Microsoft Security

Protegendo Identidades

Azure Active Directory

scansource

Desafios de Identidade atualmente nas organizações

Adaptar-se ao novo trabalho híbrido que exige experiências continuas e flexíveis

Regulamentações de conformidade em evolução com implicações de privacidade e segurança de dados, como a Lei Geral de Proteção de Dados.

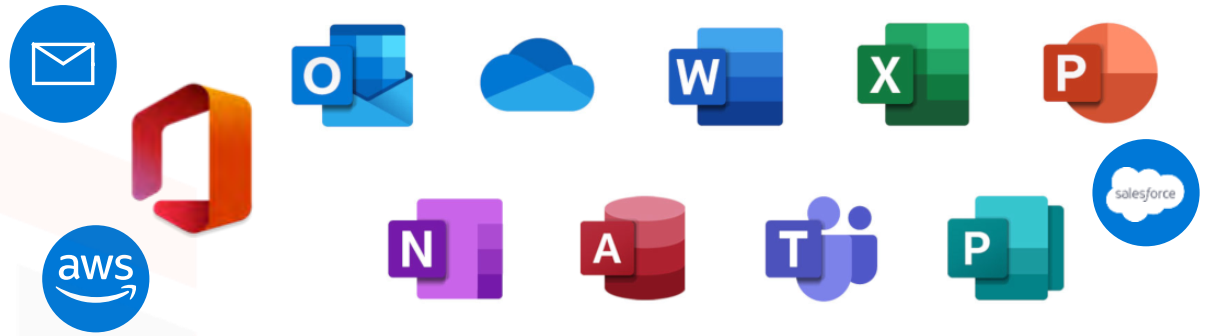
Aumento de apps, dentro e for a da empresa, **necessitando de acesso seguro**

Demandas por produtividade, segurança e modernização de TI

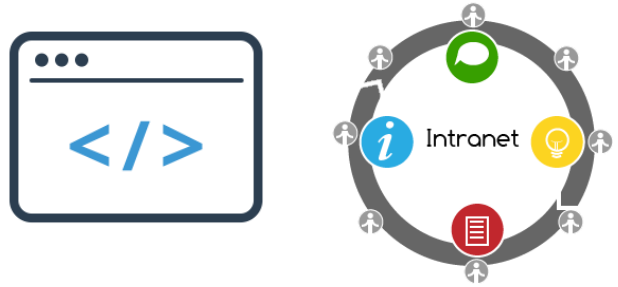
Azure AD — O maior serviço de identidade em nuvem do mundo

O Azure AD (Active Directory) é o serviço de gerenciamento de identidade e de acesso baseado em nuvem da Microsoft, que ajuda seus funcionários a se conectar e acessar os recursos de forma segura em:

Recursos externos, como o Microsoft 365, o portal do Azure e milhares de outros aplicativos.



Recursos internos, como aplicativos em sua rede corporativa e intranet, juntamente com outros aplicativos de nuvem desenvolvidos por sua organização.



Fornece ferramentas avançadas para ajudar a proteger automaticamente as credenciais e identidades de usuário e para atender aos seus requisitos de controle de acesso. Também é utilizado para dar acesso a recursos em nuvem, como Máquinas Virtuais, bancos de dados, aplicações e outros. Quando habilitados, os recursos trazem mais segurança e controle ao ambiente de TI.

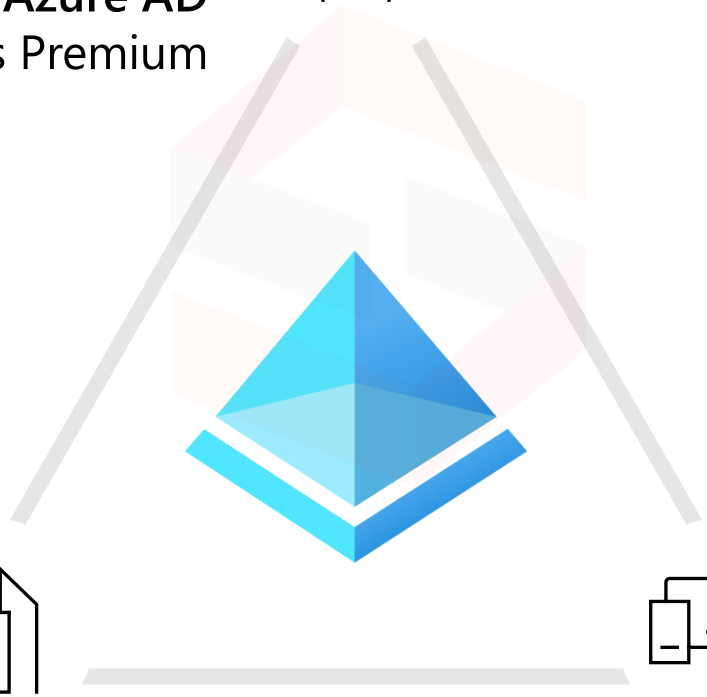
Possui integração com o Active Directory do Windows Server, promovendo maior segurança e integração entre ambiente local e de nuvem.

Azure AD — O maior serviço de identidade em nuvem do mundo

Milhares de organizações, milhões de usuários ativos, bilhões de solicitações diárias

300 Mil+

Azure AD
Empresas com recursos Premium



425 Mi+

Azure AD
Usuários mensais ativos

30Bi+

Azure AD
Solicitações de autenticação diarias

Recursos de proteção de Identidade do Azure AD

MFA

A autenticação multifator (MFA) é um processo em que um é solicitado uma forma adicional de identificação. É exigido um dos seguintes fatores a mais para que o usuário seja autenticado: Algo que você sabe (senha), algo que você tem (um dispositivo confiável como token, ou código via sms) ou algo que você é (biometria). Evita acesso em caso de roubo de senhas

Acesso Condicional

Reúne sinais para tomar decisões e impor políticas organizacionais. Exemplo: um gerente financeiro deseja acessar o aplicativo de folha de pagamento e deve a fazer autenticação a partir de um computador no Brasil. Acessos de IPs de fora do país ou dispositivos móveis, não são permitidos.

B2B

Gerencie usuários convidados e parceiros externos, como consultores, enquanto mantém o controle sobre seus próprios dados corporativos. Crie limites para o que estes podem acessar.

Identity Protection

Utiliza Machine Learning para detectar sinais de risco como viagem atípica, uso de ip anônimo, credenciais vazadas, pulverização de senhas e muito mais. Oferece ferramentas para analisar usuários entradas e detecções de risco.

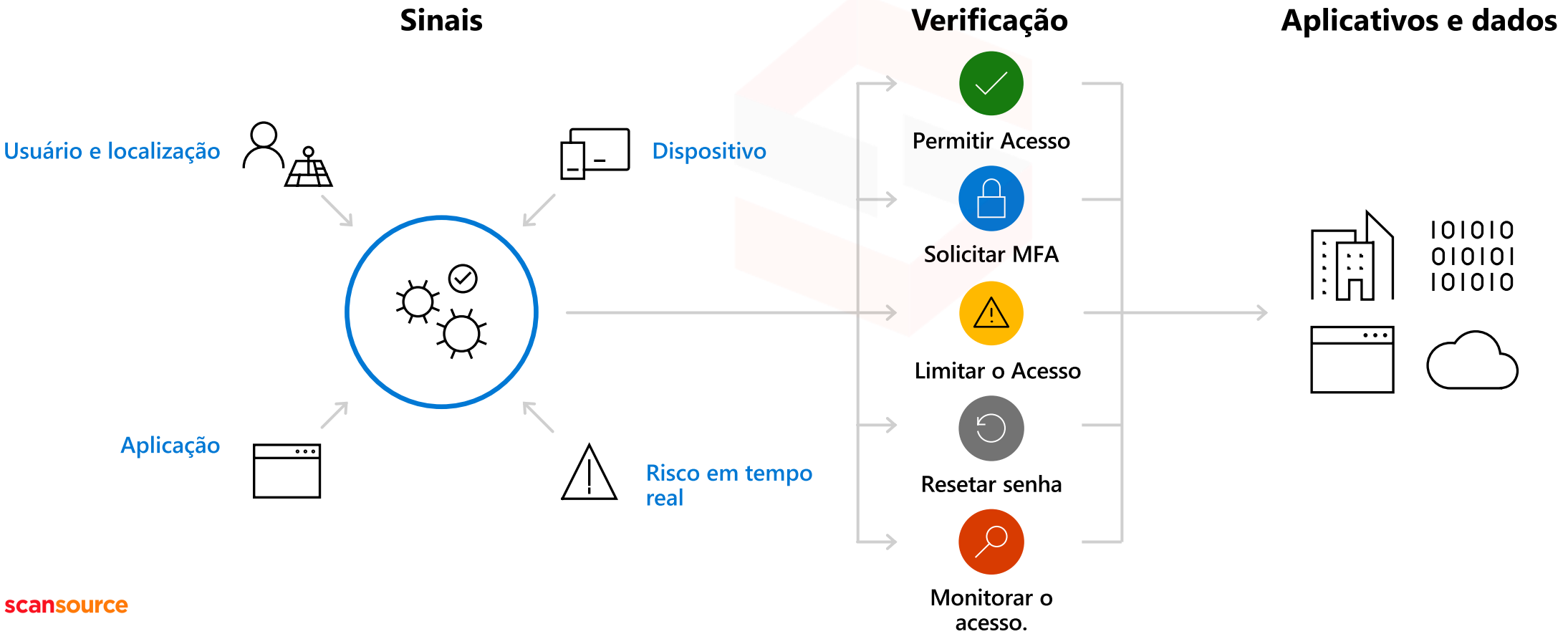
Privileged Identity Management (PIM)

Dê permissão por tempo determinado a arquivos e recursos sensíveis. O PIM fornece ativação de função baseada em tempo e aprovação, para atenuar os riscos de permissões de acesso excessivas, desnecessárias ou que foram indevidamente utilizadas em recursos importantes.

Funcionamento do Acesso Condicional

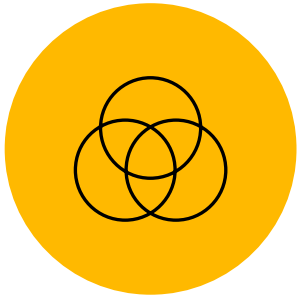
Habilita a Confiança Zero com autenticação forte e políticas adaptativas

Em sua definição mais simples, as políticas de acesso condicional são instruções “se-então”, se um usuário quiser acessar um recurso, então ele deverá concluir uma ação. Dependendo da ação concluída, o usuário terá acesso total ao dado ou aplicação, ou acesso limitado. Caso a condição não seja satisfeita, o acesso não é fornecido. A condição pode ser a versão do dispositivo, análise geográfica, comportamento, e outros. Parte-se do pressuposto que não deve-se confiar em nada e ninguém, até as condições serem satisfeitas. O Acesso Condicional evita que em caso de roubo de credencial o acesso não seja dado ao atacante, protegendo a empresa.



Edições do Azure AD

Serviço de identidade



Grátis

A edição gratuita do Azure AD está incluída com uma assinatura de um serviço online comercial, como Azure. Fornece recursos de MFA para acesso ao ambiente Cloud.

Para Microsoft 365

Recursos adicionais do Azure AD estão incluídas com as assinaturas do Microsoft 365. Fornece Pesquisa e relatórios de login por autoatendimento, além de recursos de autenticação de multifator (MFA).

Azure AD Premium P1

Além do MFA, permite que seus usuários acessem recursos locais e de nuvem. Administração avançada, como grupos dinâmicos, Microsoft Identity Manager (um conjunto de gerenciamento de acesso e identidade local) e recursos de write-back de nuvem, que permitem a redefinição de senha por autoatendimento para os usuários locais. Pode ser adicionado ao Microsoft 365 através de uma assinatura.

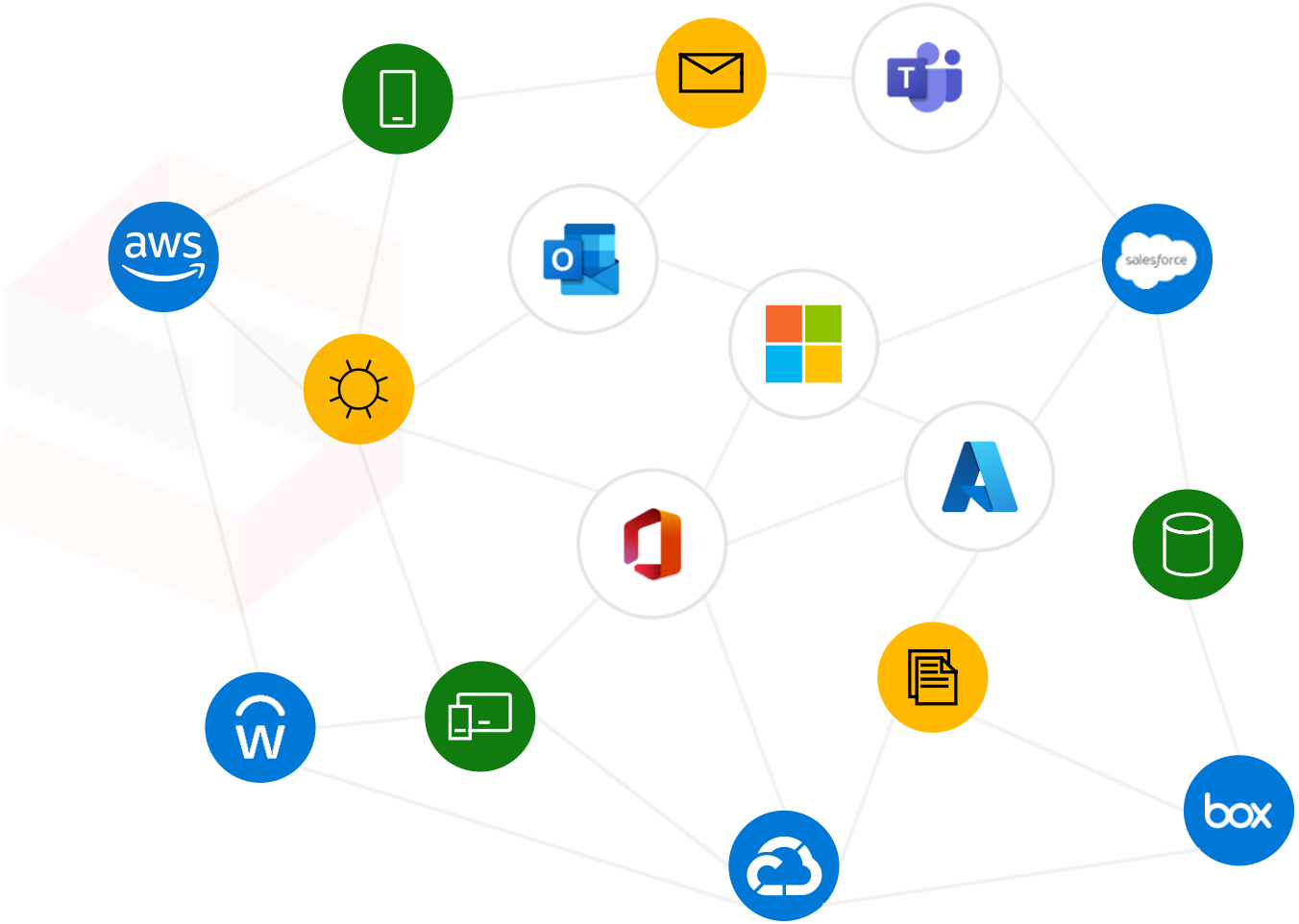
Azure AP Premium P2

Recursos do P1 e também oferece o Azure Active Directory Identity Protection, a fim de fornecer Acesso Condicional baseado em risco para seus aplicativos e dados críticos da empresa, e o Privileged Identity Management, para ajudar a descobrir, restringir e monitorar os administradores e o acesso deles a recursos e fornecer acesso Just-In-Time quando for necessário. Pode ser adicionado ao Microsoft 365 através de uma assinatura

Gerir Identidades para resolver questões de segurança

Pontos chave para uma Gestão Segura de Identidades com o Azure AD

- Habilitar o MFA previne 99,9% dos ataques a identidades.
- Habilite o SSPR (Selfie Service Password Reset) e diminua os custos com a TI, diminua o tempo de atendimento e evite compartilhamento de senhas.
- Crie políticas de Acesso Condicional para proteger os dados e aplicativos da organização.
- Modernize suas soluções locais, migrando a gestão de identidade para a nuvem sem afetar as integrações de aplicativos existentes. O Azure AD tem integração com o Active Directory do Windows.
- Utilize o Azure AD para analisar logs de auditoria, e os insights de segurança.



Microsoft Security

Obrigado.

scansource

Solicite apoio a um especialista de segurança Microsoft

microsoftcsp@scansource.com