Marcelo Sincic

MVP Microsoft® Most Valuable Professional

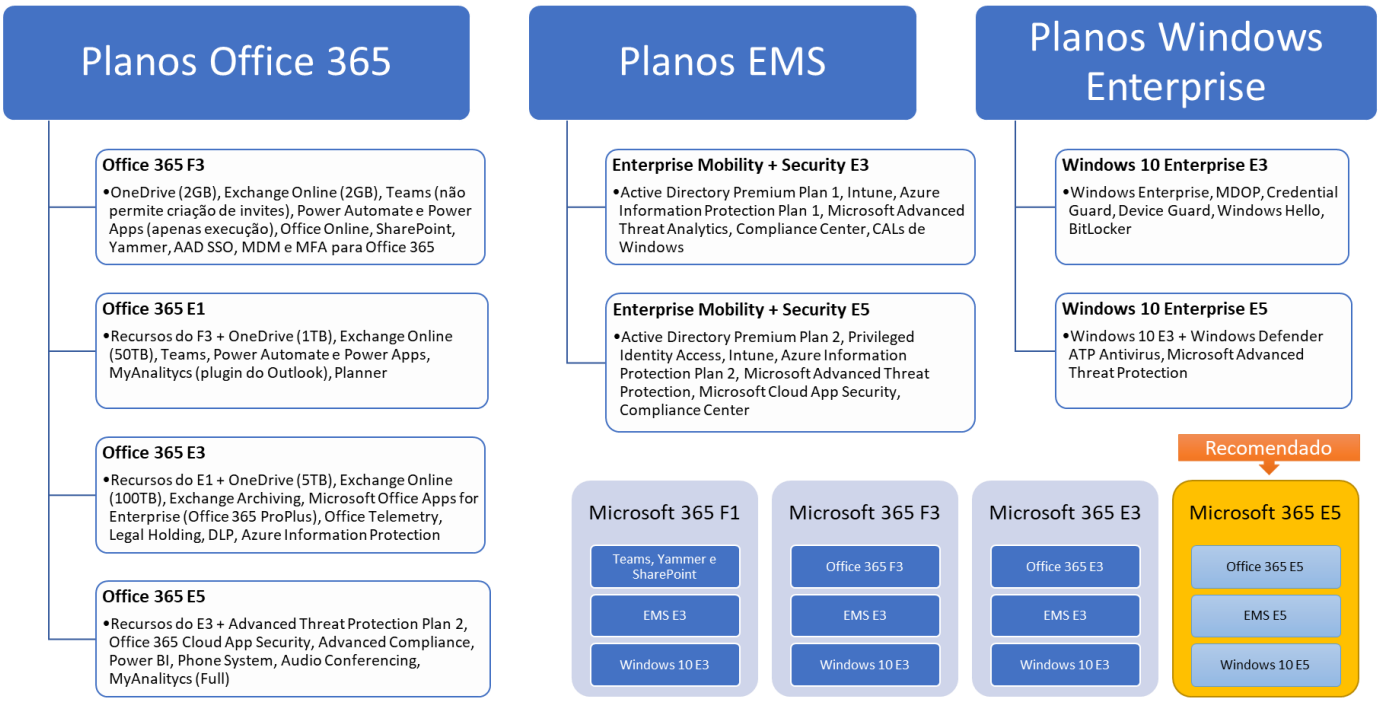
Com a entrada da LGPD (Lei Geral de Proteção de Dados) todas as organizações precisam ter segurança dos dados como uma prioridade.

Nesse guia não estamos detalhando todos os recursos e produtos do Office 365, mas focar em melhorar os níveis de segurança com algumas dicas e instruções.

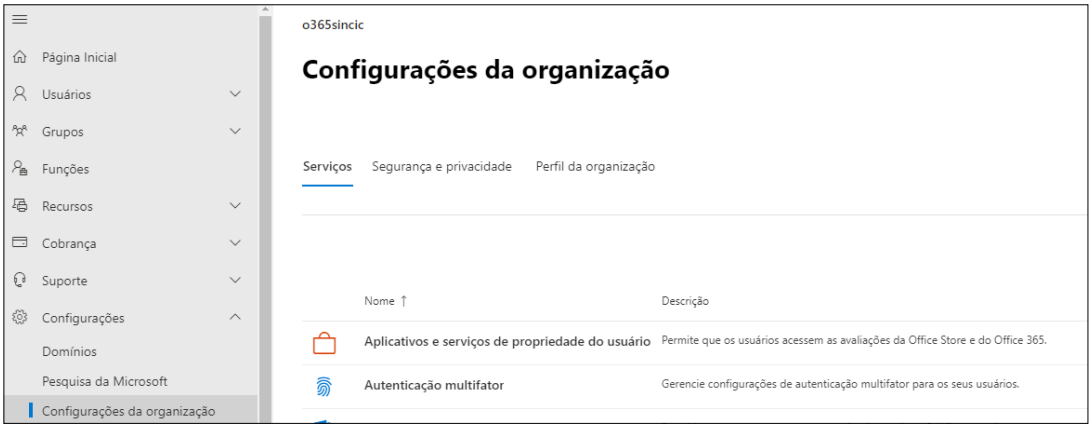
Com o desenvolvimento dos produtos é natural que ao longo do tempo algumas opções

# Índice



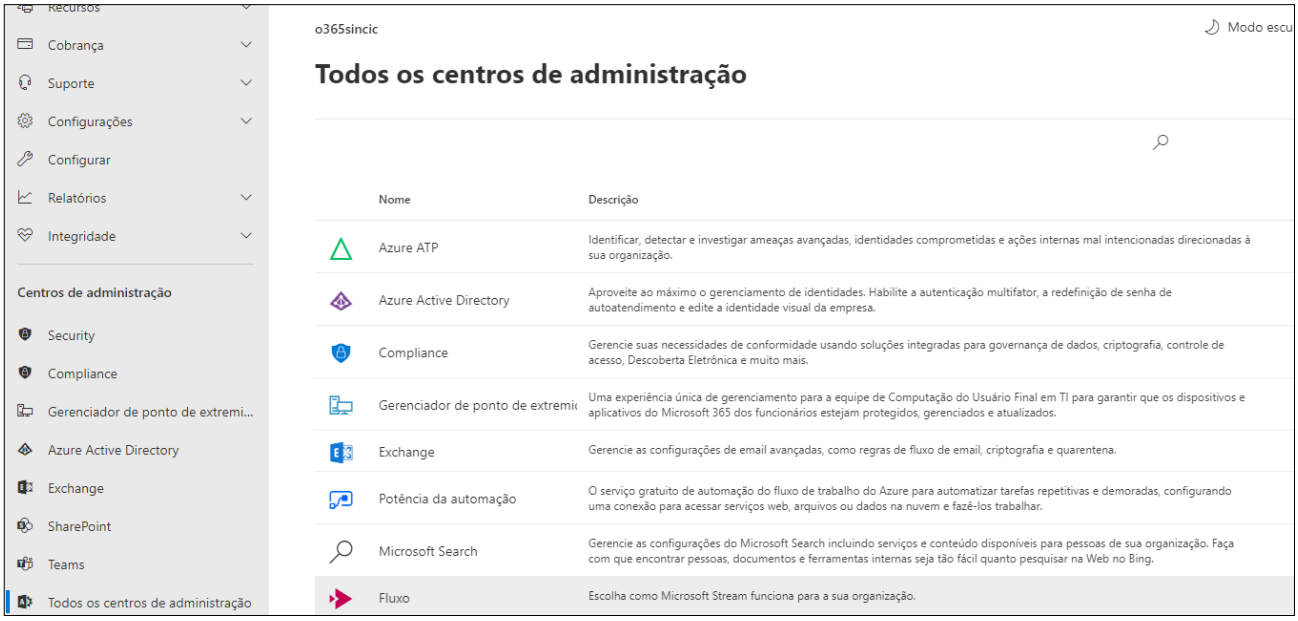


| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Configurações da Organização**<br>**Serviços**<br>**(Painel do Admin do Office 365)** | As primeiras opções de segurança que devem ser configuradas ficam no painel Configurações da organização no menu Admin do Office 365, iniciando por Serviços<br>• Um dos mais importante é a configuração do MFA (autenticação de duplo fator) que é GRATUITA para todos os usuários de Office 365 ao acessar os serviços. Usar o MFA garante que o usuário tenha um token que pode ser o app da Microsoft ou SMS/ligação (cobrado a parte). O ideal é habilitar o MFA pelo menos para os administradores e assim garantir a segurança do ambiente como um todo<br>• Em Consentimento dos usuários a empresa definir se os próprios usuários poderão permitir que aplicativos da loja Microsoft acessem dados da empresa. Se está opção estiver desabilitada o administrador deverá previamente permitir os aplicativos o que demandará tempo, mas garante apps seguros<br>• Modern authentication tem a ver com modelos de autenticação seguros. O modo Básico é usado por Offices antigos como o Office 2013 e anteriores. Usar esse método pode garantir que apps antigos e não seguros também acessem, por exemplo clientes de email em celulares. A recomendação é utilizar apenas autenticação moderna que usa tokens assim como o AD, o que é muito mais seguro que plain text usado pelos aplicativos antigos ou simplificados<br>• Relatórios tem uma opção interessante que é anonimizar os dados. Esse é o recurso que permitrá gerar os relatórios em conformidade com a LGPD onde os dados para parceiros sejam anônimos para evitar vazamentos. |
| **Configurações da Organização**<br>**Segurança e Privacidade**<br>**(Painel do Admin do Office 365)** | • Em acesso privilegiado (disponível para E5/AD Premium) permite definir quem serão os aprovadores em solicitações de uso dos processos administrativos. Chamado de PIM esse tipo de recurso evita que os usuários tenham acessos administradores permanentes, sendo necessário preencher um formulário para receber o acesso temporário como administrador. A opção Sistema de proteção de dados do cliente é relacionada a essa opção onde acesso aos reports precisa ser previamente autorizado como o PIM<br>• Autoatendimento de redefinição de senhas é um recurso interessante para o usuário, onde ele irá fornecer dados para receber uma senha temporária. Para usuários criados no Azure AD o recurso é gratuito, mas para usuários integrados com AD só está disponível a partir do EMS E3/AD Premium.<br>• Compartilhamento bloqueará todos os produtos de terem acesso convidado, ou seja quando um usuário convida alguém de fora para acessar o SharePoint é criado um contato no AD. Esse recurso bloqueia que sejam criados esses tipos de usuários convidados no Azure AD<br>• Politica de expiração de senha se aplica apenas caso não seja sincronizado o AD local, uma vez que essa configuração já é definida como padrão nas regras de GPO de dominio |
| **Configurações da Organização**<br>**Perfil da organização**<br>**(Painel do Admin do Office 365)** | • Em Preferências de lançamento especifique se as novas features e recursos serão disponíveis a todos os usuário da empresa. A opção Versão direcionada a todos permite que os usuários recebam imediatamente novos recursos, o que pode ser um problema quando em grandes organizações o processo de comunicação e treinamento é afetado por recursos que chegam ao usuário sem a prévia validação. Em geral o ideal é usar o modo direcionado para usuários “champions” que validam os recursos, assim deixando para que o restante dos usuários receba quando já for release final<br>• Blocos personalizados do inicializador de aplicativos é uma opção interessante para incluir no painel do Office 365 que o usuário tem acesso as ferramentas itens da sua empresa. Por exemplo, colocar o termo de segurança, intranet e outros sites que irão servir de treinamento e educação para seus usuários |



| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **SharePoint** | As configurações no painel de administração do SharePoint permitem fazer alterações muito similares aos do OneDrive<br>• Em Politicas -> Compartilhamento é essencial definir se as páginas do SPS poderão ser compartilhadas com usuários externos, o que é comum ser bloqueado em muitas empresas. Alem disso, configurar o tempo de validade de links caso tenha permitido acesso externo não autenticado será essencial para evitar que no futuro dados fiquem sem controle<br>• Em Controle de acesso poderá definir os IPs onde o SPS pode ser acessado e que apenas dispositivos que já estejam registrados para os usuários devem ser usados (disponível a partir do AAD Premium)<br>• Configurações adicionais poderão ser realizadas no painel de segurança para configuração de DLP e classificação (disponível a partir do E3) |
| **Teams** | No painel de configurações do Teams é possível definir diversas opções. Diferente do painel do Exchange e OneDrive, as opções no Teams são especificas<br>• Politicas de mensagens permite reduzir os recursos que o usuário poderá utilizar do Teams, muitas vezes são importantes como por exemplo o filtro Giphy que irá bloquear conteúdos adultos em imagens<br>• Uma das características do Teams é que ele permite a inclusão de aplicativos Microsoft ou terceiros, em Aplicativos do Teams o administrador poderá definir os aplicativos para apenas os autorizados pela organização, evitando assim brechas de segurança. E em Configurar politicas poderá atribuir aplicativos por grupos de usuários<br>• No menu Pacotes de política um recurso bem interessante é atribuir regras pré-definidas com base em boas práticas, o que pode servir também para que seja comparada entendo os modelos de segurança e aplicando em políticas customizadas<br>• Configurações em toda a organização tem as politicas gerais que podem restringir o IM com usuário sou externos ou apenas com domínios específicos para organizações onde existe o risco de vazamento por IM ou arquivos compartilhados pelo Teams. Nesse menu também temos o Acesso para convidado que é importante por definir o que usuário anônimos podem fazer em uma reunião ou IM, é importante configurar isso para que usuários indevidos não tenha acesso a reunião, documentos e mensagens |
| **OneDrive** | Pode ser uma fonte de vazamento sem a configuração correta de compartilhamentos e locais. Acesse o Centro de Configurações:<br>• Valide as configurações de Compartilhamento. O ideal seria configurar o link Direto evitando compartilhamento anônimo<br>• Deixe a opção Exibir quem exibiu seus arquivos ligadas para rastrear acesso indevido, mas a opção acima deve estar configurada<br>• Sincronização offline pode ser um risco se os discos rígidos não são criptografados<br>• Em Acesso do dispositivo é possível definir os ranges de IP e com isso limitar o uso apenas dentro da empresa ou mesmo bloquear certos recursos do dispositivo que o OneDrive corporativo, como por exemplo proibir a impressão ou captura de tela, obrigar o usuário a ter uma senha e outras As opções de Acesso a dispositivo do OneDrive irão funcionar apenas para esse serviço, para todos os serviços utilize o Intune (disponível no EMS) |
| **Exchange Online** | O email é um recurso que precisa ser controlado tanto por vazamento de dados ou comprovação judicial em caso de processos. Acesse o Centro de Administração:<br>• É possível configurar diversos itens como Filtro de Malware, Spam, dkim onde poderá definir o nível de SPAM que irá receber (7 é normal e 9 é bem restritivo) além de permitir usar assinatura de DNS (dkim) para validar e reduzir o número de SPAM recebidos<br>• Algumas opções bem interessantes em Fluxo de email com regras, domínios aceitos e remotos onde poderá definir por exemplo que e-mails pessoais (Hotmail, gmail, etc) devem seguir em horários específicos ou até pelo tamanho de anexos. Com isso é possível controlar o trafego e uso de links. Já em domínios remotos e aceitos poderá bloquear alguns recursos como respostas automáticas e NDR para evitar que engenharia social descubra contas reais no ambiente Tambem é possível executar essas funções no painel Security do Office 365, mas abordaremos esse painel mais adiante<br>• No menu de opções Celular pode-se criar regras para o uso do email assim como as citadas acima do OneDrive. As opções de Acesso a dispositivo do Exchange irão funcionar apenas para esse serviço, para todos os serviços utilize o Intune (disponível no EMS) |

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Power Apps e Automate** | No painel de administração do Power Platform podem ser feitas restrições a esses produtos. Levando em conta que eles podem ser utilizado como aplicações deve-se ter o cuidado de configurar de forma correta o acesso.<br>• Em Políticas de dados é possível definir conectores que serão considerados confiaveis e com isso acessar dados classificados no Office 365 como confidenciais |
| **Power BI** | No painel de administração do Power BI pode-se configurar as opções desse produto<br>• Nas Configurações de locatário é possível desabilitar a opção de exportação para Excel/PDF/PPT, aplicar rótulos de confidencialidade que é essencial para proteger dados no DLP, bloquear impressão ou acesso de usuários externos/convidados. Tambem é importante configurar os logs como habilitados<br>• No menu Métricas de proteção podemos configurar para que o Power BI automaticamente defina que os dados sejam considerados confidenciais quando a fonte de dados também é confidencial, além de identificar dados sensíveis automaticamente (disponível a partir do EMS E3) |
| **Yammer** | As configurações são bem complexas, mas as mais significativas são as que envolvem acessos externos<br>• Redes externas poderão ser configuradas para não permitir acessos de usuários de fora<br>• Em Configurações de Segurança configure os IPs que podem acessar, bem como o uso de mensagens com usuários de outras redes e bloqueio de usuários convidados sem licença<br>• Retenção de Dados irá definir se serão deletados ou não quando houver ação do usuário. Essa configuração é importante pois as regras de DLP gerais não abrangem o Yammer<br>• Em Monitorar Palavras-Chaves poderá criar uma lista de palavras que sirva de indicativo para serem enviadas ao administrador |



# Azure Active Directory (AAD)

Um dos principais e o primeiro recurso que precisam ser configurados quando se adquirem planos de Office 365 é o AAD onde temos a sincronização com os dados do AD local.

Pode ser acessado pelo painel de aplicativos do Office 365 ou pelo Azure diretamente.

Muitos recursos do AAD dependem dos planos Premium, mas mesmo no plano padrão gratuito diversas configurações podem ser realizadas.

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Identidades Externas** | Esse menu permite integrar B2B, ou seja integração de outros domínios para acesso aos dados. Por default o Google e o Facebook já são registrados, permitindo que se crie aplicativos onde esse tipo de autenticação seja utilizado como é o caso de comércio eletrônico ou sites de conteúdos registrados.<br>• Todos os provedores de identidade permitirá integrar Google, FB ou SAML de terceiros<br>• Configurações de colaboração externa deve ser utilizado para definir o que esses usuário poderão executar, é essencial se utilizar B2B que essas opções estejam bem configuradas<br>• Atributos de usuário e Fluxos dos usuários ira permitir complementar os dados que serão armazenados adicionais aos que foram importados do B2B, além de criar um fluxo onde indicará a sequencia e os dados que serão imputados, definindo por exemplo email de confirmação do usuário |
| **Funções e administradores** | Revise todas as permissões, lembre-se de a segurança é conseguida por ter usuários corretos para cada função que ele desempenhar. |
| **Aplicativos empresarias**<br>**Registro de aplicativo** | Com esse recurso podemos habilitar o SSO (Single Sign-On) para outras aplicações de mercado como SalesForce, Box e outros. É recurso importante pois garante que você tenha auditoria e a mesma segurança do seu AAD no ambiente de terceiros (auditoria disponível com AD Premium).<br>Uma vez adicionado um aplicativo do catálogo, você poderá definir o método de autenticação se é por senhas do próprio AAD ou outro método, mas em geral o método de senhas é o mais recomendado.<br>Também é possível criar aplicativos customizados em Registro de Aplicativos, onde utilizando a definição que o parceiro irá enviar, utilizará o SAML para integrar sistemas que não estejam previamente no catálogo da Microsoft. Neste menu será possível customizar as informações de integração mesmo dos aplicaivos já previamente catalogados e configurados.<br>É importante que ao utilizar esse recurso você tenha em mãos a documentação do parceiro, pois inúmeras configurações são determinadas pelo tipo de aplicativo deste parceiro. Por exemplo é possível no menu Autenticação definir que para cada tipo de dispositivo (iOS, Android, etc) sejam solicitados dados diferentes, definir as APIs que serão expostas e suas permissões. |
| **Dispositivos** | Aqui podemos validar os dispositivos registrados, se estiver com a integração com Intune poderá ver também os dispositivos locais bem como os registrados diretamente no AAD (disponível a partir do EMS). Uma vez o dispositivo registros poderá validar recursos deles.<br>Nas propriedades podemos ver as chaves de Bitlocker para dispositivos com Windows Enterprise além de opções que são disponíveis para todos os dispositivos com acesso aos recursos de email, Onedrive e outros. Poderá desabilitar um dispositivo roubado ou de um colaborador dispensado.<br>Em Configurações de Dispositivo pode-se indicar alguns itens como administradores locais e MFA.<br>Reveja com cuidado a opção Enterprise State Roaming pois ela irá permitir que um usuário com vários dispositivos possa sincronizar dados, o que deveria exigir MDM (disponível no EMS) |
| **Identity Governor, também conhecido como PIM** | Controle de acesso privilegiado já foi comentado (disponível no EMS E5), mas vale a pena ressaltar que é um recurso importante para limitar administradores com poderes fixos. Nas configurações do pacote de acesso podemos definir grupos e aplicações que precisam ter o acesso validado, por quanto tempo o privilégio permanecerá ativo e permissões que serão concedidas.<br>Com o uso do Revisões de Acesso e Logs de auditoria será possível ver quem, quando e o que foi realizado por cada um dos usuários que tiveram PIM ativado. |

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Licenças** | Fazer atribuição manual das licenças a cada usuário pode ser uma tarefa mal sucedida quando temos um numero maior de usuários. Nesses casos utilizando essas opções lhe permitirá conceder licenças baseados em regras.<br>No menu Recursos licenciados poderá ver a lista de todos os recursos que a organização tem direito e disponíveis para atribuição. No menu Todos os produtos poderá ativar licenças de EMS, AD Premium e outros para avaliação, variando dos planos que você já possui. É neste menu que você deverá selecionar os produtos que irá Atribuir aos usuários selecionados.<br>Nos detalhes da licença poderá atribuir licenças por usuários ou grupos o que facilitará a administração. Também poderá ver os detalhes do plano de serviço todos os itens que estão incluídos em cada um dos planos que irá atribuir. |
| **Redefinição de Senhas** | Disponível para usuários de EMS/AD Premium esse recurso chamado de password pass-through que precisa também ser configurado no AADSync, permite que usuário on-premisse façam a redefnição de senhas, como já comentamos em tópicos anteriores.<br>Vale a pena ressaltar que esse recurso é importantíssimo pois reduz significamente o numero de chamados de suporte e perda de produtividade quando o usuário esquece sua senha.<br>Aqui podemos ir nos detalhes desse item, onde definimos quais as formas que o usuário irá confirmar seus dados, como também notificações e auditoria do recurso, que irá justificar o investimento. |
| **Configurações de usuário** | Nesse menu temos diversas opções para definir o que um usuário final pode ou não executar.<br>Aqui temos a opção de permitir que a conta do LinkedIn seja vinculada ao AD. Esse recurso tem como finalidade mostrar no perfil dados adicionais de cada usuário.<br>Também nesse menu em Versões prévias de recurso poderá permitir que seus usuários tenham acesso a preview a aplicativos e recursos novos. Se a sua empresa tem usuários que utilizam bem recursos novos é interessante de habilitar, mas se os usuários não costumam aceitar bem mudanças em aplicativos é melhor que esses novos recursos sejam publicados quando em versão final ao invés de preview. |
| **Propriedades** | Aqui temos uma opção importante que fica escondida no final da página chamada Gerenciar Padrões de segurança onde diversas opções automáticas serão habilitadas por padrão.<br>https://docs.microsoft.com/pt-br/azure/active-directory/fundamentals/concept-fundamentals-security-defaults?wt.mc_id=4029139 |
| **Segurança**<br><br>**Acesso Condicional** | Quatro regras já são criadas por padrão e disponíveis para todos os planos de Office 365, pois e referem ao uso de MFA para acessos administrativos e são habilitados com a opção acima em Propriedades.<br>A criação de regras customizados só está disponível no EMS/AD premium 1 e oferece um importante recurso para segurança e acesso que normalmente exigem o ADFS configurado em Cloud, o que justifica seu investimento tanto pela segurança como pelo TCO de manter o ADFS em funcionamento.<br>As politicas podem ser criadas Somente relatório que é bem útil para testar e entender os riscos que hoje a organização está exposta para depois criar as regras definitivas.<br>Politicas customizadas são simples de configurar mas muito importantes na segurança do ambiente, dessa forma precisam ser bem definidas antes da criação para que sejam efetivadas<br>O primeiro passo é definir para quem a politica irá se aplicar que podem ser usuários ou grupos.<br>O segundo item é definir as aplicações que podem ser qualquer app em nuvem ou escolher na lista os aplicativos específicos. É interessante utilizar estas regras para indicar quem poderá acessar os recursos do Office 365 com requisitos específicos. Também é possível escolher Açoes onde serve para registro de atividades.<br>É importante ressaltar que essas regras são utilizadas em conformidade com o Intune para definir que o acesso aos serviços do Office 365 exigirá a instalação do agente e que regras especificas como por exemplo Espaço de trabalho com KNOX ou perfis de trabalho do iOS.<br>Nas Condições poderá definir que usuários em risco sejam bloqueados, sendo que estas condições são automaticamente detectadas pelo IA do AAD. Além disso pode-se definir regras por tipo de SO, local, aplicativo ou estado. No caso de aplicativo é possível criar regras para quando o acesso é via aplicativo ou quanto é pelo navegador; estado se o dispositivo precisa estar registrado no Azure AD para garantir que você possa bloquear ou zerar o dispositivo remotamente.<br>Em Conceder complementamos o que foi definido acima com requerimentos como MFA, ingresso no AAD, conformidade com Intune ou aplicativos específicos (exemplo Outlook Mobile).<br>Por fim em Sessão definimos o tempo máximo antes de um novo login, pode ser o tempo de sessão em um navegador aberto, dias para aplicativos serem re-autenticados e avaliação dos aplicativos. |

# Paineis de Segurança e Conformidade

A Microsoft possui 3 diferentes paines onde podemos configurar os itens de segurança e conformidade.

Muitas configurações são duplicadas, pois alguns painéis são destinados aos usuários do Office 365 e outros apenas para os usuários dos pacotes Microsoft 365. Com isso, os clientes com M365 terão acesso aos painéis dos clientes O365 tanto a partir do painel mais completo quando pelos painéis mais simples.

- https://protection.office.com/ é o painel acessível ao todos os clientes, as opções apresentadas variam conforme os planos, sendo uma parte restrita aos clientes com E5
- https://security.microsoft.com/homepage é o painel para clientes com M365, inclui algumas das opções do painel anterior
- https://compliance.microsoft.com/homepage é um painel que agrega funções dos dois painéis anteriores com foco nos clientes com M365 E5

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Centro de Segurança e Conformidade**<br><br>**Opções diversas** | • Em Alertas->Politicas de alerta defina condições para que o administrador receba avisos. Essas regras podem ser de diversos tipos baseadas em condições para gerar os alertas. Por exemplo, ao escolher um alerta de Arquivo movido poderá indicar usuário, IP, nome, URL, extensão como parâmetros de alertas. Por exemplo se existe uma pasta sensível de segurança podemos criar os alertas para todos os arquivos que sejam manipulados. Lembrando que esses alertas funcionam para dados no Office 365 e não em servidores locais<br>• Permissões permite definir usuários para servirem com as diferentes funções de segurança sem dar permissão administrativa. Usando esses modelos de permissões por papeis (roles) garantimos que um usuário tenha o acesso ao que ele precisa e não mais do que isso. Portanto, revise seus administradores e troque por usuários com permissões baseadas em papeis o que reduz a chamada superfície de ataque<br>• Fluxo de e-mails apresenta os painéis de entrada e saída de mensagens. Mas aqui é interessante ver o rastreamento de mensagens onde podemos avaliar as mensagens que tenham sido classificadas como falso ou positivo SPAM quando um usuário reportar. Assim encontramos os dados reais de trafego para achar de onde a mensagem foi originada. Tambem em Painel o bloco Clientes com Autenticação SMTP é importante para identificar usuários que utilizam portas antigas de comunicação e que podem comprometer a segurança. Em alguns casos isso é natural, por exemplo um serviço que envia e-mails para clientes, mas você identificaria como exceção e não regra.<br>• Privacidade dos Dados fornece um interessante roteiro para suprir as demandas do GDPR que são similares ao LGPD. Por exemplo ele o guiará na implementação das regras do Office 365 e tem a opção de importar dados na caixa de ferramentas, onde irá analisar arquivos PST. Isso é bem interessante quando um usuário criou a PST para e-mails pessoais e agora você precisa validar se ele usou o email pessoal para vazar dados. Tambem nesse menu temos a opção Solicitação de entidades (titular) que supre a necessidade de um usuário ou cliente que lhe pedir informações que tenha sobre ele, um direito no LGPD.<br>• Relatórios já é uma opção conhecida e que utilizamos muito para validar se nossas configurações estão surtindo efeito. Nesse temos os painéis onde podemos ver SPAM, Malware, DLP, retenção, classificações e todos os itens configurados. Não é possível fazer um agendamento de envio dos relatórios a partir dos resumos, mas entrando em cada relatório poderá agendar o envio automático a você ou outro administrador com o objetivo de serem proativos na analise das configurações de segurança.<br>• Garantia de Serivço->Relatorios de Auditoria é o caminho para encontrar os principais padrões que o Office 365 cumpre. Como a LGPD indica que para uma organização ser considerada segura ela deve implementar 'padrões de boas práticas reconhecidos', esse painel irá provar em uma auditoria que você tem a cobertura desses padrões na plataforma. Obviamente isso não indica que você implementou todos os mecanismos. |

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Centro de Segurança e Conformidade**<br><br>**Classificação** | Neste menu é onde definimos as diferentes classificações de documentos que serão enviados ou até mesmo a autoclassificação.<br>É importante ressaltar que os sensitive labels estão disponíveis hoje nos planos a partir de E1, porem opções como criptografia e archiving (retenção) estão disponíveis com todos os recursos no plano E3 ou superior com Office ProPlus 2016 ou 365.<br>• Rótulos de confidencialidade é onde definimos as tags que os usuários utilizam nos documentos e e-mails para definir como critico, confidencial, pessoal ou publico por exemplo. Esses rótulos podem carregar regras, ou seja ao definir que um documento é confidencial ele deverá ser criptografo, carregar uma marca d'água ou definir que será automático caso contenhas informações sensíveis (DLP tratado a frente). Esse é um recurso muito importante para definir futuros vazamentos ou até impedi-los uma vez que nas regras de DLP é possível avisar o administrador e o usuário ou até proibir o envio da informação se determinado rótulo estiver atribuído. E com os rótulos automáticos se o documento anexado estiver identificado como Confidencial, automaticamente o email precisará estar confidencial ou superior.<br>• Rótulos de retenção basicamente gerencia a exclusão de dados e não necessariamente dependem do archiving (arquivo morto). Assim como os rótulos de confidencialidade, na retenção utilizamos parâmetros para indicar quanto tempo um item deverá ficar disponível. Por exemplo utilizando dadso sensíveis (DLP) podemos indicar que um email que contem CNPJ ou CPF deverá ficar retido por 7 anos. Se o usuário tentar apagar antes do tempo será notificado. As opções aqui vão se granularizando, primeiro você deverá criar o rótulo, depois publicá-lo aos usuários e aplicativos desejados e por fim usar a opção de aplicar automaticamente para atribuir as regras de uso do rótulo<br>• Tipos de informações confidenciais (sensitive informations) é sem dúvida um recurso valioso. Aqui é onde a Microsoft já populou com diversos itens que são criticos usando mascaras de formato RegEx onde as informações são indicadas. Ao pesquisar por Brasil poderá ver que já constam CPF, CNPJ, CNH mas cartão de crédito também disponível para criar as regras. O interessante é que você poderá criar'as suas regras baseadas em RegEx. Por exemplo a mascara RegEx [a-zA-Z]{2}[0-9]{6} forma o numero do passaporte com duas letras e 6 números. O link abaixo mostra como foram criadas e as mascaras dos mais de 100 tipos pré-carregados pela Microsoft. Alem disso também pode-se criar como tipo de informação uma lista de palavras, por exemplo definir jargões racistas ou de conteúdo inapropriado.<br>https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-entity-definitions?wt.mc_id=4029139 |
| **Centro de Segurança e Conformidade**<br><br>**Prevenção contra perda de dados** | Este menu é sem dúvida um dos mais importantes para evitar perdas de dados, e por isso nos referimos a ele como DLP. Nele podemos criar as regras simples ou completas utilizando informações sensíveis que vimos no item acima.<br>Sendo assim, nesse caso temos apenas dois itens de menu, o de Politica e o Permissões de Aplicativos que na verdade é o CASB (disponível no E5), trataremos aqui as opções.<br>• Locais também está disponível nos outros itens como retenção e confidencialidade. O que podemos aqui é escolher os aplicativos (Exchange, SPS, OneDrive e Teams) que as regras se aplicam. Caso possua o M365 E5 as regras se aplicam também no Windows! A partir dos locais podemos criar regras especificas para um dos produtos, grupos de usuários ou itens como Site no caso do SPS. Por exemplo podemos excluir o departamento de RH das regras já que eles trocam constantemente números e dados pessoais com usuários externos<br>• Configuração de politica é o item principal onde definimos as regras de DLP. Separado em Baixo e Alto volume onde indicamos um numero mínimo ou relevante de ocorrências de dados, as regras se repetem mas podemos alterar as ações. Por exemplo podemos indicar que se um email tem 2 CPFs apenas irá emitir um aviso (baixo volume), mas se contiver 5 ou mais CPFs (grande volume) queremos que seja notificado o departamento de Compliance e riscos. Alem das regras padrão de baixo e grande volume se necessário você poderá criar regras adicionais para classificar em mais níveis o que seria um vazamento.<br>Essas regras de volume permitem que incluamos os itens que consideramos sensíveis e quantidade que a regra irá ser considerada. Na regra identificamos se o conteúdo será ou não bloqueado para acesso externo, por exemplo posso indicar que não irei considerar e-mails internos como Compliance, só externos que é o padrão. Em Notificações podemos indicar que o usuário e o administrador (ou outra pessoa) receberá um email avisando, que é o relatório de incidente. E uma opção adicional é substituição do usuário onde pode-se exigir uma justificativa para que seja feito o envio.<br>Por fim, é possível ativar ou configurar para que estas sejam apenas um teste, gerando relatórios a alertas mas não gerando as notificações e bloqueios. |

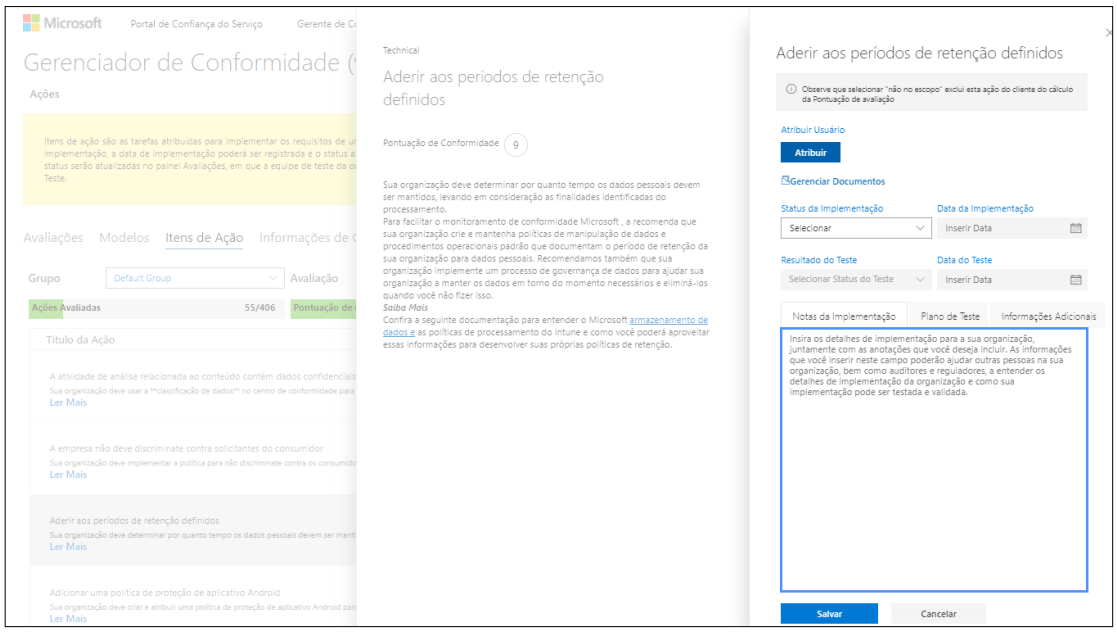
| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Centro de Segurança e Conformidade**<br><br>**Gerenciamento de ameaças** | As opções desse menu são disponíveis apenas para planos E5/Office 365 ATP e servem para detecção avançada de phishing e campanhas de educação. Sem dúvida é um recurso inestimável para proteção. Alem disso o ATP permite que você tenha acesso a recursos como safe link e attachment onde todos os links e documentos passam primeiro por um testa em *sandbox* da Microsoft.<br>https://docs.microsoft.com/pt-br/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide<br>• Na opção Gerenciador você poderá verificar todas as ameaças que foram detectadas com opções bem interessantes. Ao selecionar uma mensagem, seja ela legitima ou não, poderá ter ações como investigar a origem, criar um falso positivo, criar uma correção, baixar o conteúdo e outras. É sem dúvida um importante recurso para monitorar ameaças<br>• Campanhas irá detectar atividades que determinam que você está sofrendo um ataque sistemático de phishing ou malware da parte de um sistema complexo (não individual). Esse recurso o ajudará a detectar quando sua empresa está sendo direcionada por um ataque "zumbi" ou força-bruta<br>• No menu Envios poderá solicitar a Microsoft que analise um conteúdo especifico<br>• Simulador de ataques é um recurso excelente para validação do conhecimento dos seus usuários. Você poderá criar campanhas de diversos tipos e saber o comportamento que o usuário teve e assim disparar treinamentos específicos com os comportamentos erráticos. Alem dos ataques simulados poderá testar senhas com simulação de força bruta e detectar senhas vulneráveis no seu AAD<br>• Politicas possuem os modelos a serem adotados para melhorar a detecção de ameaças como por exemplo, ataque de usurpação de identidade e IA contra falsificação de dados |
| **Segurança do Microsoft 365** | Nesta homepage se concentram opções similares ao anterior, com diferenças nos painéis para os usuários que tem E5.<br>• Página Inicial e Relatórios permite que visualize todos os consoles e configurações que foram realizadas em todos os painéis e com isso validar a efetividades das regras criadas. Como vimos no tópico sobre o Acesso Condicional e DLP é possível criar as regras e coloca-las em modo de reportar ou teste.<br>• O painel Microsoft Secure Score é importante para que você tome todas as ações que podem melhorar a segurança. No painel de Visão Geral vemos um gráfico com a classificação geral baseada nas boas práticas de administração. Cada uma das regras é categorizada e soma ou decresce pontos da classificação geral. Uma feature interessante no painel está na combo "Incluir" onde você poderá utilizar a opção pontuação da licença ou atingível com a licença atual onde poderá ter um classificação com base no que possui nos planos. É útil utilizar para seu controle, mas como segurança corporativa uma classificação baseada apenas no que você possui pode ser que cause uma falsa sensação de proteção.<br>• Politicas é um painel interessante por permitir que todas as politicas criadas em todas as ferramentas e consoles sejam revistas. Utilizamos esse painel quando uma politica fica sobreposta ou não temos um mapeamento de todas as configurações que feitas. Ao acessar poderá rever todas as politicas aplicadas e revisar como um todo o que está sendo monitorado.<br>• Em Busca —> Busca avançada de ameaças (disponível com o pacote EMS) um administrador poderá visualizar utilizando consultas no formato KUSTO como documentado no link abaixo. Uma vez criada uma consulta você poderá utilizá-la para definir uma regra de detecção, que de modo simplificado é uma consulta que irá gerar um alerta customizado com base no resultado de sua consulta<br>https://docs.microsoft.com/pt-br/microsoft-365/security/mtp/advanced-hunting-query-language?wt.mc_id=4029139<br>• Permissões é um item interessante para rever quem tem direitos privilegiados, reveja com frequência esse item para verificar se não "vazou" algum tipo de permissão administrativa a usuários não treinados. |
| **Conformidade do Microsoft 365** | Como comentado no inicio muitas das opções já estão disponíveis em outros painéis, com algumas opções adicionais, porem disponíveis apenas para o EMS E5<br>• Conformidade com comunicações permite que criemos regras especificas baseadas nas politicas mais utilizadas. Com o assistente poderá criar regras com informações sensíveis, confidenciais ou ofensiva. Estas regras são similares as que podemos criar com o uso de informações sensíveis e regras de DLP e podem ser criadas dessa forma por usuários que não tenham o EMS E5<br>• Gerenciamento de riscos internos é um conjunto de regras pré-carregadas que permitirá detectar alguns tipos de riscos conhecidos. Poderá utilizar filtros específicos como vazamento de dados, linguagem ofensiva, eventos de RH e outras regras com AI<br>https://docs.microsoft.com/pt-br/microsoft-365/compliance/insider-risk-management |

# Gerenciador de Conformidade

Todas as ferramentas que vimos até aqui servem para criar mecanismos de segurança que apoiam e ajudam no cumprimento de normas como o GDPR e LGPD. Porem, existem diversos itens na LGPD que estão além de ferramentas e envolvem processos. Disponível apenas para E5

O Gerenciador de Conformidade irá ajudar a mapear estes processos —> https://servicetrust.microsoft.com/ComplianceManager/V3?wt.mc_id=4029139

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Gerenciador de Conformidade**<br><br>**Avaliações** | Neste item o administrador poderá validar como as ações realizadas pela Microsoft, pelos serviços e pelos processos como está a implementação de um padrão.<br>Neste painel poderá adicionar novas avaliações onde será possível escolher opções desde regras europeias como EU e GDPR, HIPAA para saúde, ISOs, NIST e SOC. Destacando obviamente as regras do LGPD que já estão disponíveis em português. |
| **Modelos** | Permite que um administrador exporte as definições dos diversos tipos de normas em XML, edite para criar regras customizadas e importe novamente para incluir no painel.<br>É uma opção útil para empresas sujeitas a normas brasileiras que não sejam um padrão internacional como as da ABNT. |
| **Itens de Ação** | A cada item do modelo que pode ser acessado em Itens de Ação ou Informações de Controle você verá uma lista com os itens cobertos pela Microsoft e os que você como corporação deverá fazer.<br>Ao clicar em Review será possível você indicar em que estágio está com aquele determinado Item de Ação.<br>Para isso informe o estágio, data que irá implementar, se os testes com a ação foram bem sucedidos e a data do teste. Também poderá incluir observações sobre como o teste foi feito, anexar os documentos e atribuir a um usuário.<br>Com isso você passa a ter um painel onde para auditoria será muito mais fácil levantar os dados e comprovar a aplicação do modelo de lei ou norma que você está se sujeitando. |
| **Informações de Controle** | Na parte seguinte das análises em Informações de Controle você terá uma visão como a abaixo onde terá acesso aos diferentes itens que deverá implementar conforme a lei, com destaque para o artigo que a impõe. No caso de leis “cruzadas”, o resumo irá indicar as diferentes leis e normas com seus artigos onde é necessário implementar determinado controle.<br>Assim como na parte de Itens de Ação aqui você poderá abrir os itens e ver quais os controles que precisam ser implementados por você ou já são satisfeitos pela segurança do próprio Office 365. |



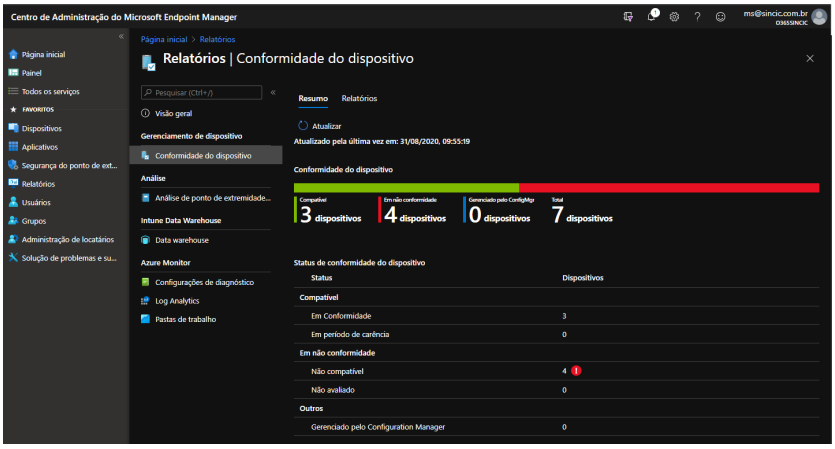
# Intune / Microsoft Endpoint Management

Para uma boa proteção de dados quando temos usuários com acesso externo a email e outros recursos, uma ferramenta de MDM (Mobile Device Manager) é imprescindível. Disponível nos planos EMS.

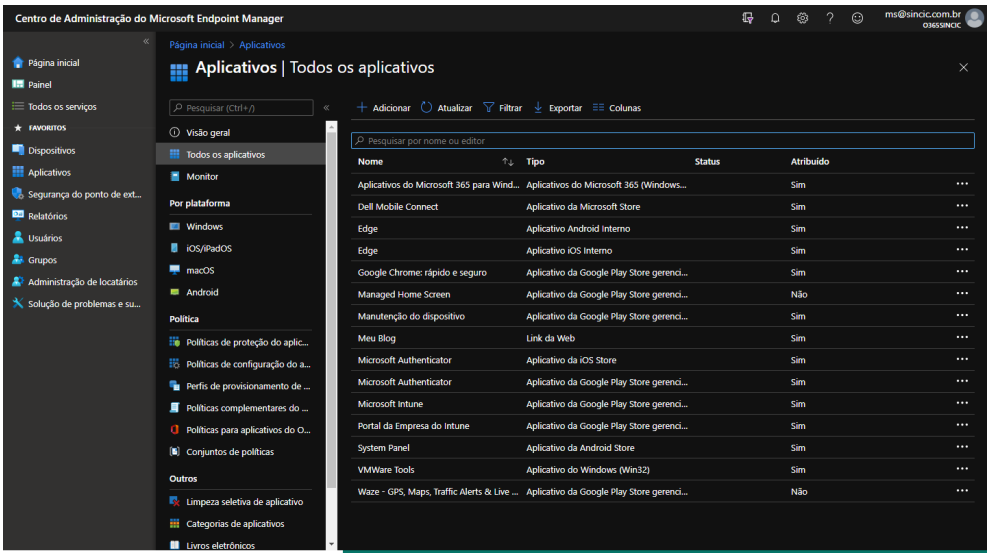
O Intune que agora se chama Endpoint Management cumpre com esse papel onde podemos controlar dispositivos Windows, MAC, iOS e Android. Link: https://endpoint.microsoft.com/

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Dispositivos** | A maior parte das configurações disponíveis aparecem neste painel, mas iremos tratar as que são exclusivas deste menu e se referem ao gerenciamento de dispositivos e politicas.<br>Nos agrupamentos por plataforma é possível ver as politicas de conformidade e configuração filtradas, mas trataremos delas como um item único. Acesso condicional já foi tratado no tópico AAD. |
| **Dispositivos**<br><br>**Windows Registro** | Aqui temos algumas opções especificas para Windows que se referem as registro de novos dispositivos.<br>É de destaque o conector do Intune com o AD para criar a lista de dispositivos híbridos como foi comentado no tópico onde abordamos o AAD.<br>Também é de destaque o item Windows Hello que é o modelo de MFA para Windows utilizando reconhecimentos biométricos como segundo fator de autenticação que podem ser PIN, reconhecimento facial ou leitor de digital. |
| **Dispositivos**<br><br>**Propriedades do dispositivo** | Ao acessar as propriedades dos dispositivos poderá validar as configurações individuais de cada um que foi registrado. Tambem é aqui que você poderá bloquear, apagar ou reiniciar o dispositivo ou enviar uma mensagem para o usuário. Em dispositivos iOS temos diversas opções adicionais como localizar o dispositivo por GPS, criptografar, revogar licença e outros. No case de Windows é possível utilizar o Autopilot para reiniciar e reinstalar o Windows no computador.<br>Nas propriedades podemos identificar a propriedade do dispositivo como pessoal (Samsung Knox ou Android) e é utilizado para BYOD ou empresarial gerenciado e dedicado que são aparelhos que pertence a empresa e recebem o acesso a todos os dados do dispositivo.<br>A diferença no tipo de Propriedade é que nos Pessoais só terá acesso ao que é instalado e perfil trabalho como do KNOX, na propriedade Empresarial terá acesso ao inventário de software completo. Lembrando que o usuário precisará aprovar quando o administrador muda de Pessoal para Profissional, já que isso poderá dar acesso a dados particulares e permitir bloqueio de um aparelho pessoal. |
| **Dispositivos**<br><br>**Politicas de conformidade** | Essas politicas permitem indicar o que será considerado um dispositivo seguro ou dentro das normas da organização. Ao criar uma política deverá incluir o sistema operacional e o tipo de regra, que pode ser apenas para o perfil trabalho ou gerenciado e dedicado que são aparelhos que pertence a empresa.<br>Essas definições possuem a opção de ações que podem ser envio de um email, notificação, bloquear ou desativar. Se não criada nenhuma ação, servirá apenas para indicar nos painéis.<br>Não trataremos todas as configurações já que cada sistema operacional tem suas características, mas a integridade de segurança fará com que o usuário tenha que cumprir os requisitos iniciais para ingressar.<br>Alguns itens merecem destaque no Android e IOS que são os mais usuais.<br>Para Android valide se o Google Play Protect está configurado, também que não esteja em nível raiz (jailbreak). Tambem verifique e criptografe o dispositivo (se for empresarial).<br>Para Android e iOS configure e valide como uma senha de tamanho e tipo especificado por você para melhorar a segurança. |

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Dispositivos**<br>**Perfis de configuração** | Os perfis de configuração são muito importantes para diversas opções. Assim como as configurações de conformidade, são separadas por plataforma e tipo de perfil da propriedade.<br>• Perfis de acessos permitem configurar diversos itens. PKCS e SCEP permitirá que sejam configurados opções para instalação de certificados corporativos que podem ser utilizados como chave de acesso para ambiente corporativo ou wifi em modos avançados de segurança (802.1x). Tambem temos configurações para perfil de Wifi para pré-carregar nos dispositivos as redes sem fio da organização que usam chaves simples. VPN permite pré-carregar configurações de diversos tipos de roteadores comuns incluindo genéricos como IKEv2.<br>• Perfis de restrições do dispositivo fazem uso de diversas configurações que serão impostas aos dispositivos, sendo que algumas repetem o que já foi configurado em perfis de conformidade. Mas aqui as opções são mais completas com restrição a uso da câmera, remover ou adicionar contas de email no perfil de trabalho, copiar e colar entre aplicativos do perfil trabalho e pessoal, trocar dados via bluetooth e outros como os métodos permitidos de autenticação.<br>Nessas configurações temos um importante ponto a configurar que é proteção dos dados que estão no perfil de trabalho com o pessoal. Com isso a organização poderá ter a garantia de que o Outlook configurado no perfil de trabalho não poderá ter contas pessoais evitando um encaminhamento, não poderá fazer cópia de dados ou até capturar telas nos perfis trabalho.<br>• Perfis de recursos no iOS trata de configurações próprias que abranger configurar o AirPrint, alterações de layout da tela inicial, mensagens e notificações na tela de bloqueio, filtro web para navegação na internet, SSO e até o papel de parede. Utilize essas opções principalmente em dispositivos que pertencem a empresa. |
| **Dispositivos**<br>**Restrição de registro** | Aqui temos algumas opções como permitir que os dispositivos sejam registrados como pessoais e as versões mínimas para isso, lembrando que também pode ser configurado nos perfis de conformidade. Mas aqui temos a restrição a numero de dispositivos que cada usuário poderá registrar, que tem o default de 10 dispositivos. |
| **Dispositivos**<br>**Conjunto de políticas** | Esse realmente é um recurso que facilita muito a administração. Como vimos são muitas regras que podem ser criadas e isso pode causar uma confusão na aplicação de cada uma a grupos específicos.<br>Aqui podemos agrupar as regras de conformidade, configuração, registro e aplicativos em um pacote e atribui-las com uma única regra facilitando o uso. |
| **Todos os Serviços**<br>**Desktop Analytics** | Esse serviço fica “escondido” e só está disponível para Windows E3 ou E5 permitindo que sejam gerados dados analíticos do uso dos equipamentos com Windows 10 integrado com o SCCM.<br>Ele utiliza os dados do serviço de telemetria do Windows para gerar dados de implementação com detalhes de updates, aplicações e outros itens que ajudam a alimentar bases de dados de segurança e risco. |
| **Administração de locatários**<br>**Criar termos e condições** | Essa opção lhe permitirá criar os termos que o usuário precisa concordar quando registrar um dispositivo. Ele é útil como aceite por parte do colaborador as regras da empresas, uma vez que ele deu um aceite legal nas normas e condições de uso. |
| **Relatórios**<br>**Configurações de diagnótico** | Neste item do menu de relatórios é possível integrar os dados do Intune para os dispositivos com o Log Analytics, armazenar em um Blob ou um hub de eventos para com o Monitor criar alertas.<br>Essas opções ajudam a ter os dados de diagnostico dentro do Azure, mas incorre em custos. |



| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Aplicativos** | As aplicações são um importante item no gerenciamento de MDM. A maior parte das empresas deseja que os dispositivos dos colaboradores tenha aplicativos corporativos instalados no perfil de trabalho protegidos contra cópia e troca de informações com outros que podem ser inseguros.<br>Tambem é possível publicar sites e assim evitar vazamento de dados usando o perfil corporativo. |
| **Aplicativos**<br>**Publicação** | A publicação vai variar conforme o dispositivo.<br>• Windows e macOS tem uma interessante funcionalidade que é a instalação do Edge ou do próprio Microsoft 365 onde você poderá criar uma regra já predefinida com as opções que estes aplicativos possuem. Por exemplo em Office 365 poderá definir quais aplicações, o canal de distribuição e como será publicado na loja.<br>• Android, iOS e Windows podem ser aplicativos das lojas bastando pegar o link publico da Apple, Google ou Microsoft Store. Nestes casos ao publicar um aplicativo indique os itens respectivos a cada plataforma, lembrando que estes ficarão disponíveis na loja e serão instalados no perfil trabalho<br>• Loja customizada de aplicativos é um importante recurso que as empresas querem e precisam utilizar. Por exemplo o seu time de desenvolvimento cria um aplicativo para Android (APK) e iOS (IPA) mas não podem publicar nas lojas por conta do perfil publico e custos envolvidos. Nestes casos utilize a opção Aplicativos de linha de negócio e publique diretamente estes arquivos.<br>O interessante é que em um dispositivo normal você só conseguiria instalar um APK ou IPA se desligasse a segurança de aplicações, o que representa um grande risco. No caso da loja corporativa os aplicativos estão previamente testados já que são pertencentes a própria empresa. |
| **Aplicativos**<br>**Politicas** | • Politicas de proteção de aplicativos é interessante para isolar aplicações que você publicou anteriormente. Por exemplo digamos que você queria definir um UBER onde o usuário não poderá compartilhar os dados, nesse caso crie essa regra e indique que os dados devem ser criptografados, não podem ser fotografados e copiados, além de outras configurações interessantes nesses cenários onde aplicativos públicos são usados na empresa nos perfis empresariais.<br>Essas regras são muito similares as regras de configuração do dispositivo, mas aqui são aplicadas especificamente para os dispositivos com aqueles aplicativos.<br>Importante ressaltar que também é aqui que você desinstalará aplicativos, pois ao criar um app você terá a opção de uninstall para mudar o comportamento da politica.<br>• Politicas para aplicativos do Office 365 são politicas onde podemos definir recursos do Office 365 permitindo até desligar recursos. Um item muito utilizado por exemplo é bloquear o uso de scripts em documentos Word ou Excel, proibir salvar arquivos em formatos antigos do Office, carregar suplementos e usar recursos beta ou incluir outros e-mails pessoais no Outlook Mobile.<br>O numero de politicas possíveis é grande, então é necessário olhar e decidir entre centenas de configurações o que você já tem ideia de que seriam recursos que seus colaboradores não poderiam usar por entender que representariam riscos.<br>• Conjunto de politicas é similar ao que já tratamos em politicas de dispositivos. |
| **Aplicativos**<br>**Limpeza seletiva** | Essa opção é utilizada para limpar os itens de aplicativos do perfil corporativo do dispositivo. Por exemplo se um usuário tem problemas no celular mas não foi extraviado, essa opção irá limpar os dados para que ele reinstale os aplicativos. |



| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Segurança do ponto de extremidade** | Diversas configurações de segurança podem ser inseridas nesse menu.<br>Em geral são realizadas com um bom controle, já que podem afetar o funcionamento do dispositivo pessoal do usuário.<br>Em alguns menus temos opções para o Windows Defender ATP disponível apenas no Windows E5. |
| **Segurança do ponto de extremidade**<br><br>**Linhas de base** | As linhas de base são predefinidas e permitem escolher as configurações desejadas.<br>• Windows tem um vasto numero de configurações, onde podemos ligar e configurar itens como bitlocker, bloqueio de tela, experiencia visual, firewall, remote desktop e até bloqueio de drivers. Em muitos casos, se não a maioria, conflitam com opções que já existem em GPO. Mas isso faz sentido uma vez que o Intune é visto como um gerenciador integrado de dispositivos, enquanto GPO se limita configurar apenas o Windows e não ser integrado a outros MDMs.<br>• Edge permitirá configurar as opções do aplicativo, destacando os protocolos, desabilitar Flash ou extensões. |
| **Segurança do ponto de extremidade**<br><br>**Antivirus e Detecção e resposta** | Aqui podemos configurar o Windows Defender nativo do Windows 10 e macOS separados em 3 tipos de configurações. A primeira se refere as configurações comuns do Windows Defender como interface, usar cloud, etc. A segunda se refere as exclusões, normalmente utilizadas para indicar diretórios onde não deverá ser verificado por questão de performance ou serem aplicativos conhecidos. O terceiro é a experiencia geral do console de segurança do Windows 10.<br>Nas opções de detecção indica se o dispositivo irá enviar dados para o Intune. |
| **Segurança do ponto de extremidade**<br><br>**Criptografia de disco** | Configure o comportamento do Bitlocker para Windows 10 e o FileVault do macOS.<br>São configurações padrões, mas importantes para que você tenha garantia de não ter vazamentos de dados por roubo de notebooks.<br>Todas as empresas deveriam ter regras de criptografia nos seus notebooks, e neste caso o Intune supera GPO pois permite configurar não só o Bitlocker mas também o FileVault. |
| **Segurança do ponto de extremidade**<br><br>**Firewall e Proteção de contas** | Este tópico dispensa explicações. Configure regras para o firewall do Windows ou do macOS de forma centralizada pelo Intune.<br>Já o item proteção de contas irá permitir poucas configurações pois está em testes e atualmente liga o Credential Guard nativo do Windows e o Windows Hello. Lembrando que o Credential Guard é uma forma que o Windows Enterprise usa para virtualizar o momento em que o usuário se autentica. |
| **Segurança do ponto de extremidade**<br><br>**Redução da superfície de ataque** | Neste menu com diversas opções para Windows 10, temos uma grande lista de opções separadas pelo tipo de perfil, ou seja conjunto de regras a serem aplicadas.<br>Em redução de superfície pode-se indicar se deseja validar scripts, chamadas de APIs nos scripts do Office, bloquear lsass e Adobe, etc. Em controle de dispositivos poderá bloquear o uso de dispositivos bluetooth de certas funções ou até limitar os que podem ser utilizados. Isolamento de aplicativos e navegador poderá indicar o comportamento do Application Guard para impedir que a partir deles se utilizem certas opções que podem gerar vazamentos como impressão de uma página. As três opções seguintes são mais simples com o uso do SmartScreen em duas que também podem ser ligadas em outros menus e exploits baseados em regras XML que precisam ser criados com as configurações desejadas.<br>https://docs.microsoft.com/pt-br/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-protection |

# Microsoft Cloud App Security (CASB)

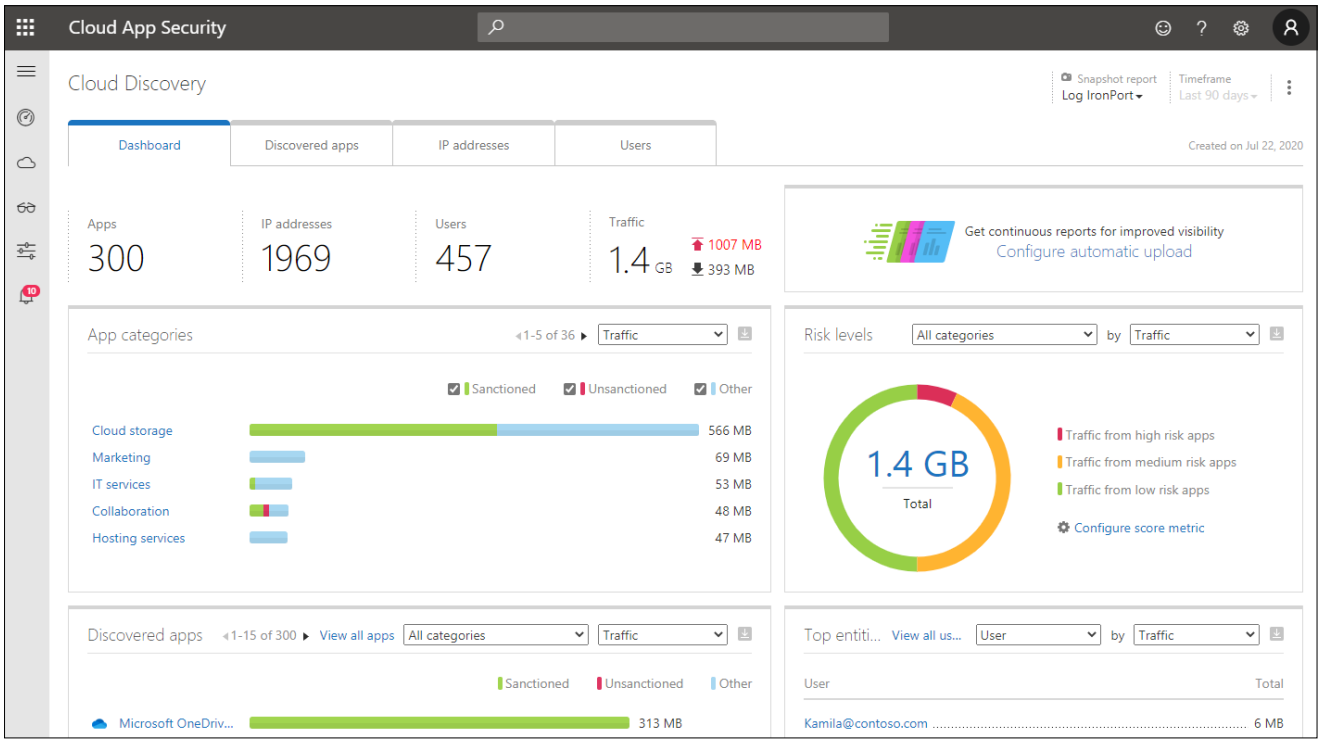
Esta ferramenta é um dos produtos essenciais para segurança corporativa com o advento da internet.

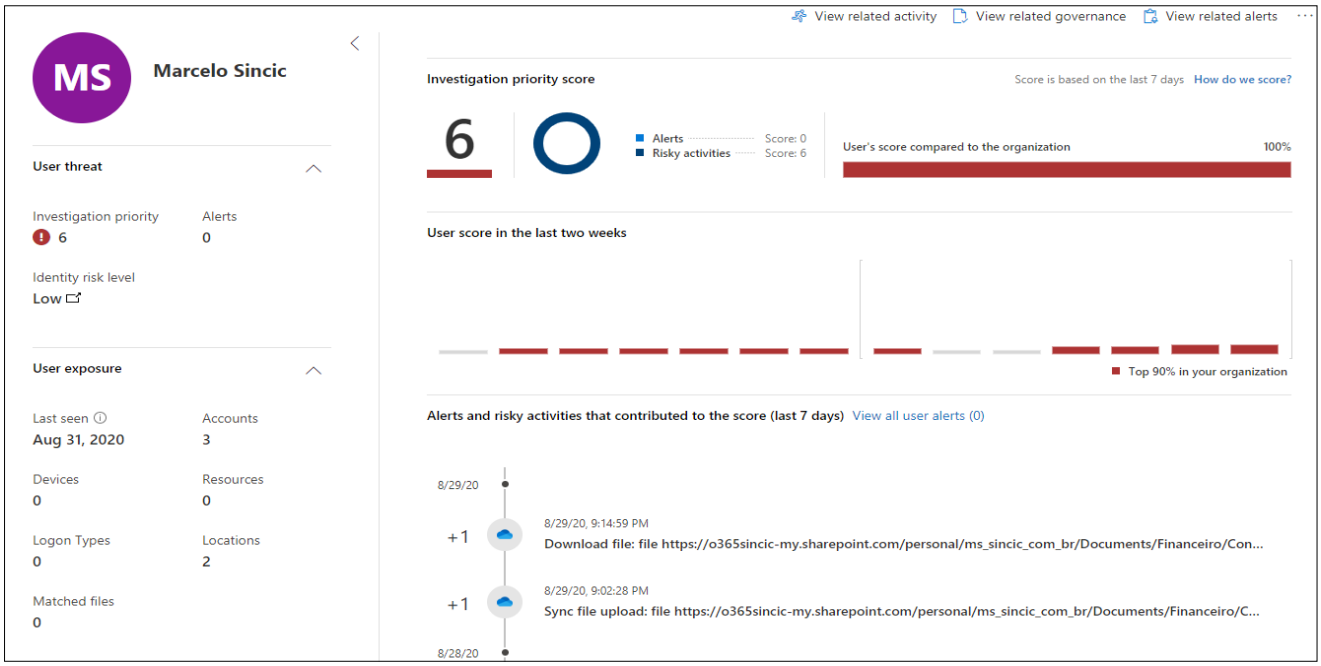
A partir da análise do fluxo de dados tanto de aplicações web quanto de seus firewalls e roteadores de borda, detectam diversos tipos de comportamento suspeito. Por exemplo a partir do log de acessos ou de um firewall poderá identificar ações de risco como logon simultâneo, em países diferentes (impossible travel), etc.

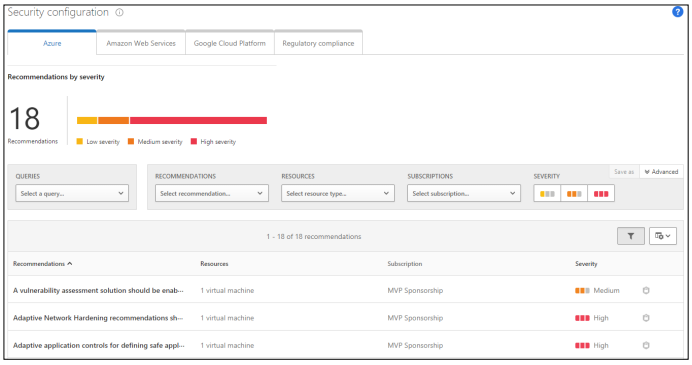
A partir da integração com diversos serviços web podemos coletar o uso e troca de dados, que incluirá as regras de DLP se estiverem habilitadas.

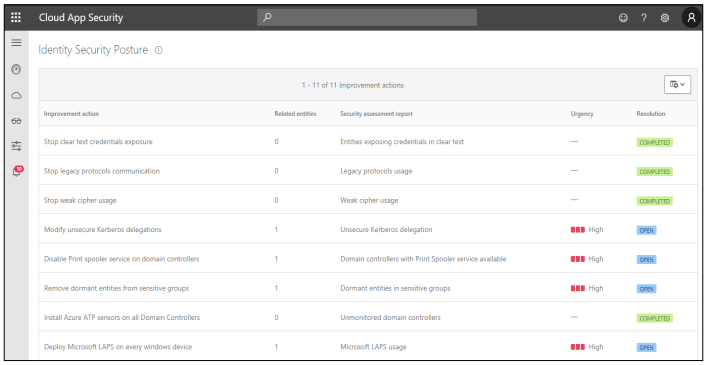
O CASB está disponível nos planos E5.

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Dashboard** | Aqui poderá visualizar todos os alertas e avisos que forem gerados. É um painel simples para que se dê foco nos principais problemas e avisos encontrados. |
| **Discover Dashboard** | Neste painel poderá visualizar toda a atividade que foi importada por um firewall, com os detalhes do tipo de aplicação, IP e tipo de uso da rede. Este sem dúvida é um dos mais informativos painéis do CASB para monitorar atividades. |
| **Discover Apps** | A Microsoft pré-configura as aplicações com base na experiencia de todos os usuários e ocorrências publicas, gerando um Score indicando o nível de segurança. Ao carregar o log será possível ver quais apps foram acessados na internet e por quantos usuários.<br>Tambem é possível não sancionar, ou seja definir que aquele app não é seguro. Mas nesse caso como barrar já que o dashboard é montado com base no log passado? Utilizando o menu dos 3 pontos no canto superior direito terá a opção *Generate Block Script* que ao informar o modelo do seu firewall ele irá gerar o script para ser importado e executado, e assim bloqueando o app não sancionado.<br>Tambem é possível se o login é com SSO usando o AAD criar uma regra condicional para determinada aplicação com base no que está sendo listado no uso |
| **Discover IP address e Users** | Permitem que se utilize um filtro por clique para cada usuário ou IP.<br>Assim se desejar ter mais detalhes sobre o que foi feito a partir de um determinado IP ou usuário, clique sobre ele e terá todo o histórico dos acessos realizados. |
| **Discover Cloud snapshot report** | Aqui é onde importamos um log de firewall.<br>De operação simples, basta informar o tipo de equipamento da origem e fazer o upload do arquivo de log e o CASB irá analisar e incluir no dashboard. |
| **Investigate Activity log e Users and Accounts** | Este dashboard filtra os usuários por tipo de ameaça ou atividade administrativa que ele tenha realizado. No menu de 3 pontos ao final de cada linha é possível ver quem fez as mesmas atividades, atividades do usuário atual, do mesmo IP ou da mesma região/pais.<br>Com isso, a partir desse painel podemos analisar se um evento aconteceu com o mesmo usuário em outros locais suspeitos ou por outros usuários, que poderia indicar um malware. |
| **Investigate Files** | Ao habilitar essa função poderá visualizar atividades em arquivos do OneDrive, SharePoint, DOCS, Google Drive ou qualquer outro SaaS de armazenamento vinculado.<br>Assim como a opção acima, ao clicar no final da linha terá varias opções para pesquisa e também poderá aplicar um label de classificação para indicar que é um documento confidencial ou precisa de retenção. |
| **Investigate Security** | Ao integrar suas contas do Azure, AWS ou GCP ao CASB poderá ter acesso as recomendações de segurança das plataformas. Por exemplo do Azure ele irá se integrar ao Security Center para que você tenha uma visão integrada das recomendações de segurança nas plataformas. |
| **Investigate Identity Security Posture** | Nesse painel são listadas ações que precisam ser tomadas para evitar certos tipos de ameaças.<br>Na lista poderá ver quantos usuários ou computadores estão vulneráveis e para aplicar as correções necessárias, lembrando que o CASB não interage com servidores, ele apenas alerta. |


Cloud App Security
Cloud Discovery
Snapshot report
Log IronPort
Timeframe
Last 90 days
Dashboard
Discovered apps
IP addresses
Users
Created on Jul 22, 2020
Apps
300
IP addresses
1969
Users
457
Traffic
1.4 GB
1007 MB
393 MB
Get continuous reports for improved visibility
Configure automatic upload
App categories
1-5 of 36
Traffic
Sanctioned
Unsanctioned
Other
Cloud storage
566 MB
Marketing
69 MB
IT services
53 MB
Collaboration
48 MB
Hosting services
47 MB
Risk levels
All categories
by
Traffic
1.4 GB
Total
Traffic from high risk apps
Traffic from medium risk apps
Traffic from low risk apps
Configure score metric
Discovered apps
1-15 of 300
View all apps
All categories
Traffic
Sanctioned
Unsanctioned
Other
Microsoft OneDriv...
313 MB
Top entiti...
View all us...
User
by
Traffic
User
Total
Kamila@contoso.com
6 MB


View related activity
View related governance
View related alerts
MS
Marcelo Sincic
User threat
Investigation priority
6
Alerts
0
Identity risk level
Low
User exposure
Last seen
Aug 31, 2020
Accounts
3
Devices
0
Resources
0
Logon Types
0
Locations
2
Matched files
0
Investigation priority score
Score is based on the last 7 days
How do we score?
6
Alerts
Score: 0
Risky activities
Score: 6
User's score compared to the organization
100%
User score in the last two weeks
Top 90% in your organization
Alerts and risky activities that contributed to the score (last 7 days)
View all user alerts (0)
8/29/20
+1
8/29/20, 9:14:59 PM
Download file: file https://o365sincic-my.sharepoint.com/personal/ms_sincic_com_br/Documents/Financeiro/Con...
+1
8/29/20, 9:02:28 PM
Sync file upload: file https://o365sincic-my.sharepoint.com/personal/ms_sincic_com_br/Documents/Financeiro/C...
8/28/20


Security configuration
Azure
Amazon Web Services
Google Cloud Platform
Regulatory compliance
Recommendations by severity
18
Recommendations
Low severity
Medium severity
High severity
QUERIES
RECOMMENDATIONS
RESOURCES
SUBSCRIPTIONS
SEVERITY
1 - 18 of 18 recommendations
Recommendations
Resources
Subscription
Severity
A vulnerability assessment solution should be enab...
1 virtual machine
MVP Sponsorship
Medium
Adaptive Network Hardening recommendations sh...
1 virtual machine
MVP Sponsorship
High
Adaptive application controls for defining safe appl...
1 virtual machine
MVP Sponsorship
High


Cloud App Security
Identity Security Posture
1 - 11 of 11 improvement actions
Improvement action
Related entities
Security assessment report
Urgency
Resolution
Stop clear text credentials exposure
Entities exposing credentials in clear text
COMPLETED
Stop legacy protocols communication
Legacy protocols usage
COMPLETED
Stop weak cipher usage
Weak cipher usage
COMPLETED
Modify unsecure Kerberos delegations
Unsecure Kerberos delegation
High
OPEN
Disable Print spooler service on domain controllers
Domain controllers with Print Spooler service available
High
OPEN
Remove dormant entities from sensitive groups
Dormant entities in sensitive groups
High
OPEN
Install Azure ATP sensors on all Domain Controllers
Unmonitored domain controllers
COMPLETED
Deploy Microsoft LAPS on every windows device
Microsoft LAPS usage
High
OPEN

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Investigate**<br>**OAuth apps** | Ë muito comum que nossos usuários utilizem o app de email do celular ou tablet para se conectar aos serviços, mas isso é risco uma vez que muitas dessas apps guardam o usuário e senha em modo texto nos aplicativos.<br>Esse painel irá mostrar apps que tem o nome e senha do usuário gravados permanentemente e o grau de risco que isso pode ocasionar, sendo um importante aliado no vazamento de acessos. |
| **Investigate**<br>**Connected apps** | Aqui é onde iremos incluir sites e serviços web para serem monitorados quando um usuário utilizar uma senha de SSO. A lista de serviços possui AWS, Dropbox, G Suite, SalesForce e outros.<br>Uma vez integrados, qualquer atividade realizada com as contas da sua organização passarão por auditoria e garantirá que arquivos trocados, acessos e tarefas sejam devidamente seguras. |
| **Control**<br>**Policies** | Muitas politicas do CASB são previamente criadas com base no retorno que a Microsoft tem dos clientes. A partir dessa lista você pode habilitar ou não as regras disponíveis.<br>Escolha na lista as regras que deseja habilitar ou desabilitar, mas a recomendação é que estejam habilitadas para melhorar a segurança e auditoria do ambiente, exceto regras que gerem falsos positivos.<br>Se isso acontecer, você poderá desabilitar a regra padrão e criar uma nova politica utilizando como modelo a regra desabilitada e adicionar um filtro que evite por exemplo o monitoramento de um servidor |
| **Control**<br>**Templates** | Muito parecido com as politicas, alguns modelos já estão precarregados, mas a diferença é que precisam ser configurados para funcionar, ou seja você deverá adicionar informação para que ele se torne uma politica.<br>Por exemplo ao escolher o modelo *New popular app* para avisar de sites novos que os usuários estão utilizando, deverá indicar quem irá receber notificação e a partir de quantos usuários terem acessado.<br>Outro template de destaque é o *File shared with unauthorized domain* onde existem ações como definir um label de confidencialidade ao documento compartilhado com pessoas de fora. Por fim, aplicar regras de DLP a todos os documentos compartilhados com outros apps também é importante para garantir sua segurança em documentos enviados que não sejam por email. |
| **System**<br>**Security Extensios** | Nas configurações do CASB (engrenagem no canto superior ao lado do usuário) poderá indicar DLPs externos, SIEM para receber ou enviar os alertas integrados com SYSLOG, tokens e playbooks (Power Automate). |
| **System**<br>**Settings** | Aqui temos uma série de opções que podem ser configuradas, vamos destacar algumas:<br>• Score metrics lhe permitirá mudar os critérios que formam a nota 1 a 10 de apps. Por exemplo se para você é obrigatório MFA suba o nível desse recurso nas notas<br>• Snapshot reports são acessíveis por outros menus acima e permitem importar o log de equipamentos de rede como firewall ou roteadores, manualmente<br>• Automatic Log upload é similar ao Snapshot porem aqui definimos um método automatizado como ler direto via SYSLOG ou carregar de um FTP o log que tenha sido pré-gravado. Com isso podemos criar rotinas de importação e exportação de dados sem fazê-lo manual<br>• Exclude entities dá a opção de IPs e usuários em “lista branca”<br>• MS Defender ATP se implementado poderá bloquear o acesso diretamente pelo agente do Defender, assim evitando ter que exportar scripts para os equipamentos de rede<br>• User enrichment é interessante para mostrar os dados do AD a partir dos logs importados, tornando a identificação dos recursos mais simples com os atribuitos do AD<br>• Anonymization irá tornar todos os reports criptografados, o que é um requisito do LGPD. Porem com as regras é possível criar usuários com poder de ver os dados depois de justificar o motivo<br><br>As demais opções você poderá habilitar serviços integrados, customizar mensagens ou lista de usuários com determinada permissão e são autoexplicativas. |

# Azure Advanced Threat Protection (ATP/ATA)

Esta ferramenta analisa atividades do Active Directory on-premisse para detectar comportamentos e ameaças que estejam ocorrendo. Seus dados se integram ao CASB, já que este não analisa dados locais.

Possui 2 versões: ATA on-premisse e ATP online. O primeiro disponível nos planos EMS E3 e o segundo EMS E5.

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Linha do tempo** | Nesse menu poderá ver as diferentes ocorrências.<br>Serão listados uso de credenciais administrativas de forma desnecessárias, acesso remoto por comandos como PowerShell, acesso de comandos de um computador para outro por meio de scripts.<br>Em geral os alertas são auto explicativos e você poderá dizer que estão em investigação, ignorar no momento ou dizer que é um falso positivo permanente.<br>Ao abrir um desses alertas verá detalhes em um esquema gráfico da execução da ameaça. |
| **Configurações** | É aqui que estão as configurações interessantes do ATA/ATP<br>• Integração com o Windows Defender ATP permitirá que ele receba dados e integre as ameaças detectadas nos servidores com o sensor, garantindo maior segurança<br>• Marcas de entidade permite que você defina usuários *fake* para determinar ataques. Por exemplo se criar um usuário diretoria poderá detectar ataques uma vez que esse usuário não existe no ambiente. São usuários que chamamos de *honeytoken* pois são nomes comuns, então lembre-se de não utilizar aqui seus usuários reais.<br>• Confidencial são usuários e grupos reais sensíveis a alterações. Por exemplo o grupo Enterprise Admins pode ser considerado sensível e todas as operações com esse grupo serão logadas<br>• Notificacões permitirá enviar alertas para SYSLOG se você possui algum outro sistema externo de monitoração que queira juntar os alertas |

# Windows Defender Antivírus/Security Center

Ferramenta mais recente da Microsoft tem funcionalidades muito boas tanto como antivírus de ultima geração (NGAV) como análise de segurança do ambiente e das maquinas.

Disponível no Windows E5 ou como add-on, atualmente já possui agente para Android, Linux e macOS.

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Threat Analytics** | Esse painel é particularmente interessante por trazer as atuais ameaças em circulação com detalhes do que elas afetam.<br>Uma vez que o agente está instalado nos dispositivos ele irá te avisar se você foi afetado. |
| **Incidents**<br>**Device Inventory**<br>**Alerts queue** | Nestes 3 painéis será possível visualizar os incidentes e inventário do ambiente.<br>É o painel usado no dia a dia para os administradores e operadores de segurança para saberem onde ocorreram e que tipo de ataque sua organização passou.<br>Cada um desses painéis mostram diferentes tipos de ataques permitindo fazer o acompanhamento gráfico ou textual do que aconteceu, utilizando a tecnologia EDR já existente em outros NGAV do mercado |
| **Partner applications** | Uma boa configuração nesse item é que irá garantir um bom desempenho e monitoração. Utilizando do Microsoft Graph for Security API estes fabricantes podem interagir com os alertas no MDSC.<br>Integrar o MDSC com outras ferramentas fará com que a analise e abrangência se tornem sólidas no conjunto das ferramentas disponíveis não só no Microsoft 365, como também do Azure e terceiros.<br>Por exemplo a integração com RSA permitirá saber se os usuários com tokens estão sendo de alguma forma imprudentes ou sendo atacados. Já a integração com ServiceNow irá gerar automaticamente Change Requests a partir de regras para agregação e mapeamento de alertas, facilitando ao seu time de operações tomar as ações necessárias o mais rápido possível. Até outros produtos de segurança como o Symantec EPM podem ser integrados como um único painel. |
| **Automated** | Defina como serão realizadas as correções utilizando os níveis determinados.<br>É importante validar essas configurações, por exemplo se o usuário deverá consentir na correção.<br>https://docs.microsoft.com/pt-br/windows/security/threat-protection/microsoft-defender-atp/automated-investigations |
| **Threat and Vulnerabilities Mgmt** | Mais um painel para visualizar os eventos ocorridos, com a diferença de alguns itens de ação como remediação onde poderá ter detalhes como softwares arriscados e até uma lista completa de todas as thrers de segurança que estão ativas, por exemplo nesse momento são mais de 117 mil avisos de segurança ativos globalmente.<br>Um painel que particularmente achamos interessante é o Event timeline, pois aqui podemos ver tendências quando um grupo de usuários é afetado. Enxergamos qual foi a sequencia em que diferentes tipos de ataques ocorreram e assim podemos treinar os usuários para se precaverem. |
| **Evaluation and tutorials** | Gerar dados para ver e treinar a equipe é importante, mas esperar que os diferentes tipos de ataque ocorram pode demorar muito tempo ou até nunca serem alvos.<br>Para isso aqui podemos baixar script para serem executados em maquinas com o agente do Defender ATP para popular os painéis em Tutorials, em Simulations catalog poderá utilizar exemplos reais de cenários com ataques, incluindo produtos de terceiros com funcionalidades especificas. |
| **Configurations e Settings** | Configurations é apenas um dashboard já que ingressar os dispositivos é realizado pelo Intune.<br>Já em Settings temos diversas opções, destacando Onboarding e Offboarding para instalar ou desinstalar os agentes.<br>As outras opções se referem a administração realizada, por exemplo reativar alertas que foram suprimidos anteriormente, criar lista de indicadores, pastas excluídas da monitoração, monitoração e coleta de memória e extensões de arquivo que obrigatoriamente devem ser analisados.<br>Lembrando que essas opções não impedem o acesso e funcionamento padrão, altere apenas após consultar a documentação referente ao item. |

# Azure Information Protection

Ferramenta no Azure para classificação automática de documentos, permitindo a instalação de sensores para classificar documentos locais (on-premisse) baseado em regras de DLP ou customizadas.

Disponível no EMS E3 (plano 1) e EMS E5 (plano 2).

| Produto ou Serviço | Definições de Segurança disponíveis |
|---|---|
| **Relatórios** | Os relatórios do AIP são importantes para detectar auto rotulagem e documentos encontrados com dados sensíveis que não foram classificados pelo usuário.<br>Em Recomendações o AIP irá lhe informar ações pró-ativas para evitar o vazamento de informações em documentos de uma forma didática como feito nos outros consoles que já comentamos. |
| **Rótulos** | São os mesmos rótulos que vimos no painel de Segurança no item classificação.<br>Porem, aqui temos algumas configurações adicionais como a fonte da marca d'agua e a regra de rótuclo automático, sendo este importante para prevenir que o usuário não tenha rotulado algo confidencial.<br>Pode parecer que é uma duplicidade em relação ao que já foi abordado em DLP, mas nesse caso é mais simples de ser visualizado uma vez que no painel de DLP as regras são separadas dos rótulos. |
| **Políticas** | Essas politicas se parecem também com as politicas do DLP e são inclusive exportadas para lá, porem aqui o visual é mais simples e tem opções adicionais como esconder o botão Encaminhar para conteúdo sensível.<br>Importante que essas politicas são aplicadas a todos os usuários (default), enquanto em DLP só se as condições forem satisfeitas. |
| **Scanner** | Este é o principal recurso do AIP e disponível apenas aqui, enquanto os acima são replicados em DLP.<br>Os sensores nada mais são do que agentes instalados nos seus File Server para vasculhar e categorizar automaticamente documentos confidenciais baseados em regras pré-definidas nos classificadores ou customizadas (disponível no EMS E5). Ele pode ser executado inclusive em servidor SQL Server<br>https://docs.microsoft.com/pt-br/azure/information-protection/deploy-aip-scanner |
| **Rotulagem unificada** | Não se esqueça de ativar essa opção, pois se estiver desligada os rótulos e politicas criadas aqui não irão aparecer em DLP e haverá confusão ou duplicação de regras. |