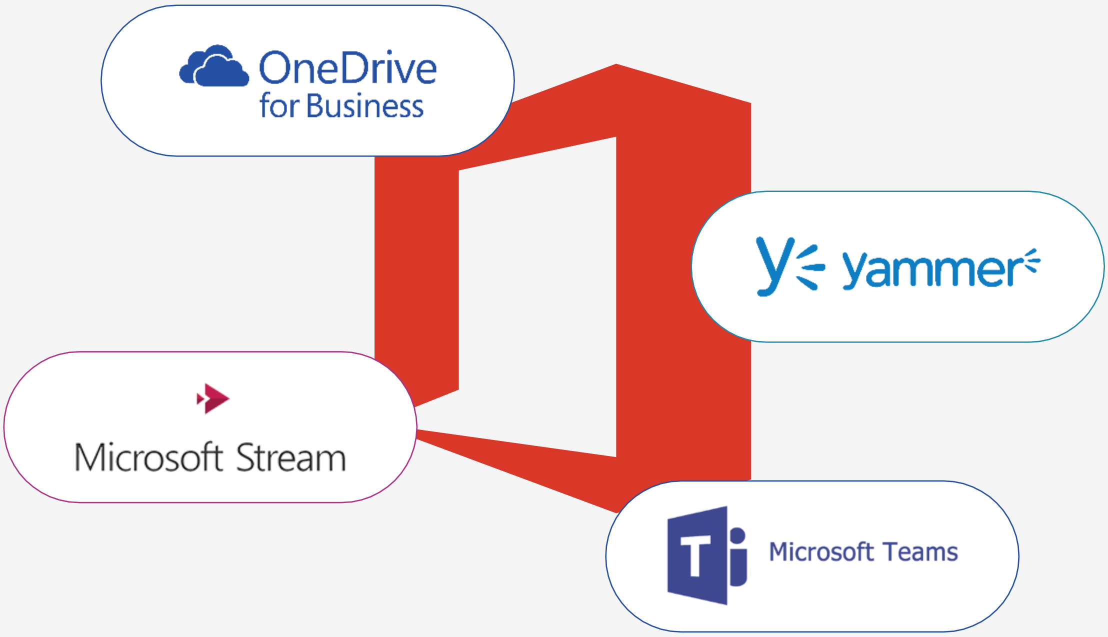
Um guia do administrador para **proteger aplicações de produtividade do Microsoft 365**



ManageEngine
M365 Manager Plus

Índice

Proteja as aplicações de produtividade do Microsoft 365:

Por que as aplicações do Microsoft 365 estão propensas a vazamentos?

De acordo com o Relatório de risco e adoção do Microsoft 365 da Sky High[1], 7,1% dos arquivos no OneDrive for Businnes têm dados confidenciais, como registros financeiros, informações de pagamento, informações de identificação pessoal (PII), informações de saúde protegidas (PHI), planos de negócios e código-fonte. Com tantos dados confidenciais disponíveis em apenas uma ferramenta de colaboração do Office 365, um desastroso vazamento de dados é uma possibilidade muito real.

Os vazamentos de dados são geralmente causados por atividades mal-intencionadas externas, como phishing, ataques de força bruta e ataques de contas privilegiadas, mas também podem ser o resultado de erros cometidos por funcionários regulares, usuários de TI privilegiados, equipe temporária e outros. Por exemplo, um funcionário pode dar, sem saber, permissão a todos os usuários para acessar um documento ou compartilhar um arquivo importante com um usuário externo.

Neste e-book, discutiremos como o monitoramento detalhado das aplicações de colaboração do Microsoft 365 pode ajudar os administradores a minimizar a chance de vazamentos de dados.

Procurando uma agulha em um palheiro

O Relatório de Adoção e Risco do Microsoft 365 também mostra que, em média, uma organização gera 5,4 milhões de eventos de usuários por mês no Office 365. Todas as atividades do usuário, como carregar, baixar, visualizar ou compartilhar arquivos, alterar configurações de documentos e muito mais, estão logadas às ferramentas de colaboração do Office 365. Desses milhões de eventos, apenas algumas centenas podem ser consideradas atividades anômalas e, dessas centenas, apenas algumas delas podem ser indicadores de uma violação de dados. Para rastrear alguns eventos ameaçadores, os administradores precisam de uma ferramenta que possa:

1. Auditar atividades de forma granular com ferramentas de colaboração e detalhes de fornecimento do Microsoft 365, como quais recursos os usuários podem acessar, quais têm privilégios elevados e se os arquivos de dados confidenciais estão sendo compartilhados interna ou externamente.
2. Informar extensivamente sobre os detalhes de um evento, incluindo o que, quem, quando e onde, para identificar problemas e avaliar se representam algum risco.
3. Enviar alertas instantâneos ao detectar atividades suspeitas para que os administradores possam investigar e reagir rapidamente a possíveis violações de dados.

---

[1] http://info.skyhighnetworks.com/rs/274-AUP-214/images/Skyhigh%20M365%20Report%20Q2%202016.pdf

Limitações da ferramenta nativa do Microsoft 365

Embora o Microsoft 365 forneça uma ferramenta nativa para auditar os eventos nas aplicações de colaboração, ela não é o suficiente para ajudar os administradores a garantir a segurança completa porque:

- As capacidades limitadas de filtragem dificultam a pesquisa em logs de auditoria e análise de possíveis riscos em uma configuração do Microsoft 365.
- A ferramenta fornece apenas alguns relatórios predefinidos sobre eventos do Microsoft 365, forçando os administradores a gastar um tempo valioso criando relatórios personalizados.
- A Central de Segurança e Conformidade permite que os administradores pesquisem somente eventos que ocorreram nos últimos 90 dias. Essa visibilidade limitada dos logs de auditoria é insuficiente para realizar auditorias e investigações de segurança.
- A limitação do armazenamento de log de 90 dias força os administradores a exportar e salvar logs de auditoria. Além de aumentar a carga de trabalho, isso ocupa uma grande quantidade de espaço de armazenamento no banco de dados da organização.
- Os administradores só podem fazer download de no máximo 50.000 entradas de log em um arquivo CSV a partir de uma única pesquisa de logs de auditoria, o que não é muito, especialmente para organizações de médio e grande porte. Além disso, arquivos CSV podem ser facilmente manipulados.

Por que o M365 Manager Plus é melhor do que as ferramentas nativas?

O M365 Manager Plus oferece uma visão abrangente dos eventos que ocorrem no OneDrive for Business, Yammer, Microsoft Teams, Microsoft Stream e outras aplicações do Microsoft 365. O M365 Manager Plus fornece:

- Relatórios pré-configurados que oferecem uma visualização granular de quaisquer mudanças em dados importantes. Os administradores podem ver facilmente aquelas que foram feitas em arquivos, pastas, grupos de segurança, configurações de acesso a arquivos e muito mais.
- Fácil acesso aos logs durante auditorias de conformidade e investigações de segurança. Os logs de auditoria também são armazenados indefinidamente.
- A opção de arquivar logs de auditoria de acordo com a conveniência do administrador e restaurar os que foram excluídos com um clique único.
- Sem restrição no número de logs que podem ser exportados. Os administradores também podem exportar ou arquivar logs nos formatos PDF, XLS e HTML.

Recursos do M365 Manager Plus

Relatórios

Gerenciamento

Auditorias

Delegação

Monitoramento

OneDrive for Business

O OneDrive for Business é uma das ferramentas de colaboração mais populares do Microsoft 365. Ele permite que os usuários armazenem e protejam arquivos, os compartilhem com colegas de trabalho ou usuários externos e muito mais. Como o OneDrive for Business armazena e permite o compartilhamento de quantidades substanciais de dados confidenciais, é importante verificar cada evento de perto. Usando o M365 Manager Plus, os administradores podem rastrear:

- **Atividades de arquivos e pastas:** Monitorar mudanças de arquivos e pastas, como criação, modificação, exclusão, renomeação, cópia e restauração.
- **Atividades de compartilhamento:** Rastrear detalhes sobre links compartilhados em toda a empresa, compartilhar convites, links anônimos, solicitações de acesso, arquivos compartilhados, pastas, sites e muito mais.
- **Atividades de sincronização:** Visualizar quais arquivos foram carregados e descarregados do OneDrive para Empresas e quais dispositivos têm permissão para sincronizar ou estão bloqueados e muito mais.
- **Mudanças de grupo de segurança:** Monitorar as mudanças de grupo de segurança, como a adição de novos membros, para que os usuários não recebam privilégios indesejados.

Caso de uso

Os funcionários de uma organização de saúde acessam os registros médicos de um paciente de alto perfil, mesmo que não tenham motivo legítimo para acessar esses dados. Esse tipo de violação das disposições da lei HIPAA poderia atrair multas enormes para uma organização se os dados contidos nos registros vazassem. Usando o perfil de alerta de ***arquivos acessados do OneDrive*** do M365 Manager Plus, os administradores receberão notificações sobre acessos a arquivos. Eles também podem criar uma exibição personalizada para arquivos confidencias para saber quem os acessou. Essa auditoria precisa maximizar as chances de encontrar cada acesso não autorizado para ajudar na correção.

Microsoft Teams

O Microsoft Teams permite que as organizações colaborem não apenas dentro dela, mas também com usuários externos. Os convidados podem participar de reuniões, além de ter acesso a chats, arquivos e muito mais. Isso é conveniente, mas também aumenta o risco de vazamentos de dados.

- **Eventos de equipes:** Auditar a criação de equipes e canais, adicionar ou remover membros de equipes e outras atividades do usuário.
- **Mudanças nas configurações:** Acompanhar as mudanças na organização, na equipe e nas configurações do canal para descobrir se o local de trabalho foi comprometido. Gerar relatórios para ver quais mudanças foram feitas por quem e quando.

Caso de uso

Uma empresa de construção inicia um novo projeto. O gerente de projetos usa o Microsoft Teams para colaborar com partes interessadas, incluindo vários gerentes e consultores. Ele adiciona esses convidados conforme necessário.

Nesse caso, o administrador de TI precisa saber os detalhes do convidado adicionado para garantir que não haja risco de segurança. Usando o perfil de auditoria e alerta do M365 Manager Plus para ***membros adicionados à equipe***, eles saberão quando um novo membro é adicionado a uma equipe.

Microsoft Stream

O Microsoft Stream permite que os usuários carreguem, visualizem e compartilhem gravações de reuniões, apresentações ou qualquer outro vídeo com segurança em toda a organização. Ao usar o M365 Manager Plus, os administradores podem verificar as seguintes atividades para garantir que nenhum vazamento de dados ocorra durante o compartilhamento de vídeos:

- **Atividades de usuário:** Monitorar a modificação das configurações do usuário, das configurações do locatário administrador, dos membros da função global do administrador e muito mais.
- **Atividades do canal de grupo:** Monitorar a criação e a modificação de grupos e canais, modificações de participação em grupos e muito mais.
- **Atividades de vídeo:** Monitorar atividades como criação, modificação e exclusão de vídeos, mudanças de permissões de vídeo e muito mais.

Caso de uso

A equipe de pesquisa e desenvolvimento de uma empresa cria um novo protótipo de produto em vídeo destinado apenas aos membros da equipe. As permissões são editadas para compartilhar o vídeo com um grupo que forma o gerenciamento de nível superior. Porém, ele é compartilhado errado e baixado por um usuário que não deveria ter acesso. Ao usar o perfil de alerta para download de vídeo do M365 Manager Plus para rastrear downloads de vídeo, os administradores podem rastrear quem os baixou e limitar qualquer dano.

Yamme

O Yammer é amplamente usado para aumentar o engajamento com pessoas dentro ou fora de uma organização. Usando o recurso de auditoria do M365 Manager Plus, os administradores podem rastrear suas ações e de usuários para reduzir o risco de violações de dados. Com o M365 Manager Plus, os administradores podem verificar:

- **Atividades de usuário:** Verificar a modificação e a criação de grupos e arquivos, compartilhamento de arquivos, downloads, atualizações e muito mais.
- **Mudanças das configurações do administrador:** Monitorar a modificação das configurações de perfil, do modo de conteúdo privado, das configurações de exclusão física/virtual e muito mais.

Caso de uso

O administrador de uma rede Yammer recebeu temporariamente acesso a conteúdo privado durante a investigação de um problema técnico. No entanto, ele não desativa o acesso após a solução de problemas, de modo que ainda tenha acesso a conteúdo privado. Isso pode resultar em alguém bisbilhotando dados importantes. Usando a capacidade do M365 Manager Plus de auditar *mudanças de configurações pelo administrador*, é possível encontrar e corrigir esse erro antes que dados confidenciais sejam acessados.

Os três melhores

recursos de segurança do M365 Manager Plus

1. Auditoria e relatórios abrangentes do Exchange Online para proteger sua organização de hackers.

   Relatórios do Exchange Online

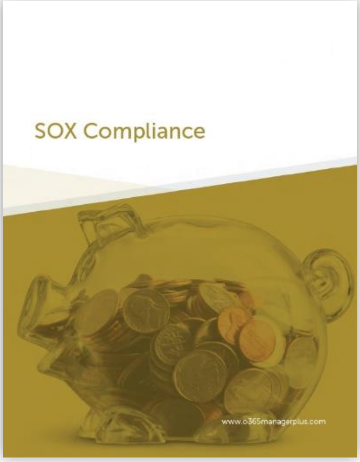
2. Auditoria e relatórios do Azure AD sem complicações para rastrear usuários, grupos, contatos e licenças.

   Relatório do AD do Azure

3. Relatórios completos sobre todas as atividades do administrador para fortalecer a segurança da sua organização.

   Relatórios de atividades do Microsoft 365

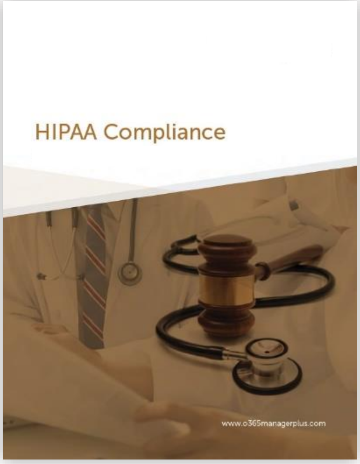
Listas de verificação de conformidade de TI com as leis **SOX, FISMA, GLBA, HIPAA** e **PCI DSS**



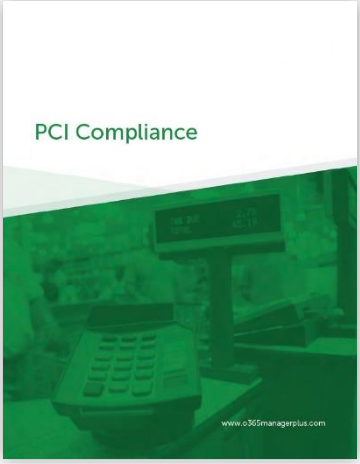
Faça download da lista de verificação de conformidade com a lei SOX

Faça download da lista de verificação de conformidade com a lei FISMA

Faça download da lista de verificação de conformidade com a lei GLBA



Faça download da lista de verificação de conformidade com o HIPAA



Faça download da lista de verificação de conformidade com o PCI DSS

ManageEngine
M365 Manager Plus

O M365 Manager Plus é uma ferramenta ampla do Microsoft 365 utilizada para relatórios, gerenciamento, monitoramento, auditoria e criação de alertas de incidentes críticas. Com sua interface amigável, você pode gerenciar facilmente o Exchange Online, Azure Active Directory, Skype para Empresas, OneDrive para Empresas, Microsoft Teams e outros serviços do Microsoft 365 em um console único.

$ Obter orçamento

Download