EBOOK

PROTEGENDO INFRAESTRUTURAS CRÍTICAS

segura®

Introdução

A Imperativa Necessidade de Proteger a Infraestrutura Crítica no Cenário Digital Atual

No mundo interconectado de hoje, a infraestrutura crítica serve como a espinha dorsal da nossa sociedade, possibilitando serviços essenciais como energia, transporte, saúde e comunicação. No entanto, garantir a segurança desses sistemas vitais tem se tornado cada vez mais desafiador à medida que as ameaças cibernéticas continuam evoluindo e se tornando mais sofisticadas. De acordo com o Relatório de Riscos Globais 2022 do Fórum Econômico Mundial, os ciberataques à infraestrutura crítica estão classificados como o 5º maior risco em termos de probabilidade nos próximos dez anos. Com a Agência da União Europeia para a Cibersegurança (ENISA) afirmando que 30% de todos os ciberataques miraram setores de infraestrutura crítica em 2019, a necessidade de medidas de segurança robustas nunca foi tão urgente.

As consequências das violações de segurança na infraestrutura crítica podem ser devastadoras. As organizações enfrentam perdas financeiras significativas, sendo que o Instituto Ponemon estima o custo médio de uma violação de dados para organizações de infraestrutura crítica em $4,35 milhões de dólares. Além disso, as interrupções nos serviços essenciais podem ter impactos sociais e econômicos de longo alcance. Como 85% da infraestrutura crítica dos Estados Unidos é de propriedade e operada pelo setor privado, a colaboração efetiva entre o governo e as entidades privadas é fundamental para garantir a segurança.

O Relatório de Infraestrutura de 2021 da Sociedade Americana de Engenheiros Civis destaca a necessidade de investimentos significativos na melhoria e segurança da infraestrutura crítica do país, atribuindo aos Estados Unidos uma nota C-. A Agência Internacional de Energia (IEA) estima que os investimentos globais em infraestrutura energética devem alcançar $3,5 trilhões de dólares anualmente até 2050 para atingir as metas globais de clima e energia, tornando a importância de proteger esses investimentos ainda mais crítica.

Ao compreender os riscos e implementar medidas de segurança robustas,as organizações podem proteger suas infraestruturas críticas e garantir a entrega contínua de serviços essenciais nos próximos anos

Neste ebook, exploraremos a importância da infraestrutura crítica, às diversas ameaças e desafios que ela enfrenta e o papel da Gestão de Acesso Privilegiado (PAM) em garantir sua segurança. Também apresentaremos a solução de PAM da Segura® e demonstraremos como ela pode proteger efetivamente os sistemas de infraestrutura crítica em um cenário digital em constante evolução.

Índice

EBOOK

PROTEGENDO INFRAESTRUTURAS CRÍTICAS

Capítulo 1

A Necessidade de Proteger a Infraestrutura Crítica no Cenário Digital Atual

Definindo Infraestrutura Crítica

À medida que o mundo se torna mais interdependente, garantir e manter a estabilidade da infraestrutura crítica se tornou indispensável para o bom funcionamento da sociedade e da economia. A infraestrutura crítica engloba os ativos, sistemas e redes, tanto físicos quanto virtuais, que são cruciais para as operações de uma nação. Isso inclui setores como energia,água, transporte, comunicações e serviços de emergência, entre outros.

A interrupção ou devastação dessas infraestruturas vitais pode levar a consequências graves, afetando não apenas setores específicos, mas também a segurança pública, a segurança nacional e a economia como um todo. Consequentemente, priorizar a segurança e a resiliência da infraestrutura crítica tem se tornado uma preocupação primordial para governos e organizações em todo o mundo.

> **Garantir a estabilidade da infraestrutura crítica se tornou indispensável para o bom funcionamento da sociedade e da economia.**

A Importância da Infraestrutura Crítica

A infraestrutura crítica forma a espinha dorsal da sociedade moderna, fornecendo serviços essenciais que afetam todos os aspectos da vida diária. A importância da infraestrutura crítica não pode ser subestimada, pois ela garante o bom funcionamento de vários setores, incluindo os citados ao lado.

A falha ou interrupção de qualquer uma dessas infraestruturas críticas pode levar a consequências generalizadas, incluindo perda de vidas, danos econômicos e erosão da confiança pública. Portanto, proteger a infraestrutura crítica é fundamental para manter a segurança nacional, a segurança pública e a estabilidade econômica.

Energia

A geração, transmissão e distribuição de eletricidade, gás natural e outras formas de energia que alimentam nossas casas, empresas e indústrias.

Comunicações

a transmissão de informações por meio de várias mídias, como Internet,redes telefô-nicas e sistemas de satélite.

Transporte

O movimento de pessoas e mercadorias por ar, terra e mar, incluindo rodovias, ferrovias, portos e aeroportos.

Água

O fornecimento de água potável limpa e segura, bem como o tratamento e o des-carte de águas residuais.

Serviços de emergência

a prestação de serviços médicos, policiais e de combate a incêndios que protegem a saúde e a segurança dos cidadãos.

A Crescente Necessidade de Proteção de Infraestrutura Crítica

À medida que nosso mundo se torna intrinsecamente conectado e dependente de tecnologia, a probabilidade de ataques cibernéticos direcionados à infraestrutura essencial aumentou. Atores mal-intencionados, como cibercriminosos e estados-nação, concentram persistentemente seus esforços em infraestrutura crítica, esforçando-se para identificar e explorar pontos fracos, ao mesmo tempo em que obtêm acesso não autorizado a informações confidenciais, sistemas de controle e outros ativos importantes.

Os riscos associados às ameaças cibernéticas à infraestrutura crítica são ainda mais exacerbados por fatores como:

- O aumento do uso de tecnologias digitais e a convergência de sistemas de tecnologia da informação (TI) e tecnologia operacional (OT), que criam novas vulnerabilidades e superfícies de ataque.
- A crescente dependência de fornecedores terceirizados e parceiros da cadeia de suprimentos, que podem apresentar riscos e complexidades adicionais.
- O ritmo acelerado da mudança tecnológica, que pode tornar desafiador para as organizações acompanhar as ameaças em evolução e manter uma postura de segurança robusta.

Diante desses desafios, é mais importante do que nunca que as organizações implementem medidas de segurança abrangentes para proteger sua infraestrutura crítica e garantir sua resiliência contínua.

O Papel do Gerenciamento de Acesso Privilegiado na Proteção de Infraestrutura Crítica

Um dos principais componentes da proteção da infraestrutura crítica é o gerenciamento e o controle eficazes do acesso privilegiado. O acesso privilegiado refere-se às permissões elevadas concedidas a usuários específicos, permitindo que eles executem tarefas confidenciais, acessem sistemas críticos ou gerenciem controles de segurança.

O gerenciamento de acesso privilegiado (PAM) é um aspecto crucial da segurança da infraestrutura crítica, pois ajuda as organizações a impedir o acesso não autorizado, detectar e responder a ameaças e manter a conformidade com os padrões e regulamentos relevantes do setor. As soluções PAM, como o Segura® PAM, fornecem as ferramentas e recursos necessários para gerenciar, monitorar e controlar o acesso privilegiado, reduzindo assim o risco de violações de segurança e protegendo a infraestrutura crítica de possíveis ataques.

Nos capítulos seguintes, aprofundaremos as ameaças e os desafios à segurança da infraestrutura crítica, o papel do gerenciamento de acesso privilegiado para enfrentar esses desafios e como a solução Segura® PAM pode ajudar as organizações a proteger seus ativos de infraestrutura crítica.

EBOOK

PROTEGENDO INFRAESTRUTURAS CRÍTICAS

Capítulo 2

Ameaças e desafios à segurança da infraestrutura crítica

Compreendendo o cenário de ameaças

A segurança da infraestrutura crítica está sob constante ameaça de uma ampla gama de atores, incluindo estados-nação, cibercriminosos, hacktivistas e até mesmo pessoas de dentro. Esses atores mal-intencionados empregam uma variedade de táticas, técnicas e procedimentos (TTPs) para comprometer sistemas críticos de infraestrutura, interromper serviços ou causar danos físicos. Algumas das ameaças mais comuns à segurança da infraestrutura crítica incluem:

Ataques cibernéticos

Os cibercriminosos e os agentes do estado-nação visam sistemas de infraestrutura crítica usando vários tipos de malware, ransomware e ataques distribuídos de negação de serviço (DDoS) para interromper operações, roubar informações confidenciais ou causar danos físicos.

Ataques à cadeia de suprimentos

Vendedores ou fornecedores terceirizados podem introduzir vulnerabilidades em sistemas críticos de infraestrutura, seja por meio de hardware ou software comprometido ou fornecendo acesso não autorizado a agentes de ameaças.

Ameaças internas

Funcionários, contratados ou outros internos com acesso privilegiado podem comprometer, intencionalmente ou não, sistemas críticos de infraestrutura, por meio de ações maliciosas ou negligência.

Ataques físicos

Os ativos de infraestrutura crítica também podem ser alvo de ameaças físicas, como terrorismo, sabotagem ou desastres naturais, que podem causar danos significativos ou interromper as operações.

Desafios na proteção da infraestrutura crítica

Proteger a infraestrutura crítica das inúmeras ameaças descritas acima é uma tarefa complexa, composta por vários desafios únicos, incluindo:

- **Convergência de TI e OT:** A integração dos sistemas de tecnologia da informação (TI)e tecnologia operacional (OT) aumentou a eficiência e a conectividade, mas também introduziu novas vulnerabilidades que podem ser exploradas por cibercriminosos.
- **Sistemas legados:** muitos setores críticos de infraestrutura dependem de sistemas desatualizados que não foram projetados tendo em mente as ameaças de segurança modernas, tornando-os mais suscetíveis a ataques.
- **Visibilidade e monitoramento inadequados:** a escala e a complexidade dos sistemas de infraestrutura crítica dificultam que as organizações mantenham visibilidade e monitoramento completos de suas redes, dispositivos e pontos de acesso.
- **Conformidade regulamentar:** as organizações responsáveis pela infraestrutura crítica devem cumprir vários regulamentos e padrões específicos do setor, que podem ser complexos e demorados de gerenciar.
- **Recursos limitados:** muitas organizações de infraestrutura crítica enfrentam restrições orçamentárias, escassez de pessoal ou falta de conhecimento interno, o que dificulta a implementação e manutenção de medidas de segurança robustas.

O Papel Crítico do Gerenciamento de Acesso Privilegiado

Dadas as ameaças e os desafios associados à segurança da infraestrutura crítica, é essencial que as organizações implementem uma solução abrangente de Privileged Access Management (PAM), como o Segura®. O PAM é um componente crítico de uma postura de segurança robusta, pois ajuda as organizações a:

Evite o acesso não autorizado

Ao controlar e gerenciar o acesso privilegiado, as organizações podem reduzir o risco de acesso não autorizado a sistemas críticos, seja de invasores externos ou internos.

Detecte e responda a ameaças

As soluções PAM podem fornecer monitoramento e alerta em tempo real de atividades suspeitas, permitindo que as organizações detectem e respondam rapidamente a possíveis incidentes de segurança.

Conformidade regulamentar

As soluções PAM podem ajudar as organizações a atender aos requisitos de vários regulamentos e padrões específicos do setor, como NERC CIP, GDPR e HIPAA, garantindo controles de acesso adequados, auditoria e recursos de geração de relatórios.

Visibilidade e o controle

uma solução PAM abrangente fornece às organizações a visibilidade e o controle necessários para gerenciar o acesso privilegiado em seus ambientes de TI e OT, reduzindo o risco de violações de segurança.

No próximo capítulo, exploraremos a função do gerenciamento de acesso privilegiado com mais detalhes, incluindo seus principais componentes e como ele pode ajudar as organizações a proteger seus ativos críticos de infraestrutura.

EBOOK

PROTEGENDO INFRAESTRUTURAS CRÍTICAS

Capítulo 3

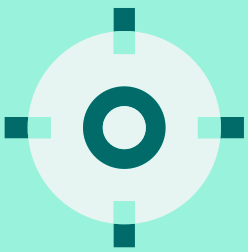
Compreendendo a Função do Gerenciamento de Acesso Privilegiado (PAM)

segura | Futureproof Identity Security | segura.security

A Importância do Gerenciamento de Acesso Privilegiado

Conforme discutido nos capítulos anteriores, a segurança da infraestrutura crítica depende fortemente do gerenciamento e controle eficazes do acesso privilegiado. Usuários privilegiados, como administradores de sistema, pessoal de TI e fornecedores terceirizados, têm permissões elevadas que lhes concedem acesso a sistemas críticos e informações confidenciais. Se não for gerenciado adequadamente, esse acesso pode ser explorado por agentes mal-intencionados, levando a violações de segurança significativas e possíveis danos à infraestrutura crítica.

Privileged Access Management (PAM) é um componente crucial de uma estratégia de segurança robusta, ajudando as organizações a impedir o acesso não autorizado, detectar e responder a ameaças e manter a conformidade com os regulamentos específicos do setor.



Principais componentes do PAM

Uma solução PAM abrangente, como o Segura® PAM, geralmente inclui os seguintes componentes principais:

- **Controle de acesso:** às soluções PAM fornecem controles de acesso granulares, permitindo que as organizações definam e imponham quem pode acessar quais sistemas, sob quais condições e por quanto tempo. Isso inclui recursos como controle de acesso baseado em função (RBAC), acesso just-in-time (JIT) e elevação temporária de privilégios.

- **Gerenciamento de credenciais:** as soluções PAM oferecem gerenciamento centralizadode credenciais privilegiadas, incluindo senhas, chaves e certificados. Isso inclui recursos como armazenamento seguro, rotação automática e auditoria periódica de credenciais.

- **Monitoramento e Gravação de Sessões:** As soluções PAM permitem que as organizações monitorem e registrem sessões de usuários privilegiados em tempo real, proporcionando total visibilidade e responsabilidade por atividades privilegiadas. Isso ajuda as organizações a detectar atividades suspeitas e facilita as investigações forenses no casode um incidente de segurança.

- **Auditoria e relatórios:** as soluções PAM fornecem recursos abrangentes de auditoria e relatórios, permitindo que as organizações rastreiem e analisem atividades de acesso privilegiado e demonstrem conformidade com regulamentos e padrões específicos do setor.

- **Detecção e Resposta a Ameaças:** As soluções avançadas de PAM incorporam aprendizado de máquina e análise comportamental para identificar anomalias e possíveis ameaças à segurança, permitindo que as organizações detectem e respondam rapidamente a incidentes antes que eles aumentem.

Benefícios da Implementação de PAM na Segurança da Infraestrutura Crítica

A implementação de uma solução PAM robusta, como o Segura® PAM, oferece inúmeros benefícios para organizações responsáveis por infraestrutura crítica, incluindo:

Segurança aprimorada

ao gerenciar e controlar o acesso privilegiado, as organizações podem reduzir significativamente o risco de acesso não autorizado e violações de segurança, protegendo seus sistemas críticos e informações confidenciais.

Conformidade aprimorada

as soluções PAM ajudam as organizações a demonstrar conformidade com vários regulamentos e padrões específicos do setor, fornecendo os controles de acesso, auditoria e recursos de relatórios necessários.

Maior eficiência operacional

ao automatizar e simplificar os processos de acesso privilegiado, as soluções PAM podem melhorar a eficiência operacional e reduzir o risco de erro humano.

Maior visibilidade e controle

as soluções PAM fornecem às organizações a visibilidade e o controle necessários para gerenciar com eficácia o acesso privilegiado em seus ambientes de TI e OT, garantindo que o acesso privilegiado seja concedido apenas àqueles que realmente precisam dele.

Nos capítulos seguintes, exploraremos o Segura® PAM com mais detalhes, incluindo seus principais recursos, como ele protege a infraestrutura crítica e estudos de caso do mundo real que demonstram sua eficácia em ação.

EBOOK

PROTEGENDO INFRAESTRUTURAS CRÍTICAS

Capítulo 4

Segura® PAM: Uma Visão Geral e os Principais Recursos

Introdução ao Segura® PAM

O Segura® Privileged Access Management (PAM) é uma solução abrangente projetada para ajudar as organizações a proteger sua infraestrutura crítica, gerenciando e controlando o acesso privilegiado em seus ambientes de TI e OT.
O Segura® PAM fornece um conjunto robusto de recursos e capacidades que permitem que as organizações impeçam o acesso não autorizado, detectem e respondam a ameaças e mantenham a conformidade com os padrões e regulamentações relevantes do setor.

Principais Recursos do Segura® PAM

O PAM oferece uma ampla variedade de recursos que o tornam uma solução Segura® ideal para organizações que buscam aprimorar a segurança de sua infraestrutura crítica. Alguns dos principais recursos do Segura® PAM incluem:

- **Controle de acesso granular:** o Segura® PAM fornece controle de acesso baseado em função (RBAC) e acesso just-in-time (JIT), garantindo que usuários privilegiados tenham acesso apenas aos sistemas de que precisam, quando precisam. Isso ajuda a minimizar o risco de acesso não autorizado e violações de segurança.

- **Gerenciamento seguro de credenciais:** o Segura® PAM oferece gerenciamento centralizado de credenciais privilegiadas, incluindo senhas, chaves e certificados.

Isso inclui armazenamento seguro, rotação automática e auditoria periódica de credenciais para garantir sua integridade e reduzir o risco de comprometimento.

- **Monitoramento e gravação de sessões:** o Segura® PAM permite que as organizações monitorem e registrem sessões de usuários privilegiados em tempo real, proporcionando total visibilidade e responsabilidade por atividades privilegiadas. Isso ajuda a detectar atividades suspeitas e facilita as investigações forenses no caso de um incidente de segurança.

- **Detecção e Resposta Avançada a Ameaças:** o Segura® PAM incorpora aprendizado de máquina e análise comportamental para identificar anomalias e possíveis ameaças à segurança, permitindo que as organizações detectem e respondam rapidamente a incidentes antes que eles aumentem.

- **Auditoria e relatórios abrangentes:** o Segura® PAM fornece recursos abrangentes de auditoria e relatórios, permitindo que as organizações rastreiem e analisem atividades de acesso privilegiado e demonstrem conformidade com regulamentos e padrões específicos do setor.

- **Integração com a infraestrutura existente:** o Segura® PAM integra-se perfeitamente aos sistemas existentes de TI e OT, tornando mais fácil para as organizações implementar e gerenciar suas políticas de acesso privilegiado sem interromper os fluxos de trabalho ou processos existentes.

O Segura® PAM é uma solução abrangente para proteger sua infraestrutura crítica

Opções de implantação do Segura® PAM

Para atender às diversas necessidades das organizações responsáveis pela infraestrutura crítica, o Segura® PAM oferece opções de implantação flexíveis, incluindo implantações locais, baseadas em nuvem e híbridas. Isso permite que as organizações escolham o método de implantação que melhor se alinha com sua infraestrutura, requisitos de segurança e restrições orçamentárias.

No próximo capítulo, exploraremos como o Segura® PAM protege a infraestrutura crítica, analisando seus vários recursos e capacidades com mais detalhes.

EBOOK

PROTEGENDO INFRAESTRUTURAS CRÍTICAS

Capítulo 5

Como o Segura® PAM Protege a Infraestrutura Crítica

Prevenção de acesso não autorizado

Um dos principais objetivos do Segura® PAM é impedir o acesso não autorizado a sistemas críticos e informações confidenciais. Isso é obtido por meio de vários recursos principais, incluindo:

- **Controle de acesso baseado em função (RBAC):** o RBAC permite que as organizações definam e imponham controles de acesso granulares com base nas funções e responsabilidades de usuários privilegiados. Ao garantir que os usuários tenham acesso apenas aos sistemas e recursos de que precisam para desempenhar suas funções, o Segura® PAM minimiza a superfície de ataque potencial para agentes mal-intencionados.

- **Acesso Just-In-Time (JIT):** o acesso JIT garante que o acesso privilegiado seja concedido somente quando necessário e revogado assim que não for mais necessário. Isso reduz o risco de acesso não autorizado, limitando a janela de oportunidade para invasores explorarem credenciais privilegiadas.

- **Gerenciamento seguro de credenciais:** o Segura® PAM fornece gerenciamento centralizado de credenciais privilegiadas, incluindo armazenamento seguro, rotação automática e auditoria periódica. Isso ajuda a evitar roubo e uso indevido de credenciais, garantindo que as credenciais privilegiadas estejam sempre atualizadas e protegidascontra acesso não autorizado.

Detecção e Resposta a Ameaças

O PAM foi projetado para ajudar as organizações a detectar e responder rapidamente a possíveis incidentes de segurança do Segura®, fornecendo recursos de monitoramento e alerta em tempo real. Os principais recursos nesta área incluem:

Monitoramento e gravação de sessões

Ao monitorar e registrar sessões de usuários privilegiados em tempo real, o Segura® PAM fornece visibilidade completa das atividades privilegiadas em toda a organização. Isso permite que as equipes de segurança detectem rapidamente comportamentos suspeitos e tomem as medidas adequadas para mitigar possíveis ameaças.

Detecção avançada de ameaças

O Segura® PAM incorpora aprendizado de máquina e análise comportamental para identificar anomalias e possíveis ameaças à segurança com base no comportamento histórico do usuário e nos padrões de acesso. Isso permite que as organizações detectem ataques em potencial em seus estágios iniciais e respondam antes que possam causar danos significativos.

Garantimos monitoramento e alerta em tempo real

Conformidade com os padrões e regulamentos do setor

Além de seus recursos de segurança, o Segura® PAM também ajuda as organizações a manter a conformidade com os padrões e regulamentos relevantes do setor, como NERC CIP, GDPR, LGPD e HIPAA. Isso é alcançado por meio de recursos abrangentes de auditoria e relatórios, que permitem às organizações:

- Rastreie e análise as atividades de acesso privilegiado em seus ambientes de TI e OT.
- Identifique possíveis violações de conformidade ou áreas de preocupação.
- Gerar relatórios e evidências para demonstrar conformidade para auditores e reguladores.

Integração com a Infraestrutura Existente

Por fim, o Segura® PAM foi projetado para integrar-se perfeitamente aos sistemas existentes de TI e OT, facilitando para as organizações a implementação e o gerenciamento de suas políticas de acesso privilegiado sem interromper os fluxos de trabalho ou processos existentes. Isso inclui integração com:

- Soluções de gerenciamento de identidade e acesso (IAM).
- Plataformas de gerenciamento de eventos e informações de segurança (SIEM).
- Ferramentas de gerenciamento de serviços de TI (ITSM).
- Dispositivos de rede e segurança.

Ao fornecer uma solução abrangente e integrada para gerenciar e controlar o acesso privilegiado, o Segura® PAM permite que as organizações protejam seus ativos críticos de infraestrutura e mantenham uma postura de segurança robusta diante de ameaças e desafios em evolução.

No próximo capítulo, exploraremos estudos de caso do mundo real que demonstram o Segura® PAM em ação, mostrando sua eficácia na proteção de ambientes de infraestrutura crítica.

EBOOK

PROTEGENDO INFRAESTRUTURAS CRÍTICAS

Capítulo 6

Estudos de Caso do Mundo Real: Segura® PAM em Ação

Como as organizações protegeram seus ativos crítucos com Segura® PAM

Estudo de Caso 1
Setor de Energia

Uma grande empresa de energia com operações em vários países enfrentou desafios no gerenciamento de acesso privilegiado à sua complexa infraestrutura de TI e OT. A empresa precisava de uma solução que fornecesse controle de acesso granular, monitoramento em tempo real e conformidade com os regulamentos do setor, como NERC CIP.

Ao implementar o Segura® PAM, a empresa conseguiu:

- Simplifique o gerenciamento de acesso privilegiado consolidando credenciais e políticas de acesso em uma plataforma centralizada;
- Aumente a segurança aplicando controle de acesso baseado em função e acesso just-in-time para usuários privilegiados;
- Melhore a visibilidade das atividades privilegiadas monitorando e registrando as sessões do usuário em tempo real;
- Obtenha conformidade com os requisitos NERC CIP por meio de recursos abrangentes de auditoria e relatórios.

Estudo de Caso 2
Setor de Transporte

Uma agência nacional de transporte responsável por gerenciar uma vasta rede de rodovias, ferrovias e portos enfrentou o desafio de proteger sua infraestrutura crítica contra ameaças externas e internas. A agência precisava de uma solução PAM que fornecesse gerenciamento seguro de credenciais, recursos de detecção de ameaças e integração com sua infraestrutura de segurança existente.

Com o Segura® PAM, a transportadora conseguiu:

- Proteger credenciais privilegiadas contra roubo e uso indevido por meio de armazenamento seguro e rotação automática;
- Detectar possíveis ameaças à segurança aproveitando o aprendizado de máquina e a análise comportamental para identificar anomalias no comportamento do usuário;
- Integrar ferramentas de segurança existentes, como plataformas SIEM e dispositivos de rede, para aprimorar a postura geral de segurança;
- Manter a conformidade com os regulamentos relevantes do setor por meio de recursos robustos de auditoria e relatórios.

Estudo de Caso 3
Serviço de Água

Uma grande concessionária de água responsável pelo fornecimento de água potável e serviços de tratamento de águas residuais para milhões de clientes enfrentou o desafio de proteger sua infraestrutura crítica contra ataques cibernéticos e ameaças internas. O utilitário exigia uma solução PAM que fornecesse controle de acesso granular, monitoramento de sessão e gerenciamento seguro de credenciais.

Ao implantar o Segura® PAM, a concessionária de água alcançou:

- Segurança aprimorada implementando controle de acesso baseado em função e acesso just-in-time para usuários privilegiados;
- Visibilidade aprimorada em atividades privilegiadas por meio de monitoramento e gravação de sessões em tempo real;
- Gerenciamento seguro de credenciais privilegiadas, incluindo senhas, chaves e certificados;
- Conformidade com regulamentos específicos do setor, como o Programa de Gerenciamento de Riscos (PRM) da EPA.

Esses estudos de caso demonstram a eficácia do Segura® PAM na proteção de infraestrutura crítica em vários setores e destacam os benefícios da implementação de uma solução abrangente de PAM.

No próximo capítulo, discutiremos como as organizações podem implementar o Segura® PAM em seus próprios ambientes e as etapas para garantir uma implantação bem-sucedida.

EBOOK

PROTEGENDO INFRAESTRUTURAS CRÍTICAS

Capítulo 7

Implementando o Segura® PAM em sua Organização

A implantação de uma solução abrangente de Gestão de Acessos Privilegiados (PAM) como o Segura® PAM é uma etapa crítica para aumentar a segurança de sua infraestrutura crítica. Neste capítulo, descreveremos as principais etapas envolvidas na implementação do Segura® PAM em sua organização e forneceremos orientações para garantir uma implantação bem-sucedida.

Avaliando sua postura de segurança atual

Antes de implementar o Segura® PAM, é essencial avaliar a postura de segurança atual da sua organização. Isso envolve identificar vulnerabilidades existentes, avaliar a conformidade de sua organização com regulamentações específicas do setor e determinar a eficácia de suas políticas e procedimentos atuais de gerenciamento de acesso privilegiado. Essa avaliação ajudará você a identificar áreas em que o Segura® PAM pode fornecer as melhorias mais significativas e orientar sua estratégia de implementação.

Definindo Funções e Políticas de Acesso

Uma das principais funções do Segura® PAM é impor controles de acesso granulares com base nas funções e responsabilidades dos usuários privilegiados. Para conseguir isso, você precisará definir as funções e políticas de acesso apropriadas para sua organização.

Isso involve:

- Identificando as várias funções de usuário privilegiado em sua organização.
- Mapeando os níveis de acesso e permissões necessários para cada função.
- Estabelecer políticas de acesso, como acesso just-in-time e elevação temporária de privilégios, para minimizar o risco de acesso não autorizado.

Implantando o Segura® PAM

Dependendo dos requisitos e infraestrutura específicos da sua organização, você pode optar por implantar o Segura® PAM no local, na nuvem ou usando uma abordagem híbrida. Independentemente da opção de implantação escolhida, o processo de implementação geralmente envolve as seguintes etapas:

- Instalação e configuração do software Segura® PAM no(s) servidor(es) apropriado(s) ou ambiente de nuvem.
- Integrando o Segura® PAM com seus sistemas existentes de TI e OT, como soluções de gerenciamento de identidade e acesso (IAM), plataformas de gerenciamento de eventos e informações de segurança (SIEM) e dispositivos de rede.
- Configurando o Segura® PAM para impor suas funções definidas e políticas de acesso.
- Importar ou criar credenciais privilegiadas na plataforma Segura® PAM.

Treinamento e Conscientização

Uma implementação PAM bem-sucedida requer não apenas a tecnologia certa, mas também o treinamento adequado e a conscientização de sua equipe. Certifique-se de que todos os usuários privilegiados em sua organização sejam treinados no uso adequado do Segura® PAM, incluindo:

- Efetuando login e autenticação pela plataforma Segura® PAM.
- Solicitar e utilizar acesso privilegiado, de acordo com as políticas estabelecidas.
- Reconhecer e relatar possíveis incidentes de segurança detectados por meio de recursos de monitoramento de sessão e detecção de ameaças.

Além disso, é essencial conscientizar os usuários não privilegiados sobre a importância do gerenciamento de acesso privilegiado e o papel que ele desempenha na proteção da infraestrutura crítica de sua organização.

Manutenção e Monitoramento Contínuos

A implementação do Segura® PAM é apenas o começo de sua jornada rumo a uma infraestrutura crítica mais segura. Manutenção e monitoramento regulares são necessários para garantir a eficácia contínua de sua solução PAM. Isso inclui:

- Revendo e atualizando periodicamente funções e políticas de acesso para refletir as mudanças em sua organização.
- Monitorando sessões de usuários privilegiados e respondendo a possíveis incidentes de segurança em tempo real.
- Auditoria e relatórios sobre atividades de acesso privilegiado para manter a conformidade com os regulamentos específicos do setor.

Seguindo essas etapas e práticas recomendadas, sua organização pode implementar com sucesso o Segura® PAM e aumentar a segurança de seus ativos críticos de infraestrutura.

No próximo capítulo, concluiremos nossa discussão e forneceremos orientações sobre as próximas etapas para organizações que desejam implantar o Segura® PAM.

EBOOK

PROTEGENDO INFRAESTRUTURAS CRÍTICAS

Conclusão e Próximos Passos

Ao longo deste ebook, exploramos a importância da segurança da infraestrutura crítica, o papel da Gestão de Acessos Privilegiado (PAM) na proteção de ativos críticos e os benefícios de implementar uma solução PAM abrangente como o Segura PAM.

Ao considerar a implementação do Segura® PAM em sua organização, lembre-se das próximas etapas:

1. Avalie a postura de segurança atual de sua organização, incluindo vulnerabilidades existentes, conformidade com regulamentos específicos do setor e a eficácia de suas políticas e procedimentos atuais de gerenciamento de acesso privilegiado.
2. Defina as funções e políticas de acesso apropriadas para sua organização, garantindo que usuários privilegiados tenham acesso apenas aos sistemas e recursos necessários para desempenhar suas funções.
3. Escolha a opção de implantação apropriada para o Segura PAM (local, baseado em nuvem ou híbrido) com base na infraestrutura, requisitos de segurança e restrições orçamentárias de sua organização.
4. Treine usuários privilegiados sobre o uso adequado do Segura PAM e conscientize usuários não privilegiados sobre a importância do gerenciamento de acesso privilegiado na proteção de infraestrutura crítica.
5. Treine usuários privilegiados sobre o uso adequado do Segura PAM e conscientize usuários não privilegiados sobre a importância do gerenciamento de acesso privilegiado na proteção de infraestrutura crítica.

Seguindo essas etapas, sua organização pode implantar com sucesso o Segura PAM e fortalecer sua postura de segurança de infraestrutura crítica.

À medida que o cenário de ameaças continua a evoluir, a implementação de uma solução PAM abrangente como o Segura PAM será essencial para proteger seus ativos críticos, garantir a segurança e o bem-estar de seus clientes e manter a estabilidade de nosso mundo interconectado.

Agende uma Demonstração: Veja Segura PAM em Ação

Você está pronto para ver em primeira mão como o Segura PAM pode melhorar a segurança da infraestrutura crítica da sua organização? Convidamos você a agendar uma demonstração personalizada com nossa equipe de especialistas, que irá guiá-lo pelos principais recursos e capacidades do Segura PAM e demonstrar como ele pode ajudá-lo a gerenciar e controlar o acesso privilegiado de forma eficaz.

Durante a demonstração, você pode esperar:

- Obtenha uma compreensão mais profunda da solução Segura PAM e como ela aborda os desafios exclusivos de proteger a infraestrutura crítica.
- Explore a interface amigável e os recursos poderosos do Segura PAM, incluindo controle de acesso granular, gerenciamento seguro de credenciais, monitoramento de sessão em tempo real e detecção avançada de ameaças.
- Discuta os requisitos de segurança e infraestrutura específicos da sua organização e saiba como o Segura PAM pode ser personalizado e implantado para atender às suas necessidades.
- Tenha a oportunidade de tirar dúvidas e receber orientação personalizada de nossa equipe de especialistas em PAM.

Não perca esta oportunidade de descobrir como o Segura PAM pode ajudar sua organização a proteger seus ativos críticos de infraestrutura, 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 e data e hora de sua preferência. Assim que sua solicitação for enviada, um membro de nossa equipe entrará em contato para confirmar os detalhes e fornecer as instruções necessárias para participar da demonstração.

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

PROTEGENDO INFRAESTRUTURAS CRÍTICAS

Document Classification: Public | April 2025