BeyondTrust

# Guia para o Gerenciamento de Acessos Privilegiados Just-In-Time

O Que é, Por Que Você Precisa e Como Implementá-lo

# SUMÁRIO

# INTRODUÇÃO

## Elevando “Apenas o Acesso Necessário” Para o Próximo Nível

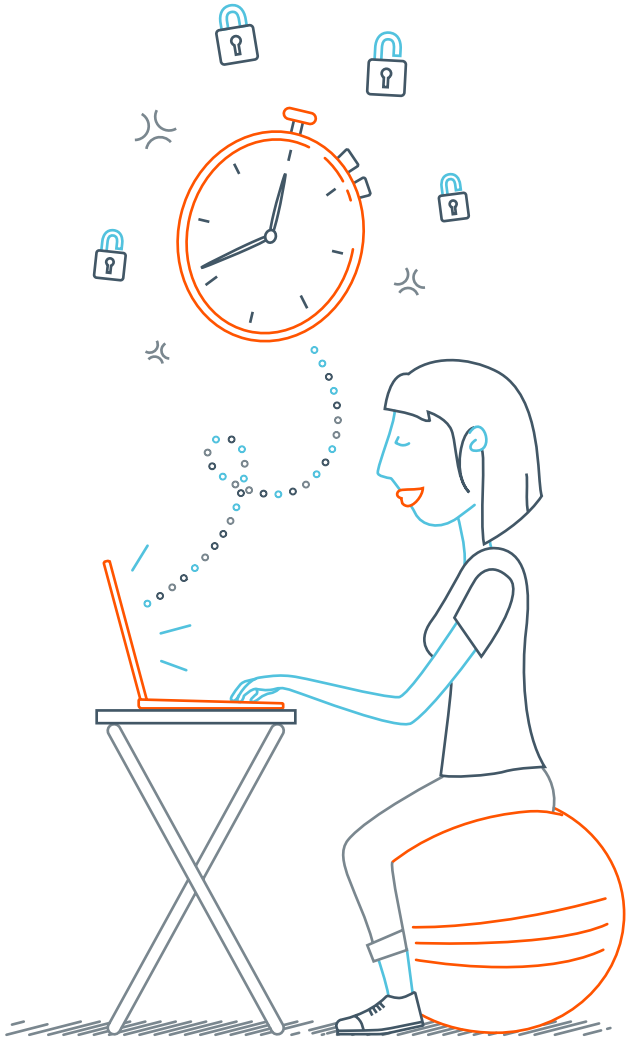
O modelo de segurança com restrições de privilégios baseia-se no conceito de que usuários, processos, aplicações e sistemas tenham direitos e acesso a “apenas o necessário” para executar suas tarefas.

As empresas são cada vez mais eficazes na implementação desse modelo usando soluções de gerenciamento de acessos privilegiados (PAM), mas negligenciam as variáveis tempo e risco das contas de usuários privilegiados.

Nos últimos 40 anos, as contas privilegiadas “sempre ativas” têm sido o modelo padrão de acesso de administrador e proliferaram nas empresas, apresentando enorme risco. Acessos privilegiados, direitos e permissões que estão sempre no modo ativo estão prontos para serem executados a qualquer momento - para atividades legítimas e ilícitas. E essa superfície de risco está se expandindo rapidamente com o aumento de ambientes virtuais, nuvem e DevOps, além de dispositivos IoT e áreas emergentes, como RPA (automação de processo robótico, do inglês Robotic Process Automation).

Nesse cenário, não é de se surpreender que o abuso e / ou uso indevido de privilégios sejam uma das principais causas dos incidentes de violação da segurança cibernética hoje. Com acessos privilegiados em mãos, um invasor se torna um insider malicioso, um cenário alarmante para qualquer profissional de TI.

Agora, é fato que as contas privilegiadas permeiam toda uma organização, e as tecnologias de segurança tradicionais baseadas em perímetro podem proteger apenas contas privilegiadas dentro de seus limites. O gerenciamento de acessos privilegiados (PAM) Just-in-time (JIT) pode ajudar a condensar drasticamente a superfície de ameaças privilegiadas e reduzir os riscos em toda a empresa. Implementar o PAM JIT significa que as identidades só têm os privilégios apropriados quando necessário e pelo menor tempo necessário. Esse processo pode ser totalmente automatizado, de modo que seja transparente e imperceptível para o usuário final.



**As empresas são cada vez mais eficazes na implementação de restrições de privilégios usando soluções de gerenciamento de acessos privilegiados (PAM), mas negligenciam as variáveis tempo e risco das contas de usuários privilegiados.**

# OVERVIEW DO PAM JIT

## O Que é Gerenciamento de Acessos Privilegiados Just In Time

O PAM (Gerenciamento de Acessos Privilegiados) JIT (Just in Time) é uma estratégia que utiliza requisitos para direitos, fluxo de trabalho e políticas de acesso para contas privilegiadas em tempo real. As empresas usam essa estratégia para proteger contas privilegiadas de falhas de acesso contínuo e ativo, impondo restrições baseadas no tempo de acesso, comportamento do usuário e parâmetros de contexto.

Entende-se como conta privilegiada à qual são concedidos privilégios e permissões além de um usuário padrão, e inclui o seguinte:

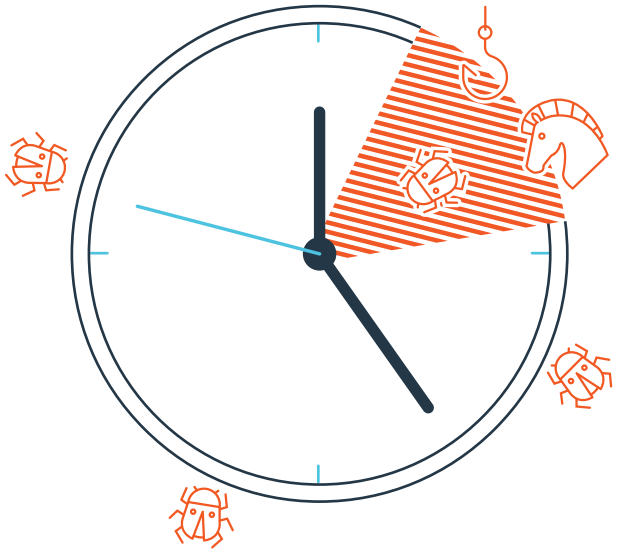
- Conta de superusuário com privilégios, como administrador (em ambientes Windows) ou raiz (em ambientes Unix/ Linux)
- Usuários avançados com privilégios que estão entre um superusuário e uma conta de usuário padrão (também chamada de não privilegiada ou conta de usuário com restrição de privilégios).

O JIT PAM limita o tempo que uma conta possui privilégios e direitos de acesso elevados, reduzindo a janela de vulnerabilidade durante um possível ataque de exploração. O JIT ajuda a aplicar o princípio de privilégio mínimo para garantir que atividades privilegiadas sejam executadas de acordo com políticas de uso aceitáveis, além de proibir as atividades privilegiadas que estão fora do contexto correto.

Quando um privilégio é solicitado, ele deve atender aos parâmetros contextuais necessários antes de fazer check-out - o privilégio nunca pertence à conta. Isso reduz o risco de uso indevido de privilégios nas contas.

Tomemos como exemplo uma conta ativa que pode ser "privilegiada e ativa" durante 168 horas por semana. Ao mudar para uma abordagem PAM JIT, você pode reduzir esse estado de privilégio ativo de 168 horas para um determinado tempo. A multiplicação desse efeito em todas as contas privilegiadas terá um impacto enorme na redução de riscos.

Adotar a estratégia de PAM JIT significa que você pode implementar o real conceito de restrição de privilégios em toda a empresa. E a exposição não se baseia apenas no tempo. Os vetores de ataque que utilizam técnicas como o movimento lateral também são mitigados, uma vez que não existe "sempre" uma conta privilegiada para alavancar recursos.



**As empresas usam essa estratégia para proteger contas privilegiadas de falhas de acesso contínuo e ativo, impondo restrições baseadas no tempo de acesso, comportamento do usuário e parâmetros de contexto.**

# AUTOMAÇÃO DO PAM JIT

## Métodos JIT

A abordagem JIT para a gestão de privilégios exige que as organizações estabeleçam critérios para acessos privilegiados just-in-time.

Embora conceitos semelhantes e bem estabelecidos para o JIT existam em outros casos de uso – como manufatura – a aplicação do modelo para uma solução de segurança e operações apresenta algumas considerações técnicas exclusivas durante uma implementação.

O objetivo de uma conta privilegiada JIT é atribuir automaticamente os privilégios necessários "on the fly" com base em uma tarefa ou missão aprovadas e, posteriormente, removê-los assim que a tarefa for concluída ou o contexto de acesso autorizado expirar.

A modelagem necessária para obter uma conta de usuário padrão e aplicar os privilégios apropriados pode ser implementada usando qualquer um dos seis métodos JIT a seguir:

### 1 PRIVILÉGIOS JIT

A conta possui privilégios, permissões ou direitos individuais extras para executar uma tarefa quando todos os critérios forem atendidos, mas apenas por um período limitado. Esses direitos precisam ser revogados assim que a missão for concluída e devem garantir que nenhum outro privilégio foi alterado de forma inadequada.

### 2 CRIAÇÃO E EXCLUSÃO DE CONTA JIT

A criação e exclusão de uma conta privilegiada apropriada para atender aos objetivos da missão. A conta deve ter características para vinculá-la novamente à identidade ou serviço solicitante que executa a operação para registro e análise forense.

### 3 CONTA DE REPRESENTAÇÃO JIT

A conta está vinculada a uma conta administrativa preexistente e, quando um aplicativo ou tarefa específica são executados, a função é elevada usando essas credenciais. Isso geralmente é feito usando automação ou script com o Windows "RunAs" ou *Nix SuDo. Normalmente, o usuário final desconhece a conta de representação para esse tipo de operação, e o processo pode se sobrepor à delegação de conta privilegiada sempre ativa.

### 4 TOKENIZAÇÃO JIT

A aplicação ou recurso tem seu token privilegiado modificado antes da injeção no kernel do sistema operacional. Essa forma de privilégio mínimo é comumente usada em endpoints para elevar os privilégios e a prioridade de um aplicativo, sem elevar privilégios para o usuário final.

### 5 ASSOCIAÇÃO JIT

Significa o acréscimo ou remoção automáticos de uma conta em um grupo administrativo privilegiado durante um determinado período de tempo. A conta só deve ser adicionada a um grupo elevado quando os critérios apropriados forem atendidos. A participação no grupo deve ser revogada imediatamente após a conclusão da missão.

### 6 CONTAS ADMIN DESABILITADAS

As contas de administrador desativadas estão presentes em um sistema com todas as permissões, privilégios e direitos para executar uma função. Elas são habilitados para executar uma missão específica e, posteriormente, desabilitados novamente quando os critérios operacionais forem atendidos. Esse conceito não é diferente de ter sempre contas administrativas ativas, com a exceção de que a funcionalidade de ativação nativa é aproveitada para controlar o acesso JIT.

## Gatilhos JIT

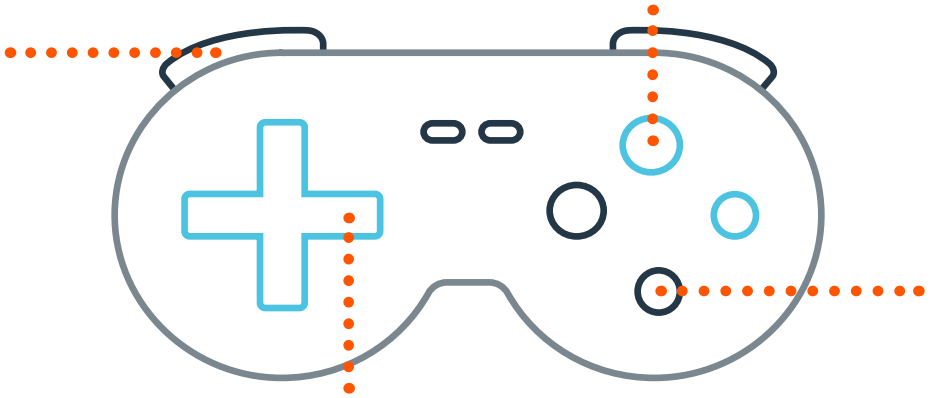
Para que qualquer um desses métodos de elevação de contas privilegiadas funcione de acordo com os princípios do just-in-time, os seguintes critérios devem ser considerados como gatilhos. Eles também devem incluir variáveis como hora e data das janelas de controle de alterações, bem como critérios de suspensão ou encerramento, se forem detectados indicadores de comprometimento.

### AUTENTICAÇÃO DE DOIS FATORES (2FA) OU MULTIFATORES (MFA)

Um método comum para autorizar os acessos privilegiados a contas sempre ativas ou JIT é 2FA ou MFA. Embora esse não seja o diferencial entre as duas técnicas de acesso, ele fornece mitigação de risco adicional ao validar que a identidade tenha acesso adequado a uma conta privilegiada. Esses métodos de autenticação podem, no entanto, ser utilizados como um gatilho JIT para uma conta usando qualquer uma das técnicas descritas acima.

### FLUXO DE TRABALHO

O conceito de aprovação do fluxo de trabalho é comumente associado a call centers, help desks e outras áreas de gerenciamento de serviços de TI (ITSM). É feita uma solicitação de acesso e, usando um fluxo de trabalho definido por aprovadores, o acesso é concedido ou negado. Depois que o fluxo de trabalho for aprovado, uma conta JIT poderá ser ativada. Normalmente, isso corresponde ao usuário, ativo, aplicativo, hora / data e ticket associado em uma solução de controle de mudanças ou suporte técnico. O monitoramento de sessão privilegiada geralmente é ativado pelas soluções PAM neste cenário para verificar se todas as ações correspondentes foram apropriadas.



### RECONHECIMENTO DE CONTEXTO

O acesso com reconhecimento de contexto é baseado em critérios como endereço IP de origem, geolocalização, associação ao grupo, sistema operacional host, aplicativos instalados ou operando na memória, vulnerabilidades documentadas etc. Com base em qualquer combinação lógica dessas características, o acesso à conta JIT pode ser concedido ou revogado para atender aos requisitos de negócios e reduzir os riscos.

### DIREITOS

Quando o gerenciamento de acessos privilegiados é integrado às soluções de gerenciamento de acesso à identidade (IAM), os direitos entre as soluções podem ser sincronizados para acessos privilegiados. Para esse fim, o acesso JIT pode ser atribuído diretamente por meio de soluções PAM ou, alternativamente, por meio de direitos IAM. Embora um fluxo de trabalho típico de direitos IAM seja um processo mais longo para sincronização e possa não ser em tempo real, ele fornece certificações de conta com base em privilégios. Isso pode ser anulado ao vincular o IAM às soluções PAM para controlar o acesso.

**Os gatilhos de automação JIT são condições para que um acesso torne-se privilegiado.**

## Políticas JIT

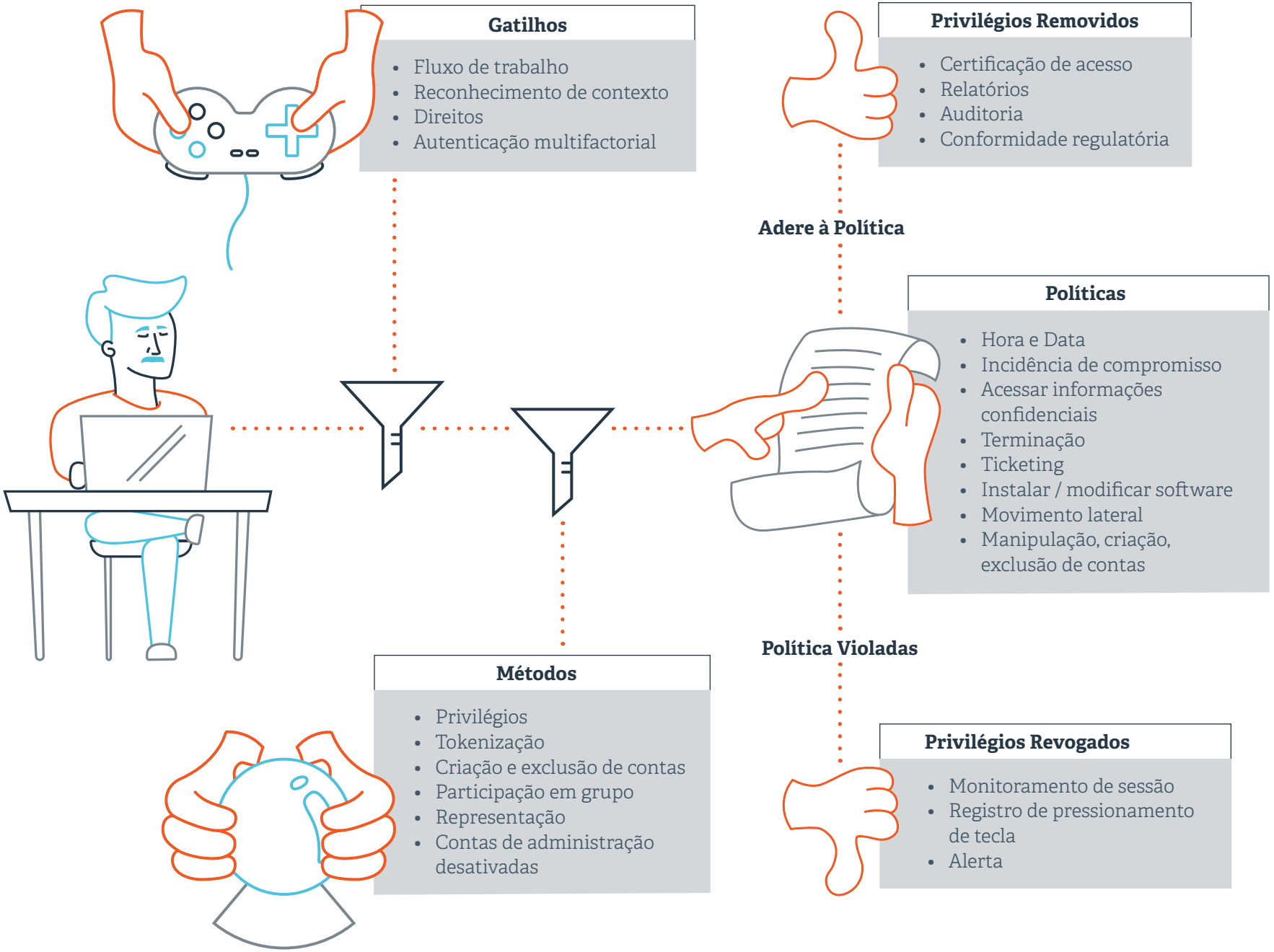
As duas questões principais a serem consideradas pelas equipes são: *"Quais políticas governam uma conta JIT para acessos privilegiados adequados"* e *"Quais condições devem ser atendidas para sua revogação?"*

Essas políticas podem incluir:

1. **Janelas de data e hora** para acesso e controle de mudanças
2. **Comandos ou aplicativos** que podem ser um indicador de comprometimento
3. **Detecção de acesso** a informações confidenciais
4. **Término** da sessão principal
5. **Existência de materiais similares**, para uma solução de ticketing
6. **Modificação inadequada** de recursos, incluindo instalação de software ou modificação de arquivos
7. **Tentativas inadequadas** de movimento lateral
8. **Manipulação, criação ou exclusão de contas** de usuário ou conjuntos de dados

Embora essa não seja de forma alguma uma lista exaustiva de todas as variáveis de política, pode ajudar a filtrar os critérios para que uma conta JIT seja disponibilizada ou encerrada com base nos gatilhos correspondentes.

## PAM JIT na Prática



## Como as Soluções da BeyondTrust Atendem ao Gerenciamento de Acessos Privilegiados Just-In-Time

A plataforma de gerenciamento de acessos privilegiados BeyondTrust pode tornar o modelo de segurança PAM JIT uma realidade para sua organização, além de ajudá-lo a melhorar a segurança ao impor outros aspectos críticos da sua estratégia IAM / PAM, como descoberta e gerenciamento de contas privilegiadas, restrição de privilégios e gerenciamento de credenciais , separação de privilégios e separação de tarefas, auditoria de privilégios e análise de ameaças privilegiadas.

A BeyondTrust suporta o modelo just-in-time, permitindo o gerenciamento centralizado de credenciais e sessões privilegiadas, elevação/delegação de privilégios entre endpoints (desktops, servidores e mais) e acesso remoto (funcionários, fornecedores, etc.) com uma grande variedade de gatilhos. A plataforma PAM BeyondTrust inclui várias soluções integradas.


**A BeyondTrust suporta o modelo just-in-time, permitindo o gerenciamento centralizado de credenciais e sessões privilegiadas, elevação/delegação de privilégios nos endpoints e acesso remoto com uma ampla variedade de gatilhos.**

| Soluções BeyondTrust | Recursos e Capacidades Compatíveis com o PAM JIT | | | | | |
|---|---|---|---|---|---|---|
| **GERENCIAMENTO DE SENHAS E SESSÕES PRIVILEGIADAS** | **DESCOBERTA E BOARDING AUTOMÁTICO DE CONTAS** | **GERENCIAMENTO SEGURO DE CHAVES SSH** | **GERENCIAMENTO DE SENHAS DE APLICAÇÃO A APLICAÇÃO** | **GERENCIAMENTO APRIMORADO DE SESSÕES PRIVILEGIADAS** | **CONTROLE DE ACESSO ADAPTÁVEL** | **ANÁLISE AVANÇADA DE AMEAÇAS PRIVILEGIADAS** |
| Descubra, gerencie, audite e monitore contas privilegiadas de todos os tipos | Aproveite um mecanismo de descoberta de rede distribuído para verificar, identificar e criar um perfil de todos os ativos. A categorização dinâmica permite a integração automática em grupos inteligentes para o gerenciamento eficiente e acesso JIT quando novas contas são detectadas. | Rotacione automaticamente as chaves SSH de acordo com uma programação definida e imponha controle de acesso granular e fluxos de trabalho. Utilize chaves privadas para registrar usuários com segurança em sistemas Unix / Linux através do proxy, sem exposição do usuário à chave e com gravação de sessão com privilégios completos. | Elimine credenciais de aplicações embutidas ou codificadas por meio de uma interface API adaptável que inclui um número ilimitado de caches de senhas para escalabilidade e redundância. Isso permite que o JIT acesse as senhas mais recentes de qualquer aplicação. | O gerenciamento aprimorado de sessões permite o verdadeiro controle duplo, possibilitando que os administradores registrem, bloqueiem e documentem comportamentos suspeitos - sem interromper sessões ou produtividade - com base em qualquer atividade JIT. | Avalie o contexto just-in-time e simplifique as solicitações de acesso, considerando o dia, a data, a hora e o local em que um usuário acessa recursos para determinar sua autorização para acessar esses sistemas. | Mensure as características dos ativos e os comportamentos dos usuários de um dia para o outro, avaliando o escopo e a velocidade de quaisquer alterações para alertá-lo sobre desvios suspeitos. |
| **GERENCIAMENTO DE PRIVILÉGIOS NOS ENDPOINTS** | **DESCOBERTA E BOARDING AUTOMÁTICO DE CONTAS** | **CONTROLE DE APLICAÇÕES** | **AUDITORIA E RELATÓRIOS COMPLETOS** | **ANÁLISE DE AMEAÇAS PRIVILEGIADAS** | **INTEGRAÇÕES DE ECOSSISTEMAS DE SEGURANÇA** | |
| Aplique a restrição de privilégios de usuários finais em ambientes Windows, Mac, Unix, Linux e dispositivos de rede | Eleve privilégios às aplicações para usuários padrão em qualquer sistema operacional através de controles detalhados e baseados em políticas, fornecendo acesso apenas o suficiente para concluir uma tarefa just-in-time . | Forneça whitelists, blacklists e greylists de aplicações com um mecanismo de política flexível para definir regras amplas. Escolha a aprovação automática para usuários avançados - protegidos por trilhas de auditoria completas - ou utilize códigos de resposta a desafios para o controle de aplicações just-in-time. | Forneça uma trilha de auditoria única de todas as atividades dos usuários que acelerem a forense e simplifique a conformidade. | Correlacione o comportamento do usuário com os dados de vulnerabilidade de ativos e a inteligência de segurança das melhores soluções de segurança para fornecer uma imagem geral dos riscos daquele Usuário final. | Os conectores integrados a uma série de soluções de terceiros, incluindo aplicações de suporte técnico, scanners de gerenciamento de vulnerabilidades e ferramentas SIEM, garantem que as organizações obtenham um retorno sobre seus investimentos em segurança. | |

| Soluções BeyondTrust | | Recursos e Capacidades Compatíveis com o PAM JIT | | | | | |
|---|---|---|---|---|---|---|---|
| **Acesso Remoto Seguro** | | **Controle de Acessos Privilegiados** | **Monitoramento de Sessões** | **Reduza a Superfície de Ataque** | **Integre-se ao Gerenciamento de Senhas** | **Consoles para celular e Web** | **Auditoria e conformidade** |
| Proteja, gerencie e audite os acessos privilegiados remotos de colaboradores e terceiros. | **Acesso Remoto de Terceiros** | Aplique a restrição de privilégios, oferecendo aos usuários o nível certo de acesso para qualquer sessão remota. | Controle e monitore as sessões usando protocolos padrão para conexões RDP, VNC, HTTP / S e SSH. | Reduza a superfície da ameaça consolidando o rastreamento, a aprovação e a auditoria de contas privilegiadas just in time, em um só lugar e criando uma única via de acesso. | Injete credenciais diretamente em servidores e sistemas com apenas um clique, just in time, para que os usuários nunca precisem conhecer ou ver credenciais. | Use aplicativos móveis ou consoles baseados na Web just in time, em qualquer lugar e a tempo de executar tarefas de acesso remoto. | Crie trilhas de auditoria, análise forense da sessão e outros recursos de relatório capturando dados detalhados em tempo real ou na revisão pós-sessão. Forneça relatórios que atendam às demandas de conformidade. |
| | **Suporte Remoto e Pessoal do HelpDesk** | **Suporte por Chat** | **Amplo Suporte à Plataforma** | **Permissões e Funções Granulares** | **Colaboração** | **Gravação de Sessões e Trilhas de Auditoria** | **Suporte do Chrome, Firefox, IE e mais** |
| | | Habilite o suporte do seu site com o Click-to-Chat, com escalonamento just-in-time, para compartilhamento de tela e controle remoto, sem nunca perder o contato com o usuário final. | Ampare e forneça suporte a partir de dispositivos Windows, Mac, Linux, iOS e Android. Ofereça suporte a dispositivos legados usando RDP, Telnet, SSH e VNC. | Gerencie equipes, usuários, funções e configurações de permissão de sessão para impor uma postura de segurança com privilégios mínimos. | Resolva os incidentes de suporte mais rapidamente e defina caminhos para recursos qualificados, enquanto melhora a satisfação do cliente, incluindo os membros da equipe apropriados, just in time. | Acompanhe o desempenho da equipe, bem como a atividade da sessão de log, para servir como uma trilha de auditoria para segurança, conformidade e treinamento. | Nosso HTML5 Web Rep Console permite que você ofereça suporte remoto seguro just-in-time a partir de qualquer navegador - sem downloads necessários - para começar imediatamente a corrigir problemas. |

## Métodos e Gatilhos de Mapeamento JIT

A matriz a seguir mapeia os gatilhos e métodos do PAM JIT para cada solução BeyondTrust.

| | Gerenciamento de Senhas e Sessões Privilegiadas | Gerenciamento de Privilégios nos Endpoints | Acesso Remoto Seguro |
|---|---|---|---|
| **Gatilhos** | | | |
| Direitos | ● | | ● |
| Fluxo de trabalho | ● | ● | ● |
| Contexto | ● | ● | ● |
| Multifator | ● | ● | ● |
| **Métodos** | | | |
| Criação e Exclusão de Conta | ● | | |
| Privilégio de associação ao grupo | ● | | |
| Representação | ● | ● | ● |
| Contas de Administração Desativadas | | ● | |
| Tokenização | | ● | |

# BEYONDTRUST & PAM JIT

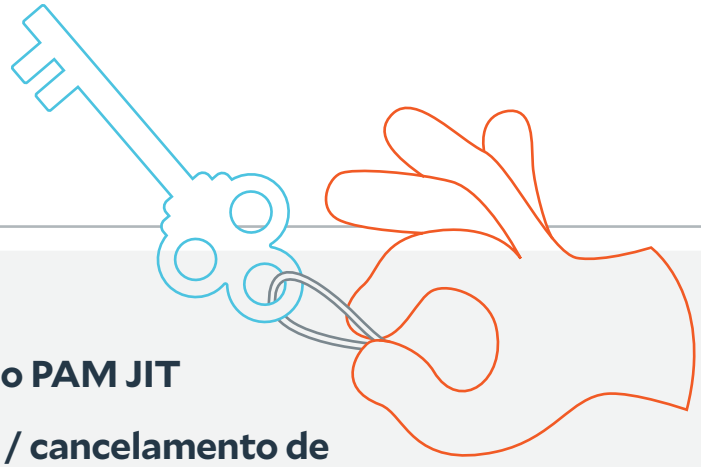
## Reduzindo Riscos com PAM JIT

Para muitas organizações, implementar uma estratégia JIT em sincronia com um modelo de acesso suficiente é fundamental para a segurança da empresa.

O gerenciamento de privilégios do JIT deve ser considerado um componente essencial de uma verdadeira estratégia de restrição de privilégios. Em vez de habilitar contas o tempo todo, uma vez autenticadas, exerça mais controle sobre quando e como elas podem ser usadas, expandindo o modelo de segurança para negar todas as atividades privilegiadas até que os critérios de negócios sejam satisfeitos para seu uso. Isso implica não apenas restringir o acesso à conta, mas também os privilégios, permissões e direitos reais que uma conta pode usar em tempo real.

Para habilitar o gerenciamento de acessos privilegiados just in time, e garantir que o comportamento dos usuários da contas privilegiadas seja apropriado com base em políticas em tempo real, o PAM JIT aborda dinamicamente os riscos em toda a empresa que as contas trazem. Isso representa não apenas a evolução natural do gerenciamento de acessos privilegiados, mas um salto considerável no gerenciamento de riscos de TI.

A plataforma de gerenciamento de acessos privilegiados da BeyondTrust permite que as organizações enderecem os desafios e riscos dos acessos privilegiados sempre ativos, mantendo seus usuários finais produtivos e seguros.



### Principais Benefícios do PAM JIT

1. **O provisionamento / cancelamento de privilégios centralizado, automatizado, contextual e baseado em tempo reduz a janela de vulnerabilidade durante a qual os privilégios podem ser potencialmente explorados**

2. **A aplicação do conceito de restrição de privilégios equivale a menos usuários privilegiados e sessões privilegiadas, que além de melhorar a segurança, simplificam as iniciativas de auditoria e conformidade**

3. **Experiência transparente para o usuário final, permitindo produtividade sem interromper os fluxos de trabalho**

4. **A eliminação de contas sempre ativas e os vetores de ataque associados a elas**

## Conceitos e terminologia relacionados

**Break-glass:** no contexto da computação, break-glass refere-se ao log out de uma senha de conta do sistema para ignorar os procedimentos normais de controle de acesso para uma emergência crítica, geralmente quando outros métodos de acesso falham ou estão inacessíveis. O break-glass fornece ao usuário acesso imediato, mas tipicamente limitado por tempo, a uma conta à qual ele normalmente não está autorizado a acessar.

**Gerenciamento de Acessos Privilegiados Just-In-Time (JIT):** O objetivo do gerenciamento de privilégios JIT é atribuir os privilégios necessários "on the fly" com base em uma tarefa ou missão aprovadas e, em seguida, removê-los quando a tarefa estiver concluída ou quando o contexto do acesso autorizado expirar. O gerenciamento de privilégios JIT permite que as organizações protejam contas privilegiadas dos acessos continuamente ativo, impondo restrições com base em parâmetros comportamentais e contextuais.

**Restrição de Privilégios:** refere-se ao conceito e prática de limitar os direitos de acesso de usuários, contas e processos de computação apenas àqueles recursos absolutamente necessários para executar atividades autorizadas de rotina. Um modelo de segurança com restrição de privilégios implica impor o nível mínimo de direitos ao usuário, ou o nível mais baixo de liberação, que permite ao usuário desempenhar sua função. A restrição de privilégios também é empregada em processos, aplicações, sistemas e dispositivos (como IoT), pois cada um deve ter apenas as permissões necessárias para executar uma atividade autorizada.

**Privilégio:** o privilégio fornece a autorização para substituir ou ignorar certas restrições de segurança e pode incluir permissões para executar ações como desligar sistemas, carregar drivers de dispositivo, configurar redes ou sistemas, provisionar e configurar contas e instâncias da nuvem.

**Gerenciamento de Acessos Privilegiados (PAM):** também conhecido como gerenciamento de contas privilegiadas, gerenciamento de identidades privilegiadas (PIM) ou simplesmente gerenciamento de privilégios, o PAM refere-se a soluções e estratégias para gerenciar e proteger contas privilegiadas e controlar atividades de delegação e escalonamento de privilégios para usuários, aplicações, serviços, processos, tarefas etc. As soluções PAM permitem que as organizações removam os direitos de administrador dos usuários (em servidores e desktops) e, em vez disso, elevam privilégios para aplicações ou tarefas autorizados, conforme necessário.

**Contas Privilegiadas:** Uma conta privilegiada é considerada qualquer conta que forneça acesso e privilégios além daqueles de contas não privilegiadas (por exemplo, contas padrão e contas de usuário convidado). Um usuário privilegiado é qualquer usuário que aproveita os acessos privilegiados por meio de uma conta privilegiada. Em função dos seus recursos e acesso elevados, os usuários / contas privilegiadas apresentam riscos consideravelmente maiores do que as contas / usuários não privilegiados.

**Sessão Privilegiada:** Uma sessão privilegiada envolve a execução de atividades que requerem privilégios que normalmente estão além dos de um usuário padrão. Uma sessão privilegiada pode ser iniciada por um usuário, sistema, aplicação ou serviço.

**Gerenciamento de Sessão Privilegiada (PSM):** O gerenciamento de sessão privilegiada (PSM) engloba o monitoramento e o gerenciamento de todas as sessões para usuários, sistemas, aplicações e serviços que envolvem acesso e permissões elevados. O PSM permite a supervisão e o controle avançados que podem ser usados para proteger melhor o ambiente contra ameaças internas ou possíveis ataques externos, além de manter informações forenses críticas cada vez mais necessárias para os mandatos de regulamentação e conformidade.

**Contas de Usuário Padrão:** as contas de usuário padrão, às vezes chamadas de contas de usuário com restrição de privilégios, têm um conjunto limitado de privilégios. Em um ambiente de privilégios mínimos, esses são os tipos de contas que a maioria dos usuários deve operar em 90 a 100% do tempo. Um usuário padrão é um usuário não privilegiado em ambientes (Windows, Mac, Linux, Unix etc.) com direitos básicos de acesso. Esse tipo de conta / usuário tem capacidade limitada de acessar recursos e configurações, em oposição a uma conta privilegiada ou superusuário (como raiz ou administrador), que pode ter vastos direitos administrativos e acessos privilegiados.

**Contas de Superusuário:** as contas de superusuário são contas altamente privilegiadas usadas principalmente por funcionários especializados em TI, fornecendo poder praticamente irrestrito para executar comandos e fazer alterações no sistema. As contas de superusuário são normalmente conhecidas como "Raiz" no Unix / Linux e "Administrador" nos sistemas Windows. Os privilégios de conta de superusuário podem fornecer acesso irrestrito a arquivos, diretórios e recursos com privilégios completos de leitura / gravação / execução. As contas de superusuário também podem processar alterações sistêmicas na rede, como criar ou instalar arquivos ou software, modificar arquivos e configurações e excluir usuários e dados. Os superusuários também podem provisionar e cancelar o acesso e permissões para outros usuários.

## Sobre a 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.

beyondtrust.com/pt

V2020_07_PRT