SERGIPE
GOVERNO DO ESTADO

GOVERNO DO ESTADO
RIO GRANDE DO SUL
SECRETARIA DA FAZENDA

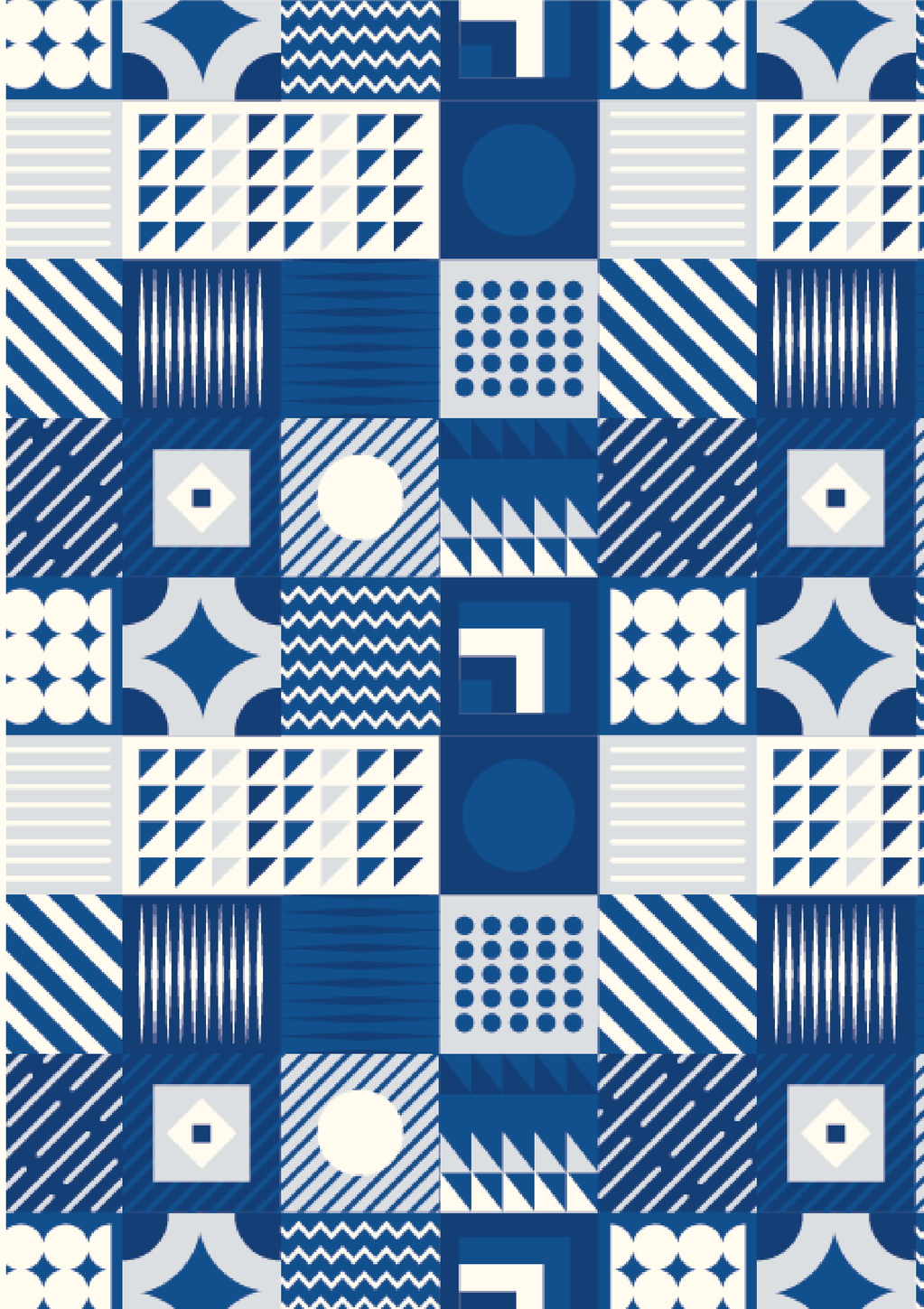
59ª Reunião

COGEF

Comissão de Gestão Fazendária

Segurança no Trabalho Remoto

André Renato Facchini – SEFAZ/RS



Ambiente atual

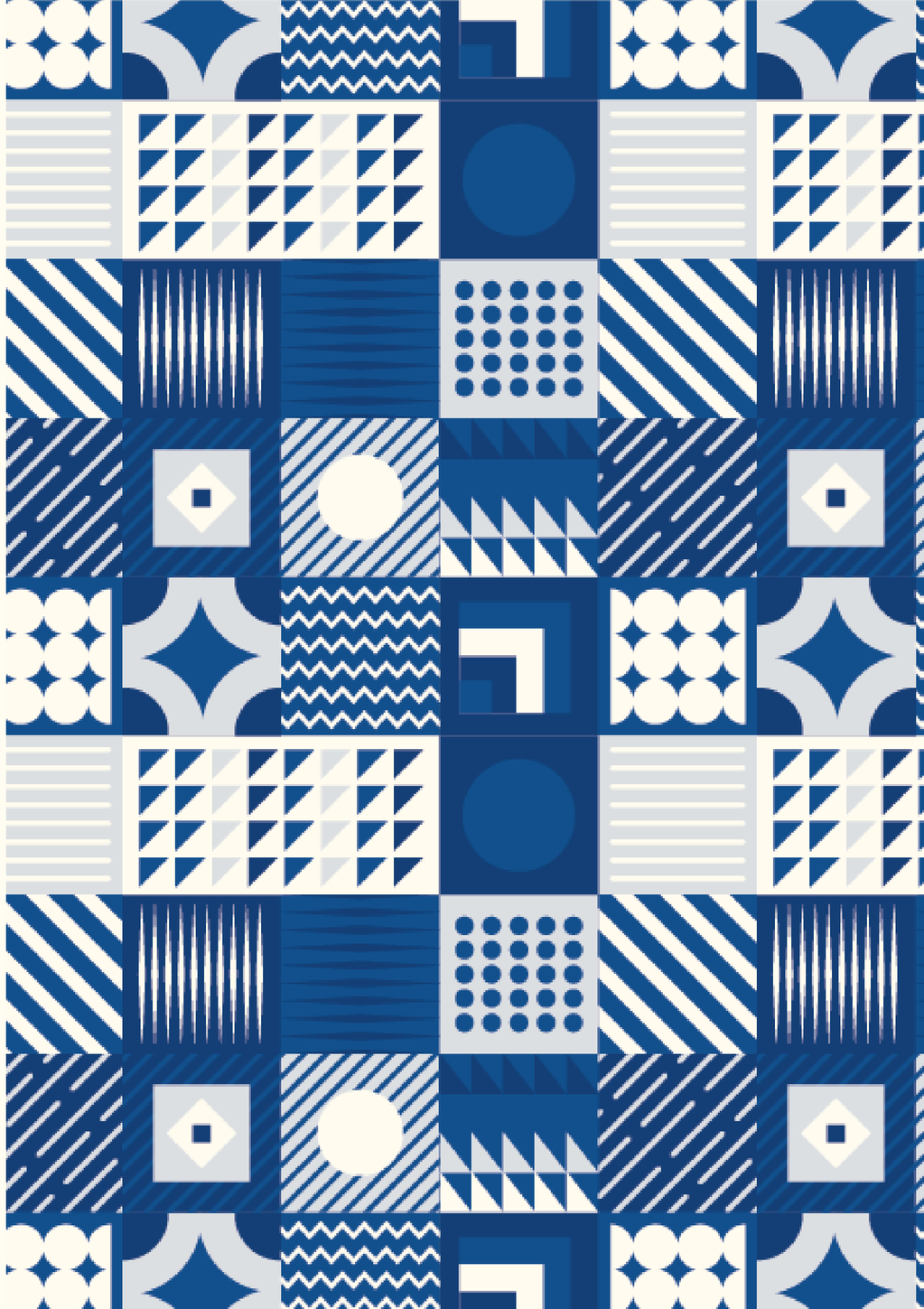
(e que não vai mudar...)

O trabalho híbrido veio para ficar... MESMO;

- Os usuários vão acessar DE QUALQUER LUGAR;
- Vão acessar DE QUALQUER EQUIPAMENTO, corporativo ou não...;
- Vão conectar a QUALQUER REDE disponível;

E...

- Suas senhas vão continuar VAZANDO;
- Seus computadores, celulares e tablets vão ser EMPRESTADOS;
- Alguns serão ROUBADOS;



Ambiente atual

(então, o que nos resta...)

Confiança Implícita

X

Confiança Adaptada ao Risco

Confiança Zero

ZERO TRUST

Pilares básicos

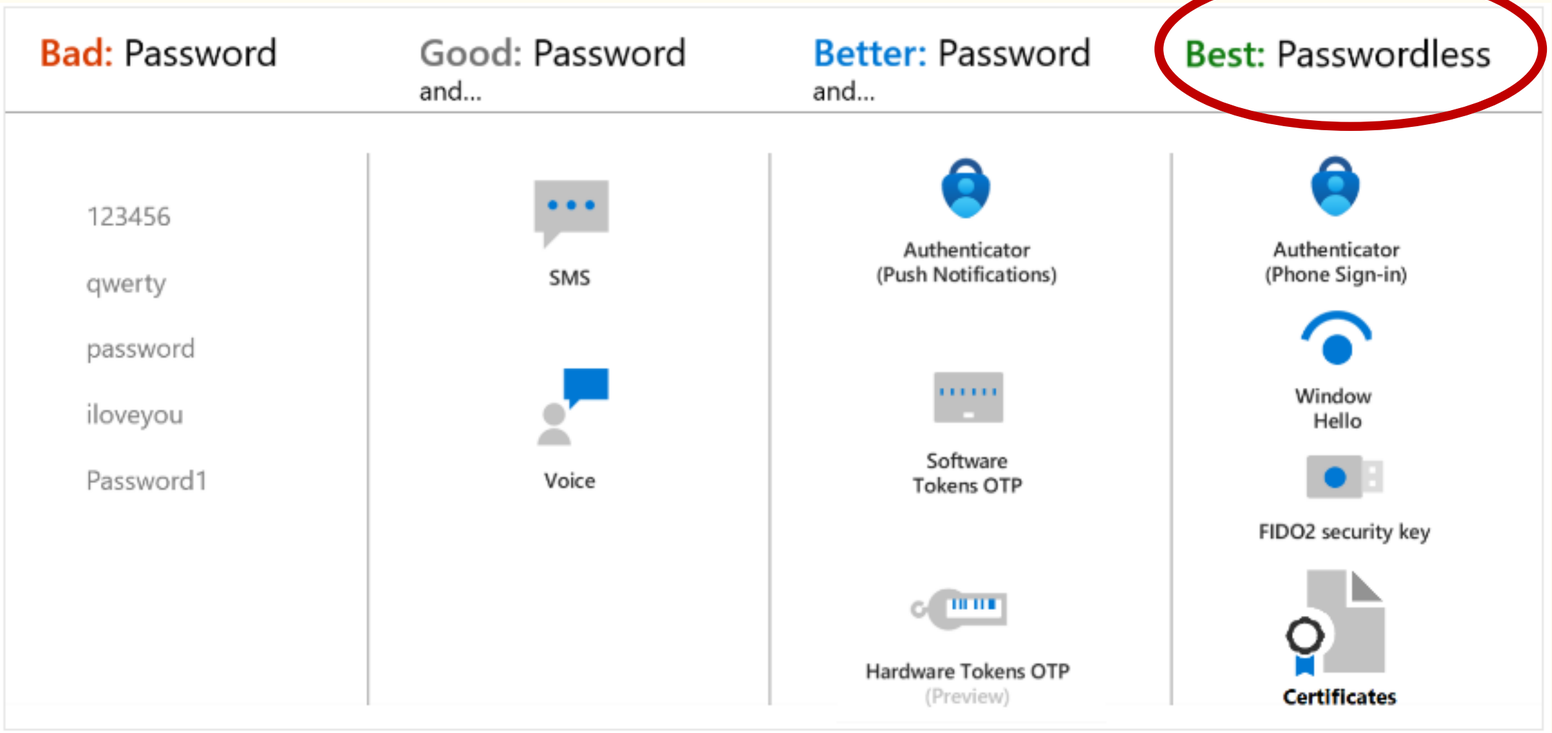
Trabalho remoto com Zero Trust

Sugestão de pontos mínimos / ordem de implementação:

1. Identidades;
2. Aplicativos / Sistemas;
3. Extremidades (equipamentos);
4. Redes;
5. Acesso Condicional;
6. Dados;

1. Proteção de Identidades

Senhas fortes + autenticação multifator (MFA)



https://learn.microsoft.com/pt-br/entra/identity/authentication/concept-authentication-methods

Preferir acesso sem senha:

- **Biometria;**
- **Reconhecimento facial;**
- **Iris;**

Condicionado ao MFA:

- **Redefinição de senha *self-service*;**

2. Proteção de Aplicativos / Sistemas

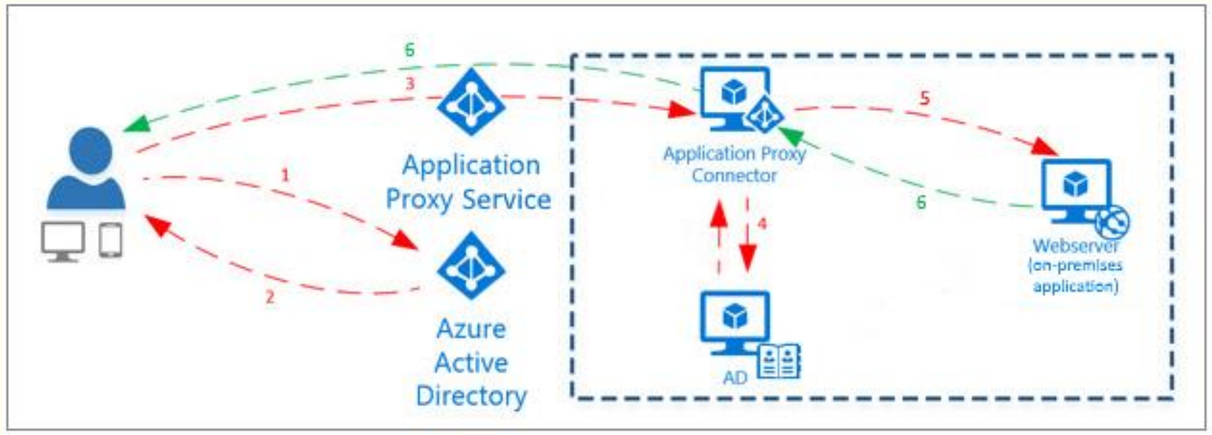
(O básico...)*

Acesso remoto a soluções web locais (on-premises)

- Firewall / Proxy de Aplicação (*SWG – Secure Web Gateway / WAF – Web Application Firewall*);

Uso de senha única para as aplicações compatíveis

- SSO – Single SignOn;



https://learn.microsoft.com/pt-br/entra/identity/app-proxy/overview-what-is-app-proxy

Alguns exemplos:

- Akamai App and API Protector (WAAP);
- AppTrana;
- AWS WAF;
- Barracuda Web Application Firewall;
- Cloudflare;
- F5 Advanced WAF;
- Fastly;
- Fortinet FortiWeb;
- Imperva WAF;
- Microsoft Azure Application Gateway;
- Radware;
- Wallarm WAF;

3. Proteção da extremidade - equipamentos

Equipamentos gerenciáveis (corporativos)

- Acesso por biometria (*password less*);
- Criptografia de disco;
- Registro no domínio;
- Gerenciamento remoto (UEM);
- *Instalação de agente local*;

Equipamentos não gerenciáveis (mobile, pessoais)

- Acesso condicional (*);
- Permissão de aplicação de políticas pelo usuário;
- Soluções UEM (*Unified Endpoint Management*)

Conforme o Gartner

O Gartner define uma **ferramenta de gerenciamento unificado de endpoints (UEM**) como uma ferramenta baseada em software, que fornece gerenciamento de computadores e dispositivos móveis com e sem agente local, por meio de um único console.

Alguns exemplos:

- 42Gears – SureMDM;
- BlackBerry - BlackBerry UEM;
- Citrix - Citrix Endpoint Management;
- FileWave – FileWave;
- HCLSoftware – BigFix;
- Hexnode - Hexnode UEM;
- IBM - MaaS360;
- Ivanti - Ivanti Neurons for UEM;
- ManageEngine - Endpoint Central;
- Matrix42 - Unified Endpoint Management;
- Microsoft - Microsoft Intune;
- Raynet - RaySuite UEM;
- Scalefusion - Scalefusion UEM;
- Syxsense - Syxsense Enterprise;
- Vmware - Workspace ONE;

https://www.gartner.com/document/4754731?ref=solrAll&refval=400637943&

3. Proteção da extremidade - equipamentos

Requisitos importantes de uma solução UEM:

- Compatibilidade **multi-OS**: Microsoft Windows, Apple macOS, iOS, iPadOS, Android;
- **Registro** e provisionamento: integração com serviços Microsoft Windows Autopilot, Apple Business/School Manager e Google Android Zero-Touch Enrollment; (***deployment* remoto**)
- Gerenciamento de configurações: **Controle das configurações e recursos do sistema operacional** do dispositivo;
- **Atualizações** do sistema operacional e de segurança;
- **Instalação, atualização e remoção de aplicativos**: Apple App Store, Google Play , Microsoft Store) e repositórios de pacotes (Chocolate Software, Ivanti, Liquit , Microsoft Windows Package, Manager/ Winget , Munki, Patch My computador);
- Abordagem hospedada em **SaaS**: não depende de conexão VPN ou rede corporativa;

Requisitos desejáveis:

- Gestão e controle de **segurança**: relatórios de firewall, endpoint;
- **Telemetria** / **Suporte** remoto;
- Capacidade de **VPN** / **ZTNA**;

https://www.gartner.com/document/4754731?ref=solrAll&refval=400637943&

4. Redes

- **Acesso remoto a máquinas físicas**
  - Network **Gateway** + MFA;
  - **ZTNA** – Zero Trust Network Access (NGFW)
    - acesso controlado com reconhecimento de identidade e contexto;
    - postura de negação padrão;
    - acesso *just-in-time* aos recursos;
    - acesso com base na identidade dos usuários e de seus dispositivos — além de outros atributos e contexto (hora/data, geolocalização, postura do dispositivo);

- Appgate
- Cisco
- Fortinet
- Google
- Microsoft
- Netskope
- Palo Alto Networks
- Zscaler

- **Máquinas Virtuais**
  - VDI – Virtual Desktop;
  - DaaS – Desktop as a Service;

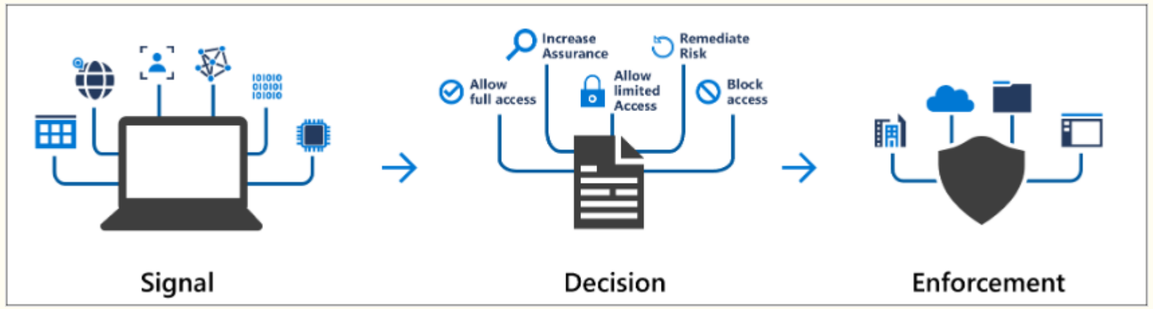
Modernize a solução de VPN (usuário + senha)!

Abandone!!!

https://www.gartner.com/document/4710299?toggle=1&ref=solrAll&refval=400651833

5. Acesso Condicional
(se... então...)

- É o componente verdadeiramente inteligente da solução de identidade, definido como **PDP – Ponto de Decisão de Política**;
- Parte integrante de soluções **IAM – Identity Access Management**;
- São instruções **“se-então”: se** um usuário quiser acessar um recurso, **então** ele deverá preencher um requisito;



Segundo o NIST (National Institute of Standards and Technology)

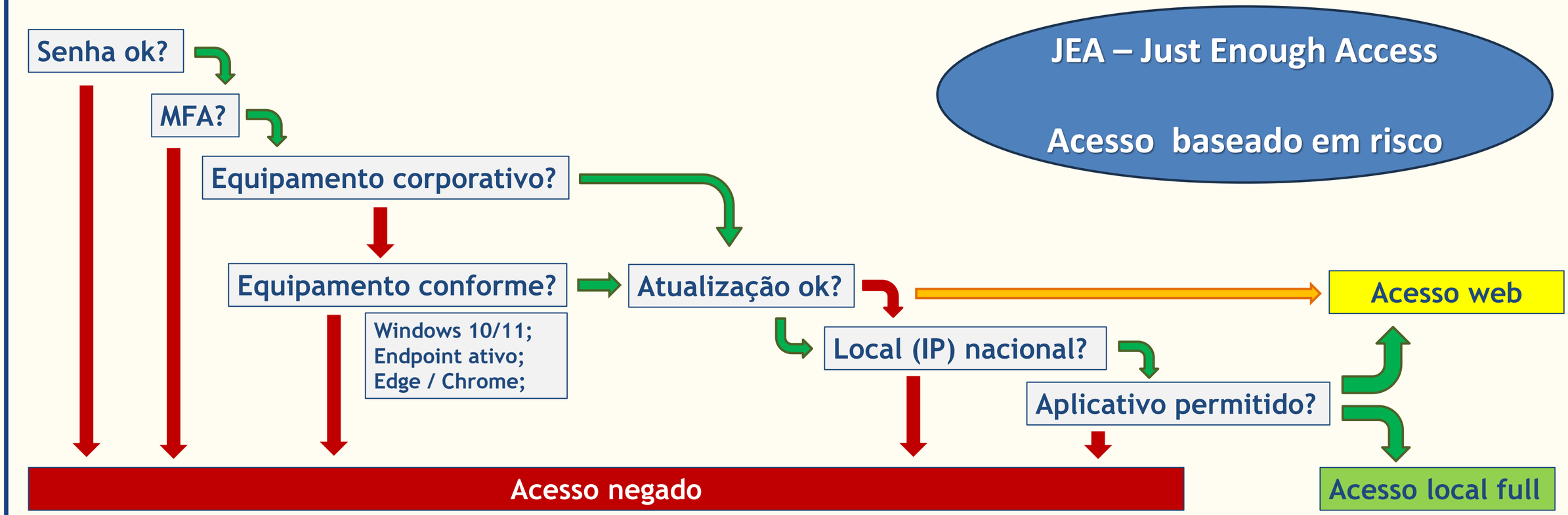
Ponto de Decisão de Política (PDP) é um componente de um sistema que toma decisões com base em políticas que foram definidas nesse sistema. É parte crucial de um sistema de gestão baseado em políticas, para gerir uma rede ou sistema.

https://learn.microsoft.com/pt-br/entra/identity/conditional-access/overview

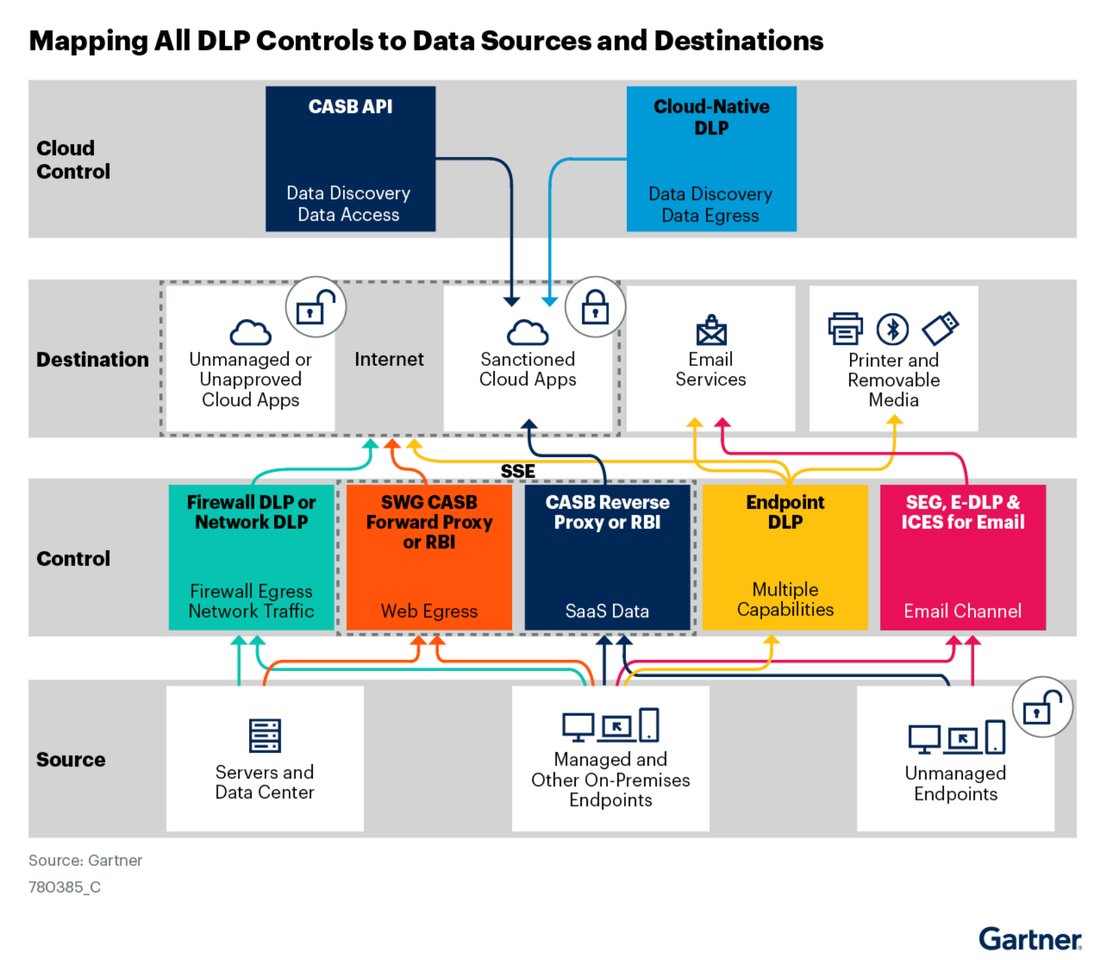
5. Acesso Condicional

Caso prático

Facchini quer acessar o aplicativo Onedrive a partir de um equipamento “X”



6. Dados

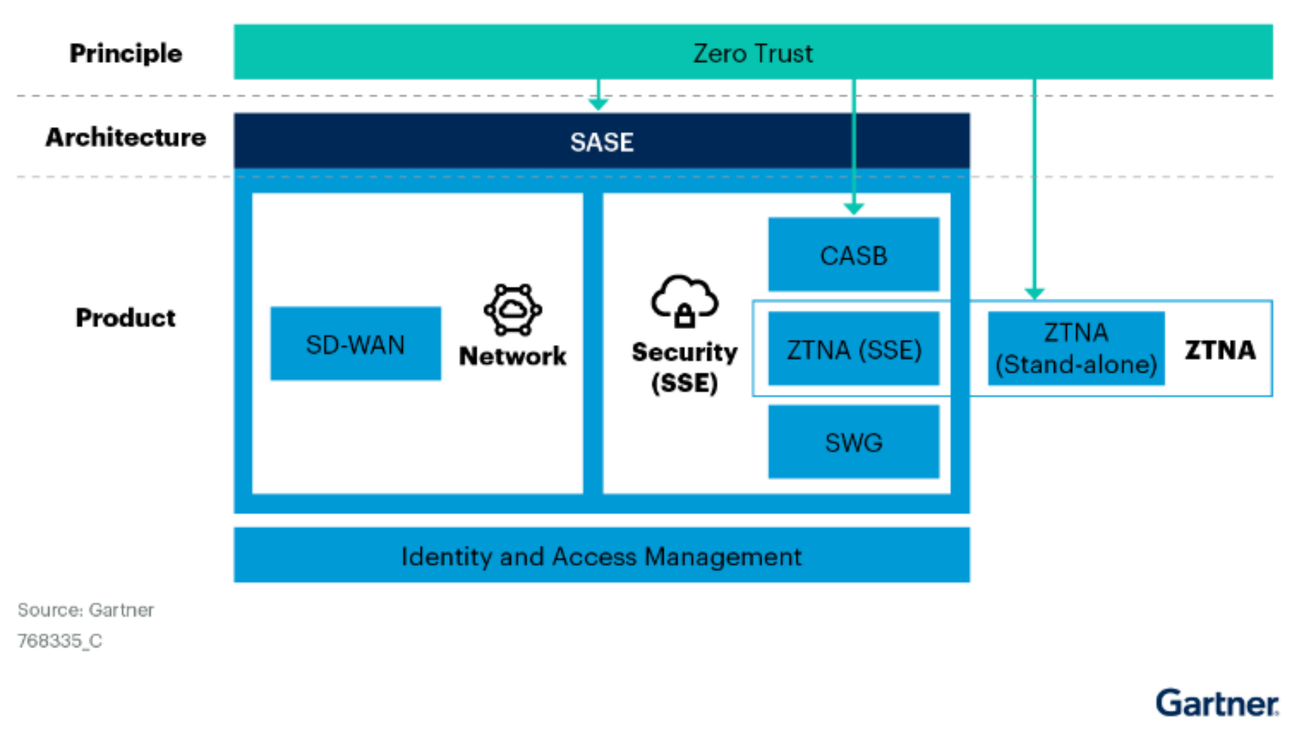


- **DLP - Data Loss Prevention**
  - DLP está presente em várias soluções, e em diferentes níveis de capacidade em cada uma delas;
  - Trabalho reside fortemente no mapeamento de dados e informações;
  - Vários fornecedores oferecem capacidade de classificação automática de informações;
  - Tentar concentrar funcionalidades em menos players. (ex: SSE/CASB, SWG, e-mail e endpoint DLP).

https://www.gartner.com/document/4237199?ref=solrAllImg&refval=400658518&

Zero Trust / SSE / SASE

Para ir além



- **SSE - Security Service Edge**
  - é um serviço de segurança hospedado na nuvem, podendo ter componentes locais, que protege o acesso à web (SWG), serviços em nuvem (CASB) e aplicativos privados (WAF/ZTNA).

- **SASE - Secure Access Service Edge**
  - padrão de arquitetura de segurança, que reúne o SSE às redes distribuídas (SD-WAN).
  - Objetivo: para que **qualquer entidade** (usuário ou máquina) possa acessar com segurança **qualquer recurso** (web, nuvem ou aplicativo privado) de **qualquer lugar**;

https://www.gartner.com/document/4022972?ref=solrAll&refval=400616032&

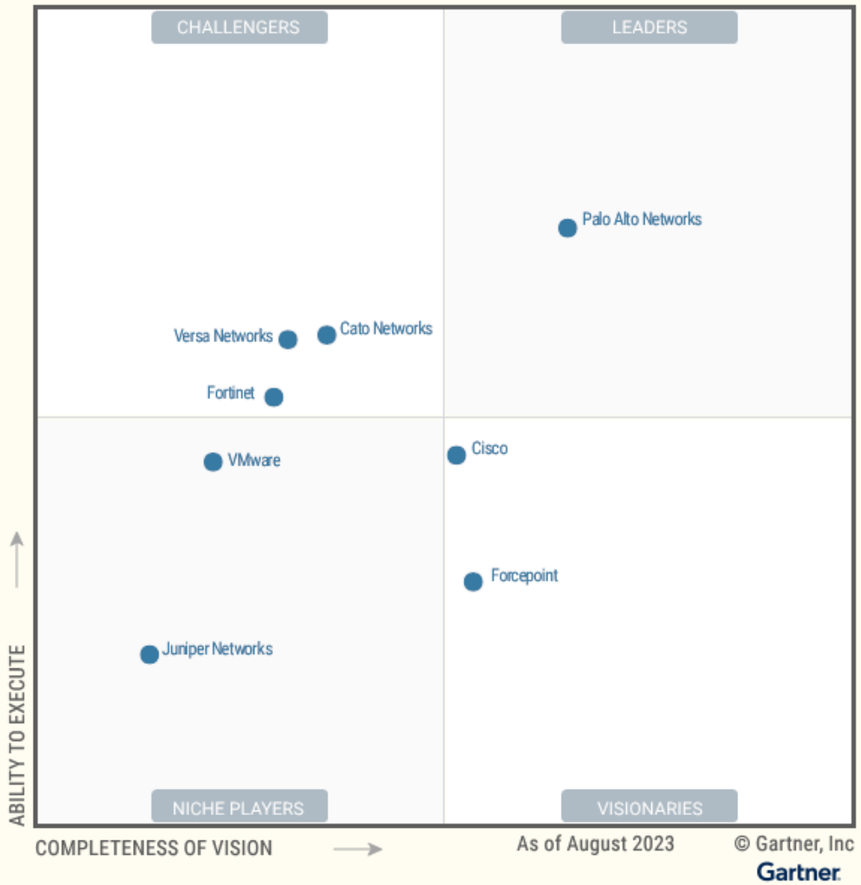
Zero Trust / SSE / SASE

Para ir além

Magic Quadrant for Single-Vendor SSE

https://www.gartner.com/document/4254699?toggle=1&ref=solrAll&refval=400618789

Magic Quadrant for Single-Vendor SASE



https://www.gartner.com/document/4639999?toggle=1&ref=solrAll&refval=400618601

Resumindo

Proteção tradicional com controles de rede

- depende de **firewalls** de rede e redes virtuais privadas (**VPNs**) para isolar e restringir recursos corporativos.
- funcionários se identificam fisicamente no escritório e usam sua **conta de usuário e senha** para iniciar sessão com o dispositivo. A conta de usuário e o dispositivo são **confiáveis por padrão**.

Proteção moderna com confiança zero

- combina políticas, processos e tecnologia para estabelecer **confiança da nuvem à borda**, **independentemente de onde os usuários acessam sua rede**.
- **não presume** que qualquer identidade do usuário ou dispositivo esteja seguro em qualquer rede. A abordagem **exige que você verifique** a **identidade** do usuário e o **dispositivo** e faça isso enquanto monitora continuamente a segurança da **rede**, dos **dados** e dos **aplicativos** no escritório, em casa e entre dispositivos.

Não presuma, não confie. O padrão é não permitir.

SERGIPE
GOVERNO DO ESTADO

GOVERNO DO ESTADO
RIO GRANDE DO SUL
SECRETARIA DA FAZENDA

Muito Obrigado !!

André Renato Facchini – SEFAZ/RS
andrerf@sefaz.rs.gov.br