ManageEngine
PAM360

Prepare-se para o seguro cibernético com o ManageEngine PAM360

A lista de verificação completa do PAM para todas as suas necessidades de seguro cibernético

O seguro cibernético protege os interesses das organizações no caso de incidentes relacionados à infraestrutura e à segurança da rede de TI.

Nos últimos 3 anos, os pagamentos de seguro cibernético aumentaram em 200%, com o número máximo de sinistros chegando a 8.100 somente em 2021. Embora o número de sinistros possa parecer exorbitante, um estudo de mercado sugere que apenas 55% de todas as organizações têm apólices de seguro cibernético em vigor.

Consequentemente, isso fez com que as apólices de seguro cibernético se tornassem mais rigorosas, com altos custos de prêmio e vigilância obrigatória sobre a segurança de todas as entidades de TI.

Os provedores de seguro cibernético reconhecem os controles de gerenciamento de acesso a privilégios (PAM) como essenciais para a postura de segurança de uma organização. Esses controles desempenham um papel fundamental no impedimento de diversas ameaças cibernéticas e na redução das ramificações de uma violação de dados.

Neste e-book, exploraremos como uma solução de PAM pode ajudá-lo a atender a esses requisitos complexos de seguro cibernético. Vamos nos concentrar especificamente em como o PAM360 implementa ideologias críticas de PAM que otimizarão a sua próxima aquisição de seguro cibernético para garantir que você seja considerado elegível para custos de prêmio minimizados e indenizações de seguro maiores.

Requisitos de seguro cibernético	Práticas recomendadas	Como o PAM360 ajuda
Sua organização tem alguma medida em vigor para gerenciar identidades privilegiadas?	Descubra, agrupe, regule e compartilhe com segurança todas as identidades privilegiadas na rede de TI da organização.	O PAM360 pode descobrir, consolidar e integrar usuários e endpoints de uma série de serviços de diretório corporativo na solução. Em seguida, ele atribui funções e responsabilidades específicas a esses usuários e endpoints privilegiados, respectivamente, e os agrupa de acordo com os requisitos exigidos pela política de acesso da organização. Com o PAM360, você pode compartilhar de forma seletiva e segura essas contas privilegiadas em endpoints remotos com usuários privilegiados.
Todos os funcionários da sua organização usam a autenticação multifator (MFA) ao fazer login nos ativos e no software de TI da empresa?	Autentique os usuários que fazem login na solução com credenciais armazenadas no respectivo diretório e aplique a MFA a todos os usuários do ativo ou software de TI.	O PAM360 oferece uma ampla gama de integrações com todas as soluções MFA de toda a empresa, como Google Authenticator, Microsoft Authenticator, Okta Verify, RSA SecurID, YubiKey, entre outras. Também vem com uma aplicação TOTP nativo, o Zoho OneAuth, que suporta a autenticação de usuário baseada em biometria.

Requisitos de seguro cibernético	Práticas recomendadas	Como o PAM360 ajuda
Que medidas sua organização toma para prevenir, detectar e impedir ataques de ransomware?	Evite a manipulação de malware implementando o acesso regulamentado aos endpoints, aplique o princípio dos quatro olhos para solicitações de acesso, padronize a prática do privilégio mínimo e aplique a segmentação rigorosa da rede.	O PAM360 permite o compartilhamento seletivo de contas privilegiadas em endpoints remotos para usuários individuais ou a um grupo, verificando as funções e responsabilidades do usuário. Também permite o compartilhamento dessas informações privilegiadas por meio de fluxos de trabalho de solicitação e liberação de senhas. Essas solicitações de acesso são primeiro levantadas pelo usuário com uma finalidade mencionada e, em seguida, recebem a aprovação de um administrador selecionado. Os administradores podem configurar o acesso temporário, monitorado e just-in-time (JIT) a recursos altamente privilegiados por meio de controles nativos de gerenciamento de delegação e elevação de privilégios (PEDM) que podem encerrar a sessão em caso de atividade suspeita. Usando o módulo de controle de acesso baseado em políticas (PBAC) do PAM360, os administradores podem criar políticas de acesso personalizáveis com base nas pontuações de confiança do usuário e do dispositivo e em outros fatores vitais. Os índices de confiança são derivados dinamicamente com base em vários parâmetros de segurança, como legitimidade da rede, comportamento do usuário e do terminal, entre outros. Para cada privilégio concedido a um usuário, nossa solução coloca uma proteção contra falhas que monitora, evita, detecta e impede que esses privilégios sejam usados indevidamente.

Requisitos de seguro cibernético	Práticas recomendadas	Como o PAM360 ajuda
Sua organização controla todas as atividades privilegiadas na rede??	Audite e registre todas as atividades privilegiadas em relação a quem, quando e onde uma sessão foi iniciada, e registre quais atividades foram realizadas durante essas sessões. O "o quê" pode incluir, entre outras coisas, alterações de senha, solicitações de acesso aprovadas e negadas, sessões remotas e usuários e recursos integrados e não integrados.	As auditorias e os relatórios do PAM360 são um arquivo abrangente de todas as atividades realizadas por todos os usuários da solução. As auditorias e os relatórios variam amplamente, desde relatórios de atividades de endpoints e usuários e relatórios de sessões privilegiadas (ativas e registradas) até relatórios de chaves SSH e operações de certificados SSL/TLS. Além disso, o PAM360 oferece aos usuários a capacidade de gerar relatórios usando a linguagem de consulta estrutural (SQL). O esquema completo do banco de dados do PAM360 está disponível para ser aproveitado pelos administradores do banco de dados, com base no qual os usuários podem regular a geração de relatórios com consultas ao banco de dados para atender aos requisitos da SOX e da HIPPA. O PAM360 permite que as empresas registrem todas as atividades privilegiadas realizadas por meio da solução que as equipes de segurança usam para auditorias e fins forenses.
Todos os seus funcionários têm acesso de administrador?	Separe o acesso administrativo para usuários privilegiados e conceda acesso com privilégios mínimos para outros.	O PAM360 trabalha com o princípio do menor privilégio. Cada controle, por padrão, é deslocado funcionalmente para fornecer o menor privilégio necessário para um usuário específico. Essa funcionalidade é totalmente personalizável e permite que as organizações implementem funções de usuário exclusivas para aplicar o controle de acesso baseado em funções.

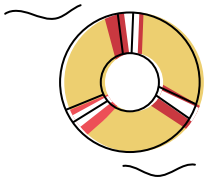
Requisitos de seguro cibernético	Práticas recomendadas	Como o PAM360 ajuda
		Todos os recursos e funcionalidades são ajustados de forma coerente para refletir o princípio do menor privilégio em toda a empresa, limitando assim o acesso de administrador a usuários seletivos que precisam dele, quando precisam.
A sua organização possui controles para auxiliar no backup e na recuperação no caso de um incidente cibernético?	Faça backup de dados essenciais, implemente medidas de emergência e garanta a rápida restauração de dados com base em critérios predefinidos.	A configuração break-glass do PAM360 ajuda os usuários a fazer backup de todas as identidades privilegiadas e garante a ativação automática de mecanismos à prova de falhas com base nos critérios selecionados pelo administrador. Os serviços de failover do PAM360 são totalmente automatizados para operar em situações adversas; eles não exigem intervenção manual. Inevitavelmente, se o imprevisto ocorrer, use o servidor de backup somente leitura para fornecer acesso ininterrupto a todos os seus dados críticos. Esses recursos de break-glass e acesso off-line também podem ser acessados remotamente por meio de aplicações móveis para dispositivos portáteis Android e iOS. Observe que esses recursos e procedimentos de backup só podem ser acessados por usuários com privilégios elevados, evitando assim a ativação não autorizada de medidas de emergência.

Requisitos de seguro cibernético	Práticas recomendadas	Como o PAM360 ajuda
As soluções de TI de sua organização estão em conformidade com os padrões de software mais recentes??	Atenda aos requisitos críticos de TI, como diretrizes governamentais ou padrões reconhecidos, reconhecendo as recomendações estabelecidas pelas normas de proteção de dados.	O PAM360 oferece geração de relatórios prontos para uso para regulamentações governamentais e do setor, como PCI DSS, ISO/IEC 27001, NERC CIP e GDPR. Esses relatórios podem ser obtidos por cláusula ou integralmente, dependendo do requisito. A solução PAM examina seus endpoints para validar se eles estão em conformidade ou em violação do respectivo padrão. No caso de uma violação, o PAM360 sugerirá etapas de correção.
Como sua organização evita a expiração despercebida de certificados de sites e chaves de dispositivos de rede?	Crie, proteja, implante e gerencie certificados SSL/TLS para sites, outros endpoints e chaves SSH de rede.	O módulo nativo de gerenciamento de certificados e chaves do PAM360 oferece gerenciamento de ciclo de vida de ponta a ponta de certificados SSL/TLS e chaves SSH por meio de integrações abrangentes com autoridades de certificação de terceiros, como GoDaddy, Verisign, DigiCert, Thawte e outras. O PAM360 também alerta os administradores antes da expiração de tais certificados e chaves essenciais, capacitando-os com governança e gerenciamento completos de certificados e chaves. Isso reduz significativamente a sobrecarga administrativa que surge naturalmente ao gerenciar certificados e chaves manualmente. O PAM360 elimina a necessidade de uma solução de TI autônoma para gerenciar chaves SSH e certificados SSL/TLS.

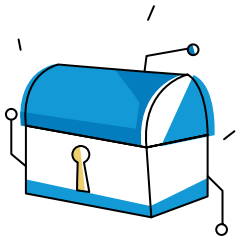
As perguntas listadas acima são derivadas de requisitos críticos de seguro cibernético que as seguradoras usam para testar a elegibilidade de seus clientes em potencial para taxas de prêmio mais baixas e indenizações de seguro mais altas.

Em resumo, espera-se que as organizações implementem:

Autenticação multifator



Medidas estatutárias contra ataques cibernéticos



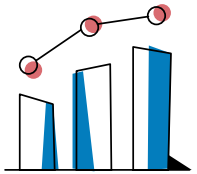
Cofre secreto com acesso central

Compartilhamento de segredos monitorado

Certificação regulamentada de ativos de TI

Software que facilita a obtenção de padrões de conformidade

Mecanismos de backup confiáveis



Trilhas de auditoria obrigatórias de todas as atividades privilegiadas

Otimize seu processo de seguro cibernético com o PAM360

O ManageEngine PAM360 é o principal produto da suíte de gerenciamento de acesso privilegiado da ManageEngine. A ferramenta é reconhecida pelos analistas do setor por suas opções flexíveis de implementação, facilidade de uso, manutenção e recursos de uso rápido, projetados para reduzir a fadiga operacional e priorizar a segurança acima de tudo.

O PAM360 é ajustado e auditado regularmente para atender aos requisitos anuais de seguro cibernético e está atualizado com as métricas de seguro de 2023. Dito isso, mais de 5.000 clientes de todo o mundo confiam no pacote PAM da ManageEngine para atender aos requisitos de elegibilidade de seguro cibernético para reduzir os premiums de seguro e aumentar os pagamentos.

Reduza a superfície de ataque e atenda efetivamente às suas necessidades de seguro cibernético com o PAM360

Converse com nossos especialistas

Inicie um teste gratuito