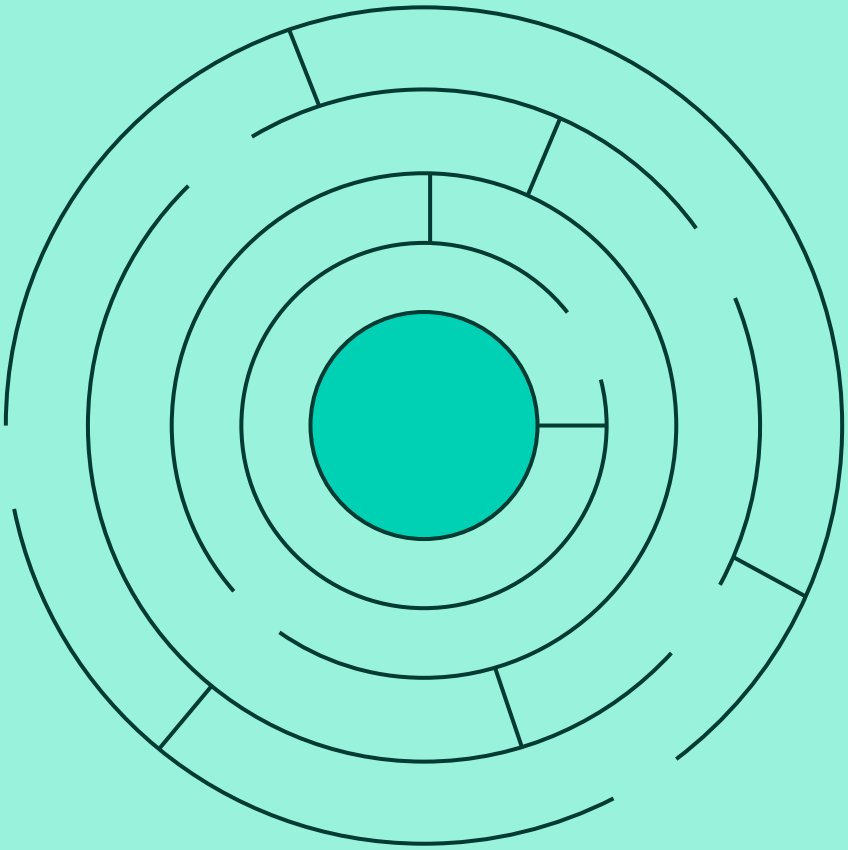
EBOOK

GUIA PARA A GESTÃO DE SUPERFÍCIES DE ATAQUE



segura®

Introdução

Em um mundo altamente conectado, o significado da segurança cibernética atingiu níveis incomparáveis. À medida que as ameaças cibernéticas avançam e se intensificam de maneira contínua, é imperativo que as organizações, independentemente do tamanho, priorizem a proteção de seus ativos digitais. “Reduzindo Seu Risco de Segurança Cibernética: Um Guia para a Gestão de Superfícies de Ataque Usando o Segura® PAM” tem como objetivo auxiliar você a navegar pelo intrincado mundo da segurança cibernética, permitindo que desenvolva uma estratégia eficiente para diminuir sua suscetibilidade a ameaças potenciais. Ao compreender sua superfície de ataque e aproveitar a força do Gerenciamento de Acesso Privilegiado (PAM), você pode reduzir substancialmente as chances de um ataque cibernético catastrófico.

Um estudo recente realizado pela Cybersecurity Ventures prevê que, até 2025, o custo global de crimes cibernéticos aumentará para US$ 10,5 trilhões por ano, uma disparada gritante dos US$ 3 trilhões em 2015. Isso enfatiza a necessidade de as organizações protegerem proativamente seus ativos digitais. Além disso, uma pesquisa do Ponemon Institute revela que o tempo médio para identificar e controlar uma violação de dados é de 280 dias, potencialmente resultando em danos financeiros e de reputação consideráveis para a empresa em questão.

Este guia abrangente vai te guiar no processo de compreender sua superfície de ataque, oferecendo estratégias pragmáticas para a sua redução. Além disso, vamos nos aprofundar no papel vital do Gerenciamento de Acesso Privilegiado na fortificação dos dados e sistemas confidenciais da sua organização. Ao se aproximar da conclusão do guia, você estará completamente preparado para incorporar o Segura® PAM em sua empresa, reforçando assim sua postura geral de segurança e diminuindo significativamente sua vulnerabilidade de segurança cibernética.

Não espere que um ataque cibernético debilite sua empresa – aja agora e garanta o futuro da sua organização.

Índice

EBOOK

GUIA PARA A GESTÃO DE SUPERFÍCIES DE ATAQUE

Capítulo 1

Compreendendo Sua Superfície de Ataque

Neste capítulo, vamos nos aprofundar no conceito de superfície de ataque, sua importância, componentes comuns e como identificar a superfície de ataque da sua organização.

Definindo uma Superfície de Ataque

Uma superfície de ataque engloba todos os pontos possíveis dentro da infraestrutura digital de uma empresa que poderiam ser explorados por indivíduos não autorizados ou cibercriminosos para acessar dados, sistemas ou redes confidenciais. Ela compreende vários elementos, como hardware, software, redes, terminais e até mesmo usuários humanos. Uma superfície de ataque maior e mais complexa aumenta o risco de violações de segurança em uma organização.

A Importância da Sua Superfície de Ataque

Compreender e controlar sua superfície de ataque é vital por vários motivos:

- Maior risco de ataques cibernéticos: uma superfície de ataque maior equivale a mais pontos de entrada possíveis para os cibercriminosos, tornando sua empresa mais suscetível a violações de segurança.
- Necessidades de conformidade: vários setores possuem regulamentos rigorosos e requisitos de conformidade para proteger informações confidenciais. A incapacidade de gerenciar sua superfície de ataque pode resultar em inconformidade e multas substanciais.
- Reputação da empresa: uma violação de segurança pode prejudicar gravemente a reputação da sua organização, levando à perda de clientes, parceiros e receita.

- Perdas financeiras: o custo de recuperação de um ataque cibernético pode ser impactante, incluindo despesas relacionadas à resposta a incidentes, honorários advocatícios e perda de produtividade.

Componentes Típicos de uma Superfície de Ataque

Os componentes de uma superfície de ataque geralmente podem ser divididos em três áreas principais:

Rede

engloba todos os dispositivos conectados à rede da sua empresa, como roteadores, comutadores (switches), firewalls e servidores. Ela também inclui pontos de acesso remotos, como conexões VPN e aplicativos baseados em nuvem.

Software

abrange todos os aplicativos, sistemas operacionais e firmware que operam nos dispositivos da sua organização. Inclui software desenvolvido internamente e aplicativos de terceiros.

Humano

refere-se a indivíduos dentro de sua empresa que possuem acesso a dados e sistemas confidenciais. Inclui funcionários, terceirizados e fornecedores.

Determinando Sua Superfície de Ataque

A gestão eficaz da sua superfície de ataque requer a identificação de todos os pontos de entrada potenciais na infraestrutura digital da sua organização. Abaixo seguem alguns passos para te ajudar a conseguir isso:

- Crie um inventário de todos os dispositivos conectados à sua rede, incluindo seus componentes de hardware e software.
- Identifique todos os pontos de acesso remotos, como conexões VPN e aplicativos baseados em nuvem.
- Revise as contas e permissões de usuários para garantir que apenas indivíduos autorizados tenham acesso a dados e sistemas confidenciais.
- Avalie fornecedores e parceiros terceirizados para garantir que eles estejam em conformidade com as políticas de segurança da sua empresa.
- Realize auditorias de segurança regulares para identificar possíveis vulnerabilidades e áreas de melhoria.

Em conclusão, compreender sua superfície de ataque é o passo inicial para diminuir o risco de segurança cibernética da sua organização. Ao identificar possíveis pontos de entrada e tratar das vulnerabilidades, você pode diminuir significativamente a probabilidade de um ataque cibernético e proteger seus valiosos ativos digitais. No próximo capítulo, discutiremos estratégias para reduzir sua superfície de ataque e reforçar a postura de segurança de sua empresa.

EBOOK

GUIA PARA A GESTÃO DE SUPERFÍCIES DE ATAQUE

Capítulo 2

Diminuindo Sua Superfície de Ataque

Agora que temos uma compreensão clara do que é uma superfície de ataque e seu significado, vamos avaliar várias estratégias para diminuir sua superfície de ataque e melhorar a postura de segurança da sua organização.

Estabelecendo uma Política de Privilégio Mínimo

Uma política de privilégio mínimo garante que os usuários tenham acesso apenas aos recursos e dados necessários para executar suas funções de trabalho. Ao restringir o acesso a informações e sistemas confidenciais, você pode minimizar o risco de acesso não autorizado e reduzir sua superfície de ataque.

Para implementar uma política de privilégio mínimo:

- Revise regularmente as contas e permissões dos usuários para garantir que elas estejam alinhadas com as responsabilidades de trabalho de cada indivíduo.
- Remova ou modifique permissões que não são mais necessárias.
- Incorpore o controle de acesso baseado em função (RBAC) para limitar ainda mais o acesso a dados e sistemas confidenciais.

Identificando e Remediando Vulnerabilidades

A detecção e remediação de vulnerabilidades são componentes cruciais para reduzir sua superfície de ataque. Ao identificar e abordar vulnerabilidades na infraestrutura digital da sua empresa, você pode limitar os possíveis pontos de entrada para os cibercriminosos.

Para identificar e corrigir vulnerabilidades:

- Empregue ferramentas de verificação de vulnerabilidades para verificar regularmente sua rede, dispositivos e softwares em busca de possíveis vulnerabilidades.
- Estabeleça um processo para priorizar e abordar vulnerabilidades identificadas com base em sua gravidade e impacto potencial.
- Desenvolva um plano abrangente de resposta a incidentes para orientar sua empresa no caso de uma violação de segurança.

Avaliando e Atualizando Continuamente Sua Postura de Segurança

Manter uma superfície de ataque mínima requer avaliações proativas e atualizações em sua postura de segurança. Isso inclui:

- Auditorias de segurança regulares para identificar possíveis vulnerabilidades e áreas de melhoria.
- Garantir que todos os softwares e firmwares estejam atualizados com os patches de segurança mais recentes.
- Monitorar e lidar com novas ameaças e vulnerabilidades conforme elas surgem.

Fortalecendo a Segurança da Rede

Melhorar a segurança da rede da sua organização é outra estratégia vital para reduzir sua superfície de ataque. Algumas etapas para melhorar a segurança da rede incluem:

- Implementação de firewalls e sistemas de detecção de invasão para monitorar e bloquear o tráfego malicioso.
- Segmentação da sua rede para restringir a propagação potencial de um ataque.
- Implementação de controles de acesso robustos e medidas de autenticação para pontos de acesso remotos, como conexões VPN e aplicativos baseados em nuvem.
- Monitoramento regular da atividade da rede em busca de sinais de comportamento suspeito ou acesso não autorizado.

Instruindo os Funcionários Sobre as Melhores Práticas de Segurança Cibernética

Os funcionários são muitas vezes o elo mais fraco na postura de segurança de uma organização. Ao treinar sua força de trabalho sobre as melhores práticas de segurança cibernética, você pode reduzir significativamente o risco de erro humano que leva a uma violação de segurança. Para educar os funcionários:

- Forneça treinamento regular sobre as melhores práticas de segurança cibernética, incluindo gerenciamento de senhas, conscientização sobre phishing e hábitos seguros de navegação na Internet.
- Estabeleça políticas e diretrizes claras para lidar com dados confidenciais e o uso de dispositivos da empresa.
- Incentive os funcionários a relatar qualquer atividade suspeita ou possíveis ameaças à segurança.

Para concluir, reduzir sua superfície de ataque exige uma abordagem multifacetada que englobe várias estratégias, incluindo a implementação de uma política de privilégio mínimo, a avaliação e atualização de sua postura de segurança, a detecção e correção de vulnerabilidades, o aprimoramento da segurança da rede e a educação dos funcionários. Ao tomar essas medidas, você pode diminuir significativamente o risco de segurança cibernética da sua empresa e proteger melhor seus ativos digitais.

No próximo capítulo, exploraremos o papel do Gerenciamento de Acesso Privilegiado (PAM) na redução da superfície de ataque.

EBOOK

GUIA PARA A GESTÃO DE SUPERFÍCIES DE ATAQUE

Capítulo 3

O Papel do Gerenciamento de Acesso Privilegiado

Neste capítulo, abordaremos o conceito de Gerenciamento de Acesso Privilegiado (PAM), sua importância na redução da superfície de ataque e os recursos essenciais que uma solução PAM eficaz deve oferecer.

Definindo o Gerenciamento de Acesso Privilegiado (PAM)

Usuários privilegiados são indivíduos com permissões elevadas, o que lhes permite acessar informações confidenciais, realizar tarefas cruciais ou fazer alterações ao nível do sistema. As soluções PAM auxiliam as empresas em:

- Controlar e limitar o acesso dos usuários privilegiados a sistemas e dados confidenciais.
- Monitoramento e auditoria de atividades de usuários privilegiados.
- Detectar e responder a possíveis ameaças de segurança envolvendo usuários privilegiados.

Importância do PAM na Redução da Superfície de Ataque

O PAM desempenha um papel crítico na minimização da sua superfície de ataque por vários motivos:

Usuários Privilegiados

devido ao seu acesso elevado, os usuários privilegiados são os principais alvos dos cibercriminosos. Uma conta privilegiada comprometida pode levar a acesso não autorizado, violações de dados ou danos graves ao sistema.

Ameaças internas

o PAM ajuda na proteção contra ameaças internas, que podem resultar de funcionários mal-intencionados ou erro humano não intencional por usuários privilegiados.

Requisitos de conformidade

vários setores possuem regulamentos rigorosos em relação à gestão do acesso rivilegiado. A implementação de uma solução PAM pode ajudar sua organização a manter a conformidade com esses requisitos.

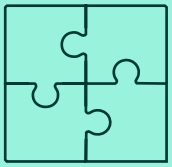
Visibilidade e controle

o PAM oferece maior visibilidade das atividades de usuários privilegiados, permitindo que você gerencie e controle melhor o acesso a recursos confidenciais.

Recursos Essenciais de uma Solução PAM Eficaz

Uma solução PAM eficaz deve abranger os seguintes recursos essenciais:

- **Controle de acesso centralizado:** uma solução PAM deve fornecer um sistema centralizado para gerenciar e controlar o acesso de usuários privilegiados, simplificando o processo e reduzindo o risco de acesso não autorizado.
- **Controle de acesso baseado em função (RBAC):** o RBAC permite atribuir permissões com base em funções predefinidas, garantindo que os usuários privilegiados tenham apenas o acesso necessário para executar suas funções de trabalho.
- **Monitoramento e gravação de sessões:** o monitoramento e a gravação de sessões de usuários privilegiados fornecem uma trilha de auditoria de atividades, permitindo que você detecte possíveis ameaças à segurança e cumpra os requisitos de conformidade.
- **Autenticação multifator (MFA):** a MFA adiciona uma camada adicional de segurança, exigindo que os usuários privilegiados forneçam mais de uma forma de identificação para acessar recursos confidenciais.
- **Rotação e gerenciamento automatizados de senhas:** as soluções PAM devem automatizar o processo de rotação e gerenciamento de senhas de contas privilegiadas,reduzindo o risco de violações de segurança relacionadas a senhas.



Como o PAM Complementa Outras Medidas de Segurança

O PAM é um componente essencial de uma estratégia abrangente de segurança cibernética, complementando outras medidas de segurança, tais como:

- Gestão de vulnerabilidades: o PAM ajuda a proteger contra vulnerabilidades que podem surgir pelo acesso privilegiado mal gerenciado.
- O PAM melhora a segurança da rede controlando e monitorando o acesso de usuários privilegiados a componentes críticos da rede.
- Treinamento em conscientização de segurança: o PAM apoia o treinamento de segurança dos funcionários, reforçando a importância do gerenciamento adequado de acesso e fornecendo ferramentas para gerenciar o acesso privilegiado de forma eficaz.

Para concluir, a implementação de uma solução robusta de Gerenciamento de Acesso Privilegiado é um passo crítico para reduzir sua superfície de ataque e melhorar a postura geral de segurança da sua empresa. No próximo capítulo, apresentaremos o Segura PAM e como ele pode ajudar sua organização a gerenciar efetivamente o acesso privilegiado e reduzir o risco de segurança cibernética.

EBOOK

GUIA PARA A GESTÃO DE SUPERFÍCIES DE ATAQUE

Capítulo 4

Apresentando o Segura® PAM

Neste capítulo, forneceremos uma visão geral do Segura® PAM, seus principais recursos e como ele pode ajudar a reduzir o risco de segurança cibernética da sua organização gerenciando o acesso privilegiado com eficácia.

Visão Geral do Segura® PAM

O Segura® PAM é uma solução abrangente de Gerenciamento de Acesso Privilegiado projetada para ajudar as organizações a proteger seus ativos críticos e reduzir sua superfície de ataque. Ao fornecer controle centralizado sobre o acesso privilegiado, monitorar as atividades dos usuários e automatizar o gerenciamento de senhas, o Segura® PAM permite que as empresas aprimorem sua postura de segurança e mitiguem os riscos associados aos usuários privilegiados.

Principais Recursos do Segura® PAM

O Segura® PAM oferece uma ampla gama de recursos que o tornam uma escolha ideal para organizações que buscam melhorar seu gerenciamento de acesso privilegiado:

- Controle de Acesso Centralizado: o Segura® PAM fornece uma plataforma única e unificada para gerenciar o acesso de usuários privilegiados em toda a sua empresa, agilizando o processo e reduzindo o risco de acesso não autorizado.
- Controle de Acesso Baseado em Função (RBAC): Com o RBAC, você pode definir facilmente funções e atribuir permissões com base em funções de trabalho, garantindo que os usuários privilegiados tenham apenas o acesso necessário para desempenhar suas funções.
- Monitoramento e Gravação de Sessões: o Segura® PAM permite monitorar e gravar sessões de usuários privilegia-

dos em tempo real, fornecendo uma trilha completa de auditoria de atividades e permitindo detectar possíveis ameaças à segurança.

- Autenticação Multifator (MFA): fortaleça a segurança do seu acesso privilegiado, exigindo que os usuários forneçam várias formas de identificação antes de obter acesso a recursos confidenciais.

- Rotação e Gerenciamento Automatizados de Senhas: o Segura® PAM automatiza o processo de rotação e gerenciamento de senhas de contas privilegiadas, ajudando a reduzir o risco de violações de segurança relacionadas a senhas.

- Integração com Outras Soluções de Segurança: o Segura® PAM pode se integrar facilmente a outras ferramentas de segurança, incluindo SIEM, ITSM e soluções de gestão de identidade, fornecendo uma abordagem perfeita e abrangente para a segurança da sua organização.

Como o Segura® PAM Reduz Seu Risco de Segurança Cibernética

Ao implementar o Segura® PAM em sua empresa, você pode reduzir seu risco de segurança cibernética com eficiência por meio de várias vantagens importantes:

Reduzindo o acesso não autorizado

Com controle de acesso centralizado e permissões baseadas em função, o Segura® PAM ajuda a impedir o acesso não autorizado a sistemas e dados críticos.

Detecção e resposta a ameaças

O monitoramento e a gravação de sessões em tempo real fornecem visibilidade das atividades de usuários privilegiados, permitindo detectar possíveis ameaças à segurança e responder de acordo.

Fortalecimento da segurança de senhas

A rotação e o gerenciamento automatizados de senhas reduzem o risco de violações de segurança relacionadas a senhas e garantem que as senhas de contas privilegiadas permaneçam seguras.

Apoio aos esforços de conformidade

A abrangente trilha de auditoria e os recursos de geração de relatórios do Segura® PAM ajudam sua empresa a atender aos requisitos regulatórios e a manter a conformidade com os padrões do setor.

Para concluir, o Segura® PAM fornece uma solução poderosa e abrangente para gerenciar o acesso privilegiado em sua organização, ajudando a reduzir sua superfície de ataque e aprimorar sua postura geral de segurança.

No próximo capítulo, discutiremos como implementar o Segura® PAM em sua organização e integrá-lo à sua infraestrutura de segurança existente.

EBOOK

GUIA PARA A GESTÃO DE SUPERFÍCIES DE ATAQUE

Capítulo 5

Implementando o Segura® PAM em Sua Empresa

Neste capítulo final, vamos guiar você pelo processo de implementação do Segura® PAM em sua organização, integrando-o com sua infraestrutura de segurança existente e treinando sua equipe sobre seu uso adequado.

Avaliando Sua Infraestrutura de Segurança Atual

Antes de implementar o Segura® PAM, é essencial avaliar sua infraestrutura de segurança atual e identificar quaisquer lacunas ou pontos fracos. Essa avaliação ajudará você a determinar a melhor abordagem para integrar o Segura® PAM e garantir que ele complemente suas medidas de segurança existentes.

Algumas áreas importantes a serem consideradas durante esta avaliação incluem: mecanismos de controle de acesso existentes.; políticas e práticas de gerenciamento de senhas; medidas de segurança de rede, como firewalls e sistemas de detecção de invasão; processos de gerenciamento de vulnerabilidades; conformidade com os regulamentos e normas do setor.

Implantando o Segura PAM

Depois de avaliar sua infraestrutura de segurança atual, está na hora de implementar o Segura PAM. Aqui estão algumas etapas que vão te guiar através do processo de implementação:

- Defina suas metas e objetivos de gerenciamento de acesso privilegiado. Isso ajudará você a priorizar recursos e opções de personalização durante o processo de implementação.

- Estabeleça um cronograma do projeto e atribua um gerente de projeto para supervisionar a implantação.

- Colabore com a equipe de implementação do Segura para configurar e personalizar a solução para atender às necessidades exclusivas da sua empresa.
- Teste a solução em um ambiente controlado para garantir que ela funcione como pretendido e resolva quaisquer problemas que possam surgir.
- Implemente gradualmente a solução em toda a sua organização, monitorando seu desempenho e fazendo ajustes conforme necessário.

Integração do Segura PAM com Outras Soluções de Segurança

Para maximizar a eficácia do Segura PAM e criar um ecossistema de segurança abrangente, é essencial integrá-lo às suas ferramentas de segurança existentes. O Segura PAM pode se integrar facilmente a várias soluções de segurança, incluindo:

- Sistemas de Gestão de Eventos e Informações de Segurança (SIEM)
- Plataformas de Gerenciamento de Identidade e Acesso (IAM)
- Soluções de Gerenciamento de Serviços de TI (ITSM)
- Ferramentas de resposta a incidentes e inteligência contra ameaças

Ao integrar o Segura PAM a essas soluções, você pode criar uma infraestrutura de segurança completa e perfeita que ofereça visibilidade, controle e proteção aprimorados em toda a sua organização.

Treinando Sua Equipe no Segura PAM

Para maximizar a eficácia do Segura PAM e criar um ecossistema de segurança abrangente, é essencial integrá-lo às suas ferramentas de segurança existentes. O Segura PAM pode se integrar facilmente a várias soluções de segurança, incluindo:

- Sistemas de Gestão de Eventos e Informações de Segurança (SIEM)
- Plataformas de Gerenciamento de Identidade e Acesso (IAM)
- Soluções de Gerenciamento de Serviços de TI (ITSM)
- Ferramentas de resposta a incidentes e inteligência contra ameaças

Ao integrar o Segura PAM a essas soluções, você pode criar uma infraestrutura de segurança completa e perfeita que ofereça visibilidade, controle e proteção aprimorados em toda a sua organização.

Conclusão

A implementação do Segura PAM em sua organização é um passo crucial para reduzir sua superfície de ataque e melhorar sua postura geral de segurança. Ao compreender sua superfície de ataque, empregar estratégias para minimizá-la e aproveitar o poder do Segura PAM, você pode proteger sua organização contra ameaças cibernéticas e manter uma forte infraestrutura de segurança no cenário digital em constante evolução dos dias de hoje.

Não espere até que seja tarde demais. Invista na segurança da sua empresa implementando o Segura PAM hoje mesmo e dê o primeiro passo em direção a um futuro mais seguro para o seu negócio.

Agende uma Demo: Experimente o Segura PAM em Ação

Você está pronto para experimentar na prática e ver como o Segura® PAM pode aprimorar a estratégia de Gerenciamento de Superfície de Ataque (ASM) da sua organização? Convidamos você a agendar uma demonstração personalizada com nossa equipe de especialistas, que vai te guiar através dos principais recursos e capacidades do Segura PAM e demonstrar como ele pode te ajudar a gerenciar e controlar o acesso privilegiado de forma eficaz.

Durante a demonstração, você poderá:

- Explorar o papel do Segura® PAM no fortalecimento da estratégia ASM da sua organização, incluindo o controle e monitoramento do acesso de usuários privilegiados a sistemas e dados críticos.
- Descobrir como os recursos do Segura® PAM, tais como controle de acesso centralizado, controle de acesso baseado em função e gerenciamento automatizado de senhas, podem te ajudar a reduzir sua superfície de ataque e minimizar os riscos de segurança cibernética.
- Descobrir como o Segura® PAM se integra a outras soluções de segurança para criar uma infraestrutura de segurança abrangente e de ponta a ponta que ofereça visibilidade, controle e proteção aprimorados em toda a sua empresa.

Não perca esta oportunidade de descobrir como o Segura® PAM pode ajudar sua organização a proteger seus ativos digitais, manter a conformidade com os regulamentos específicos do setor e ficar à frente das ameaças de segurança em evolução.

Para agendar sua demonstração, basta **clicar aqui** e preencher o formulário de solicitação com suas informações de contato, data e hora de preferência. Assim que sua solicitação for enviada, um membro da nossa equipe entrará em contato para confirmar os detalhes e fornecer as instruções necessárias para participar da demo.

Pronto para elevar a segurança cibernética de sua organização?

Descubra as soluções de ponta da Segura® para proteger dados sensíveis e sistemas críticos contra ameaças cibernéticas.

SOLICITE UMA DEMONSTRAÇÃO AGORA

Segura®: Futureproof Identity Security.

A Segura® é líder em Privileged Access Management (PAM), entregando às equipes de TI uma solução rápida e fácil de usar, sem complexidade na implementação.

Simplificamos o gerenciamento de acessos privilegiados com uma plataforma intuitiva, escalável e pensada para o dia a dia real das equipes. Nossa inovação, robustez e experiência do cliente foram reconhecidas globalmente por Gartner, KuppingerCole e Frost & Sullivan. Além disso, somos classificados como solução PAM nº 1 por usuários reais no Gartner Peer Insights.

> Com implantação ágil, automação precisa e zero custos ocultos, a Segura® é segurança que trabalha por você—simples assim

segura® | Futureproof Identity Security | segura.security

segura®

EBOOK

GUIA PARA A GESTÃO DE SUPERFÍCIES DE ATAQUE

Document Classification: Public | April 2025