THALES

O Desafio da Gestão de Acesso na Nuvem

A Desconstrução do Perímetro

Sergio Muniz

VP LATAM Gestão de Acesso e Identidade

O gerenciamento de acesso é essencial para a transformação para a nuvem

98%

acredita que soluções fortes de autenticação e gerenciamento de acesso podem **facilitar a adoção segura da nuvem.**

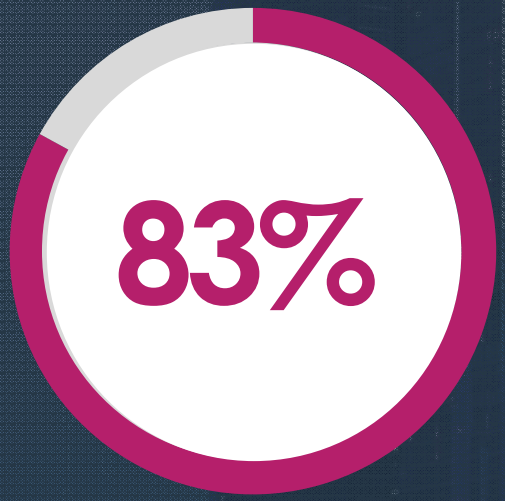
97%

Vislumbra problemas e vulnerabilidades para as suas empresas se os aplicativos em nuvem não estiverem protegidos de forma apropriada

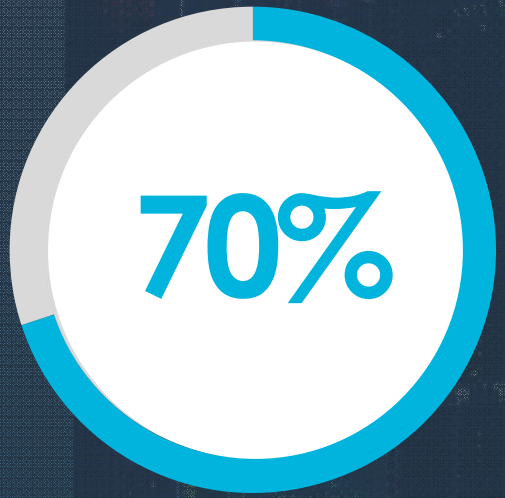
Estudo sobre Gerenciamento de Acesso no Brasil em 2020

THALES

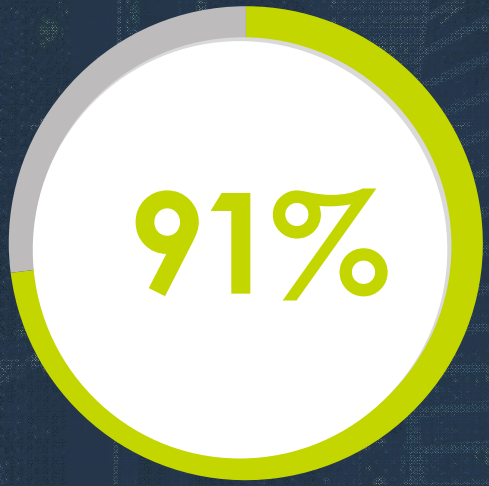
Zero trust: proteja-se em qualquer lugar, não confie em ninguém



acredita que o gerenciamento de acesso baseado em **políticas é o futuro** da gestão de acesso segura



acredita que uma combinação de gerenciamento de acesso **por contexto e sem uso de senhas** é a situação ideal



planeja **expandir o uso de SSO inteligen**te nos próximos 3 anos

Estudo sobre Gerenciamento de Acesso no Brasil em 2020

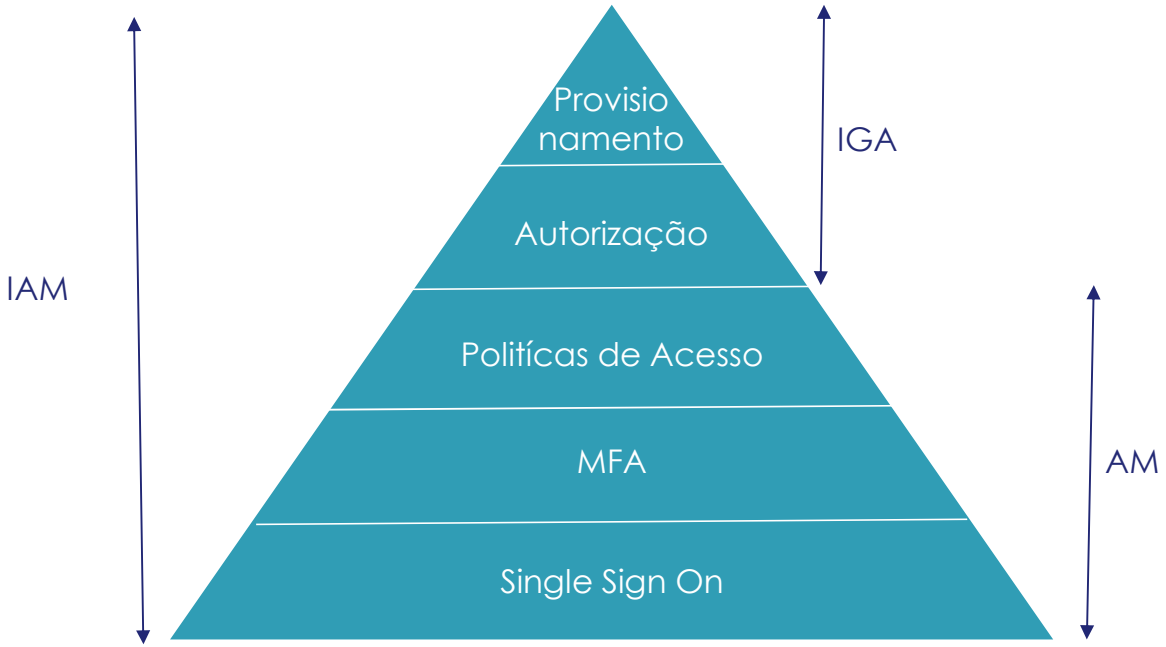
THALES

O que é a Gestão de Acesso e Identidades - IAM

IAM – Identity Access Management

IGA – Identity Governance Access

AM – Access Management



THALES

Análise por contexto – Políticas de Acesso

Rede:

- Definição de Ranges de IP
- Detectar proxy ou VPN de anonimização (TOR)

Sistema Operacional:

- Definição de sistemas operacionais e versões suportadas

Dispositivo:

- Ajuste de acordo com o tipo de dispositivo
- Dispositivo conhecido: baseado em autenticações anteriores

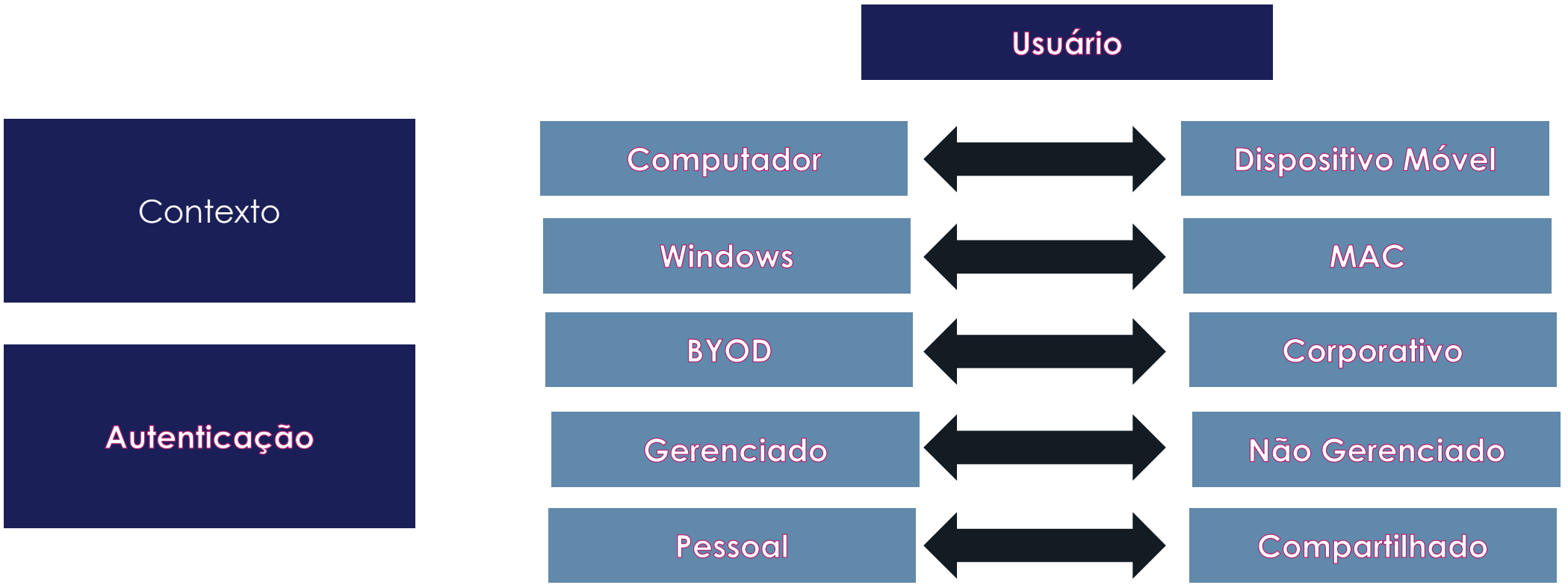
Localização:

- País
- Troca de País

THALES

Autenticação

Políticas por usuário baseadas em contexto e tipo de autenticação



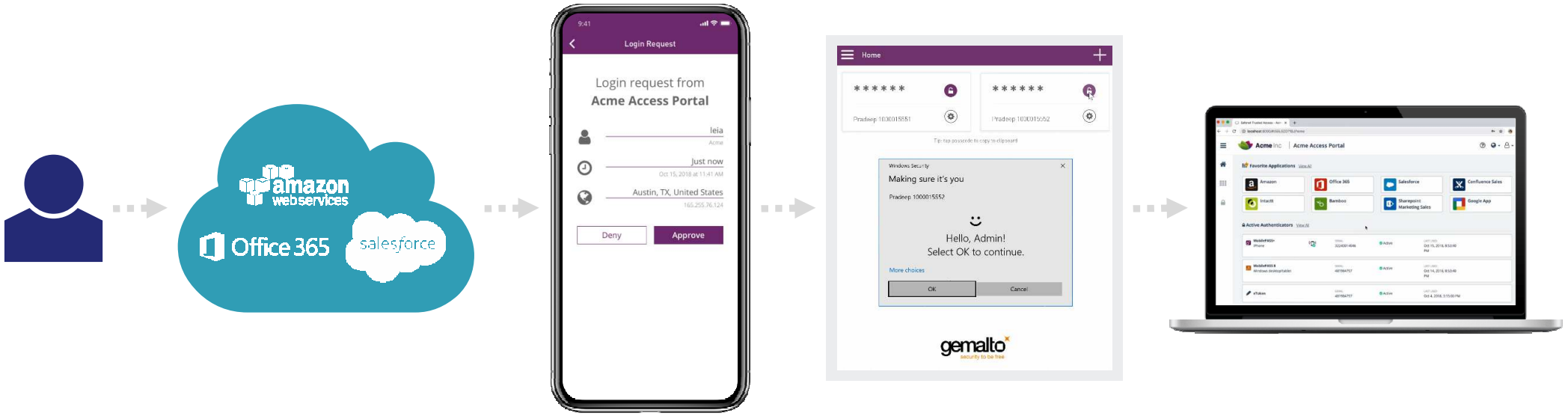
SafeNet Trusted Access

Métodos de autenticação

Passwordless

Autenticação segura, sem a necessidade de lembrar a senha

Push OTP + (Windows Hello / Biometria iOS ou Android)



É possível configurar um OTP Push e a biometria faz o papel do segundo fator de autenticação

THALES

Single Sign On Simples VS Single Sign On Inteligente

Descubra as vantagens de utilizar uma política de login único inteligente (Smart SSO) ao invés de login único simples (Simple SSO)

SSO Simples VS Inteligente

Risco à segurança

Se a credencial do SSO estiver comprometida, todas as aplicações ficam vulneráveis

Seguro

O usuário se beneficia da experiência do SSO, mas o risco é atenuado pela autenticação avançada apenas quando necessário

Falta de visibilidade

Não é possível rastrear quais aplicativos estão sendo acessados, onde e quando

Rastreabilidade

Capacidade de monitorar logs, ver quem, acessa o que, quando, onde e como

SSO Simples VS Inteligente

Acesso aberto

Uma única política de acesso para todos os usuários e aplicações

Determinar políticas

Definir políticas de acesso por necessidade do negócio, sensibilidade do aplicativo e função do funcionário

Ponto de autenticação

O usuário tem o mesmo método de autenticação para acessar todos os serviços

Autenticação universal

Aplique a autorização multifatorial ou métodos de autenticação contextual apropriados a cada tentativa de login

Estudo de caso IAM Thales

Instituição: Administração pública na esfera estadual nos Estados Unidos

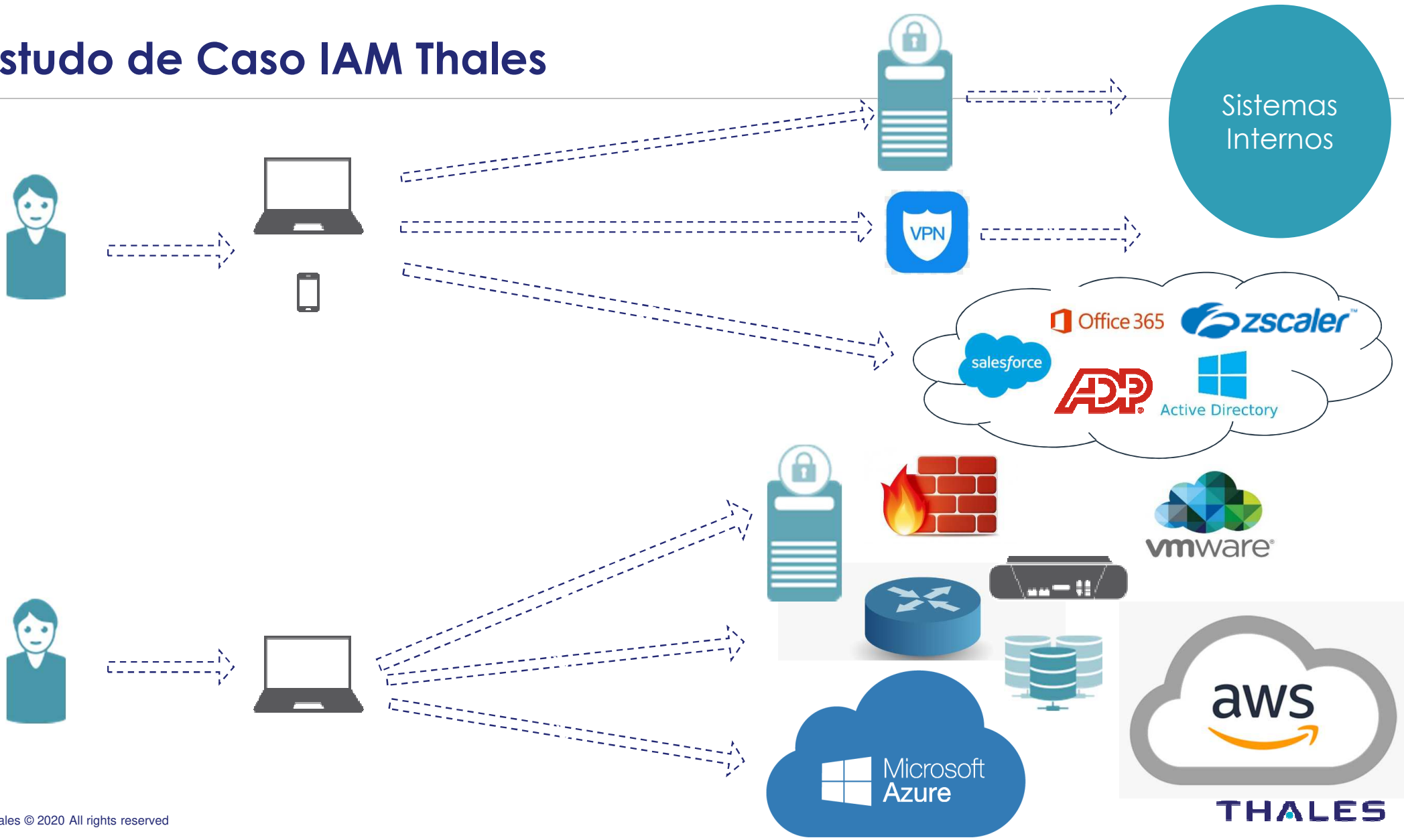
30 mil funcionários

Prioridade: Proteger acessos dos funcionários da gestão pública com MFA (30 K usuários)

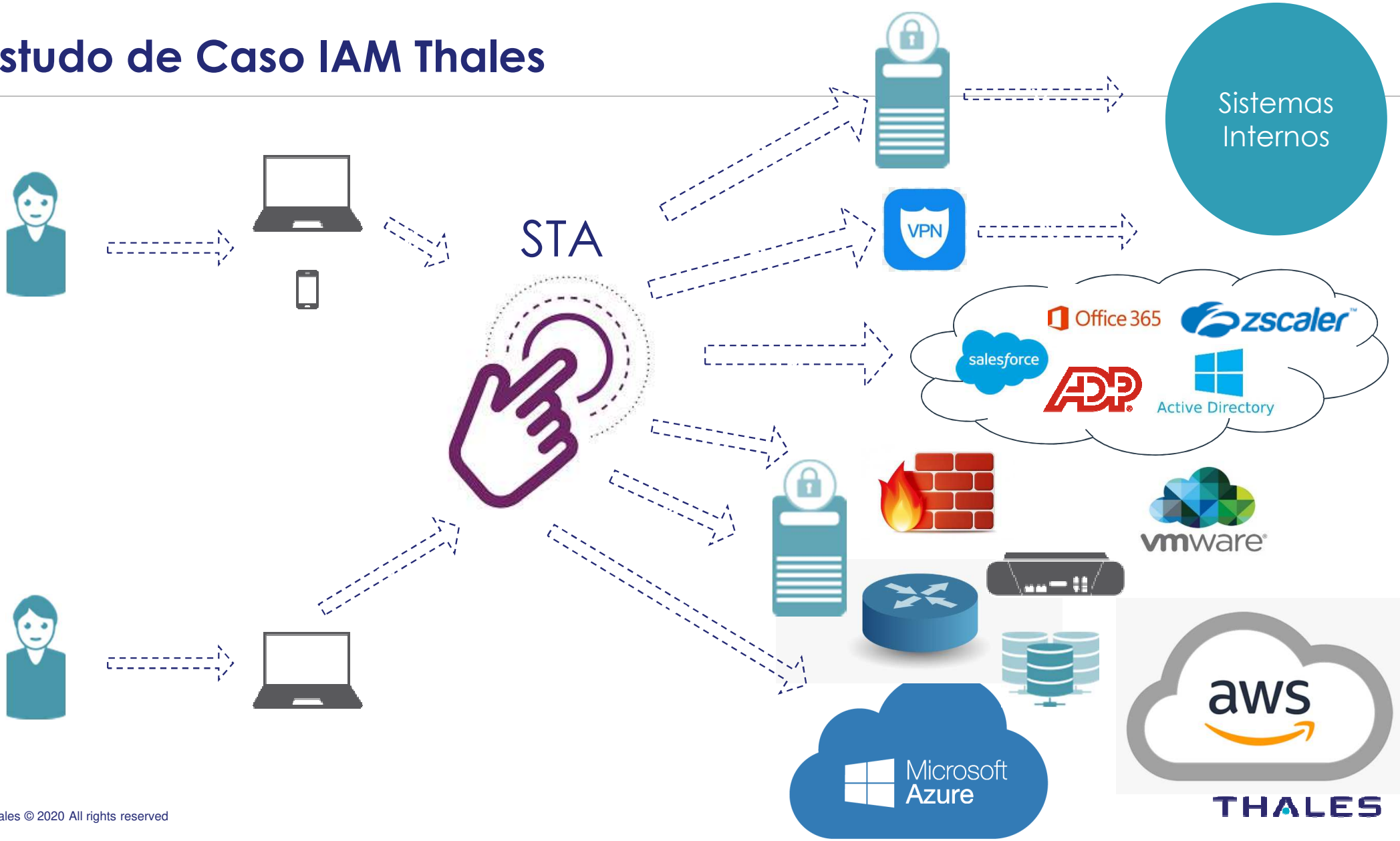
Oferta Thales: Safenet Trusted Access

Diferencial Thales: Solução com integrações prontas para diferentes tecnologias na nuvem

Estudo de Caso IAM Thales



Estudo de Caso IAM Thales



THALES

Obrigado !!!!!

Sergio Muniz

sergio.muniz@thalesgroup.com