Concepts of security, compliance and identity

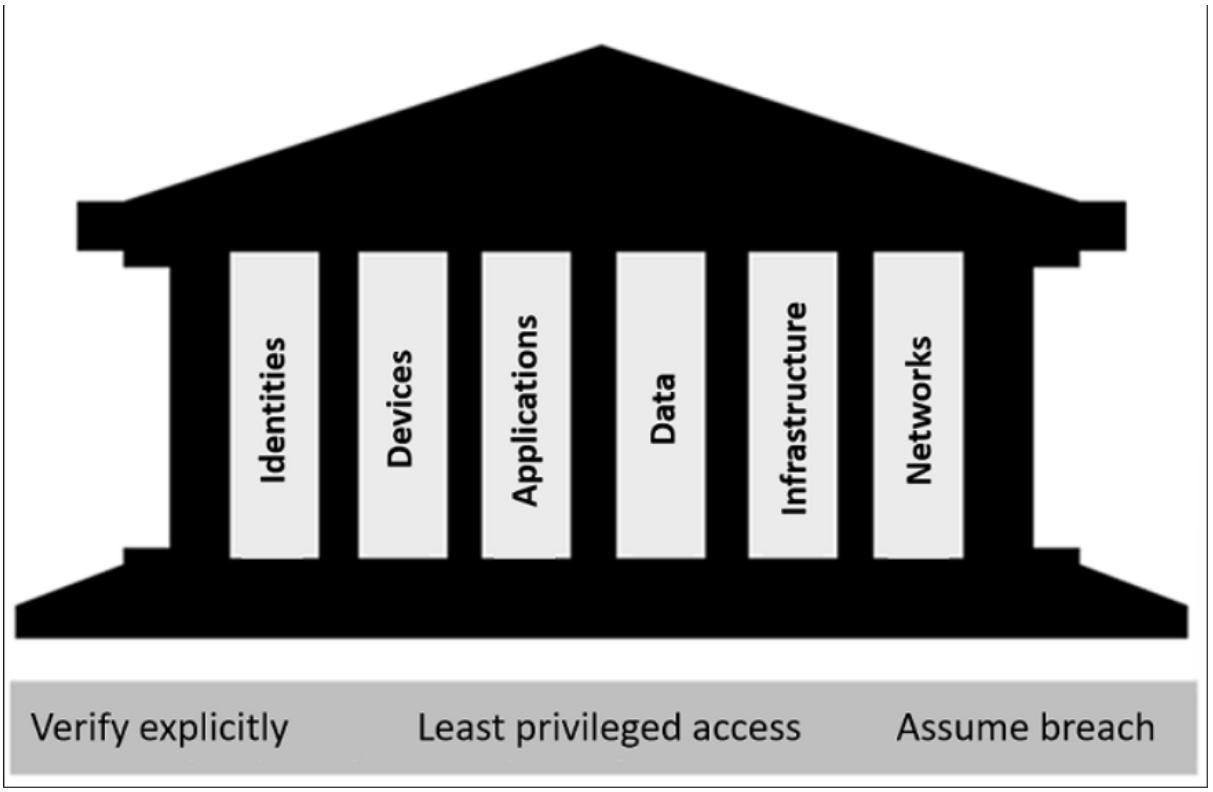
Shared Responsibility Model - define quais são as responsabilidades do *CSP* e do cliente na segurança da *cloud*. A ordem de menor responsabilidade para maior é: *SaaS*, *PaaS*, *IaaS* e *On-Premise*;

Defense In Depth - tem como propósito criar camadas de segurança para proibir possíveis ataques em diversos níveis. As camadas são: **física** (*datacenter*), **identidade e acesso**, **perímetro**, **rede**, **computação**, **aplicação** e **dados**;

Zero Trust - "*trust no one, verify everything*". Esse modelo assume que tudo está em uma rede aberta e sem controle, por isso a necessidade de se verificar tudo. É baseado em 3 princípios:

- *Verify explicitly*: sempre autentique e autorize com a maior quantidade de pontos de segurança possíveis (localização, dispositivo, *workload*, etc.);
- *Least privileged access*: fornecer acesso apenas o que é necessário e essencial;
- *Assume breach*: criptografar informações, ter visibilidade do ambiente, detectar ameaças;

Pilares do modelo *zero trus*t: ***identities***, ***devices***, ***applications***, ***data***, ***infrastructure*** e ***networks***;



Data Residency - localidade física onde os dados estão armazenados;
Data Sovereignty - as informações ficam sujeitas às regulações da região onde estão armazenadas;
Data Privacy - deixar claro e ser transparente quanto a coleta, processamento, uso e compartilhamento dos dados;

Autenticação - é o processo para provar que uma pessoa é quem ela diz ser. Sua abreviação é ***AuthN***;
Autorização - processo de verificar o que o usuário pode acessar. Sua abreviação é ***AuthZ***;

4 pilares da infraestrutura de identidade: administração, autenticação, autorização e auditoria;

Single Sign-On (SSO) - o usuário faz o login apenas uma vez e a credencial é utilizada para acessar múltiplos aplicativos;

On-Premise Active Directory:
- *AD DS - Active Directory Domain Services* é um serviço que armazena as informações dos usuários do domínio. É o recurso utilizado para fornecer serviço de identidade no ambiente *on-premises* das empresas;
- *AD DC - Active Directory Domain Controller* é o servidor que executa o *AD DS*;
- **Federação** é o termo utilizado para definir quando um serviço utiliza serviços de autenticação de outro. Um exemplo é a utilização da conta do google, twitter e facebook para realizar login em aplicativos. O usuário não precisa criar credenciais diferentes para acessar o serviço, pode utilizar a mesma em todos;

Capabilities of Microsoft Azure Active Directory

Service Principal - é a identidade para uma aplicação. Os desenvolvedores precisam gerenciar e proteger as credenciais;

Managed Identity - é um tipo de identidade para aplicação onde as credenciais são completamente gerenciadas;

Devices - a *device identity* fornece aos os administradores informações que podem ser utilizadas depois quando estiverem liberando acesso ou realizando configurações;
- *Azure AD registered devices*: permite aos usuários registrar os dispositivos pessoais no *Azure AD* sem a necessidade de uma conta no domínio da organização;
- *Azure AD joined*: utilizado para dispositivos da organização;
- *Hybrid Azure AD joined devices*: permite estender as funcionalidades do *Azure AD* para o *AD on-premise*;

Azure AD password hash synchronization - realiza uma cópia do *hash* da senha que estava no *on-premise* para a *cloud*;
Azure AD pass-through authentication - autentica o usuário no *AD on-premise*;
Federated authentication - é o modo de autenticação recomendado para empresas que utilizam meios não suportados pelo *Azure AD* (como *sign-on* com *smart cards*, *MFA* no *on-premise*). Todo o processo de autenticação ocorre no ambiente *on-premise*;

External Identity types:
- *B2B*: compartilhar os aplicativos e serviços da organização com outras pessoas;
- *B2C*: CIAM. Pode ter a identidade visual da plataforma modificada de acordo com o desejo da organização;

Métodos de login suportados pelo *Azure AD*:

- senha;
- telefone:
    - *sms-based*;
    - *voice call verification*;
- OATH:
    - Software OATH tokens;
    - OATH TOTP hardware tokens;
- *passwordless*;
- windows *hello for business*;
- FIDO2;
- microsoft *authenticator* app;

Security Defaults - são uma série de regras que são ativas por default para garantir um nível mínimo de segurança;

Self-service password reset - se ativo pelos administradores, os usuários poderão fazer a recuperação de senha caso necessário;

Password Protection - juntam uma série de artefatos para garantir que as senhas dos usuários estejam em conformidade com alguns requerimentos. É possível determinar as especificações que uma senha deve ter, utilizar *banned passwords list* que não só contém uma enorme quantidade de senhas vazadas na internet, como permite que a organização cadastre senhas e palavras-chave que não devem ser utilizadas;

Conditional Access - permite construir uma série de requerimentos para que o login de um usuário possa ser permitido;
Azure AD built-in roles:

- *global administrator*;
- *user administrator*;
- *billing administrator*;

Entitlement Management - é um conjunto de acessos à recursos que usuários (internos e guests) podem receber através de uma aprovação;

- *access package*: é o objeto principal do entitlement management, e contém tudo que será dado de acesso a ele, como acesso a recursos, grupos, sharepoint sites ou roles;

Azure AD PIM - serviço que permite gerenciar, controlar e monitorar o acesso a recursos da organização;

Identity Protection - automatiza a detecção e remediação de sign-in risks, investiga riscos usando dados coletados pelo portal e exporta dados de análise de risco para ferramentas externas (SIEM);

- *Sign-in Risk*: representa a probabilidade do login não ter sido autorizado pelo usuário. Alguns tipos de riscos que são detectados: IP anônimo, localização atípica, IP linkado com malware e *password spray*;

- *User risk*: representa a probabilidade da determinada conta estar comprometida. Vazamento de credenciais é um risco captado pela Microsoft;

Capabilities of Microsoft Security Solutions

Azure DDoS Protection - protege contra ataques *DDoS*. Existe em 2 *tiers*:
- *Default*: habilitado por padrão e sem custos extras;
- *Standard*: capacidades de monitoramento e defesa avançadas;

Azure Firewall - *firewall* gerenciado;

Azure WAF - protege as aplicações *web* de falhas e ataques comuns (como SQL Injection e XSS);

Azure Bastion - é um serviço disponível no *Azure Portal* que possibilita logar em uma VM sem a necessidade de se ter um IP público. Usar o *bastion* protege suas VMs visto que não é necessário a exposição de portas *RDP* e *SSH*. O *deploy* do *Bastion* é feito por VNet, possibilitando o *peering*;

Just-in-time access - é uma feature do *Microsoft Defender for Cloud* que permite liberar as portas de uma VM apenas quando deseja-se acessá-la;

Data Encryption:
- *Azure Storage Service Encryption:* criptografa os dados *at rest* presentes nos *managed-disks*, *blob storage*, *files* ou *queue storage*;
- *Azure Disk Encryption*: criptografa os dados de VMs Windows (usando *bitlocker*) e Linux (usando *dm-crypt*);
- *Transparent data encryption:* usado para proteção do *Azure SQL Database* e do *Azure Data Warehouse* criptografando e descriptografando as informações em tempo real;

Cloud Security Posture Management (CSPM) é o termo utilizado para descrever um conjunto de recursos utilizados para deixar a segurança na *cloud* mais robusta. Esses recursos monitoram a *cloud*, utilizam um sistema de pontuação para indicar o quão aderente o ambiente está com as principais regras e recomendações de mercado, aplicam *guardrails*, mapeiam riscos, entre outras capacidades;

Microsoft Defender for Cloud - CSPM da Azure. Pontua constantemente o ambiente, age contra ameaças aos workloads e recomenda melhorias para a segurança do ambiente. O *Defender for Cloud* vem em dois modos:
- *Free*: habilitado por padrão, oferece as funcionalidades básicas do recurso, como pontuação do ambiente e suas funcionalidades agregadas;
- *Defender for Cloud with enhanced security features*: estende as capacidades do plano *free* para outros ambientes (*on-premise*, outras *clouds*). Capacidades oferecidas pelo *enhanced security features*: segurança *multi-cloud* e *híbrida*, alerta contra ameaças, escaneamento de vulnerabilidades em VMs, *endpoint detection*;

O recurso de *workload protection* do *Defender for cloud* vem em diversas capacidades: *defender for servers*, *defender for app service*, *defender for storage*, *defender for sql*,

defender for kubernetes, *defender for container registries*, *defender for key vault*, *defender for resource manager*, *defender for DNS e defender for open-source relational protections*;

Azure Security Benchmark - é uma planilha fornecida pela Microsoft que auxilia as equipes de TI a gerenciar o ambiente *cloud* junto das melhores práticas do mercado;

O Microsoft *Defender for Cloud* utiliza o *Azure Security Benchmark* para realizar o *assessment* do ambiente;

SIEM - *Security Information Event Management*. É uma ferramenta de coleta de informações de toda a infraestrutura, aplicações e recursos;
SOAR - *Security Orchestration Automated Response*. Recebe alertas de múltiplas origens (como um *SIEM*) e dispara um gatilho que realiza uma ação em resposta ao alerta;
XDR - *Extended Detection and Response*.

Sentinel - *cloud-native SIEM/SOAR*. O *sentinel* coleta informações da organização, detecta possíveis ameaças, utiliza IA para investigar os incidentes e age contra eles. O *sentinel* contém diversos conectores para serviços da *Microsoft* e para serviços terceiros, como fonte de dados.

- *Workbooks*: visualizações de diversas informações de diversas origens (ex: *AD sign-in logs*, contendo diversas informações sobre o *sign-in* realizado pelos usuários);
- *Analytics*: regras prontas para análise de ameaças e de riscos. Os *logs* são armazenados em um *Log Analytics Workspace*;
- *Incidents*: gerados pelos alertas, são direcionados para os responsáveis e contém informações sobre o que ocorreu;
- *Hunting*: permite construir e executar *queries* nos incidentes e eventos gerados;
- *Automation*: execução de respostas aos incidentes;
- *Entity Behavior*: identifica anomalias e comportamento estranho nos dados utilizando inteligência artificial;

O *pricing* do *sentinel* ocorre de duas formas, *Capacity Reservations* permitem a contratação de um *tier* de serviços sendo cobrado pela capacidade contratada, *pay-as-you-go* sendo cobrado pela ingestão das informações no *analytics* e pelo armazenamento no *workspace*;

Microsoft 365 Defender - *cross-domain threat detection*. Domínios: *identity*, *endpoints*, *apps* e *email*. Disponível em 2 planos:

- *Plan* 1: configuração, detecção e proteção nos serviços do Office 365;
- *Plan* 2: tudo presente no *plan* 1 + automação, investigação, remediação e simulação;

Defender for Endpoint - detecta vulnerabilidades, redução de área de ataque (assegura que os dispositivos contenham as configurações mais recomendadas), usa *ML* para melhorar a proteção, detecta e responde à incidentes, investigação e remediação automatizada;

Defender for Cloud Apps - é um *CASB* (*Cloud Access Security Broker*), que fornece para a organização visibilidade, proteção contra ameaças, segurança de dados e compliance aos apps;

Defender for Identity - utiliza o *AD on-premise* para coleta de dados, identificação de ameaças e análise das informações;
Defender for Office 365 - proteção para usuários que estão utilizando o *office* 365.

Microsoft 365 Defender portal - contém todas as capacidades do *Defender for 365* em um portal *web* centralizado;

Capabilities of Microsoft compliance solutions

Service Trust Portal - é um portal público da Microsoft que fornece relatórios de compliance que falam sobre o tratamento dos dados pela parte da Microsoft. Para acessar o site, é necessário estar autenticado com uma conta da Azure. O portal fornece uma aba "*my library*" que permite salvar os documentos desejados para serem encontrados mais rápido;

Microsoft's 6 privacy principles:

- *Control*: o cliente tem controle de seus dados;
- *Transparency*: a Microsoft é transparente quanto aos dados coletados;
- *Security*: todas as informações confiadas à Microsoft são criptografadas e seguramente armazenadas;
- *Strong legal protections*: as leis aplicadas onde os dados residem são respeitadas e a privacidade é considerada um direito humano;
- *No-content based targeting*: as informações armazenadas não serão utilizadas para campanhas de marketing e venda de produtos;
- *Benefits to you*: quando informações são coletadas pela Microsoft, o intuito é sempre de melhorar a experiência do usuário;

Microsoft Priva - solução para gerenciamento de privacidade. As informações avaliadas são provindas do *Exchange Online*, *SharePoint Online*, *OneDrive for Business* e *Microsoft Teams*.

- *Priva Privacy Risk Management*: fornece uma visão geral dos dados da organização que estão compartilhados nos apps do 365;
- *Priva Subject Rights Requests*: fornece meios de automação para lidar com os pedidos dos clientes para rever as informações compartilhadas com a empresa em questão;

Purview compliance portal - acessado em "*compliance.microsoft.com*", é um portal centralizado que fornece visão das necessidades de *compliance* da organização. Usuários que sejam *global administrators*, *compliance administrator* ou *compliance data administrator* tem acesso ao portal;
Compliance Manager (aba) - oferece um *card* contendo a pontuação de *compliance* das ferramentas utilizadas. Oferece também uma visão centralizada do *assessment* feito no ambiente em relação aos principais órgãos e políticas reguladoras da região (*ISO*, *GDPR*, etc) e fornece soluções para os problemas do ambiente;
Algumas abas do *purview*:

- *Data Map*: realiza *data discovery* e *data governance*;
- *Data Catalog*: permite que os usuários procurem informações desejadas;
- *Data Estate Insights*: visão de alto nível de todos os dados que são analisados;

- *Data Sharing and Data Policy*: *data sharing* permite o compartilhamento das informações de maneira segura;

Control - é um requerimento de uma regulação. Define como gerenciar e avaliar as configurações para estar de acordo com alguma lei/regra;

Data Classification (aba) - identificar e classificar informações e documentos que são compartilhados entre os *apps* da organização.

- *Trainable Classifiers*: utiliza *ML* para analisar a informação e classificar ela (treinar o *classifier* para identificar o item);
- *Security Information Types*: informações sensíveis são identificadas por uma série de expressões regulares (*regex*). É possível construir um *regex* próprio para identificar informações sensíveis referente à organização;
- *Content Explorer*: permite visualizar o conteúdo que foi classificado. O acesso a esse recurso é e deve ser altamente gerenciado e restrito;
- *Activity Explorer*: fornece visibilidade nos arquivos que foram alterados ou tiveram suas labels alteradas;

Information Protection (aba) - descobre, classifica e protege informações sensíveis (de usuário e de negócio);

- *Sensitivity Labels*: *labeling* de emails e documentos. As *labels* criadas podem ser usadas para criptografar o conteúdo, adicionar marcas d'água, classificar o conteúdo (interno, confidencial, …), etc;
- *Label Policies*: as *label policies* são utilizadas para realizar a aplicação das *sensitivity labels*;

Data Loss Prevention (aba) - é uma capacidade do *microsoft purview* de identificar e prevenir informações confidenciais de serem divulgadas;

Endpoint Data Loss Prevention - estende as capacidades do *DLP* para itens sensíveis que estão fisicamente armazenados em máquinas com *Windows 10*, *Windows 11* e *macOS*;

Data Loss Prevention in Microsoft Teams - capacidades de *DLP* para mensagens em grupos e em canais privados;

Retention Labels - configuram as regras de retenção no nível de um documento, pasta ou e-mail;

Retention Policies - configuram as regras de retenção no nível de uma plataforma ou serviço da Microsoft (*ex*: excluir um documento no sharepoint que estiver lá há mais de 3 anos);

Records Management (aba) - permite utilizar das *retention labels* para transformar documentos e e-mails em registros, que não poderão ser editados ou deletados e serão armazenados em um local do sharepoint ou OneDrive;

Insider Risk Management - gerenciamento de riscos internos de uma organização. Esses riscos podem ser: vazamento de informações sensíveis, roubo de propriedade, fraude, violação regulatória, entre outros. Com os *workflows* a organização pode investigar as atividades suspeitas identificadas e agir em cima delas;

Communication Compliance - detecta, captura e age contra mensagens inapropriadas. Os "revisores" poderão investigar emails e mensagens que foram escaneadas no *Teams*, *Exchange Online*, *Yammer* ou outros serviços de comunicação;

Information Barriers - permite que a organização restrinja a interação e comunicação entre certos grupos e usuários. Algumas comunicações que podem ser bloqueadas são: procurar um usuário, adicionar um usuário em uma equipe, iniciar uma conversa,, ligar para outro usuário, compartilhar a tela, entre outros;

eDiscovery - ou *Eletronic Discovery*, é o processo de identificação e entrega de informações que podem ser usadas como evidência em demandas legais. Pode-se utilizar a ferramenta no *Teams*, *Exchange Online*, *OneDrive*, entre outros serviços;

- *Content Search*: procurar as informações entre todos os *data sources* do *Microsoft 365*;
- *eDiscovery Standard*: permite a criação de *eDiscovery Cases* e linkar *eDiscovery Managers* para cada caso;
- *eDiscovery Premium*: contém tudo que o plano *standard* fornece + *end-to-end workflow* para controlar todo o *lifecycle* de procura e gestão das informações encontradas. Contém ferramentas de *analytics* e *ML* para auxiliar na procura de conteúdo relevante para o caso;

Auditing Solutions - resposta a eventos de segurança, investigações internas, investigações externas e obrigações regulatórias.

- *Audit Standard*: fornece capacidades de *logging* e procura para atividades auditáveis. É o plano habilitado por padrão. Permite a exportação das atividades em uma planilha *excel*. As informações capturadas são retidas por padrão por 90 dias;
- *Audit Premium*: contém tudo que o plano *standard* oferece + retenções mais longas;

Azure Policy - auxiliam no estabelecimento de padrões e gestão de *compliance* dos recursos;

Azure Blueprints - “planta” que contém todos os recursos “base” que devem ter o *deploy* feito. Normalmente utilizada na criação de dezenas/centenas de recursos ao mesmo tempo;

Customer Lockbox - é a funcionalidade de aprovação de acesso aos dados pessoais de um cliente por parte de um engenheiro da *Microsoft*. Caso haja algum problema com a conta do usuário, o engenheiro irá solicitar acesso aos dados, sendo autorizado ou não pelo cliente;