May 31 – June 2, Oslo Spektrum

10th anniversary

Marius Sandbu

How to provide secure remote access in 2022?

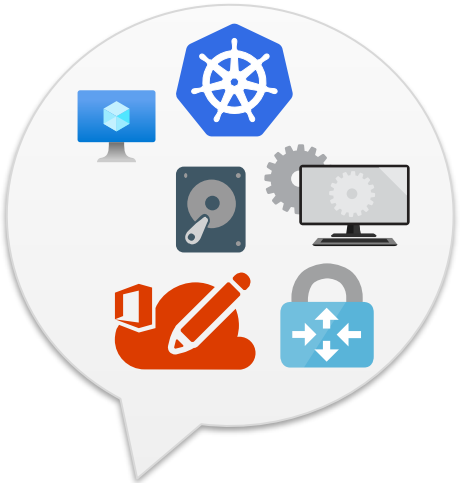
Agenda

- **Working habits and what kind of services do we need to access?**
- **Security risks with “old-fashioned” access**
- **Zero-Trust, SASE and what now?**
- **What kind of options to we have?**

Working habits and user groups

End-user

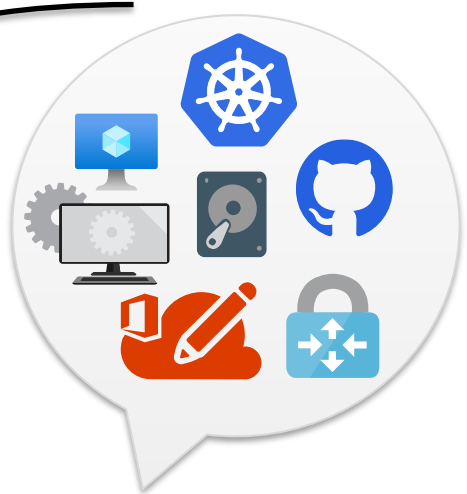
Developer



Administrator

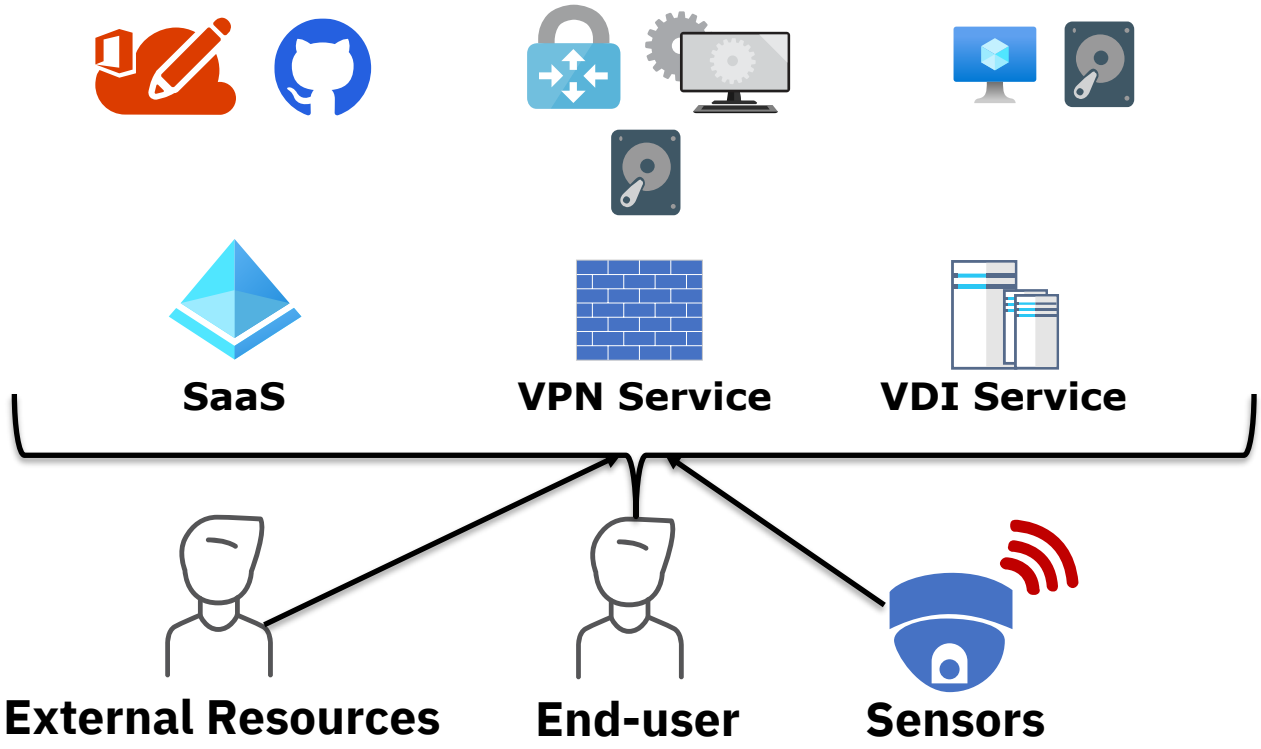
What kind of Services do we need to access?

SaaS
TCP/UDP
Web Apps
Windows Apps
File Storage
Jumphosts
(Admin access)

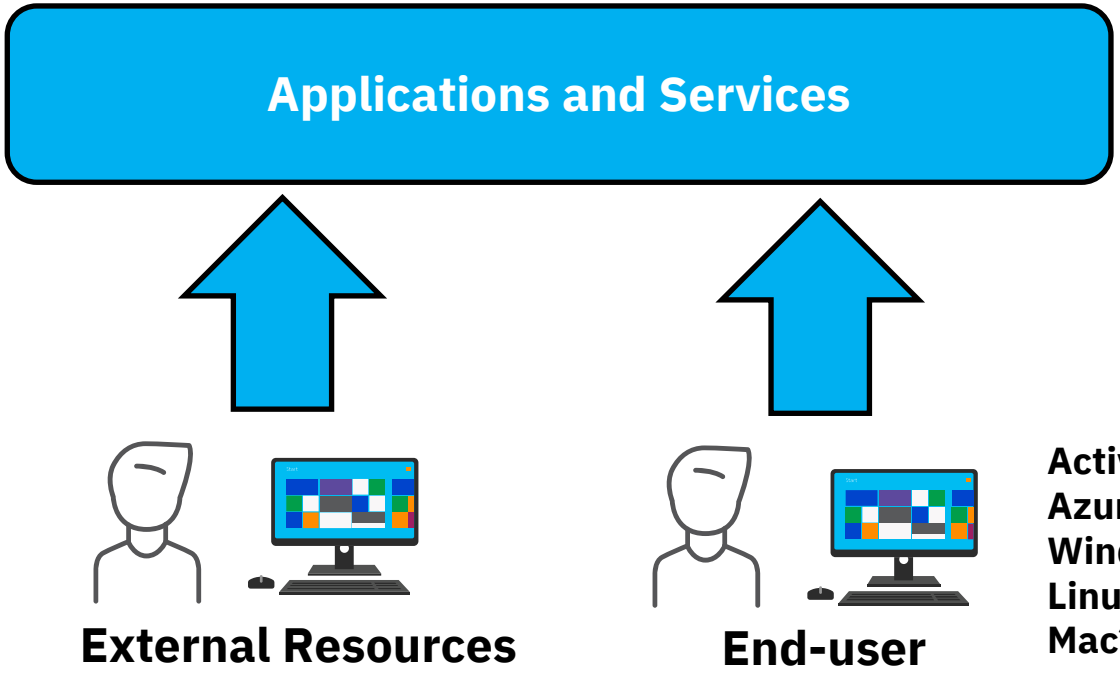


End-user

What kind of Services do we need to access?

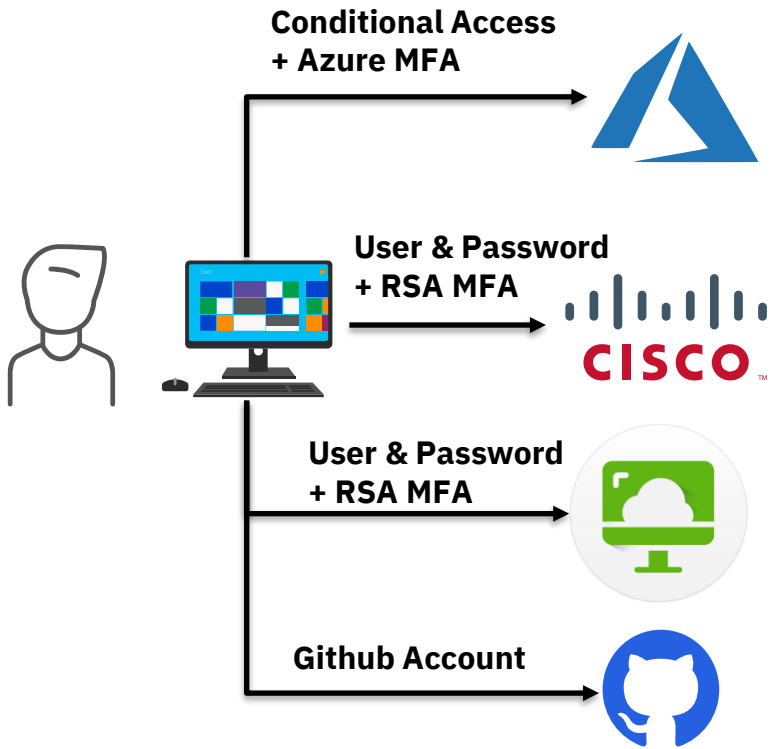


What kind of Services do we need to access?



Active Directory?
Azure AD?
Windows?
Linux?
Mac?

One example from actual environment..

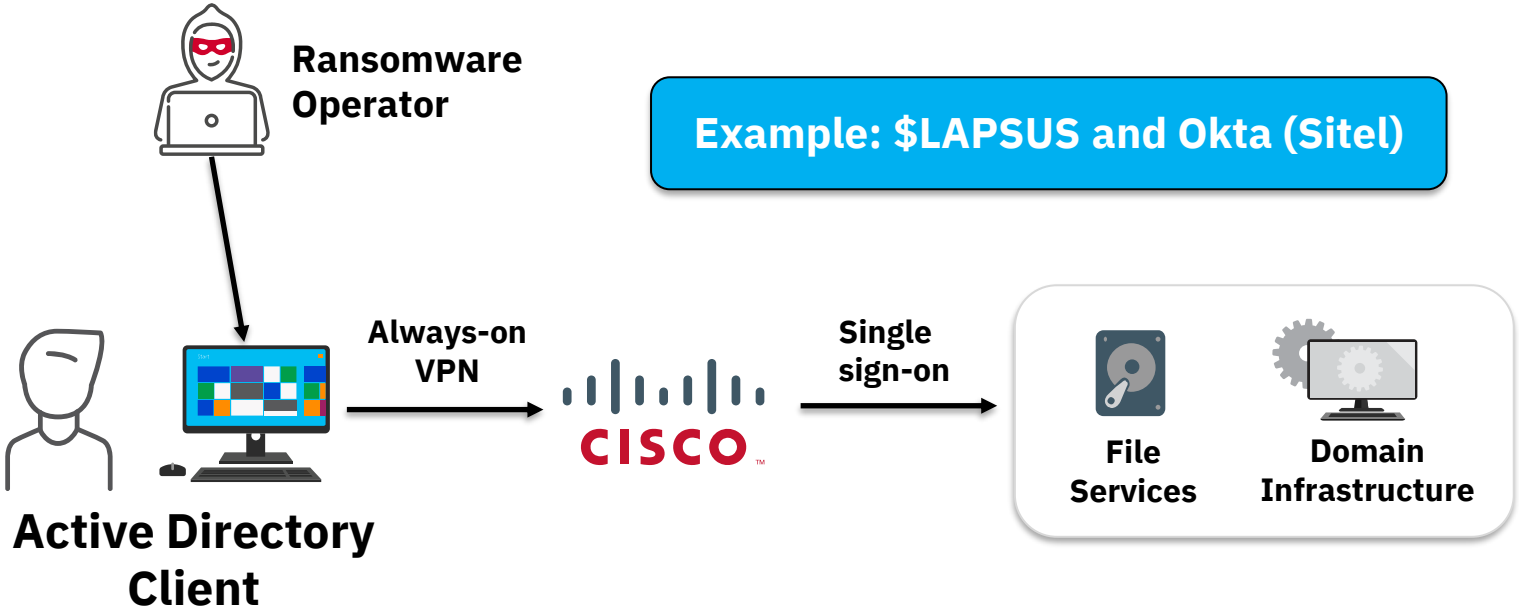


Access to fileshares via VDI....

No Device checks....

Multiple Agents and diferent MFA prompts for user

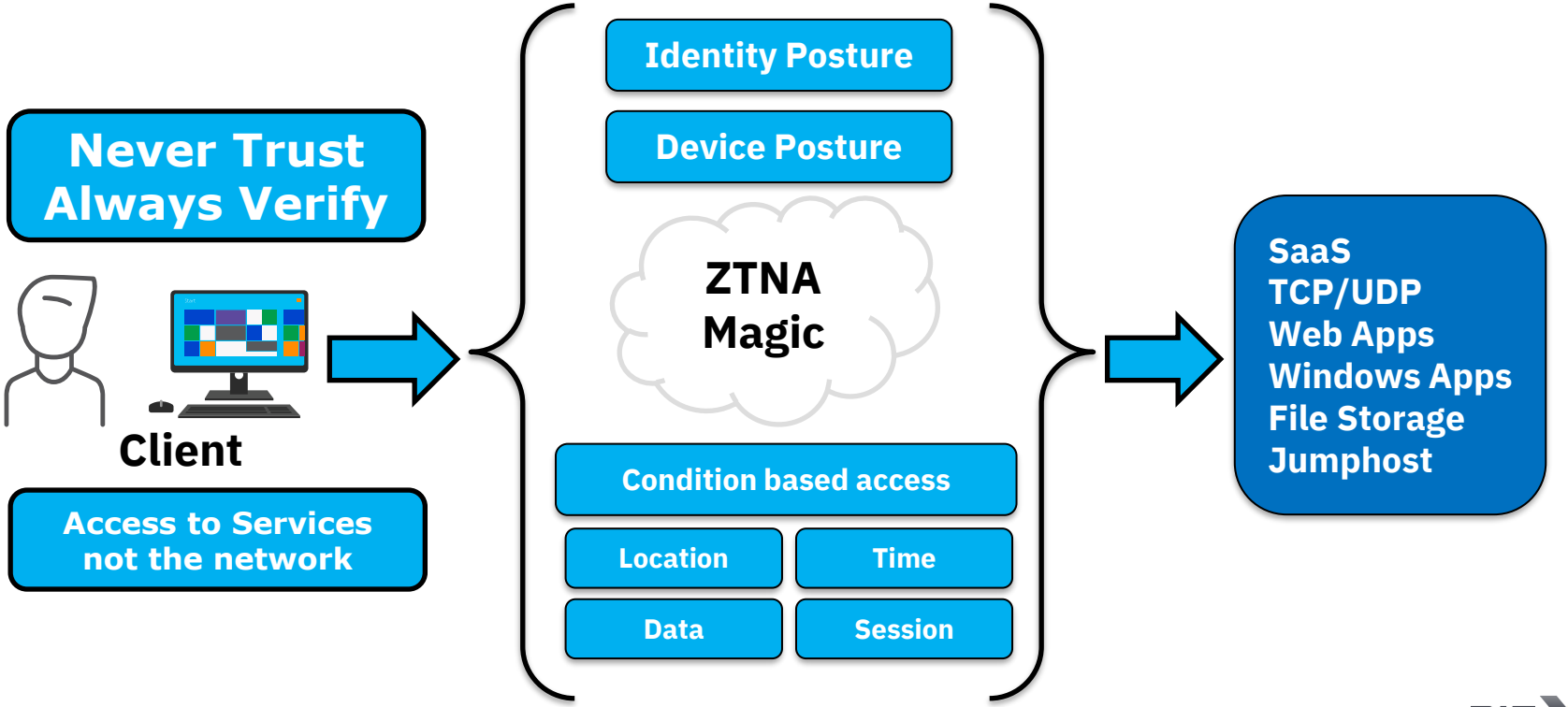
One of the security risks



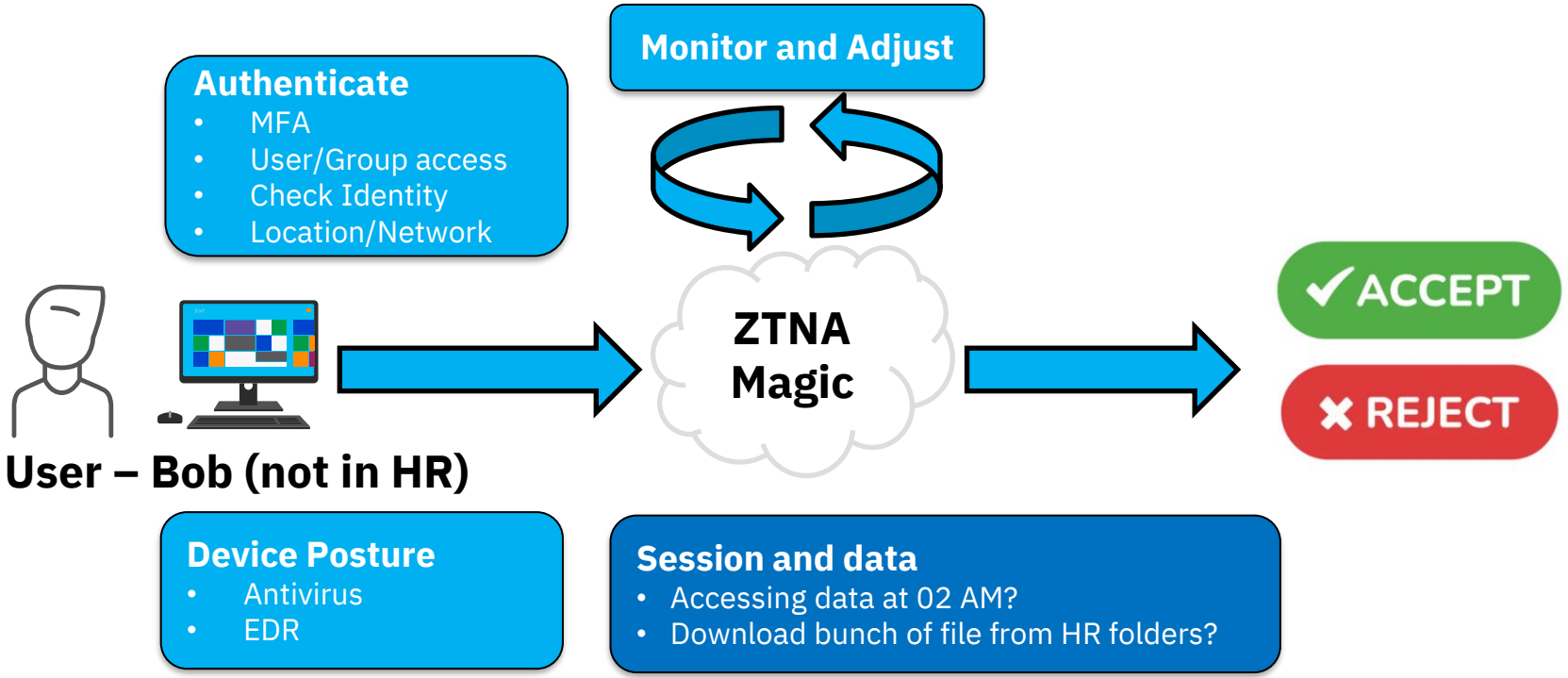
More Security risks

- **How do we know users are who they say they are?**
- **Are their devices up to date?**
- **What’s on the network?**
- **How can we view and secure all connections?**
- **How does the cloud connect to our enviroment?**

ZTNA (Zero-Trust Network access)

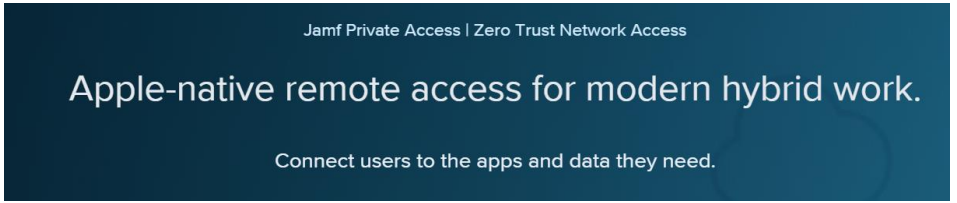


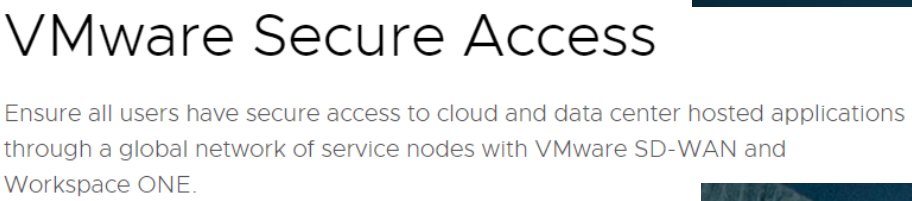
ZTNA (Zero-Trust Network access)

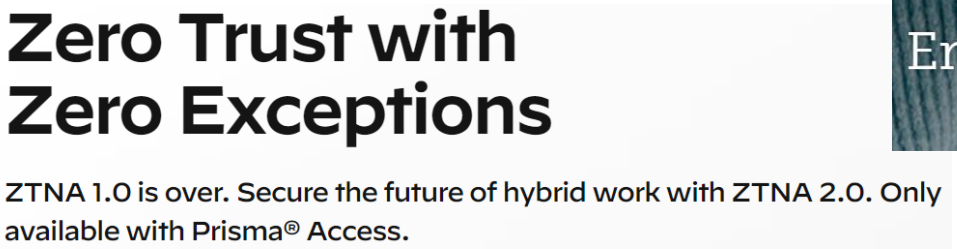


What kind of vendors provide this?

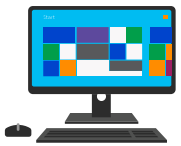
Apparently, everyone....







Microsoft



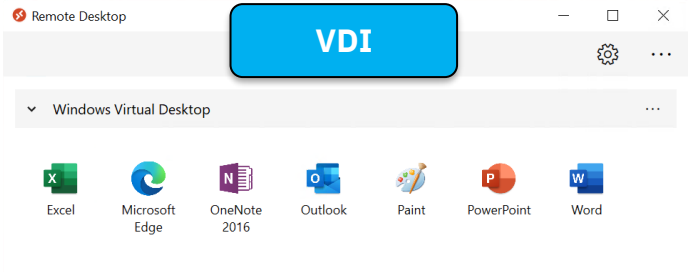
Azure Active Directory

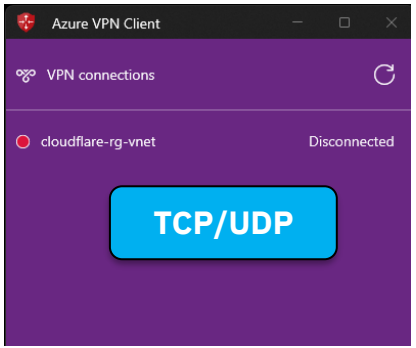
Intune & Defender

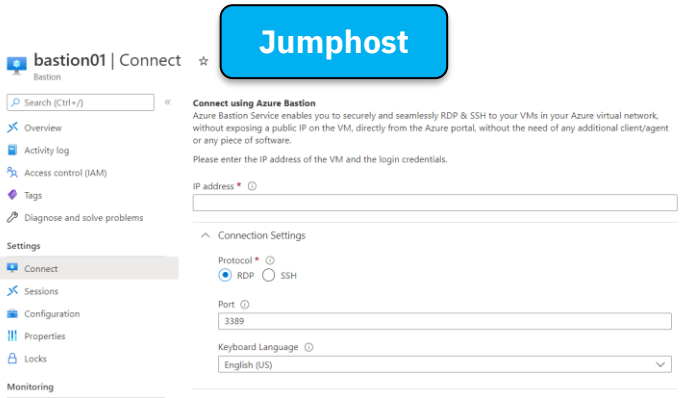
Conditional Access

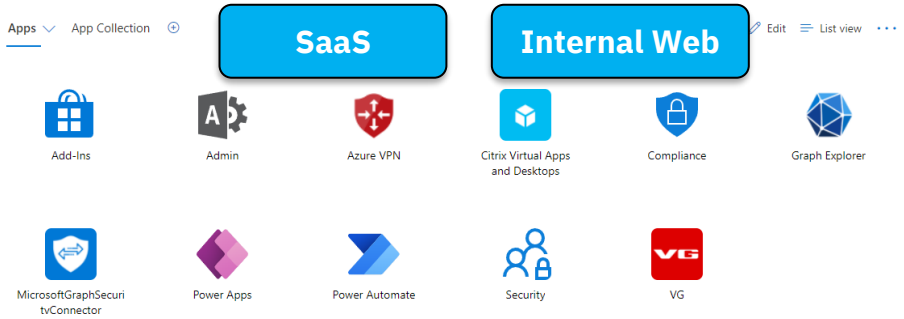
Azure AD SaaS apps	SaaS
Azure Bastion	Jumphost
Azure Application Proxy	Internal Web
Azure Virtual Desktop	VDI
Azure VPN with Azure AD	TCP/UDP
Azure Arc	SSH/K8s

So...what would it look like?







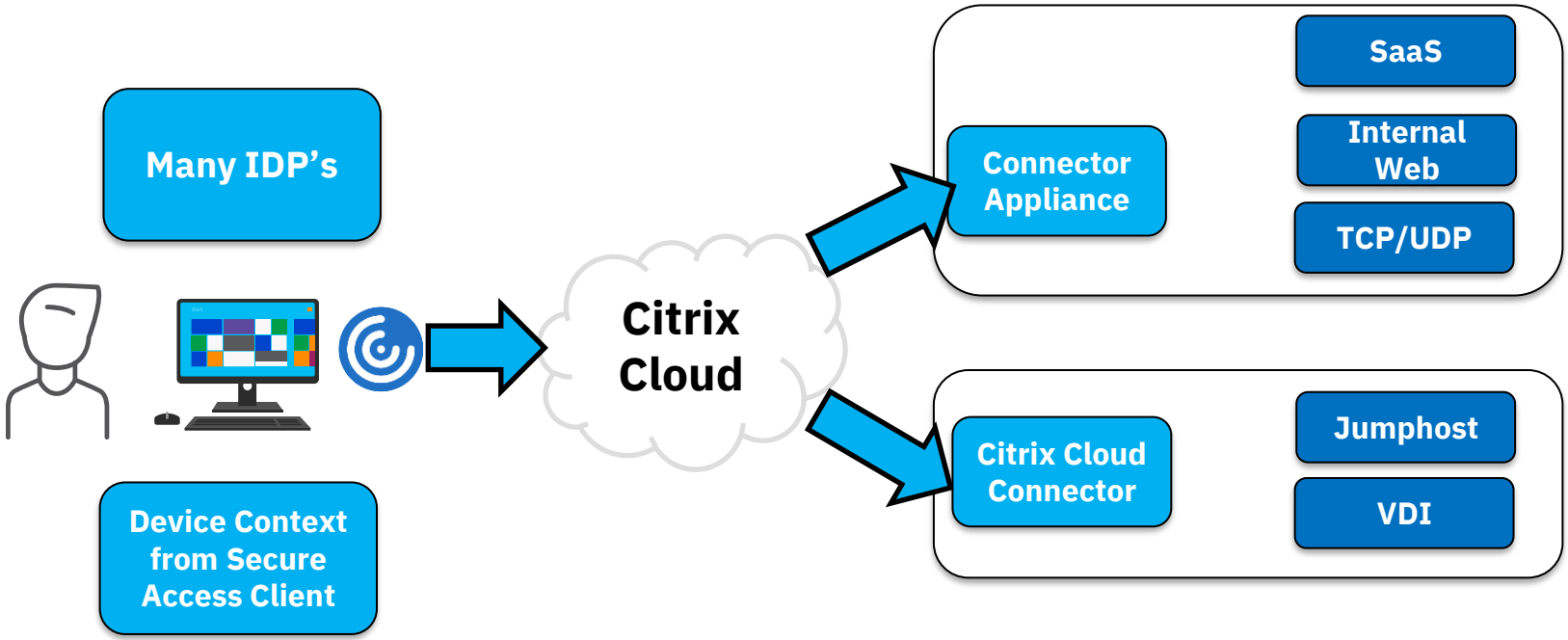


nicX edition

Microsoft

- So many services…
- Best when it comes to Web based services
- Supports «only» Azure AD and Intune
- Azure Application Proxy for internal web services
- VDI only in Azure and no SSO yet
- Bastion recently introduced connection to IP

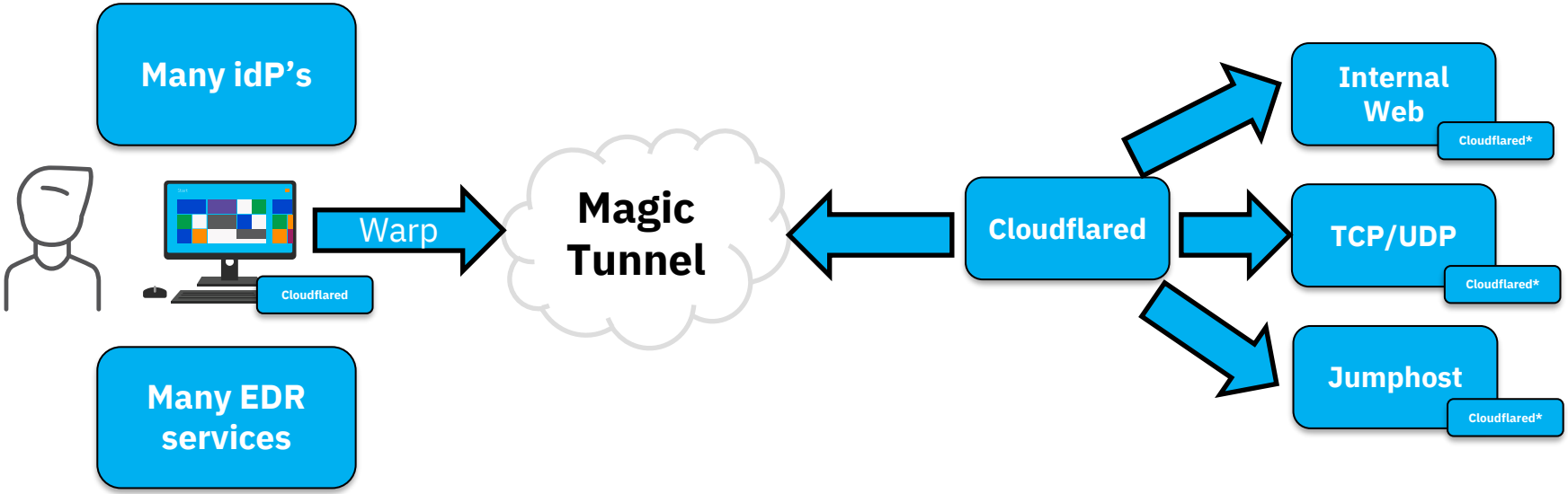
Citrix Secure Private Access



Citrix Secure Private Access

- Supports most iDP’s
- Provides SSO across the whole stack
  - Including support for Azure AD based devices
- Single Agent & UI for most services
- Supports native device context check
  - However, with their own client….
- Anomaly detection is based upon Citrix Analytics

Cloudflare Zero-Trust



Cloudflare Zero-Trust

- **Supports most iDP’s**
- **Supports a lot of EDR/MDM services**
- **Can run Container based**
- **Uses Wireguard for tunnel traffic**
- **Traffic routed trough Cloudflare**
- **Uses QUIC as Transport**
- **Setup is kinda “funky”**
- **Remote Browser Isolation & CASB in the making**

Demo time

- **Microsoft**
  - Azure VPN with Azure AD
  - Azure Arc and SSH
- **Citrix**
- **Cloudflare**

Active Directory vs Azure AD

- **Zero-Trust and Active Directory is not a good match**
  - Clients still need a bunch of ports and services
- **Endpoints should be moved to Azure AD**
- **Requires rearchitecture of network and application access**
- **«ZTNA» services should use Azure AD authentication**
- **Provides somewhat of zero-trust based access to services**
- **What about file and print?**
  - **Regular file storage** = Microsoft Teams / OneDrive
  - **Print** = Universal Print, Printix, Canon Uniflow

File Storage with Azure AD support

Services	Integration	Authentication	Data location
Avepoint Cloud Index	Integration between SharePoint and SMB	Azure AD	On-prem
Azure Blob Storage	Azure Data Explorer	Access Key	Azure
Azure Files	Mount using SMB	Active Directory	Azure
Azure NetApp Files	Mount using SMB	Active Directory	Azure
Fileflex	Mount using Web/SMB	Azure AD / Active Directory	On-prem
Nasuni	Mount using SMB	Active Directory	Azure
HubStor	Mount using Web	Azure AD	Azure
Egnyte	Mount using Web, Mount via Desktop App	Azure AD	On-prem
MyWorkDrive	Client and SMB	Azure AD	On-Prem

The conclusion at one customer

Azure Active Directory joined devices

Intune & Defender

Conditional Access

Azure AD

AVD & Bastion

Cloudflare Access

Egnyte

Canon Uniflow

SaaS

Internal Web

Jumphost

VDI

TCP/UDP

SSH/K8s

File

Print

Some additonal context

- **Azure AD Conditional Access for Verfication**
- **Intune & Defender for Endpoint for Device Context**
  - Cloudflare support in beta
- **Sentinel used for SIEM og SOAR**
- **Providing SSO across all the different services**
- **Pretty seamless for the end-user**

Are we there yet?

- **Difficult to have a single product to solve all needs**
  - **Cloudflare:** Flexible, but not scaleable with management
  - **Microsoft:** So many services, but not good DX
  - **Citrix:** Best DX but lacking external sources for device
- **Vendors also provide additional features**

Honorable mentions

- **Palo Alto Prisma Access**
- **Zscaler Private Access**
- **Cisco Duo**

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2022

Questions? Marius.sandbu@soprasteria.com