ManageEngine
PAM360

Gerenciamento de acesso privilegiado em um mundo Zero Trust

- Melanie Karunaratne

www.manageengine.com/br/privileged-access-management/om/pam360

Introdução

Nos primeiros meses da pandemia de covid-19, com a mudança em larga escala para o trabalho em home office, a conectividade foi o foco principal das organizações. Os administradores de TI rapidamente colocaram em prática reuniões virtuais, streaming ao vivo, educação virtual, aplicações em nuvem e recursos para dar suporte a seus usuários remotos finais. Com muitas organizações sinalizando sua intenção de ampliar o trabalho em home office (WFH), fica claro que o trabalho remoto e a dinâmica de trabalho híbrida vieram para ficar. Este documento descreve as implicações de segurança do novo ambiente de trabalho, explica a mudança das organizações para uma mentalidade Zero Trust e a importância do gerenciamento de acesso privilegiado para dar suporte a um modelo de segurança Zero Trust.

Acesso a todas as áreas

A reviravolta causada pela exigência do trabalho em home office (WFH) e a necessidade de manter os trabalhadores produtivos a todo custo deu origem ao rápido acesso à tecnologia. Esse acesso frequentemente ignorou as verificações e garantias regulares relacionadas a solicitações de acesso. Algumas das descobertas decorrentes da adoção cada vez maior das políticas do trabalho em home office (WFH) são:

- Empresas, assistência médica, educação e governos aceleraram a adoção da tecnologia em nuvem, migrando rapidamente alguns serviços do local para aplicações do tipo SaaS (Software as a Service, software como serviço), que usam endereços públicos de internet como pontos de entrada.

- Os funcionários receberam acesso a recursos fora da rede corporativa.

- Novos contratos de fornecedores de TI foram adotados rapidamente, adicionando mais acesso de terceiros a infraestruturas e aplicações corporativas.

- As VPNs se expandiram, aumentando os custos de licença e o número de incidentes de TI registrados.

- Notebooks foram adquiridos e provisionados, deixando as portas das empresas com maiores direitos de acesso para garantir que a força de trabalho pudesse entrar em operação rapidamente.

- Os funcionários organizaram escritórios domésticos, acessando sistemas usando seus telefones pessoais, notebooks e tablets e, em alguns casos, dispositivos compartilhados com a família. Esses dispositivos pessoais geralmente têm configurações de segurança mais fracas. Esses mesmos dispositivos se conectam a sites de compras de consumidores, mídias sociais e sites de entretenimento doméstico usando as mesmas credenciais. Isso aumenta a probabilidade de dispositivos comprometidos acessarem aplicações que armazenam dados corporativos.

- As empresas não construídas para trabalho remoto agora estão lidando com uma explosão de endpoints conhecidos e desconhecidos acessando suas redes em redes Wi-Fi inseguras.

Os dados corporativos anteriormente armazenados em software monitorado e mantido pelas equipes de TI agora residem em aplicações SaaS não verificadas, com senhas compartilhadas que podem ser usadas em dispositivos pessoais, aumentando os riscos de segurança da exposição por meio da ampliação das áreas de superfície de ataque. À medida que o trabalho remoto se tornou o novo normal, testemunhamos um surto e persistência de ataques cibernéticos no mesmo período. Os agentes de ameaça se agarraram à mudança para o trabalho em home office, penetrando persistentemente os perímetros da rede. Os ataques sofisticados estão prejudicando as empresas, as cadeias de fornecimento e os serviços de saúde a um custo enorme.

Zero Trust – Não confie em ninguém

Com os usuários trabalhando em vários dispositivos, dentro e fora da rede corporativa, há um jogo de gato e rato para proteger o perímetro da rede contra os esforços de agentes mal-intencionados. A abordagem de fortalecimento rege o acesso a partir de um perímetro de rede estático. Mas a combinação desarticulada de VPNs, segurança de e-mail, firewalls, etc., está obsoleta em nosso novo ambiente de vida profissional. Ambientes complexos em multinuvem, usando plataformas como Amazon AWS e Microsoft Azure, ambientes híbridos, e a rápida adoção de aplicações de nuvem, significam que uma abordagem baseada em perímetro não é mais defensável. Os adversários estão usando a abordagem de segurança baseada em perímetro contra organizações. Alguns dos piores ataques foram bem-sucedidos porque os criminosos cibernéticos penetraram em firewalls. Eles mudaram de dispositivo para dispositivo sem ser detectados usando credenciais confiáveis, explorando privilégios ou escalando privilégios internamente.

Confiar em todos dentro do perímetro não é mais eficaz. É por isso que as principais organizações estão mudando para os modelos Zero Trust, a fim de reforçar sua postura de segurança e impedir os piores efeitos de ataques e violações. Um modelo de segurança Zero Trust reconhece que existem ameaças potenciais dentro e fora do perímetro tradicional. A suposição é que você nunca está seguro. Um ataque é inevitável ou já está em andamento. Os dispositivos podem já estar comprometidos e as solicitações de acesso não são confiáveis até serem verificadas. É uma mudança na mentalidade que elimina a confiança implícita. As organizações operam sem confiar em ninguém dentro ou fora dos perímetros da rede. Em vez disso, trata-se cada usuário e dispositivo como uma ameaça.

Em um ambiente Zero Trust, todos os usuários, dispositivos e aplicações são verificados antes de se conectarem a redes corporativas. Eles são continuamente avaliados durante uma sessão em busca de atividade incomum até que saiam da rede, oferecendo proteção em tempo real. A avaliação usa detalhes granulares e a aplicação de políticas. Considera-se o contexto e a localização, a postura de endpoints e aplicações, os controles de acesso a dados e a automação, limitando o acesso apenas ao que é necessário.

Acesso privilegiado

Um modelo de segurança Zero Trust permeia as redes, aproveitando várias camadas de ferramentas e métodos de segurança para minimizar os riscos. Aqui, mergulharemos em uma camada: o PAM (Privileged Access Management, gerenciamento de acesso privilegiado).

As ferramentas e políticas do PAM são uma de suas últimas linhas de defesa para impedir que os adversários se infiltrem. No novo mundo Zero Trust, as ferramentas do PAM tratam todos de dentro e fora da organização como uma ameaça potencial, para reduzirem o risco das ameaças de que

invasores possam obter seus dados críticos se os sistemas forem comprometidos. Mesmo sem uma abordagem Zero Trust, o gerenciamento de acesso privilegiado era um elemento fundamental reconhecido da segurança cibernética que muitas organizações já colocavam em prática.

Mas quando foi a última vez que a sua organização revisou as configurações e políticas da ferramenta de gerenciamento de acesso privilegiado? Não há espaço para complacência. Pode haver centenas ou milhares de servidores em seu ambiente e muitos superusuários administradores cuja seção sobre os recursos não é identificável no momento. O software do PAM não pode ser tratado como uma atividade de "configurar e esquecer". A TI muda ao longo do tempo em operações, e os dispositivos acomodam as demandas do trabalho em home office. Os líderes de gerenciamento de riscos e segurança devem visualizar o gerenciamento de privilégios como um processo contínuo. Identificar, verificar, proteger e monitorar constantemente quaisquer contas privilegiadas. Isso inclui contas de administradores de domínio e de serviços externos, contas de administradores locais e outras contas para instalação e gerenciamento de software.

Defina controles granulares

A revisão e auditoria do acesso é um componente principal da segurança Zero Trust, abordando a intenção de um criminoso virtual em relação ao movimento lateral. E seu software de gerenciamento de acesso privilegiado é uma ferramenta fundamental.

Chegou a hora de recalibrar suas políticas e tecnologias para o PAM. Aplique políticas de acesso refinadas com base na função e no local do usuário, no status de conformidade do dispositivo, na integridade e nos dados acessíveis. Um usuário que acessa uma aplicação no ambiente do escritório é menos arriscado do que se ele acessar a aplicação via Wi-Fi público, portanto o contexto é fundamental.

Defina níveis de privilégio

Reconheça que diferentes tipos de conta estão em uso em toda a organização. Isso inclui contas de privilégio pessoais ou compartilhadas, contas de serviço, contas de administrador local e raiz, credenciais de aplicação para aplicação e níveis de privilégio individuais. Essas diferentes contas devem ser configuradas e implantadas com base em políticas privilegiadas. A identificação de níveis de acesso, como usuários padrão, usuários de serviço e superusuários, simplificará o processo de limitação do acesso a níveis mais altos de privilégio, reduzindo a exposição.

Identifique contas privilegiadas

Nos primeiros dias da pandemia, as equipes de TI concederam aos usuários mais direitos de acesso devido à pressa de manter a produtividade. Por exemplo, foi necessário instalar novos programas para que as operações fossem executadas rapidamente. Mas essas permissões elevadas geralmente permaneceram em vigor meses após o usuário precisar delas. No entanto, vimos um aumento na engenharia social sofisticada através da pandemia. E-mails de phishing com temas relacionados ao coronavírus implantaram o malware Emotet Trojan, permitindo que os hackers ganhassem uma base nas contas. Uma vez dentro dos sistemas, os invasores usaram contas de usuário privilegiadas para se mover pela rede. Portanto, é vital analisar as contas de administrador concedidas para uma tarefa específica e revertê-las para contas de usuário padrão.

Contas privilegiadas e contas de serviço que foram esquecidas há muito tempo, estão órfãs ou não são gerenciadas oferecem portas de entrada acessíveis que colocam sua organização em risco desnecessário. A existência de acesso privilegiado não contabilizado acarreta riscos significativos, ampliando a área de superfície de ataque para criminosos cibernéticos.

Veja como as ferramentas do PAM devem encontrar contas privilegiadas. Comece verificando e

descobrindo cada conta privilegiada e caso de uso. Especifique quem tem acesso a contas de administrador e privilégios elevados. Classifique o acesso com base no risco e na exposição a ativos e dados críticos. Investigue todos os cenários. Por exemplo, um usuário com acesso privilegiado para trabalhar em uma tarefa em um ativo pode inadvertidamente obter acesso a outros controles ou aplicações?

É essencial entender quais contas privilegiadas estão acessando registros, quem possui recursos, e quem supervisiona a concessão de acesso. Além disso, é importante colocar em prática processos para descobrir todos os servidores ou aplicações que ofereçam direitos de acesso privilegiado. Compare quem recebeu acesso a contas, aplicações e bancos de dados antes com quem tem acesso agora.

Destacamos anteriormente que o contexto é fundamental, e é igualmente importante considerar e registrar onde o acesso ocorre e quando. Depois que os usuários com acesso de administrador ou maior forem identificados, determine se os privilégios adicionais ainda são necessários com base nas políticas granulares e remova o acesso excessivo. Para manter-se a par das constantes mudanças na equipe, nos dispositivos, nos sistemas e na infraestrutura, a descoberta e a identificação abrangentes do acesso privilegiado devem ser uma atividade contínua.

Use o princípio do menor privilégio

A segurança Zero Trust exerce o princípio de conceder o menor privilégio para usuários, aplicações e dispositivos. Emita privilégios suficientes para usuários, administradores de sistema e administradores de banco de dados, e autorize privilégios elevados somente quando necessário. Para seguir essa premissa, conceda aos usuários direitos de acesso privilegiado com base em quem solicita permissões. Descubra por que um indivíduo precisa de acesso. Garanta o nível mínimo de acesso necessário para executar uma função e o mínimo de tempo necessário. É igualmente importante aplicar a lente menos privilegiada entre entidades não humanas. Revise tudo o que usa credenciais, como ferramentas robóticas de automação de processos, scripts PowerShell ou credenciais codificadas em ferramentas DevOps, como Chef e Puppet. Aproveite a solução do PAM para empregar chamadas de API para recuperar senhas e erradicar as senhas embutidas em código.

O aumento na terceirização de funções internas e centrais levou ao aumento do acesso de fornecedores a sistemas críticos, como sistemas de saúde. Aplique o mesmo conceito principal de menor privilégio a cada decisão de acesso para fornecedores e prestadores de serviços terceirizados. Certifique-se de monitorar e registrar suas atividades de acesso como parte de seus processos. Quando os funcionários precisarem de mais privilégios, use controles just-in-time para limitar a exposição. A melhor maneira de conseguir isso é colocar em prática solicitações de acesso just-in-time e processos de aprovação. Peça aos usuários que enviem solicitações para elevar privilégios por um determinado período. Um processo de solicitação e aprovação definido garante que a produtividade não seja afetada, mas a segurança Zero Trust ainda está na vanguarda das decisões de acesso. Usar suas ferramentas de gerenciamento de acesso a privilégios para

gerenciar como e por que as contas de privilégio são configuradas impedirá a proliferação futura.

Bloqueie dispositivos e aplicações

Seguindo a abordagem Zero Trust, tome as medidas necessárias para analisar os notebooks e as estações de trabalho dos usuários finais. Bloqueie cada um deles, removendo os direitos de administradores locais. Mesmo uma ação tão simples quanto a capacidade do usuário de alterar data e hora da sua máquina pode causar complicações, afetando os esforços de auditoria. Depois, fique mais granular. Por exemplo, atualize as configurações e selecione os processos e aplicações que um usuário pode encerrar em suas máquinas. A regulagem das configurações garantirá que os usuários evitem desativar inadvertidamente o software de proteção de segurança. Reduza o risco de introduzir malware, restringindo o download de aplicações. Permita que apenas aplicações confiáveis sejam executadas e bloqueie o resto. As aplicações confiáveis ainda devem ser executadas com privilégios padrão para mitigar os riscos de segurança. Quando uma aplicação não estiver mais em uso, desprovisione-a. O desprovisionamento não só ajuda a proteger os sistemas, mas também economiza dinheiro em potencial por meio da recuperação e reutilização de licenças.

Separe credenciais

Por questões de velocidade, muitos administradores atualmente não estão separando suas contas de administrador de suas contas de trabalho de usuário final. Essas mesmas credenciais também são usadas entre servidores. Por que isso é preocupante? Os agentes de ameaça visam contas com privilégios de administrador para acessar recursos corporativos e executar ataques. O ataque à SolarWinds Sunburst em dezembro de 2020 é um exemplo importante, pois outras empresas de segurança se tornaram um caminho para outros ataques. As consequências afetaram centenas das maiores corporações e órgãos governamentais dos Estados Unidos. Os superusuários não devem executar tarefas de usuário final, como acessar e-mails enquanto estiverem conectados usando contas de administrador do Windows ou privilégios de conta raiz do Linux. Aplique a separação de privilégios. Estabeleça contas monitoradas separadas para tarefas administrativas. Separe-as de suas contas padrão de usuário final e contas de auditoria.

Gerenciar contas privilegiadas

Sob a regra da confiança em ninguém, é importante gerenciar até mesmo contas privilegiadas legítimas. Comece com as verificações básicas de higiene cibernética. Por exemplo, certifique-se de que essas contas não usem senhas padrão. Lembre-se de que os invasores roubam contas privilegiadas para iniciar ataques internos e não são detectados. Portanto, as contas privilegiadas devem ser verificadas quando se conectam à rede. Enquanto a sessão estiver em andamento, use as ferramentas do PAM para continuar monitorando a atividade da conta. Investigue qualquer desvio no comportamento do usuário para garantir que uma conta não tenha sido comprometida. As atividades de risco identificadas devem acionar automaticamente o encerramento da sessão para proteger contra o uso indevido de privilégios. Exerça os mesmos níveis de gerenciamento e supervisão em relação a fornecedores e prestadores de serviços terceirizados com acesso privilegiado aos seus sistemas. Monitore de perto os fornecedores terceirizados e as sessões privilegiadas dos fornecedores ou até mesmo as sessões de sombra. Encerre qualquer sessão que pareça suspeita ou viole políticas de acesso privilegiado.

Automatize e integre

Para estabelecer total visibilidade e controle em seu modelo Zero Trust, automatize e integre ferramentas o máximo possível. Restrinja a experiência de solicitações de acesso privilegiado. Integre as ferramentas do PAM às suas ferramentas de gerenciamento de serviços de TI. Crie fluxos de trabalho para gerenciar solicitações just-in-time para o aumento de privilégios a partir de suas ferramentas de gerenciamento de serviços. Além disso, use fluxos de trabalho automatizados para revogar o acesso temporário com eficiência. Evite a ocorrência de um cenário do tipo “configurar e esquecer”. Impeça que hackers encontrem contas órfãs ou abandonadas e aumentem privilégios. Adicione fluxos de trabalho automatizados para identificar e remover essas contas e economizar tempo de detecção no futuro. Às vezes, os administradores confiáveis acessam contas e fazem alterações fora das ferramentas de proteção do PAM. Erradique esses pontos cegos. O compartilhamento de dados e a correlação de eventos com outras ferramentas, como gerenciamento de eventos e informações de segurança (SIEM), dão suporte à sua abordagem Zero Trust. É mais fácil detectar o acesso ou as anomalias em operações de acesso privilegiado dentro e fora do ambiente do PAM com mais informações.

Esteja pronto para auditoria

Os padrões de conformidade e as normas do setor, como SOX, HIPAA e PCI DSS, exigem que as organizações rastreiem e monitorem o acesso a sistemas críticos e comprovem aos auditores que os controles de segurança necessários estão em vigor. Use as ferramentas do PAM para aliviar a sobrecarga de auditoria. As ferramentas do PAM devem registrar, monitorar e auditar qualquer acesso privilegiado e atividade de sessão privilegiada. Certifique-se de registrar os dados sobre as

aprovações de acesso também. Relatórios granulares e gravações de sessão à prova de violações facilitam a melhor governança e a responsabilidade pelo acesso privilegiado.

Como o ManageEngine pode ajudar na sua jornada Zero Trust

À medida que as organizações adotam ambientes de trabalho remotos ou híbridos e recorram a modelos Zero Trust para proteção, é essencial garantir que nenhum acesso privilegiado a sistemas críticos, dados ou outros ativos seja deixado não gerenciado, desconhecido ou não monitorado. A ManageEngine fornece soluções para gerenciar contas de usuários privilegiados, acesso de administrador a ativos de TI críticos e requisitos de conformidade. O PAM360 da ManageEngine é uma solução abrangente de gerenciamento de acesso a privilégios facilmente incorporada ao modelo Zero Trust de uma organização. Ele defende as organizações contra o uso indevido de privilégios, regulando o acesso a informações confidenciais da empresa. O PAM360 ajuda a gerenciar o acesso à infraestrutura de TI como um todo, incluindo bancos de dados, switches, roteadores, firewalls, e balanceadores de carga. A solução incorpora governança de acesso avançada e privilegiada, automação do fluxo de trabalho e lógica analítica avançada.

O PAM360 também inclui integrações contextuais com vários serviços de TI para uma correlação mais profunda dos dados de acesso privilegiado e dos dados gerais da rede. Essas integrações permitem controle e governança mais rígidos sobre suas permissões administrativas e acesso em toda a sua infraestrutura de TI: usuários, sistemas e aplicações.

Suporte à governança de contas

A primeira etapa para Zero Trust é entender seu ambiente de segurança. O PAM360 descobre automaticamente todas as contas privilegiadas na infraestrutura de TI, incluindo aplicações em nuvem. A solução pode redefinir remotamente senhas de contas para contas de administrador local do Windows e contas de rota do Linux. É simples capturar todos os eventos associados a contas privilegiadas, como relatórios e logs de auditoria ricos em contexto. Relatórios granulares e gravações de sessão facilitam a governança e fornecem melhores percepções sobre sessões privilegiadas. O PAM360 fornece um ponto crucial de gerenciamento para auditoria e conformidade. Evite lutar para reunir dados para auditorias de conformidade no último minuto; demonstre prontamente a conformidade com auditores e investigadores forenses usando os relatórios prontos do PAM360 sobre várias normas de conformidade, como PCI-DSS, NERC-CIP, ISO/IEC 27001 e RGPD.

Privilégio elevado

O PAM360 é uma ferramenta poderosa para regular privilégios. Ele permite a autorização, atribuição e rastreamento de controles para contas de domínio e contas locais. O software pode aumentar privilégios com um cronograma limitado, o que reduz o risco de exposição contínua. Para solicitações de acesso just-in-time, o PAM360 conta com um mecanismo de fluxo de trabalho de solicitação/aprovação, para que os usuários enviem uma solicitação. Com aplicações para iPhone, Android e Windows, os administradores podem autorizar solicitações de qualquer lugar.

Onde várias equipes possuem um único dispositivo, aprovações duplas também são possíveis com o PAM360.

Privilégios de monitoramento

Depois que os privilégios são concedidos conforme a abordagem de confiar em ninguém, é vital monitorar de perto as atividades dos usuários privilegiados. O PAM360 fornece a capacidade de acompanhar sessões privilegiadas em tempo real, por exemplo, para verificar atividades de fornecedores ou prestadores de serviços terceirizados. A solução permite o encerramento imediato da sessão em caso de detecção do uso indevido de privilégios. O PAM360 também pode gravar, salvar e reproduzir uma sessão como um arquivo de vídeo, para fins de rastreamento e auditoria.

Gerenciando sessões

Para impedir o acesso não autorizado e garantir que os sistemas estejam seguros, os administradores de TI devem desativar as permissões de acesso SSH e os serviços de desktop remoto em dispositivos corporativos. O PAM360 atua como um gateway para iniciar uma sessão remota, iniciar conexões remotas e fazer login em máquinas de destino por meio de conexões RDP, SSH, SQL, VNC ou Web. Aproveite a função do PAM360 para controle granular e para restringir as atividades do usuário. A solução pode controlar a quais aplicações um usuário tem acesso por meio de capacidades da lista de permissões.

Automatização e integração de fluxos de trabalho

O apoio do PAM360 a um modelo Zero Trust é amplo. A integração contextual do PAM360 com aplicações e dispositivos em toda a infraestrutura de TI permite a automação de tarefas e a visibilidade aprimorada. As organizações podem eliminar credenciais codificadas nos scripts de automação com o PAM360. A solução se integra às ferramentas DevOps para buscar credenciais em tempo real. Use a API RESTful e a API SSH CLI para substituir nomes de usuário e senhas em scripts do PowerShell, arquivos de configuração ou em qualquer lugar em que haja credenciais codificadas. Integre o PAM360 com ferramentas robóticas de automação de processos para buscar credenciais com segurança e entregá-las aos bots para realizar operações.

O PAM360 também se integra às suas ferramentas de gerenciamento de serviços de TI. Essa integração permite que solicitações e aprovações de credenciais sejam realizadas no ambiente ITSM. Sem o contexto necessário, é fácil ser enganado por pontos cegos e incidentes de insegurança. O PAM360 combina dados privilegiados com logs de eventos de endpoint para correlação de eventos com reconhecimento de contexto. A integração com ferramentas SIEM permite encaminhar todos os dados brutos de auditoria do PAM360 para soluções SIEM, como o Splunk, para obter percepções

mais detalhadas. As integrações garantem acesso completo, aumentando a conscientização e a visibilidade para permitir decisões mais informadas.

Gerenciando chaves SSH e certificados SSL

Gerencie chaves SSH e certificados SSL com facilidade. O PAM360 fornece um repositório centralizado para armazenar chaves SSH para administração do ciclo de vida e aplicação de políticas. A solução detecta e remove chaves não utilizadas, além de gerar e implantar novas chaves nos sistemas de destino. Além disso, o PAM360 descobre, consolida e gerencia certificados SSL. A solução pode enviar alertas de expiração e verificar as certificações quanto a vulnerabilidades. Ele também pode automatizar fluxos de trabalho para geração de certificados.

Detectando anomalias

Quanto mais rápido você conseguir descobrir ameaças prejudiciais, mais rápido poderá limitar os danos. Integrando-se ao Analytics Plus do ManageEngine, o PAM360 permite uma análise abrangente das atividades de contas privilegiadas. Inteligência artificial e capacidades de aprendizado de máquina

podem detectar continuamente as atividades suspeitas e prejudiciais. Usando dados do PAM360, uma avaliação de risco e uma pontuação de risco são designadas para cada operação. Se uma pontuação de risco for violada, uma notificação de limiar será enviada. A solução pode acionar controles de mitigação, como o encerramento da sessão. Ela aprende continuamente o comportamento e os padrões do usuário para detectar anomalias.

Um sinal de alerta

O trabalho remoto, as plataformas em nuvem e as aplicações em nuvem redefiniram o perímetro de segurança de uma organização. Os líderes de gerenciamento de riscos e segurança devem reavaliar o perímetro de segurança e fortalecer as defesas com Zero Trust. O modelo abrange nosso ambiente de trabalho pandêmico e pós-pandêmico, protegendo os usuários independentemente de sua localização ou dispositivo. Em vez de proteger o perímetro da rede, uma abordagem Zero Trust realoca medidas de segurança restritas à aplicação, sistema ou recurso que precisam de proteção.

Para que você fique em uma posição forte e construa uma base Zero Trust, aproveite toda a extensão das práticas e processos do PAM aplicadas pelas capacidades de ferramentas eficazes. Use as ferramentas do PAM para aproveitar a funcionalidade de auditoria a fim de identificar uma linha de base e continuar a geração de relatórios. Aplique políticas mais granulares. Introduza fluxos de trabalho para solicitar e revogar o acesso. Verifique o acesso de administrador e privilegiado aos seus sistemas. Registre e monitore as sessões de acesso continuamente. Mitigue ataques e use o PAM como a base de um modelo Zero Trust. De muitas maneiras, a covid-19 serviu como um sinal de alerta.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton, CA
94588, USA
US +1 888 204 3539
Reino Unido: +44(20)35647890
Austrália: +61 2 80662898
www.manageengine.com/pam360

PAM360
ManageEngine