloqueado que oferece suporte a injeção automática de credenciais da internet e gravações de sessões de registros (logs)
- Fornece registros e alertas de auditoria detalhados, bem como integração em provedores de identidade (como o Azure) com MFA integrado

Aproveitando o gerenciamento de senhas privilegiadas como um proxy de serviço de acesso à nuvem

Como alternativa, o BeyondTrust Password Safe pode atuar como um proxy de serviço de acesso à nuvem para contas privilegiadas, impondo controles de acesso e auditoria em um nível mais profundo do que está disponível por meio de controles nativos e protocolos de acesso remoto comuns.

O Password Safe utiliza um servidor jump seguro com autenticação multifator, autorização de acesso adaptável e monitoramento de sessão para acesso que precisa passar por zonas de confiança. Isso permite que as equipes de TI segmentem o acesso com base no contexto do usuário, função, aplicação e dados solicitados. Essa configuração reduz o risco, minimizando acesso do tipo "linha de visão" que os invasores têm aos sistemas internos. Com o Password Safe, por exemplo, você pode bloquear o gerenciamento de funções de Administrador Global do Azure/O365, restringindo o tráfego de rede apenas à própria solução.

O diagrama abaixo descreve esse recurso:

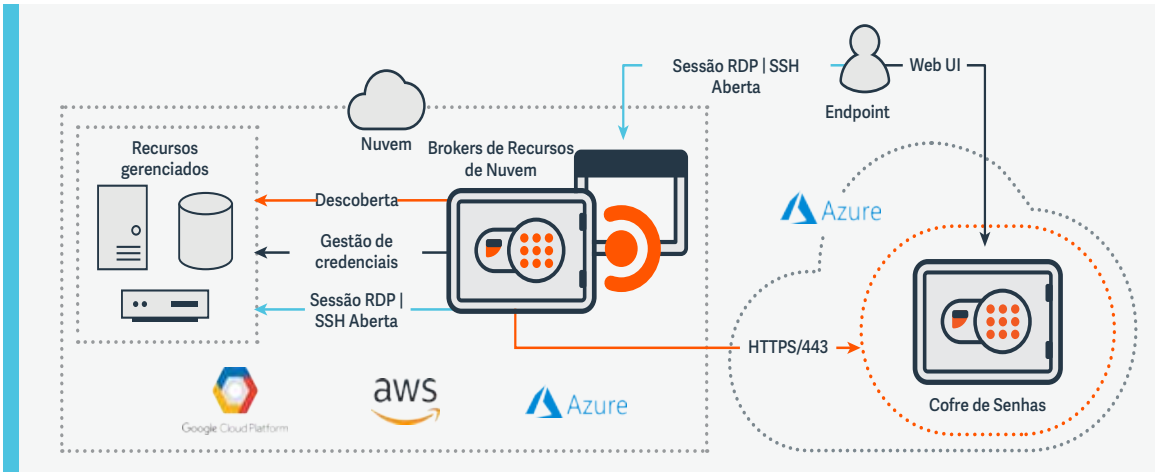


Figura 8: Arquitetura do Password Safe da BeyondTrust

Utilizar o Password Safe como um único túnel para sessões na nuvem permite um controle rígido e auditoria de todas as atividades. A imagem acima descreve como as implementações locais e IaaS da solução BeyondTrust funcionam. Entretanto, o Password Safe Cloud utilizaria um "Resource Broker" entre o Password Safe e os alvos, e permitiria que a implementação fosse entregue como um serviço embutido.

Os recursos de proteção de senha vão além dos CASBs típicos por:

- Aplicar práticas recomendadas de gerenciamento de senhas com privilégios - descoberta de senhas, armazenamento em cofre de senhas rotação de senhas, etc.
- Monitorar, gerenciar e registrar todas as sessões, com a capacidade de bloquear e encerrar sessões suspeitas
- Fornecer contexto adicional para solicitações de acesso do usuário, considerando o dia, data, hora e local
- Implementar segmentação avançada, roteando todas as sessões de acesso remoto por meio do proxy Password Safe

Esses recursos garantem que todo o acesso aos ativos da nuvem seja segmentado, protegido, monitorado e auditado.

4. APLICAR RESTRIÇÃO DE PRIVILÉGIOS E ACESSO JUST-IN-TIME DE FORMA CONSISTENTE

Os privilégios são necessários para que administradores de TI e outros usuários façam seus trabalhos e para que as aplicações e outras contas, sistemas e ativos não humanos operem adequadamente. Está bem estabelecido que os privilégios de administrador, ou mesmo contas de administrador temporárias, fornecem aos invasores os meios para pousar e expandir dentro do ambiente da nuvem. O privilégio que não está devidamente bloqueado também entra em conflito com um número crescente de regulamentos. Ao limitar os privilégios ao mínimo necessário, você pode obter resultados drásticos na redução de riscos corporativos e melhorar a postura de conformidade.

O problema é que colaboradores, fornecedores, outros usuários e contas não humanas recebem rotineiramente acesso e permissões excessivas a sistemas em nuvem e dados que podem não ser monitorados. Além disso, os consoles de gerenciamento administrativo para nuvem, virtualização e plataformas DevOps administram toda a infraestrutura em nuvem e fornecem privilégios de super usuário que podem ser exercidos em grande escala. Por exemplo, os consoles oferecem a capacidade de ativar instantaneamente milhares de máquinas virtuais - e cada uma delas vem com sua própria conta privilegiada e lacunas de segurança que precisam ser gerenciadas. Restringir o acesso ao plano de controle e dentro dele é fundamental para ter um ambiente de nuvem seguro e estável.

Nuvem nativa (ou seja, PIM da Azure), código aberto (ou seja, sudo) e ferramentas ad hoc são frequentemente usadas pelas equipes de TI para "sobreviver", mas todas são inadequadas para abordar a segurança de acessos privilegiados para ambientes de servidor e desktop.

As deficiências típicas dessas ferramentas incluem:

- Incapacidade de começar a funcionar em apenas algumas horas, com políticas baseadas no usuário
- Falta de uma estrutura de integração que permita às organizações criar integrações rapidamente
- Falta de proteção e controle avançado de aplicações
- Incapacidade de monitorar atividades dentro de scripts ou aplicações de terceiros
- Deficiências na supervisão, análise forense e auditoria: falta de monitoramento da integridade de arquivos, segurança de registro ou capacidade de registrar sessões e pressionamentos de tecla para auditorias
- Falta de amplo suporte à plataforma - o que significa que são necessárias muitas ferramentas sobrepostas para administrar em um ambiente heterogêneo

O BeyondTrust Endpoint Privilege Management oferece os recursos de elevação e delegação de privilégios (PEDM) mais abrangentes do mundo. A solução pode delegar tarefas e autorização com segurança em ambientes de nuvem, híbridos, virtuais e nas instalações da empresa, incluindo AWS, Azure, Google Cloud e muito mais. A solução é composta por:

- Privilege Management for Windows and Mac
- Privilege Management for Unix/Linux (que também inclui o Active Directory Bridge)

O BeyondTrust Endpoint Privilege Management é uma solução preventiva de segurança de endpoint, permitindo a você remover facilmente privilégios de administrador e realizar administração sem senha. A solução fornece permissões dinamicamente apenas para os sistemas, aplicações e dados de que os usuários precisam - não para a conta humana. A solução permite que você não apenas restrinja e proteja o acesso aos planos de controle da nuvem, mas também gerencie com precisão as atividades privilegiadas realizadas usando a tecnologia de agente ou gateway no plano de dados.

O BeyondTrust Endpoint Privilege Management também inclui recursos avançados de proteção e controle de aplicações. Isso significa que nossos clientes podem implementar os recursos padrão esperados das soluções de controle de aplicações, ao mesmo tempo em que obtêm proteção avançada contra ameaças de dia zero e até mesmo ataques sem arquivo que podem aproveitar aplicações legítimas.

Analistas líderes, como no Gartner's Critical Capabilities Report for PAM, também reconheceram a BeyondTrust como tendo a abordagem mais ampla para a aplicação de gerenciamento de acessos privilegiados Just-in-Time (JIT). Em vez de ter privilégios habilitados e sempre ativos (também chamados de acessos privilegiados persistente ou permanente), portanto, sempre pronto para uso indevido ou abuso, a BeyondTrust permite a elevação de privilégios conforme a necessidade e apenas pelo tempo necessário.

Um modelo de acesso JIT dinâmico reduz a superfície de ameaças e ataques de escalonamento de privilégios e movimento lateral, enquanto minimiza o risco de ameaças, como phishing e ransomware. O JIT PAM para contas de usuário também é um modelo administrativo natural para ambientes sem servidor. Para obter mais informações sobre como a BeyondTrust ativa o JIT PAM, baixe o Guia para gerenciamento de acessos privilegiados Just-in-Time.

Além disso, a gestão sem senha elimina a necessidade de qualquer senha a ser usada neste modelo JIT. A gestão sem senha se refere à concessão de privilégios à aplicação e não ao usuário. Isso elimina a necessidade de seus usuários se autenticarem com privilégio de administrador e evita a exploração de privilégios, associando-os às tarefas.

Os erros na nuvem desempenham um papel importante em violações nesse tipo de ambiente (ou seja, vazamentos de contêineres) e interrupções. A solução da BeyondTrust pode prevenir e mitigar esses tipos de erros por meio da combinação de seus privilégios mínimos e recursos de filtragem de comando. Por exemplo, o BeyondTrust Privilege Management for Unix and Linux tem uma linguagem de política que pode elevar comandos através de privilégios mínimos e inspecionar todas as opções (incluindo o que está embutido nos scripts). Isso permite que ele identifique comandos mal formados ou inadequados.

Com o Privilege Management for Unix e Linux, os usuários recebem comandos que possuem permissão para executar, podem executar com privilégios elevados sem a necessidade de sudo ou root, e o conteúdo dos comandos pode ser verificado quanto a atividades potencialmente maliciosas. Todos os comandos digitados, scripts executados e saída de tela são registrados para futura auditoria e análise forense. Aplicados corretamente, esses recursos podem proteger os ambientes de nuvem contra interrupções, como aquele resultante do "erro de digitação de USD 150 milhões" mencionado anteriormente neste White Paper.

O BeyondTrust Endpoint Privilege Management protege os endpoints, usuários e ativos da nuvem, e possibilita:

- Reforçar o verdadeiro privilégio mínimo em todos os ativos de nuvem, usuários, endpoints e sessões
- Habilitar a administração sem senha ao elevar dinamicamente o acesso conforme necessário para tarefas e aplicações
- Exercer controle granular sobre aplicações, comandos, arquivos e scripts para prevenir ou mitigar erros, eliminar a proliferação de privilégios e reduzir a superfície de ataque
- Substituir ou aumentar as ferramentas nativas ou de código aberto (ou seja, sudo), colocando os recursos que resolvem as deficiências de segurança, auditoria e administração dessas ferramentas em camadas
- Monitorar e indexar todas as sessões privilegiadas, incluindo todos os comandos digitados, para descoberta rápida durante as auditorias (Gerenciamento de privilégios apenas para Unix e Linux)
- Consolidar registros de auditoria e centralizar relatórios em todos os domínios do seu servidor
- Auditar e relatar mudanças na política crítica, sistema, aplicações e arquivos de dados para evitar adulteração
- Reduzir de forma proativa a exposição a malware avançado sem arquivo e cavalos de Troia por meio da proteção de aplicações confiáveis
- Fornecimento de modelos de início rápido (estilo de trabalho), que permitem aos clientes obter uma postura de redução de privilégios (Privilege Management for Windows/Mac)

5. INFRAESTRUTURA DEVOPS SEGURA

O DevOps tende a exacerbar as áreas de risco mais perigosas na nuvem. Com as características essenciais de agilidade e autoatendimento do DevOps, não é surpreendente que a shadow TI seja excessiva. Os usuários nesses ambientes também tendem a ter altos níveis de privilégio. As senhas são comumente incorporadas em ferramentas, código e em repositórios, como o GitHub.

Conjuntos de ferramentas CI/CD e DevOps, como Jenkins, Chef, Puppet e Ansible, comumente aproveitam e fazem interface com recursos da nuvem. Os consoles para essas ferramentas, suas interações e as contas de serviço criadas devem ser gerenciados e monitorados na velocidade e na escala exigidas das práticas de DevOps.

Gerenciar credenciais e aplicar o princípio do menor privilégio são importantes para controlar o acesso autorizado a sistemas de desenvolvimento, gerenciamento, DevOps e produção, ao mesmo tempo que concede apenas as permissões necessárias para montar máquinas e imagens de maneira adequada.

A BeyondTrust habilita e protege ambientes DevOps na nuvem da seguinte forma:

- O BeyondTrust Endpoint Privilege Management impõe privilégios mínimos granulares em cada sessão e conta com privilégios na cadeia de ferramentas DevOps e CI/CD. O controle de aplicações da solução também ajuda a dar visibilidade, controle e segurança em torno do shadow TI.
- O BeyondTrust DevOps Secrets Safe impõe práticas recomendadas de segurança de senha para usuários com privilégios e processos de orquestração de pipeline de DevOps, ao mesmo tempo em que permite agilidade de DevOps de pico. A solução pode remover credenciais codificadas embutidas em contas de serviço, aplicações e código, substituindo-os por segredos dinâmicos.
- O BeyondTrust Password Safe pode descobrir e proteger segredos DevOps e outras credenciais, impondo ao mesmo tempo limites entre sistemas de desenvolvimento, teste e produção, fornecendo proteção adicional por meio de segmentação. A solução também oferece camadas de monitoramento e gerenciamento avançados sobre cada sessão privilegiada, fornecendo escalabilidade insuperável para sessões gerenciadas simultâneas.

6. MONITORAR E GERENCIAR CADA SESSÃO ENVOLVENDO ACESSOS PRIVILEGIADOS

O monitoramento de sessão é absolutamente essencial para garantir a segurança, capacidade de auditoria e responsabilidade sobre atividades privilegiadas em ambientes de nuvem. Ainda assim, os recursos nativos da nuvem para monitoramento e gerenciamento de sessão são ausentes, imaturos ou impossíveis de implementar.

Embora algumas técnicas possam monitorar outros protocolos ou acesso baseado em API à nuvem, apenas o monitoramento de sessão pode capturar o comportamento em tempo real dos usuários. E, se os usuários souberem que estão sendo gravados (ou surfados/espiados eletronicamente), o impedimento por si só pode ser suficiente para conter algum comportamento malicioso.

Os mandatos de conformidade regulamentar estão exigindo cada vez mais que certos tipos de sessões - como sessões privilegiadas em sistemas confidenciais - tenham capacidade de auditoria total (registro, monitoramento de atividade, etc.). O monitoramento de sessão fornece a documentação futura necessária para revisar, analisar e determinar se a sessão foi autorizada, continha comportamento malicioso e foi conduzida de forma adequada. Isso inclui gravação de vídeo de sessões gráficas, saída de texto completo para sessões baseadas em terminal e registro de pressionamento de teclas das entradas do usuário.

As soluções da BeyondTrust para Gerenciamento de Senha Privilegiada e Acesso Remoto Seguro permitem que as organizações monitorem e gerenciem sessões na escala de centenas ou milhares de sessões simultâneas.

Os recursos da BeyondTrust em relação ao monitoramento e gerenciamento de sessão incluem:

- Monitorar e gerenciar qualquer sessão envolvendo acessos privilegiados - seja na nuvem, nas instalações da empesa, por funcionários ou fornecedores
- Gravar e inspecionar em tempo real todo o texto na tela, processos iniciados, títulos em quadros de aplicações e pressionamentos de tecla, excluindo ao mesmo tempo e automaticamente senhas e segredos inseridos manualmente
- Identificar sessões anômalas e automatizar fluxos de trabalho para encerrar ou pausar/bloquear a sessão até que seja feita uma determinação se essa atividade é apropriada ou não
- Uma lista crítica de recursos prontos para uso para monitorar comandos de banco de dados potencialmente inadequados, movimento lateral, comandos confidenciais do sistema operacional e outros comportamentos suspeitos

7. INTEGRANDO TUDO

Quanto mais complexa for sua infraestrutura, mais importante para sua equipe ter menos ferramentas, entretanto mais poderosas, para administrar e gerenciar. Simplificar sua abordagem de gerenciamento ajuda a reduzir a complexidade e os erros, ao mesmo tempo que torna mais fácil ver e resolver quaisquer lacunas. Também é essencial que suas ferramentas sejam compatíveis e se integrem ao restante do seu ecossistema de TI e de segurança. Uma ferramenta autônoma sem integração, realisticamente, tem uma vida finita até que o problema seja resolvido.

Unifique o gerenciamento de privilégios em toda a nuvem e no ambiente das instalações da empresa

Na BeyondTrust, chamamos isto simplesmente de Universal Privilege Management (UPM). Nossas soluções são projetadas para descobrir, proteger e auditar continuamente todas as contas, ativos e sessões com privilégios - em qualquer lugar.

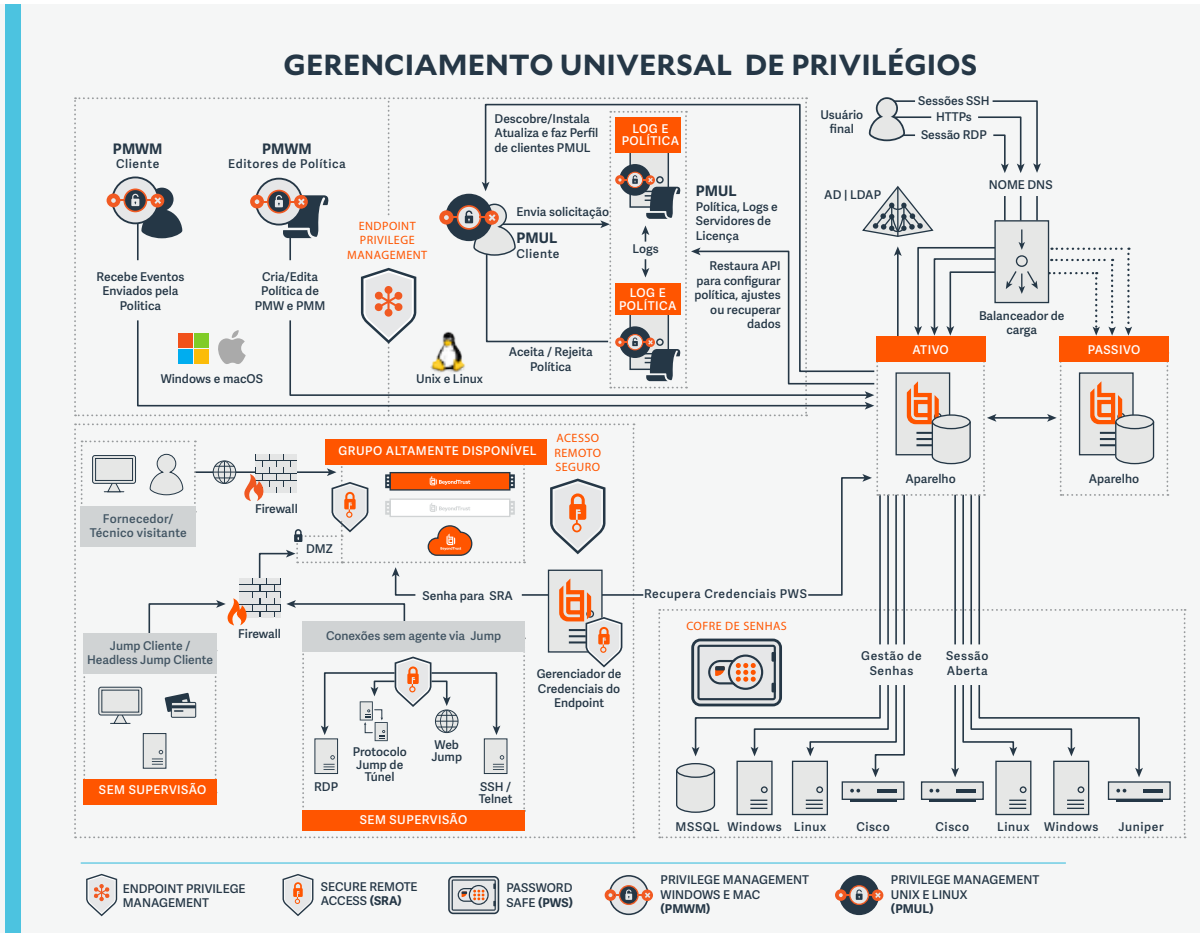


Figura 9: Arquitetura PAM da BeyondTrust

Utilize a plataforma BeyondTrust PAM para gerenciar todo o seu universo de privilégios de forma consistente em ativos na empresa e na nuvem.

A BeyondTrust fornece a cobertura de plataforma mais ampla do mundo como parte de nossa abordagem de gerenciamento universal de privilégios. A seguir apresentamos uma lista parcial de ambientes baseados em nuvem que nossas soluções suportam:

IaaS / PaaS

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud
- RackSpace
- GoGrid

SaaS

- Microsoft Office 365
- Box
- Dropbox
- Salesforce
- Workday

Social (SaaS)

- Facebook
- Instagram
- LinkedIn
- Pinterest
- Twitter
- XING

Unificar o Gerenciamento de Identidades Privilegiadas e Não Privilegiadas

Embora as soluções de IAM, incluindo aquelas nativas de vários ambientes de nuvem, ofereçam recursos como logon único, provisionamento/desprovisionamento de usuários, gerenciamento de usuários com base em funções, controle de acesso e governança, elas não têm a capacidade de gerenciar privilégios e monitorar sessões de maneira granular.

A integração de IAM bidirecional e do gerenciamento de acessos privilegiados é fundamental para gerenciar, proteger e auditar identidades, contas e funções de forma holística para garantir que a atividade seja apropriada. A BeyondTrust se integra com vários provedores de gerenciamento de identidade, permitindo que as organizações se beneficiem de visibilidade holística.

Além disso, a BeyondTrust fornece recursos do Active Directory Bridge (AD) pela nossa solução Endpoint Privilege Management. O AD Bridge permite logon único em ambientes Windows, Unix, Linux e macOS, estendendo o Active Directory da Microsoft para plataformas não Windows, habilitando o SSO.

Integrar com o Restante do Ecossistema de Segurança e de TI

Nossas soluções se integram e têm sinergias com as principais ferramentas ITSM, SSO, MFA, IDAM (via SCIM), SIEM, RPA, DevOps, inteligência de ameaças e outras ferramentas.

4

Via rápida de proteção na nuvem com a plataforma PAM da BeyondTrust

As organizações que definem o escopo correto de suas implantações na nuvem e identificam e abordam lacunas com ferramentas de classe empresarial continuarão a colher os diversos benefícios da nuvem. A BeyondTrust aborda lacunas de segurança, visibilidade e gerenciamento de nuvem cruciais e pode ajudar a proteger seus recursos e identidades baseados na nuvem contra vetores de ataque privilegiados.

A BeyondTrust protege todo o seu ambiente de nuvem:

1. Descobre e integra continuamente contas privilegiadas e instâncias de nuvem
2. Aplica as melhores práticas de segurança de credenciais em todas as contas humanas e não humanas, incluindo a implementação de arquiteturas de confiança zero
3. Reduz o número de usuários com acessos privilegiados
4. Restringe os privilégios que qualquer usuário, aplicação, serviço ou ativo possui para acesso e automação
5. Previne e mitiga erros humanos em acessos privilegiados
6. Condensa a janela de tempo durante a qual os privilégios podem ser executados e, portanto, abusados, aplicando o princípio do acesso Just-in-Time
7. Reforça a segmentação do ambiente de nuvem e proteger/criar proxy de acesso remoto para consoles de gerenciamento de nuvem e recursos de computação
8. Gerencia e monitora de forma robusta cada sessão privilegiada e fornece certificação para conformidade regulamentar
9. Fornece uma plataforma única e centralizada para todas as atividades de gerenciamento de privilégios que são arquitetadas para se integrar com o restante do seu ecossistema de segurança e tecnologia da informação

Por fim, diferentemente de outras soluções de gerenciamento de privilégios que podem levar muitos meses para serem configuradas corretamente, as soluções BeyondTrust ajudam a reduzir riscos rapidamente.

As soluções da BeyondTrust podem ser implantadas na nuvem, nas instalações da empresa ou por meio de um modelo híbrido para atender às necessidades exclusivas da sua organização. O Privileged Password Management, o Endpoint Privilege Management e o Secure Remote Access podem ser implantados individualmente, ou você pode combinar várias soluções BeyondTrust para obter o máximo de controle de privilégios e redução de riscos. As soluções podem ser gerenciadas por meio da plataforma BeyondInsight, que centraliza a administração, oferece auditoria de relatórios e muito mais.

A plataforma PAM da BeyondTrust

A BeyondTrust oferece o que os especialistas do setor consideram o espectro completo de soluções de gerenciamento de acessos privilegiados.

A solução BeyondTrust completa permite que você aborde toda a jornada para o Gerenciamento Universal de Privilégios para reduzir drasticamente a superfície de ataques e as janelas de ameaças.

Ao unir o mais amplo conjunto de recursos de segurança com privilégios, a BeyondTrust simplifica as implantações, reduz custos, melhora a utilização e reduz os riscos dos privilégios.

SOBRE A BEYONDTRUST

A BeyondTrust é líder mundial em Gestão de Privilégios (PAM), capacitando as organizações a proteger e gerenciar todo o seu universo de privilégios. Nossos produtos integrados e plataformas oferecem a solução PAM mais avançada do setor, permitindo que as organizações reduzam rapidamente sua superfície de ataques em ambientes tradicionais, na nuvem e em ambientes híbridos.

A abordagem da Gestão Universal de Privilégios da BeyondTrust protege os privilégios entre senhas, endpoints e acessos, dando às empresas a visibilidade e o controle de que precisam para reduzir riscos, obter conformidade e aumentar o desempenho operacional. Nossos produtos permitem o nível certo de privilégios apenas pelo tempo necessário, criando uma experiência transparente para os usuários, o que aumenta a produtividade.

Com um histórico de inovação e um compromisso com os clientes, as soluções BeyondTrust são fáceis de implantar, gerenciar e escalar. Mais de 20.000 clientes confiam na BeyondTrust, incluindo 70% das empresas da Lista Fortune 500 e uma rede global de parceiros.

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