ManageEngine
ADManager Plus

5 sinais reveladores de que você está caminhando para uma VIOLAÇÃO DE CONFORMIDADE

www.admanagerplus.com

Overview

Quando se trata de gerenciar identidades e direitos de acesso dos usuários, o Active Directory (AD) desempenha um papel vital. As alterações feitas no AD não afetam apenas a segurança de uma empresa, mas também afetam sua conformidade com os regulamentos de TI. Não é nenhuma surpresa que os auditores de conformidade estejam interessados em revisar as atividades realizadas no AD.

A penalização por não conformidade pode resultar em multas pesadas, bem como na perda da confiança do cliente nas empresas. É melhor verificar de forma proativa e regular a postura de conformidade da sua empresa para evitar o nervosismo de última hora que você possa sentir em uma auditoria de conformidade.

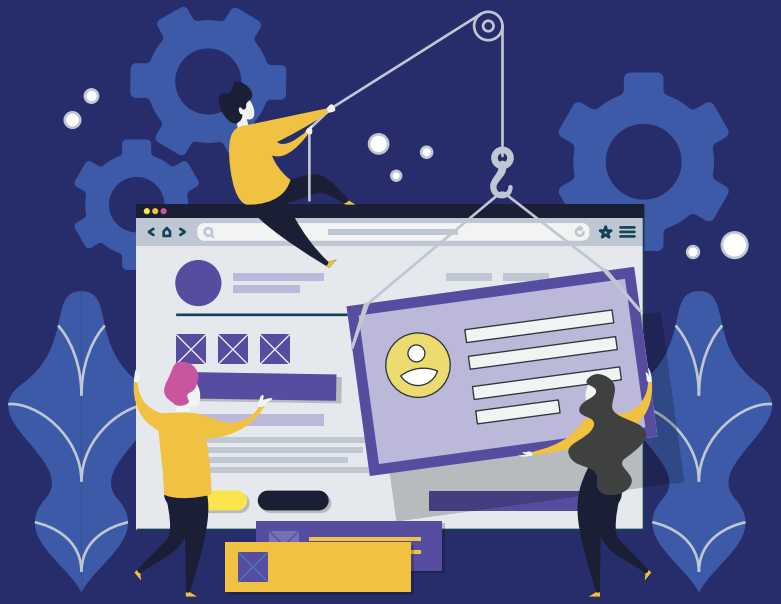
Sinal 1

SISTEMA DE GERENCIAMENTO SEM

Fazer alterações nas permissões do AD sem que elas sejam revisadas primeiro pode, sem querer, expor dados comerciais confidenciais a vulnerabilidades de segurança. É essencial ter uma política de controle de acesso em vigor para cada ação crítica feita no AD para evitar que os usuários obtenham privilégios não autorizados. O melhor curso de ação é seguir um processo de análise em que cada solicitação de alteração do usuário é avaliada por um gerente antes de ser transferida para um administrador de TI. Cada solicitação, como acesso a compartilhamentos essenciais ou alterações na associação ao grupo, deve ser analisada por um gerente de TI ou líder de equipe para garantir que os recursos corporativos não sejam comprometidos

O ADManager Plus da ManageEngine permite fluxos de trabalho personalizáveis que ajudam você a otimizar e monitorar as tarefas do AD. Com esse recurso, os usuários podem gerar solicitações de acesso a recursos que podem ser analisadas por uma autoridade designada antes que o administrador de TI execute a tarefa.

SAIBA MAIS



Sinal 2

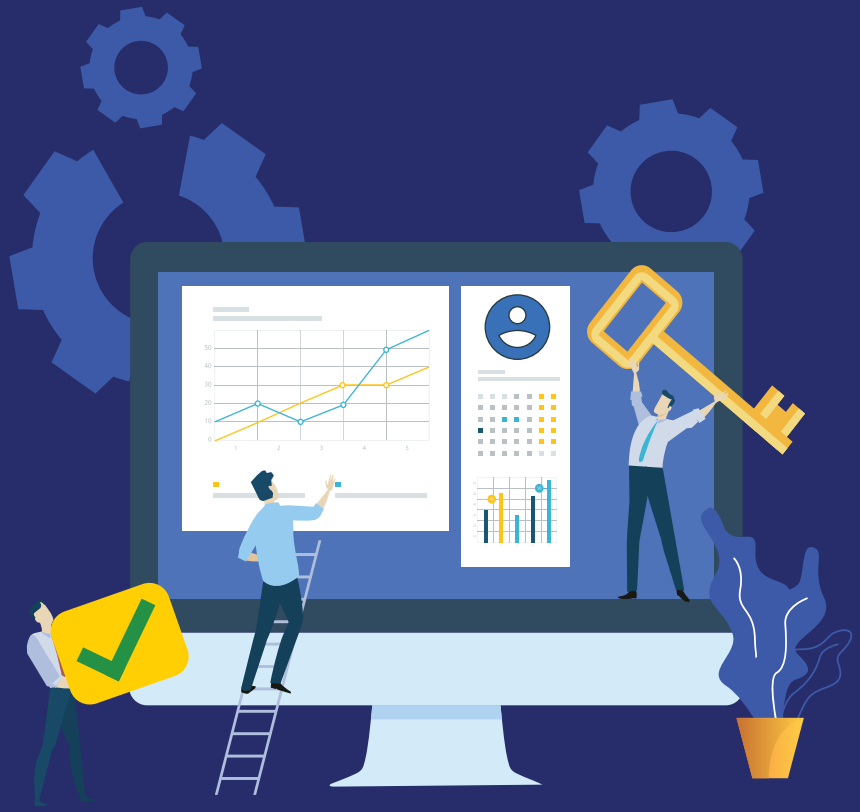
SEM PRIVILÉGIOS BASEADOS EM FUNÇÕES

Os administradores de TI criam contas de usuário rotineiramente, atribuem a elas permissões relevantes e modificam os privilégios existentes. Se não houver uma lista de verificação contendo detalhes de acesso do usuário por departamento, os administradores de TI não poderão conceder permissões aos usuários de maneira uniforme. Às vezes, os usuários são adicionados aos grupos errados, o que pode fazer com que eles tenham permissões excessivas ou menos privilégios do que os necessários para sua função.

Por exemplo, um funcionário de marketing e um funcionário de RH devem ter permissões para diferentes recursos específicos para suas funções. Da mesma forma, quando os usuários estão sendo transferidos para um local diferente, eles devem ter acesso aos recursos que seu trabalho exige e nada mais.

O ADManager Plus tem modelos personalizáveis para agilizar a criação e modificação de objetos do AD; você também pode definir regras e atributos com base em grupos de segurança, horas de login e detalhes de contato que podem ser atualizados automaticamente com base no departamento ou na função.

SAIBA MAIS



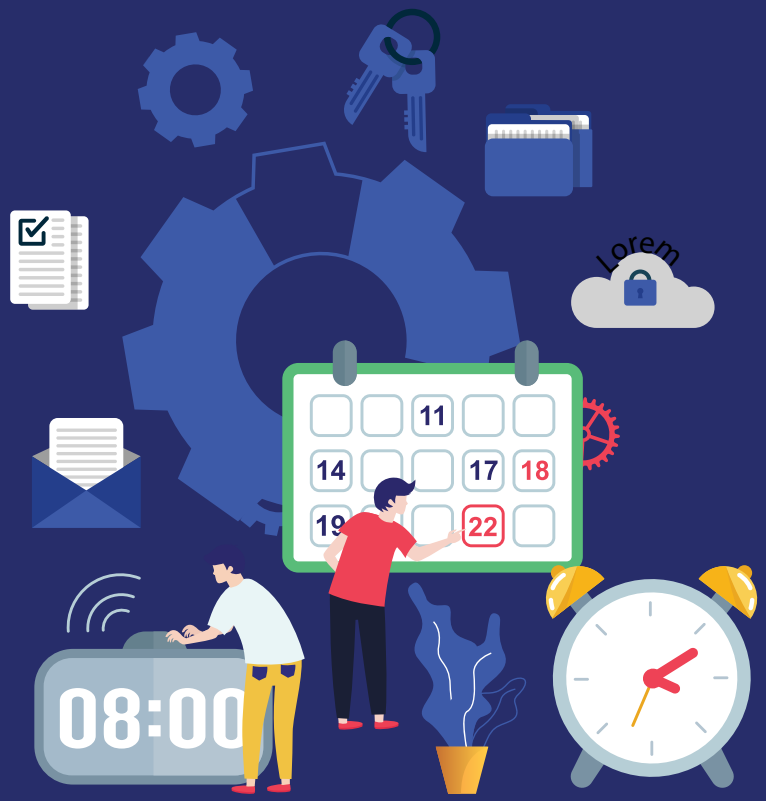
Sinal 3

AUMENTO DE PRIVILÉGIO

Quando os usuários ingressam na organização, os administradores de TI concedem a eles permissões para acessar recursos relevantes para suas funções de trabalho. Com o tempo, para diferentes tarefas ou projetos, os usuários podem receber permissão para recursos diferentes. Esses direitos de acesso devem ser revogados após a conclusão da tarefa. É uma boa prática que os administradores de TI revisem periodicamente todos os direitos de acesso do usuário por função em relação a uma lista de verificação de permissões. Os usuários podem ter acesso a grupos de segurança de alto nível ou a pastas e arquivos importantes que não são mais necessários para suas funções. Rastrear periodicamente todas as permissões atribuídas aos usuários para um projeto específico e revogá-las após a conclusão do projeto resolve esse problema; no entanto, essa tarefa pode ser entediante.

O ADManager Plus oferece um recurso automatizado de gerenciamento de permissões de grupo com limite de tempo para que os administradores de TI possam atribuir usuários a grupos específicos e revogá-los após um período de tempo especificado. Além disso, a ferramenta fornece relatórios predefinidos sobre NTFS e permissões de compartilhamento para que você possa identificar servidores e compartilhamentos em sua organização e verificar o nível de acesso que cada usuário ou grupo tem a eles.

SAIBA MAIS



Sinal 4

FALTA DE REVISÃO PERIÓDICA

Está preparando relatórios para autoridades de conformidade de último hora? É essencial identificar o acesso não autorizado a arquivos e pastas essenciais com bastante antecedência para que você possa tomar medidas corretivas e evitar problemas de não conformidade. Uma prática recomendada é verificar periodicamente as permissões de acesso. Se você não tem informações sobre quem pode acessar pastas confidenciais e quem pertence a quais grupos de segurança, é apenas uma questão de tempo até que a segurança de dados da sua organização esteja em risco. A maioria das ferramentas nativas não oferece a flexibilidade de obter informações granulares do AD por meio de relatórios. Alertas em tempo real sobre quando uma conta de usuário, grupo de segurança ou senha é alterada podem solicitar que você tome medidas imediatas.

O ADManager Plus fornece relatórios acionáveis e predefinidos para regulamentos de conformidade PCI DSS, SOX, HIPAA, GLBA, GDPR, POPIA e FISMA.

Você também pode automatizar todo o processo de emissão de relatórios de conformidade ao agendar relatórios para que sejam enviados às principais partes interessadas responsáveis pelo gerenciamento dos programas de conformidade.

SAIBA MAIS

Sinal 5

AUMENTO DE CONTAS BUILD UP

A manutenção da TI é uma parte importante da prevenção contra invasores entrando sem autorização nos recursos de uma empresa. Contas de usuário e computadores inativos são pontos de entrada para cibercriminosos que desejam obter acesso a contas com permissões elevadas ou acessar remotamente arquivos confidenciais e dados financeiros. Também é arriscado deixar desprotegidos quaisquer grupos de segurança que concedem permissões.

Usando o ADManager Plus, você pode configurar o desprovisionamento usando uma automação que identifica objetos inativos, remove seus privilégios, move-os para um contêiner diferente e exclui suas contas. Para simplificar esse processo, o recurso de política Desativar/Excluir no ADManager Plus permite remover contas associadas do Microsoft 365 e do Google Workspace, exportar a caixa de correio do usuário para um local específico e revogar as licenças de software aplicáveis.

SAIBA MAIS

Baixe um teste gratuito de 30 dias para testar esses recursos e aproveitar todos os benefícios que o **ADManager Plus oferece.**

Obter cotação Download

Nossos produtos

AD360 | Log360 | ADAudit Plus | ADSelfService Plus | M365 Manager Plus | RecoveryManager Plus

ManageEngine
ADManager Plus

O ADManager Plus é uma solução IGA (Identity Governance and Administration), ou seja, uma solução de governança e administração de identidades que simplifica o gerenciamento de identidades, garante a segurança e aprimora a conformidade. Com o ADManager Plus é possível gerenciar o ciclo de vida do usuário, do provisionamento ao desprovisionamento, executar campanhas de certificação de acesso, orquestrar o gerenciamento de identidades em aplicativos corporativos e proteger os dados em suas plataformas corporativas com backups regulares. Use mais de 200 relatórios para obter informações valiosas sobre identidades e seus direitos de acesso. Melhore a eficiência de suas operações de IGA com workflows, automações e políticas de controle de acesso baseadas em funções. Os aplicativos Android e iOS do ADManager Plus ajudam no gerenciamento dinâmico do AD e do Azure AD. Para obter mais informações sobre o ADManager Plus, acesse manageengine.com/products/ad-manager/.