ManageEngine

Como as soluções de segurança de TI podem ajudar a atender aos

Requisitos GDPR com Facilidade

Um guia de soluções para administradores de segurança de TI

www.manageengine.com

Índice

O GDPR e seu papel na resolução de problemas de segurança

Com o advento de violações de dados mais sofisticadas contra empresas, uma regulamentação rigorosa era inevitável. O Regulamento Geral sobre a Proteção de Dados (GDPR) da UE cumpre legitimamente esse propósito. O GDPR tem como objetivo unificar e padronizar a coleta de dados pessoais e métodos de processamento em toda a UE. O GDPR estende o seu âmbito de aplicação territorial. O regulamento é aplicável a todas as empresas que coletam e processam dados pessoais de cidadãos da UE, independentemente da sua localização. As organizações devem entrar em conformidade com o GDPR antes de 25 de maio de 2018, mesmo que o tratamento de dados aconteça fora da União Europeia.

O que torna o GDPR especial?

Além das duras penas de violação dos seus critérios, as regras do GDPR para coleta e tratamento de dados fazem dele um dos mais rigorosos mandatos de regulamentação. Com o advento dos ataques “zero-day”, ameaças persistentes avançadas (APT), e outros ataques sofisticados, o GDPR insiste que as organizações que lidam com dados pessoais adotem medidas técnicas adequadas e técnicas de avaliação de risco para proteger seus dados. No entanto, os órgãos reguladores da UE também perceberam que a proteção de dados contra violações não é sempre possível. Apesar da adoção e implementação de medidas de segurança adequadas, ainda há uma grande chance de ataques de segurança acontecerem em instalações de rede. Portanto, as organizações devem ser instruídas sobre o que fazer e o que não fazer em caso de violação de dados.

O que há neste guia de soluções

Este guia de soluções dá detalhes sobre os requisitos do GDPR em matéria de medidas de segurança que as organizações devem adotar durante o manuseio de dados pessoais. Ele também ilustra como as soluções da ManageEngine podem ajudar as organizações a cumprirem estes requisitos com facilidade.

Atendendo aos critérios do GDPR com as soluções da ManageEngine

O Log360 e o DataSecurity Plus, duas soluções de segurança de TI da ManageEngine, ajudam as organizações a cumprirem perfeitamente os requisitos relacionados a manter dados pessoais seguros e auditar métodos de processamento de dados

O Log360 é uma solução abrangente de SIEM que coleta, processa e analisa dados de log de fontes em toda uma rede. Ele audita alterações críticas para o Active Directory em tempo real e imediatamente notifica os administradores sobre incidentes anômalos de segurança, tentativas de violação de dados ou ataques de segurança. O Log360 é uma integração de duas poderosas ferramentas de auditoria da ManageEngine, o EventLog Analyzer e o ADAudit Plus. Enquanto o EventLog Analyzer resolve qualquer adversidade no gerenciamento de logs e ajuda a detectar e combater ataques de segurança externa, o ADAudit Plus audita extensivamente o Active Directory para monitorar as atividades dos usuários e, assim, evitar ameaças internas.

O DataSecurity Plus é uma solução de segurança e visibilidade dos dados que oferece descobrimento de dados, análise de armazenamento de arquivos e auditoria, alertas e relatórios do servidor de arquivos do Windows. Ele localiza, analisa e protege dados pessoais sensíveis em seus arquivos e, pastas e compartilhamentos contra várias ameaças internas e externas. Ganhe visibilidade sobre as tendências de uso de dados, padrões de acesso a arquivos, volume de dados pessoais em arquivos, alterações de permissões de arquivos e muito mais. O DataSecurity Plus ajuda você a atender aos vários regulamentos de conformidade e gerar registros de auditorias claros e concisos para uso como provas legais.

Além destas soluções, a ManageEngine também tem as soluções abaixo, que podem ajudar as empresas a cumprir os requisitos de auditoria e monitoramento específicos para a tecnologia e as plataformas que utilizam.

ADManager Plus, uma solução de gerenciamento e produção de relatórios baseada em web do Active Directory que ajuda a verificar as permissões atribuídas aos usuários para acessar os dados pessoais.

Exchange Reporter Plus, uma solução abrangente de produção de relatórios, auditoria e gerenciamento do Exchange server que ajuda a tomar conta da transmissão de dados pessoais por e-mail.

O365 Manager Plus, uma extensa ferramenta de auditoria e produção de relatórios do Office 365 que ajuda a garantir que todas as atividades acontecendo no Office 365 estejam em conformidade com os requisitos do regulamento.

Resumo rápido

As ferramentas da ManageEngine ajudam as organizações a entrarem em conformidade com vários artigos do GDPR, incluindo:

- **Capítulo 2**
  - Artigo 5º - 1(b), 1(d) e 1(f) e 2
- **Capítulo 4**
  - Artigo 24º - 1
  - Artigo 25º - 2
  - Artigo 32º - 1(b), 1(d), 2 e 4
  - Artigo 33º - 1, 2 e 3(a)

Adotar medidas técnicas para conformidade com o GDPR

O GDPR insiste que as empresas tomem “medidas técnicas para garantir a segurança de dados”. Por que o GDPR usa uma linguagem genérica nessa afirmação? Porque as empresas não têm, todas, a mesma arquitetura de rede.

Dependendo da atividade, a rede de cada organização é única. Algumas podem ser uma área com Windows usando o Microsoft Active Directory para gerenciar seus recursos computacionais e contas de usuário, enquanto outras podem também ser áreas sem Windows. Algumas empresas podem usar os Exchange servers para gerenciar suas caixas de entrada, enquanto outras podem hospedá-las em nuvem.

Redes organizacionais nunca podem ser generalizadas. É por isso que o GDPR afirma que, independentemente da tecnologia adotada ou sistemas usados, as empresas devem adotar as medidas técnicas adequadas para garantir a segurança dos dados pessoais. Isso traz uma única opção para as empresas: monitorar e auditar os sistemas e processos que armazenam ou interagem com dados pessoais. Mas não se preocupe! Nós temos o que você precisa.

A ManageEngine também tem uma série de soluções que ajudam as empresas a cumprir os requisitos de auditoria e monitoramento específicos para a tecnologia e as plataformas que utilizam.

- O ADManager Plus, uma solução abrangente de gerenciamento e produção de relatórios para o Active Directory, ajuda a auditar e gerenciar as permissões concedidas aos usuários para acessar dados pessoais.
- Se você usa o Office 365, então o O365 Manager Plus, nossa extensa ferramenta de monitoramento e auditoria do Office 365, pode ajudá-lo a monitorar o fluxo de dados pessoais para mantê-lo seguro.
- Você está usando Exchange servers para hospedar os seus e-mails? Você quer tomar conta das transações por e-mail e garantir que dados pessoais não sejam transferidos por e-mail? O Exchange Reporter Plus, uma solução completa de análise e produção de relatórios para o Exchange, pode ajudá-lo com isso.

Os critérios e o mapeamento de recursos

Esta seção dá detalhes sobre os requisitos de segurança de dados do GDPR, os passos que as organizações devem tomar para atender a esses requisitos, e como as soluções da ManageEngine podem ajudar.

Artigo 5 - Princípios relativos ao tratamento de dados pessoais

Requisito	Como estar em conformidade	Como a ManageEngine pode ajudar
1 (b) “Os dados pessoais devem ser: Coletados para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89º (1) (‘limitação das finalidades’)...”	Na maioria das empresas, os dados pessoais são coletados e armazenados em um banco de dados ou em um servidor de arquivos. Para garantir que os dados estejam sendo tratados somente para a finalidade para a qual foram coletados, é necessário monitorar acessos a estes sistemas e aos dados pessoais. As empresas devem estar atentas ao acesso anormal, modificação e exclusão de dados pessoais, o que pode resultar em dados tratados de uma forma que não foi originalmente prevista. As notificações devem ser enviadas às autoridades competentes para tais atividades anormais.	No caso de dados pessoais armazenados em bancos de dados, o **Log360** ajuda as empresas a monitorarem alterações críticas com seu console de alerta em tempo real. Com perfis de alerta pré-elaborados, o Log360 pode gerar notificações instantâneas por e-mail ou SMS sempre que houver atividade anormal. Além disso, o Log360 também tem pacotes de relatórios que fornecem informações sobre as alterações para a tabela do banco de dados, incluindo: • Seleção • Criação • Alteração • Exclusão Se os dados estiverem armazenados em quaisquer servidores de arquivos do Windows, o **DataSecurity Plus** fornece relatórios de auditoria de acesso sobre:

		• Alterações de conteúdo e localização (arquivos/pastas criados, modificados, substituídos, movidos, restaurados, renomeados e excluídos). • Alterações de permissões de segurança (alterações de permissões, proprietário e SACL de arquivo/pasta). • Tentativas de acesso malsucedidas (leitura, gravação ou exclusão de arquivo/pasta). Os relatórios do DataSecurity Plus ajudam a detectar o tratamento de dados não autorizado.
1 (d) “Os dados pessoais devem ser precisos e, quando necessário, atualizados; todos os passos razoáveis devem ser tomados para garantir que os dados pessoais que são imprecisos, levando em conta as finalidades para as quais eles são processados, sejam apagados ou retificados sem demora (“precisão”) ...”	As empresas devem coletar insights sobre seu armazenamento de dados. Isso inclui a implementação de sistemas adequados que forneçam informações sobre quanto tempo os dados foram armazenados, de forma que possam ser apagados assim que o período de tempo limite para armazenamento for atingido.	O **DataSecurity Plus** fornece informações sobre arquivos antigos com seus relatórios de **análise de arquivos e análise de armazenamento,** que garantem a precisão dos dados e também ajudam com o processo de remoção mencionado no requisito 1 (d). Além disso, o **Log360** ajuda a monitorar a “precisão” dos dados pessoais armazenados em bancos de dados e alerta administradores em tempo real caso os dados forem violados. Os relatórios DataSecurity Plus, mencionados acima, e a capacidade de auditoria de banco de dados do Log360 ajudam a garantir a precisão dos dados pessoais e a estar atento a qualquer modificação não autorizada de dados pessoais armazenados em servidores de arquivos, servidores (incluindo servidores EMC e filtros NetApp) e bancos de dados (incluindo Oracle e MS SQL).

1 (f) “Os dados pessoais devem ser processados de maneira a garantir a segurança apropriada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou danos acidentais, utilizando medidas técnicas ou organizacionais apropriadas (“integridade e confidencialidade”)”.	Implemente soluções que avisam os responsáveis pela proteção de dados ou os administradores de segurança sempre que a integridade dos dados pessoais estiver comprometida.	O **Log360** ajuda a confirmar a integridade e a confidencialidade dos dados pessoais coletados e armazenados. Com perfis de alerta predefinidos, o Log360 envia notificações de alerta em tempo real sempre que o arquivo, pasta ou tabela do banco de dados em que os dados pessoais estiverem armazenados for: Acessado de maneira não autorizada (falha de login não autorizado, alterações de permissão, criação de contas no servidor do banco de dados ou alterações no esquema do banco de dados). Modificado. Excluído. Além disso, o Log360 fornece informações detalhadas sobre quem fez a alteração não autorizada, quando e onde. Isso ajuda na apresentação de um relatório de incidente, se necessário. **Relatórios relacionados no Log360:** • Acesso a arquivos • Arquivos modificados • Exclusão de arquivos • Tabela de banco de dados excluída • Modificada (execução de query DDL) • Falhas de login não autorizado • Alterações de permissão de arquivo ou pasta • Criação de conta de banco de dados • Alteração de esquema de banco de dados

Artigo 24° - Responsabilidade do controlador

Se você for um controlador (a pessoa, autoridade pública, agência ou qualquer outro organismo que pode determinar a finalidade e os meios de tratamento de dados pessoais), então você deve atender aos seguintes requisitos de tratamento de dados do GDPR.

Requisito	Como estar em conformidade	Como a ManageEngine pode ajudar
. “Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revisadas e atualizadas de acordo com as necessidades.”	**Certifique-se de:** • Fornecer acesso a dados pessoais somente para aqueles que precisam acessá-los. • Permitir somente que usuários autorizados acessem os sistemas ou serviços em que os seus dados pessoais são armazenados. E, para provar que não haja acesso ilegal ou não autorizado ou manipulação de dados, os controladores precisam realizar auditoria extensa e contínua. Monitore as atividades dos usuários e implante soluções que demonstrem que somente usuários com permissões válidas estão acessando dados pessoais.	Se você é uma loja do Windows, você provavelmente usa Active Directory para conceder a usuários permissões de recursos e dados. O **ADManager Plus** pode ajudar a gerenciar e auditar o processo de concessão de permissão. Os seguintes relatórios do ADManager Plus fornecem insights sobre quem pode acessar dados pessoais e também ajudam a identificar qualquer acesso não autorizado aos dados pessoais que possam prejudicar sua integridade: • Users in groups • Groups for users • Shares in the servers • Permissions for folders • Folders accessible by accounts • Servers accessible by accounts • Server permissions Esses relatórios também ajudam a revisar o processo de concessão de permissão sempre que necessário.

Artigo 25° - Proteção de dados por projeto e por padrão

Requisito	Como estar em conformidade	Como a ManageEngine pode ajudar
2 “O controlador deve aplicar medidas técnicas e organizativas para assegurar que, por padrão, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais coletados, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por padrão, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.”	Implemente soluções para validar as permissões de acesso concedidas aos usuários. Audite eventos de alteração de permissão para identificar as alterações de permissões ilegais ou não autorizadas relacionadas a dados pessoais.	O fluxo de trabalho no **ADManager Plus** ajuda com isso. O ADManager Plus também tem regras de notificação que atualizam os agentes do fluxo de trabalho a respeito de pedidos que foram feitos, revisados ou aprovados. Basicamente, o ADManager Plus mapeia o tipo de ação (pedido está criado, revisado, aprovado ou executado) para agentes do fluxo de trabalho para propósitos de notificação. Ele também permite que você comunique informações de solicitações aos técnicos e outros interessados através de e-mail e SMS.

Artigo 32° - Segurança do processamento

Requisito	Como estar em conformidade	Como a ManageEngine pode ajudar
1(b) “A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de processamento...”	Monitore e audite continuamente os sistemas de armazenamento que armazenam dados pessoais, bem como os serviços (ou aplicativos) que tratam dados pessoais. Esteja atento a tentativas de acesso anormais e não autorizadas nas atividades do usuário sobre estes sistemas e serviços.	Se você armazena dados pessoais em bancos de dados como MS SQL e Oracle, o **360 Log** pode ajudar a detectar eventuais atividades anormais em seus bancos de dados para identificar: • Tentativas de acesso não autorizado aos servidores de banco de dados ou a qualquer servidor em que os dados pessoais estejam armazenados. • Alterações de contas de usuário com privilégios no sistema onde os dados confidenciais estão armazenados. Se você armazenar seus dados pessoais em quaisquer servidores de arquivos do Windows, o **DataSecurity Plus** pode ajudar a garantir a integridade dos sistemas ao tomar conta de: • Alterações de permissão para arquivos e pastas. • Armazenamento no servidor de arquivos e espaço em disco para garantir a disponibilidade. Estes relatórios **garantem que apenas usuários autorizados acessem os dados pessoais.** Dessa forma, eles ajudam a manter a integridade e disponibilidade dos sistemas e serviços em que os dados são armazenados.

1(d) “...um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do processamento”.	Para garantir a segurança do processamento, as empresas devem estar atentas a qualquer atividade anormal na rede que possa ser uma potencial violação de dados. Implante soluções de segurança que possam: **1.** Auditar e enviar alertas em tempo real quando for detectada qualquer alteração de recursos críticos, como firewalls, Active Directory, bancos de dados e servidores de arquivos. **2.** Centralizar e correlacionar os dados de segurança a partir de diferentes fontes para identificar potenciais violações de dados instantaneamente e evitar a perda de dados.	Como uma solução abrangente de SIEM, o Log360 coleta os dados de registro de todos os dispositivos, incluindo firewalls, scanners de vulnerabilidade, aplicações críticas que tratam de dados pessoais, servidores de arquivos, bancos de dados, máquinas Linux/Unix, sistemas IBM AS400 e muito mais. Ele correlaciona os dados coletados e gera alertas em tempo real para qualquer potencial evento de violação de dados. Os administradores de segurança podem mitigar o ataque ou tomar medidas adequadas para evitar a perda de dados. O Log360 também fornece relatórios e alertas em tempo real sobre: - Alterações de configuração de Firewall, o que pode causar uma violação de dados. • Acesso não autorizado a servidores de arquivos, bancos de dados e outros servidores críticos. • Alterações críticas no Active Directory, incluindo alterações de atributos, GPOs e grupos de segurança, que podem resultar em acesso não autorizado a dados pessoais. • Alterações de permissão para arquivos/pastas onde os dados pessoais são armazenados. • Atividades anormais de usuários, incluindo início e encerramento de sessão do usuário durante horário não comercial, falhas de logon e muito mais.

2. “Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento dos dados, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento de dados.”	Implemente soluções e audite alterações de dados pessoais (por exemplo, alteração, exclusão, renomeação ou até alterações de permissão). Tome conta das caixas de entrada para detectar quando dados pessoais são transmitidos via e-mail.	Se você armazena seus dados pessoais em um servidor de arquivos Windows, use o **DataSecurity Plus** para gerar relatórios detalhados e **alertas em tempo real** sobre: • Eventos de acesso/alteração de arquivo. • Alterações de conteúdo e localização (arquivos/pastas modificados, substituídos, movidos, restaurados, renomeados e excluídos). • Alterações de permissões de segurança (alterações de permissões, proprietário e SACL de arquivo/pasta). • Tentativas malsucedidas de acesso ou processamento de arquivos/pastas (leitura, gravação ou exclusão). **Para dados pessoais armazenados em um banco de dados** Empresas usando bancos de dados MS SQL ou Oracle para armazenar dados pessoais precisam auditar qualquer alteração ou acesso a esses bancos de dados. Com o Log360, obtenha relatórios predefinidos exaustivos para auditoria de alterações em banco de dados: quem fez qual alteração, quando e onde. Gere rapidamente relatórios de incidentes a partir de modelos predefinidos de relatório. Obtenha alertas em tempo real para qualquer uso não autorizado ou atividades ilegais, como: • Tabela de banco de dados excluída • Tabela de banco de dados modificada (execução de query DDL)

- Falhas de login não autorizado
- Alterações de permissão para arquivos ou pastas
- Criação de conta de banco de dados
- Alterações de esquema de banco de dados

Além disso, empresas que usam outros servidores de arquivo, NetApp, cluster EMC e cluster de servidor de arquivos, também podem obter informações sobre alterações em arquivos e pastas críticas (incluindo alterações de permissões de pasta) com o Log360.

Os relatórios e alertas em tempo real do Log360 ajudam as organizações a detectar o acesso não autorizado e divulgação, bem como perda de dados.

Auditoria da transmissão de dados por e-mail Empresas que usam Exchange servers uma comunicação por e-mail pode usar o Exchange Reporter Plus para detectar e informar sobre transmissões de dados pessoais não autorizada ou ilegal. Identifique os dados pessoais enviados por e-mail usando os relatórios Attachment by Filename Keyword e Attachment by File Extension Keyword.

Visualize alterações de permissão utilizando o relatório Mailbox Permission Changes.

Use o relatório Mails Deleted or Moved para identificar qualquer violação de suas políticas de proteção de dados. Este relatório mostra detalhes como o assunto da mensagem.

4 “O controlador e o processador devem tomar medidas para assegurar que qualquer pessoa física que, agindo sob a autoridade do controlador ou do processador que tenha acesso a dados pessoais, somente proceda o tratamento dos dados mediante instruções do controlador, exceto se tal lhe for exigido pelo direito da União ou de um Estado-Membro.”	Implemente soluções que ajudam a detectar quando os usuários acessam dados pessoais sem a devida permissão.	Use o ADManager Plus para manter o rastreamento dos registros de permissão. Revise a permissão dada aos usuários usando relatórios que fornecem informações sobre: • Usuários em grupos • Grupos para usuários • Compartilhamentos nos servidores • Permissões de pastas • Pastas acessíveis por contas • Servidores acessíveis por contas • Permissões de servidor Gere alertas se qualquer pessoa que não tiver permissão explícita tentar acessar os dados.

Artigo 33° - Notificação de violação de dados

1. “Em caso de violação de dados pessoais, o controlador deve notificar desse fato à autoridade de supervisão competente nos termos do artigo 55º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas físicas.” “Se a notificação à autoridade de supervisão não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.”

2. “O processador notifica o controlador sem demora injustificada após ter conhecimento de uma violação de dados pessoais.”

3. “O controlador deve documentar quaisquer violações de dados pessoais, compreendendo os fatos relacionados com as mesmas, os respectivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controle verificar o cumprimento do disposto no presente artigo.”

A solução de SIEM da ManageEngine, Log360, pode ajudar as organizações a atenderem a todos os requisitos acima. Com um console de alerta em tempo real e motor de correlação, o Log360 detecta qualquer violação de dados na rede instantaneamente.

Com perfis de alerta predefinidos e regras de correlação, o Log360 pode detectar e conter padrões de ataque conhecidos, como:

- **Ataques de negação de serviço (DoS) e negação de serviço distribuída (DDoS),** que derrubam o sistema ou serviços que contêm dados pessoais.
- **Ataques de injeção de SQL,** que podem alterar, expor ou excluir dados pessoais armazenados em bancos de dados SQL.
- **Ataques ransomware,** que podem expor ou transmitir dados pessoais sem a devida permissão.

Além disso, o Log360 também vem com um **construtor de regra de correlação personalizada e criador de perfil de alerta,** que pode criar novas regras de correlação e perfis de alerta para a detecção de padrões de ataque desconhecidos, mantendo os dados pessoais seguros.

Extração de relatório de incidentes com o Log360

Conforme o requisito descrito no Artigo 33º (5), o controlador é responsável por documentar a violação de dados, fornecendo informações sobre o impacto da violação e as medidas corretivas tomadas.

O Log360 atende essa necessidade com seu poderoso **motor de busca de log,** que ajuda a realizar análise forense. O Log360 vem com diversas opções de pesquisa, incluindo booleano, intervalo, grupo e pesquisas com curingas, que ajudam as empresas a encontrar a causa raiz de uma violação com facilidade.
A análise forense fornece informações sobre:

- Quando a violação ocorreu.
- Os sistemas que foram afetados pela violação de dados.
- Os dados que foram adulterados, excluídos, expostos ou transmitidos.
- Quem foi o responsável pela violação.

Além disso, toda essa informação forense pode ser exportada como relatórios, ajudando as organizações a construírem um relatório de incidentes, a ser apresentado ao ICO em caso de violação.

Prepare-se para a implementação do GDPR com as soluções de segurança de TI da ManageEngine Audite sua rede, detecte violações e prove que você está em dia com os requisitos do regulamento. Para mais informações sobre a implantação de qualquer uma das soluções mencionadas neste guia, entre em contato conosco no e-mail itsecurity-solutions@manageengine.com

ManageEngine

Soluções de segurança de TI da ManageEngine para a conformidade com o GDPR

Log360

Uma solução integrada de SIEM que combina o ADAudit Plus e o EventLog Analyzer, nossas duas mais poderosas ferramentas de auditoria, para resolver todos os problemas de gerenciamento de log e desafios de segurança de rede. Impeça ataques de segurança interna, defenda a sua rede de ataques externos, proteja informações confidenciais e atenda às crescentes demandas de conformidade.

Obtenha o teste gratuito de 30 dias

Saiba mais

DataSecurity Plus

O DataSecurity Plus é uma solução de segurança e visibilidade dos dados que oferece descobrimento de dados, análise de armazenamento de arquivos e auditoria, alertas e relatórios em tempo real do servidor de arquivos do Windows. Ele também ajuda a atender a vários requisitos de conformidade e gera alertas instantâneos de e-mail definidos pelo usuário, enquanto realiza respostas predefinidas automáticas quando potenciais ameaças de segurança ocorrem.

Obtenha o teste gratuito de 30 dias

Saiba mais

ADManager Plus

Uma solução simples e eficiente para gerenciar e produzir relatórios sobre o ambiente Windows Active Directory. Garanta que somente usuários específicos obtenham acesso a dados pessoais com o fluxo de trabalho e cuidadosamente estruturado e as capacidades de automação desta solução. Gerencie e controle as permissões concedidas e revogadas de usuários e assegure que os dados pessoais sejam processados de forma segura.

Obtenha o teste gratuito de 30 dias

Saiba mais

ManageEngine

Como a divisão de gerenciamento de TI da Zoho Corporation, a ManageEngine prioriza soluções flexíveis que funcionam para todas as empresas, independentemente do tamanho ou orçamento. A ManageEngine cria software abrangente para gerenciamento de TI, com foco em em facilitar o seu trabalho. Nossos mais de 90 produtos e ferramentas gratuitas abrangem tudo o que sua TI precisa, a preços que você pode pagar. De gerenciamento de redes e dispositivos até software de segurança e service desk, oferecemos uma abordagem integrada e abrangente para otimizar sua TI.