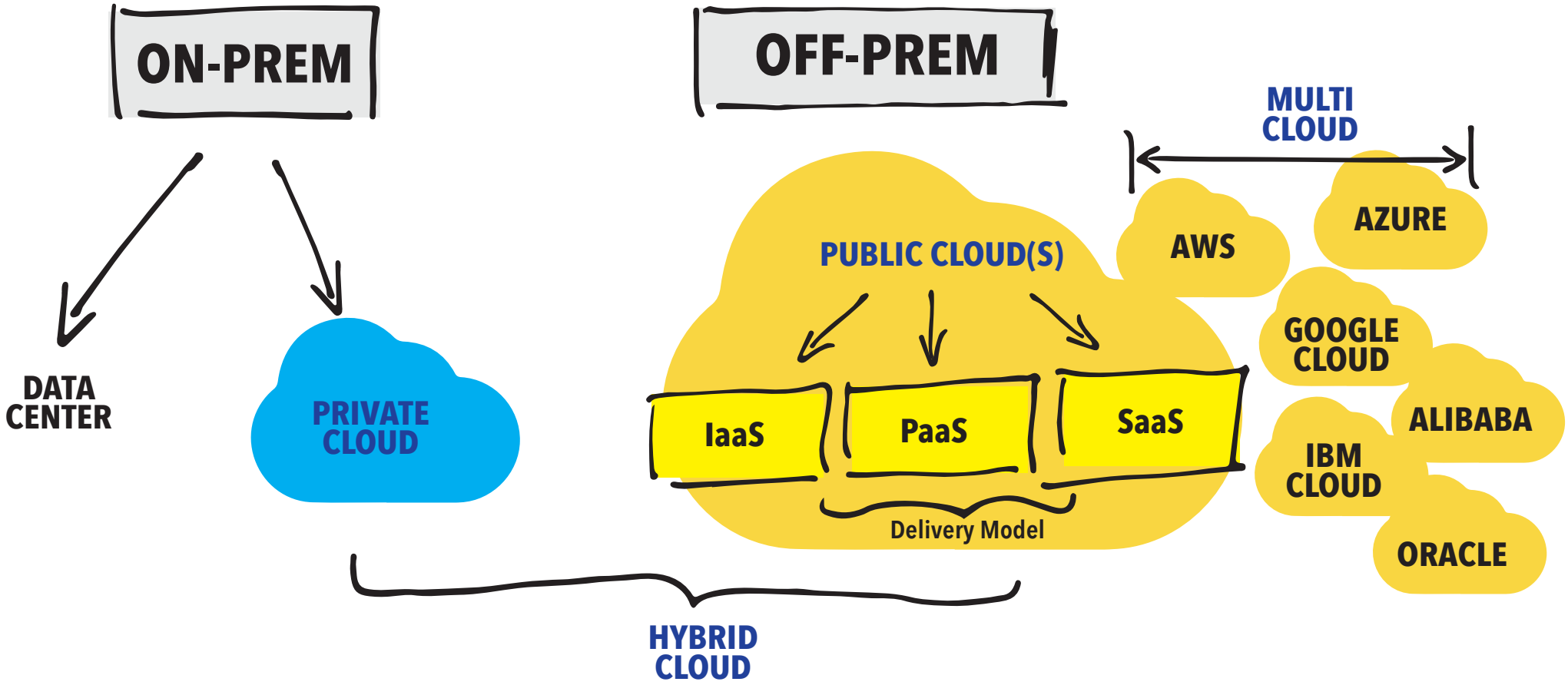
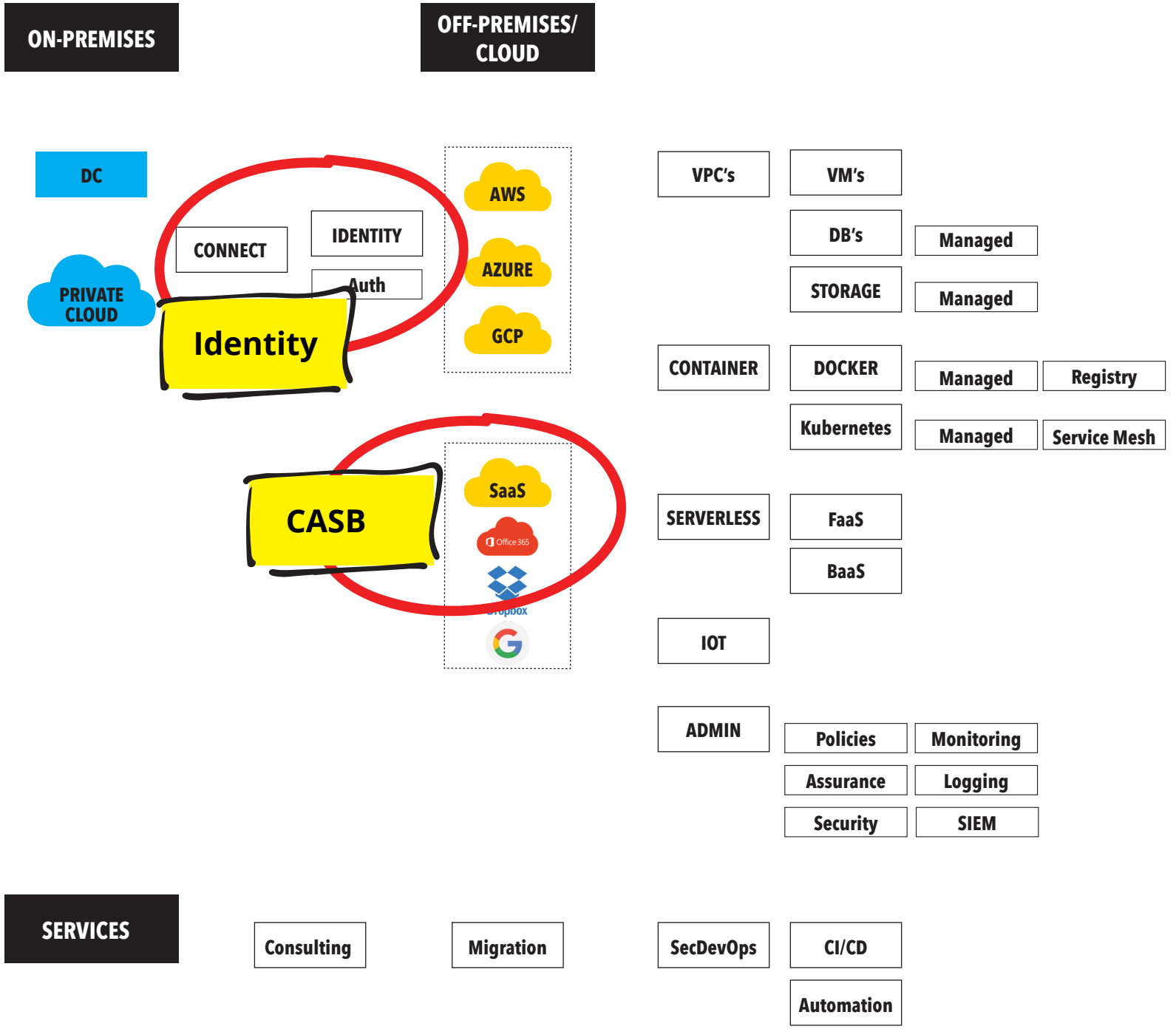
Identity, SaaS & CASB

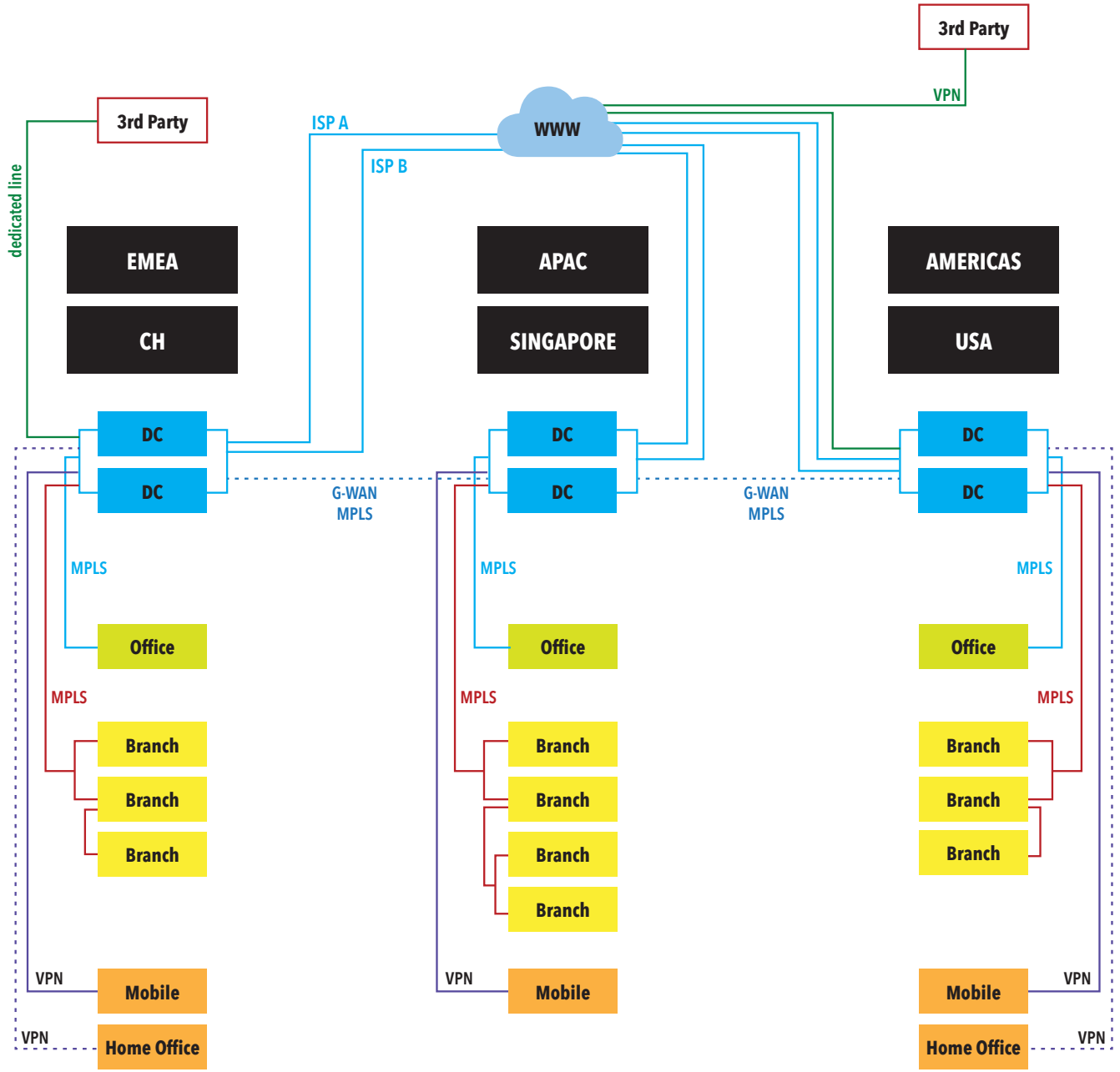
Matthias Geiser

AVANTEC
Competence. Security. Trust.





AVANTEC
Competence. Security. Trust.

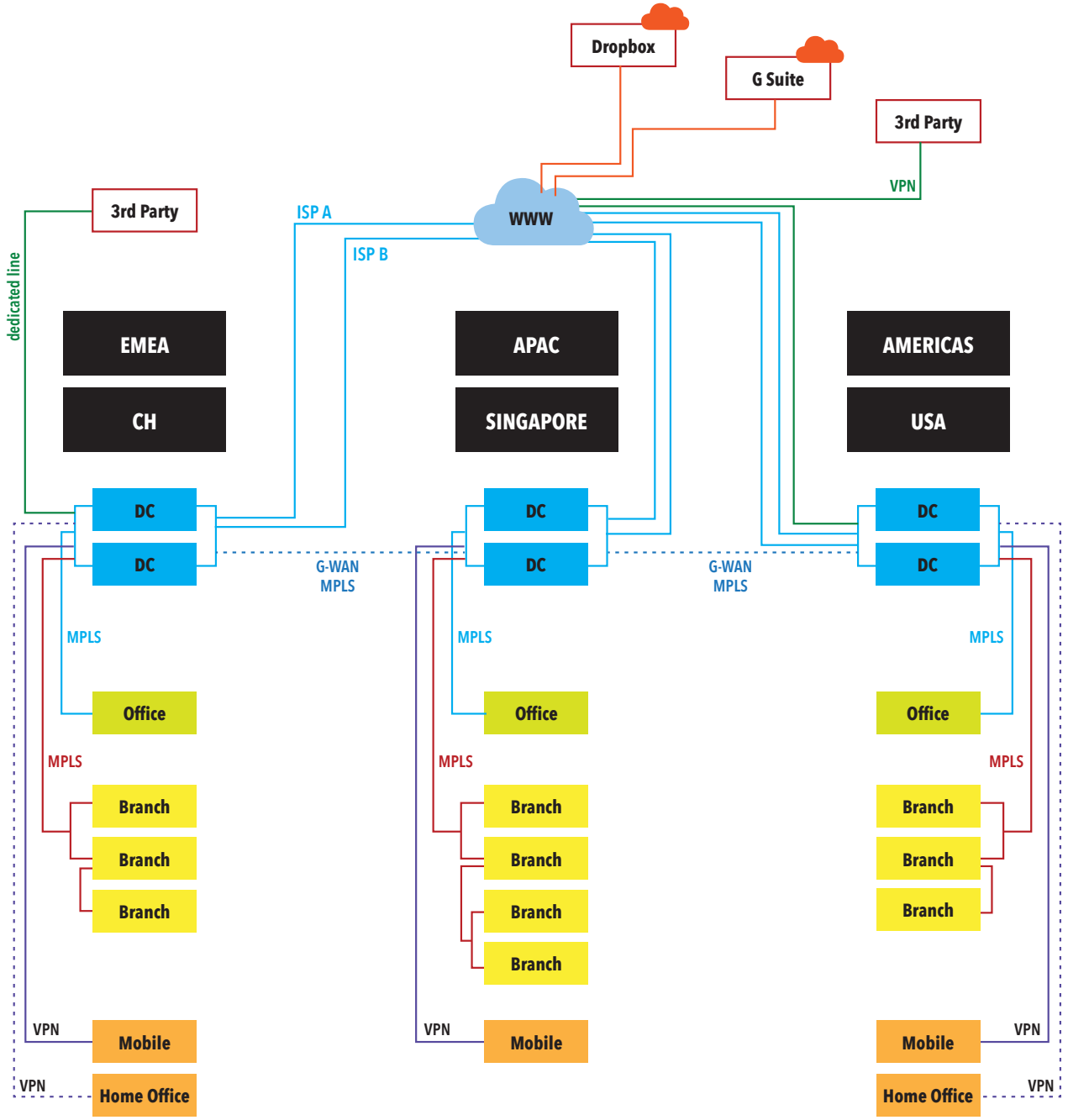

3rd Party
VPN
3rd Party
ISP A
WWW
ISP B
dedicated line
EMEA
APAC
AMERICAS
CH
SINGAPORE
USA
DC
DC
DC
DC
DC
DC
G-WAN
MPLS
G-WAN
MPLS
MPLS
MPLS
MPLS
Office
Office
Office
MPLS
MPLS
MPLS
Branch
Branch
Branch
Branch
Branch
Branch
Branch
Branch
Branch
VPN
VPN
VPN
Mobile
Mobile
Mobile
VPN
VPN
VPN
Home Office
Home Office
VPN

TecBite Industries doesn’t use cloud services.

Except Anna in Marketing.
She’s using Dropbox.

And Peter, in Sales.
He’s using G-Suite with his whole team.

AVANTEC
Competence. Security. Trust.


Dropbox
G Suite
3rd Party
VPN
3rd Party
ISP A
WWW
ISP B
dedicated line
EMEA
CH
APAC
SINGAPORE
AMERICAS
USA
DC
DC
DC
DC
DC
DC
G-WAN
MPLS
G-WAN
MPLS
MPLS
MPLS
MPLS
Office
Office
Office
MPLS
MPLS
MPLS
Branch
Branch
Branch
Branch
Branch
Branch
Branch
Branch
Branch
VPN
VPN
VPN
Mobile
Mobile
Mobile
VPN
VPN
Home Office
Home Office
VPN

On average* >1200 Cloud Apps are in use in a Fortune-1000 company.

Approx. 50% for personal use.

The average employee actively uses 36 cloud services at work.

*McAfee Cloud Adoption Report

AVANTEC
Competence. Security. Trust.

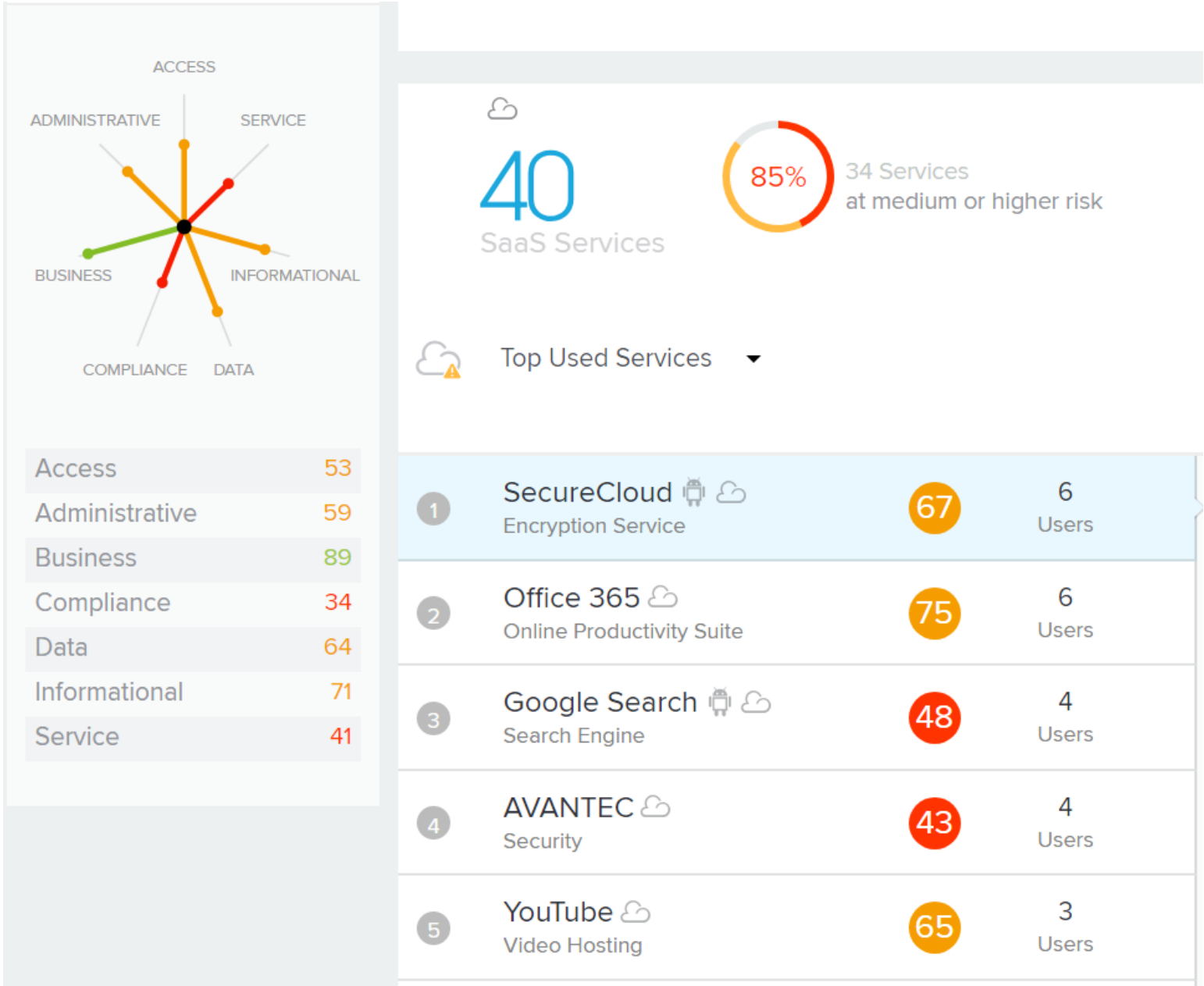
And how many of those is your Organisation aware of?

How do you find out what Cloud Apps your Organisation is using?

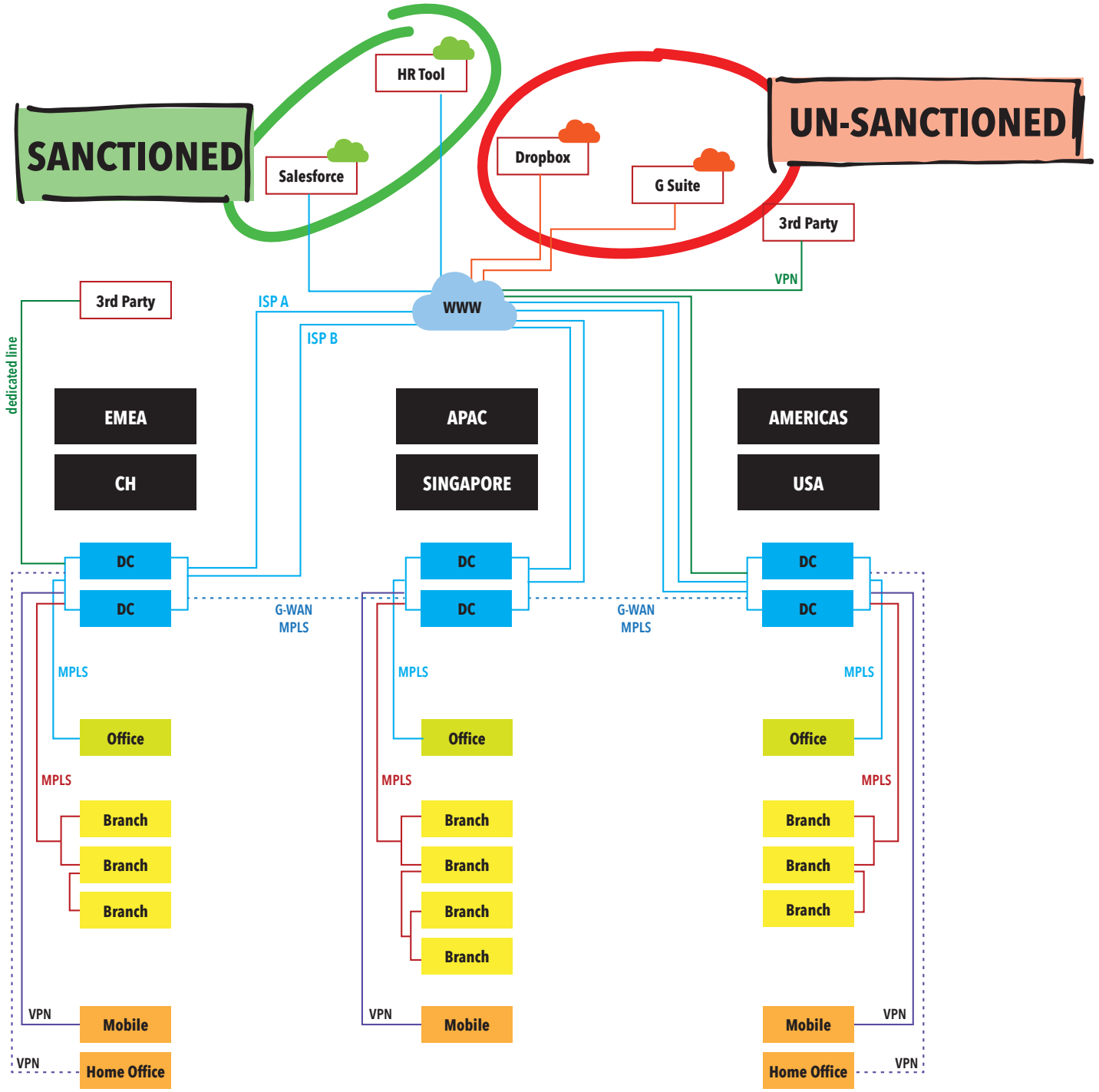
AVANTEC
Competence. Security. Trust.

CASB: Audit

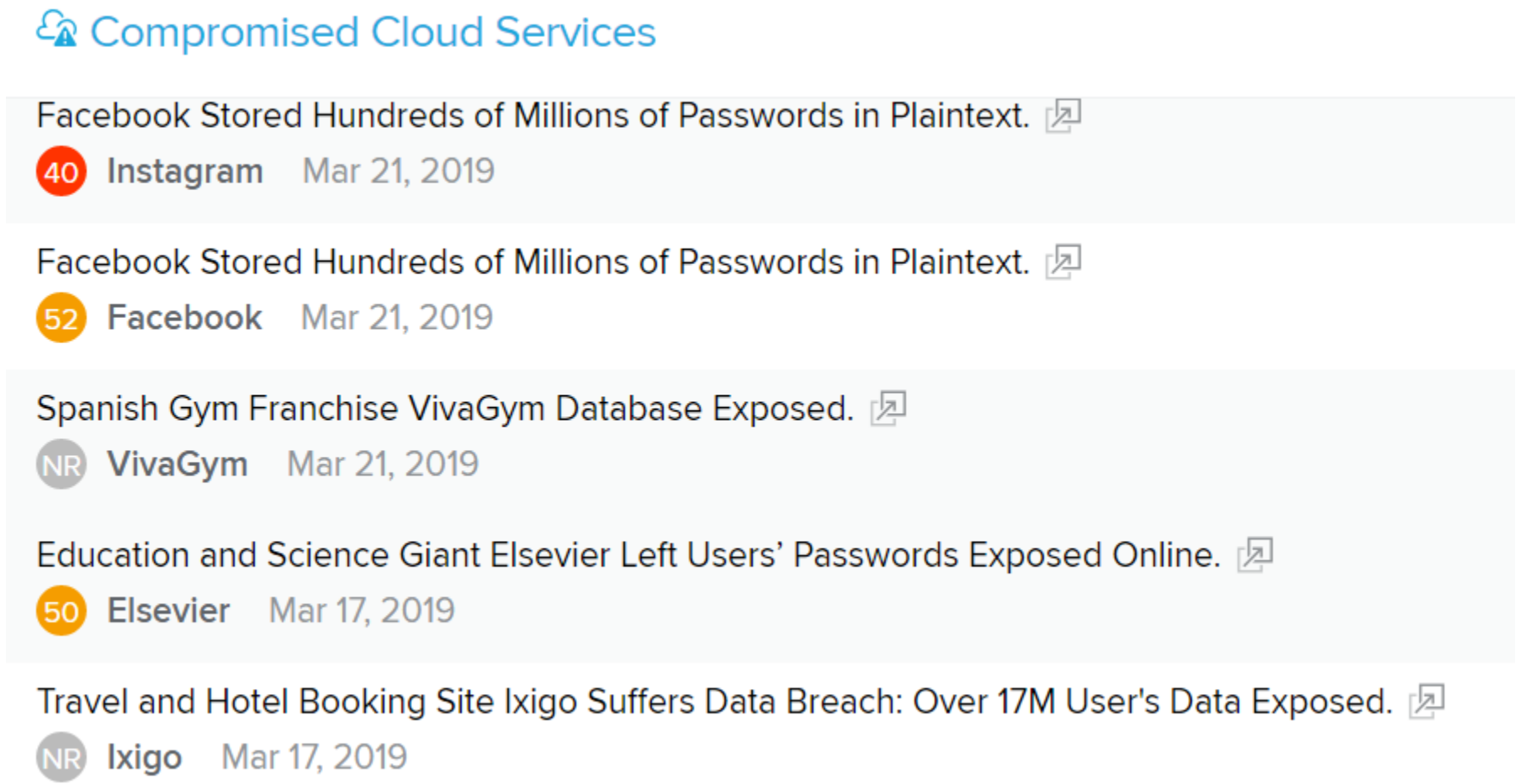
- **Audit directly on the Proxy**
- **Evaluate Proxy / Firewall Logs**



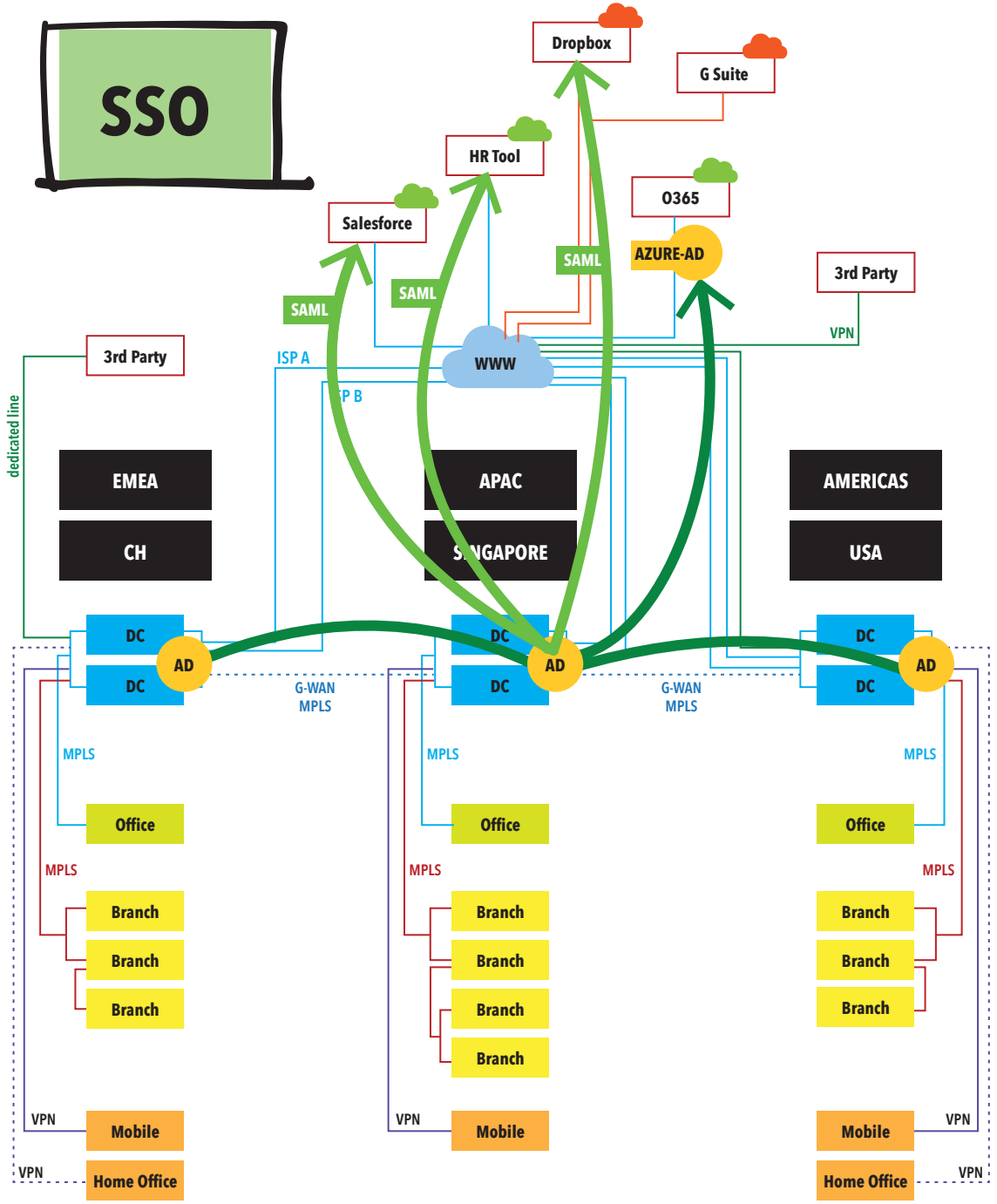
AVANTEC
Competence. Security. Trust.


SANCTIONED
HR Tool
Salesforce
UN-SANCTIONED
Dropbox
G Suite
3rd Party
VPN
3rd Party
ISP A
WWW
ISP B
dedicated line
EMEA
CH
APAC
SINGAPORE
AMERICAS
USA
DC
DC
DC
DC
DC
DC
G-WAN
MPLS
G-WAN
MPLS
MPLS
MPLS
MPLS
Office
Office
Office
MPLS
MPLS
MPLS
Branch
Branch
Branch
Branch
Branch
Branch
Branch
Branch
Branch
VPN
Mobile
VPN
Mobile
Mobile
VPN
VPN
Home Office
Home Office
VPN

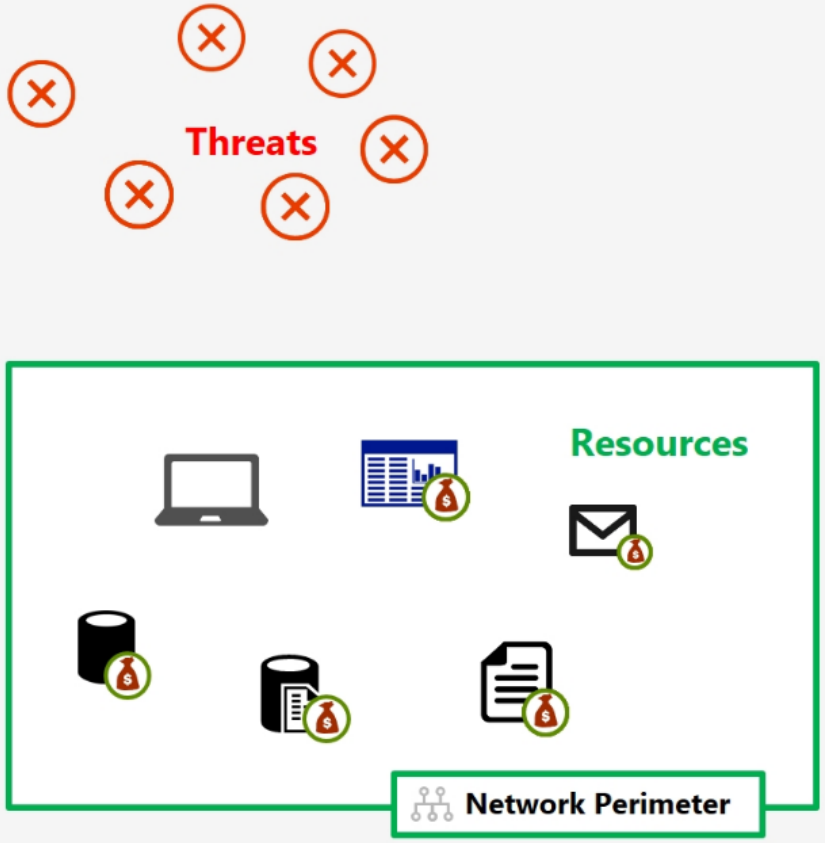
Authenticate in a secure way



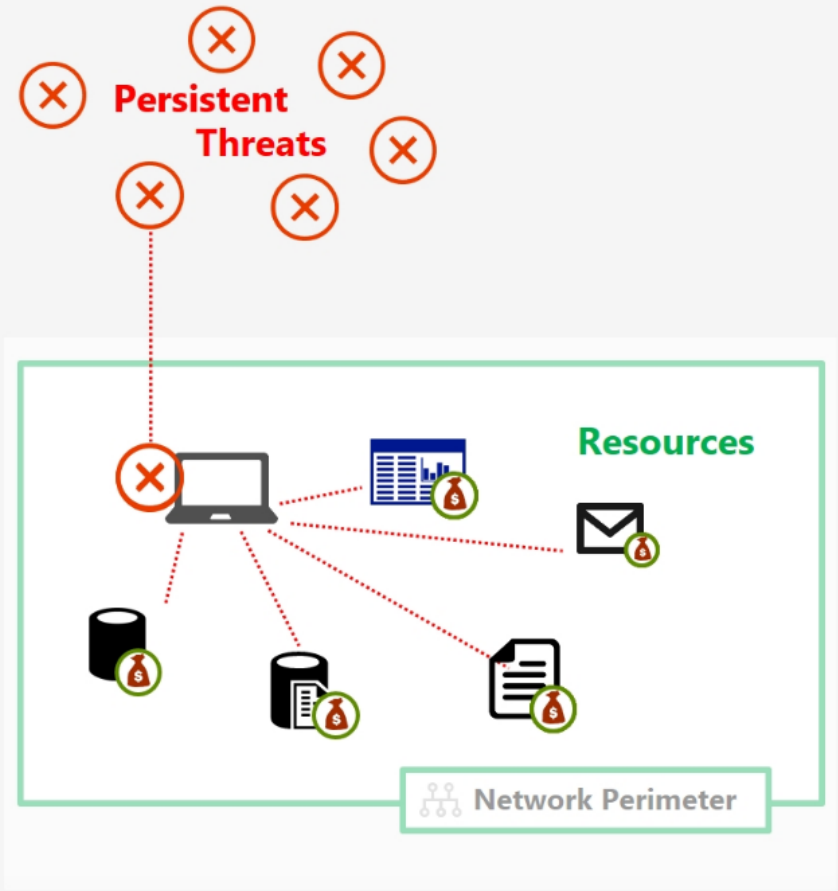
AVANTEC
Competence. Security. Trust.


SSO
Dropbox
G Suite
HR Tool
Salesforce
O365
AZURE-AD
SAML
SAML
SAML
3rd Party
VPN
3rd Party
ISP A
ISP B
WWW
dedicated line
EMEA
CH
APAC
SINGAPORE
AMERICAS
USA
DC
DC
AD
DC
DC
AD
DC
DC
AD
G-WAN
MPLS
G-WAN
MPLS
MPLS
MPLS
MPLS
Office
Office
Office
MPLS
MPLS
MPLS
Branch
Branch
Branch
Branch
Branch
Branch
Branch
Branch
Branch
Branch
Branch
Branch
VPN
Mobile
VPN
Mobile
Mobile
VPN
VPN
Home Office
Home Office
VPN

Modernizing the Security Perimeter



Modernizing the Security Perimeter

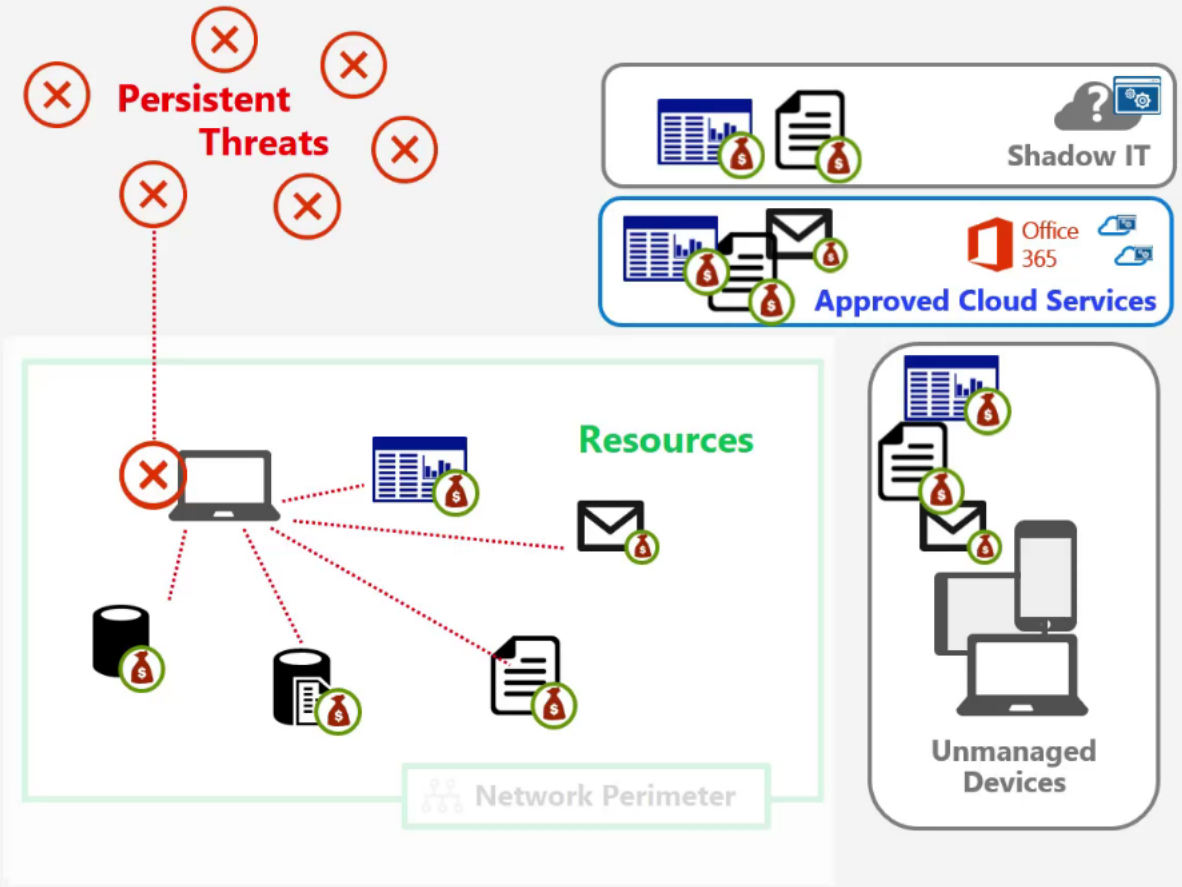


Network protects against classic attacks...

...but bypassed reliably with

- Phishing
- Credential theft

Modernizing the Security Perimeter

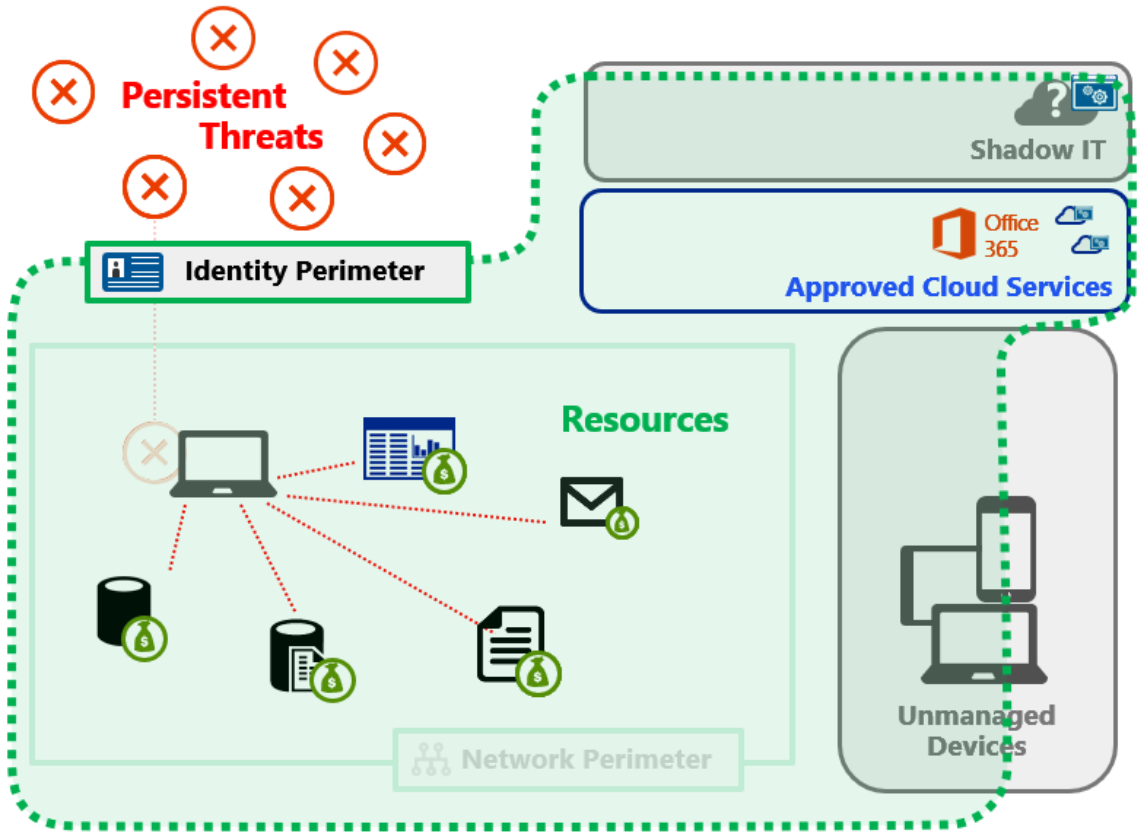


Network protects against classic attacks...

...but bypassed reliably with
- Phishing
- Credential theft

\+ Data moving out of the network

Modernizing the Security Perimeter

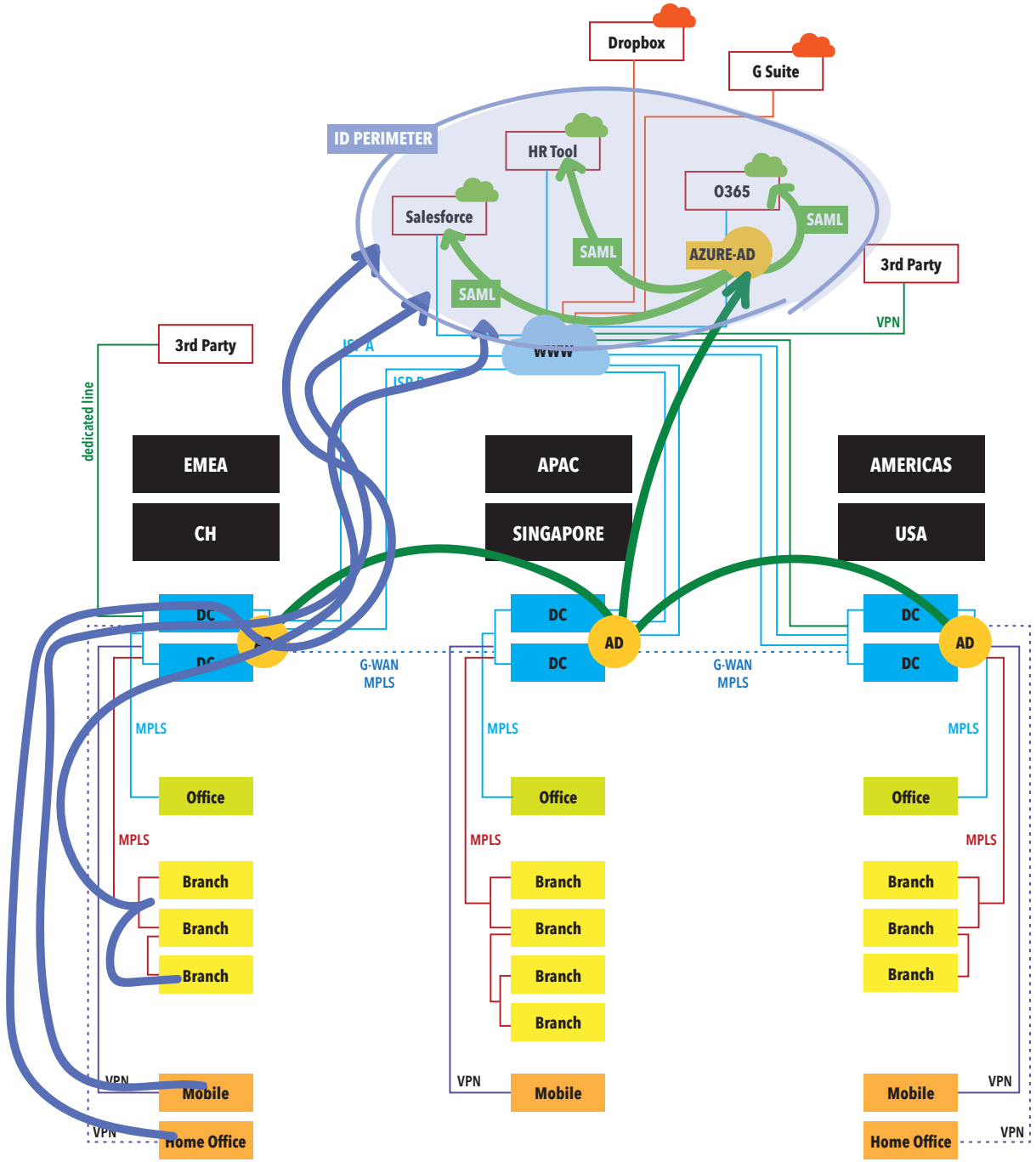


Network protects against classic attacks…

…but bypassed reliably with
- Phishing
- Credential theft

\+ Data moving out of the network

= Critical to build an **Identity security perimeter**
- ***Identity*** - Strong Authentication
- ***Access Management*** – Monitor and enforce access policies
- **Threat intelligence** integration into protections and detections



AVANTEC
Competence. Security. Trust.

Who are you?

Role-based access

Last sign-in?

Where are you coming from?

Corporate, Public Internet, Wi-Fi, Geographic Region

Last seen where from?

What device are you using?

Corporate Laptop, home PC
Tablet, Mobile

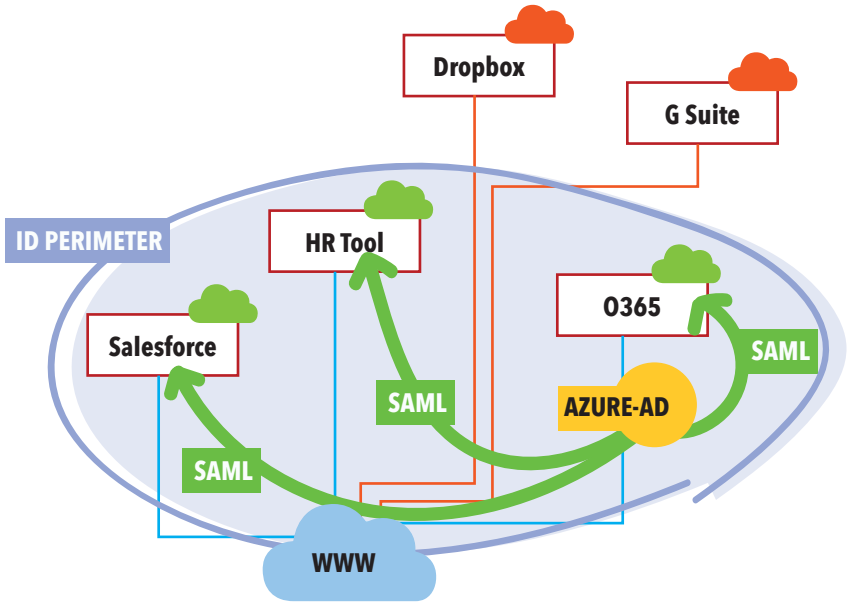
State of device?
Health / Integrity?

Additional factors

What time of day is it?
Are you authorised to access during that time?
Do you usually access during this time?
Correlation...

Conditional access:

- Allow / Block
- Allow read-only
- Enforce 2FA
- Allow restricted access
- Force remediation
- etc.



AVANTEC
Competence. Security. Trust.

Who are you?
Role-based access — Sales

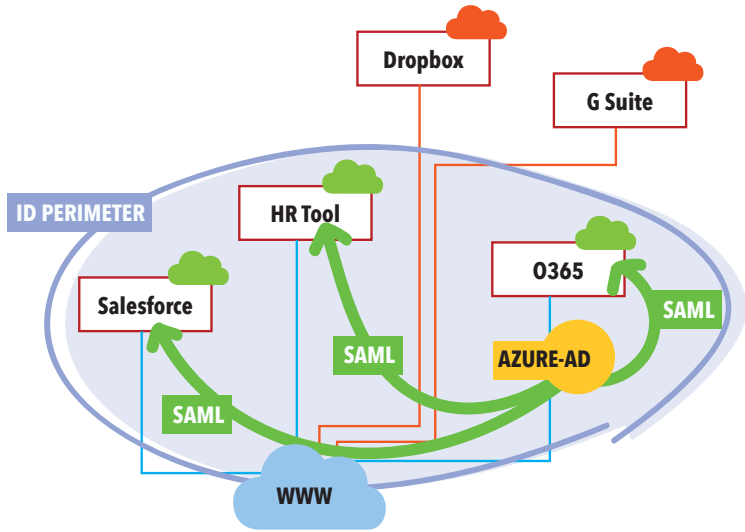
Where are you coming from?
Corporate, Public Internet, Wi-Fi, Geographic Region — Singapore, Public Internet

What device are you using?
Corporate Laptop, home PC Tablet, Mobile — Browser, Config mismatch, Device compromised

Additional factors
What time of day is it?
Are you authorised to access during that time?
Do you usually access during this time?
Correlation... — Now is 02:45 at night - unusual time, Last access from Switzerland, 22:45 - 4 hours ago

Conditional access:
- Block access
- Force remediation
- Generate alert

Or:
- Enforce 2FA
- Grant limited access
- Read-only



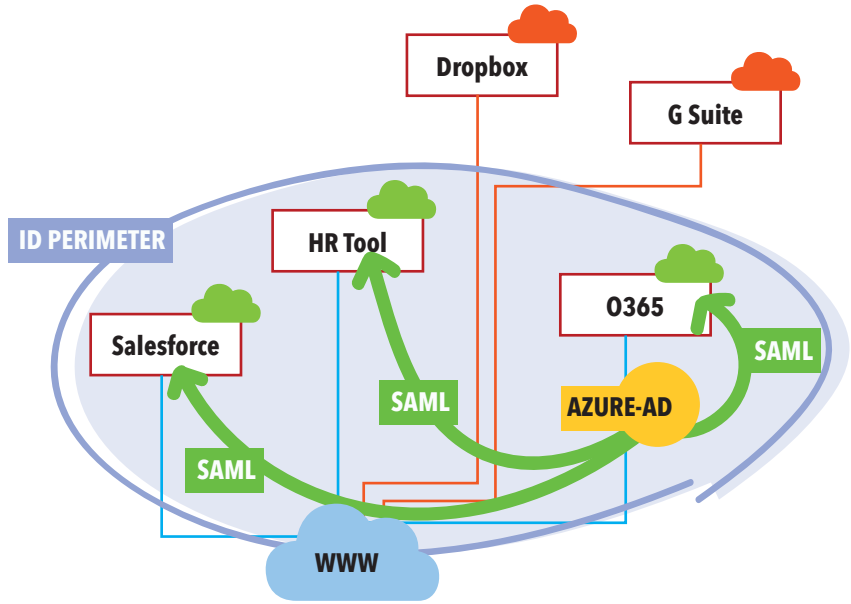
AVANTEC
Competence. Security. Trust.

Problems that can be addressed:

- Weak IAM
- Brute-force password
- SMS spoofing
- Endpoint compromise
- Account takeover

Best practices:

- Strong Password policy
- 2FA / MFA
- Least privilege
- Just-in-time authorisation
- Audit-logs



AVANTEC
Competence. Security. Trust.

Now about Anna & Peter:

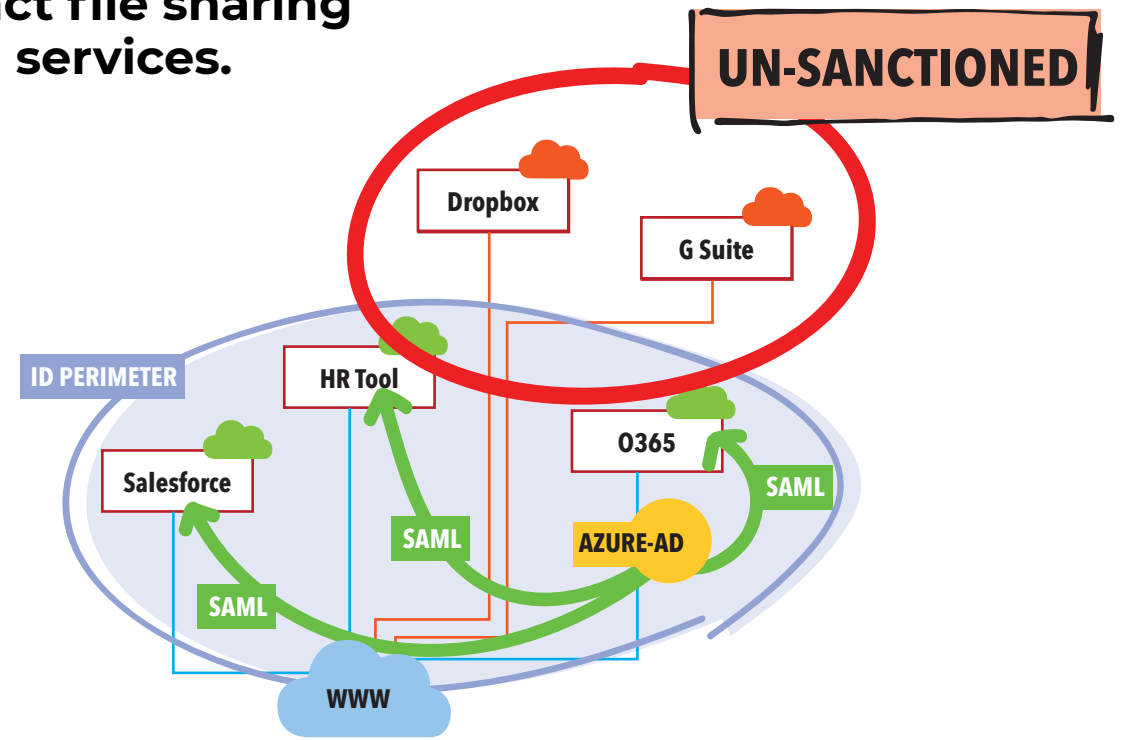
Anna is using Dropbox.
And Peter’s team is using G-Suite.

AVANTEC
Competence. Security. Trust.

The average enterprise uses 76 distinct file sharing cloud services.

The average enterprise uses 210 distinct collaboration cloud services.

18% percent of files uploaded to cloud-based file-sharing and collaboration services contain sensitive data.



“Shadow IT”

AVANTEC
Competence. Security. Trust.

What’s the problem?

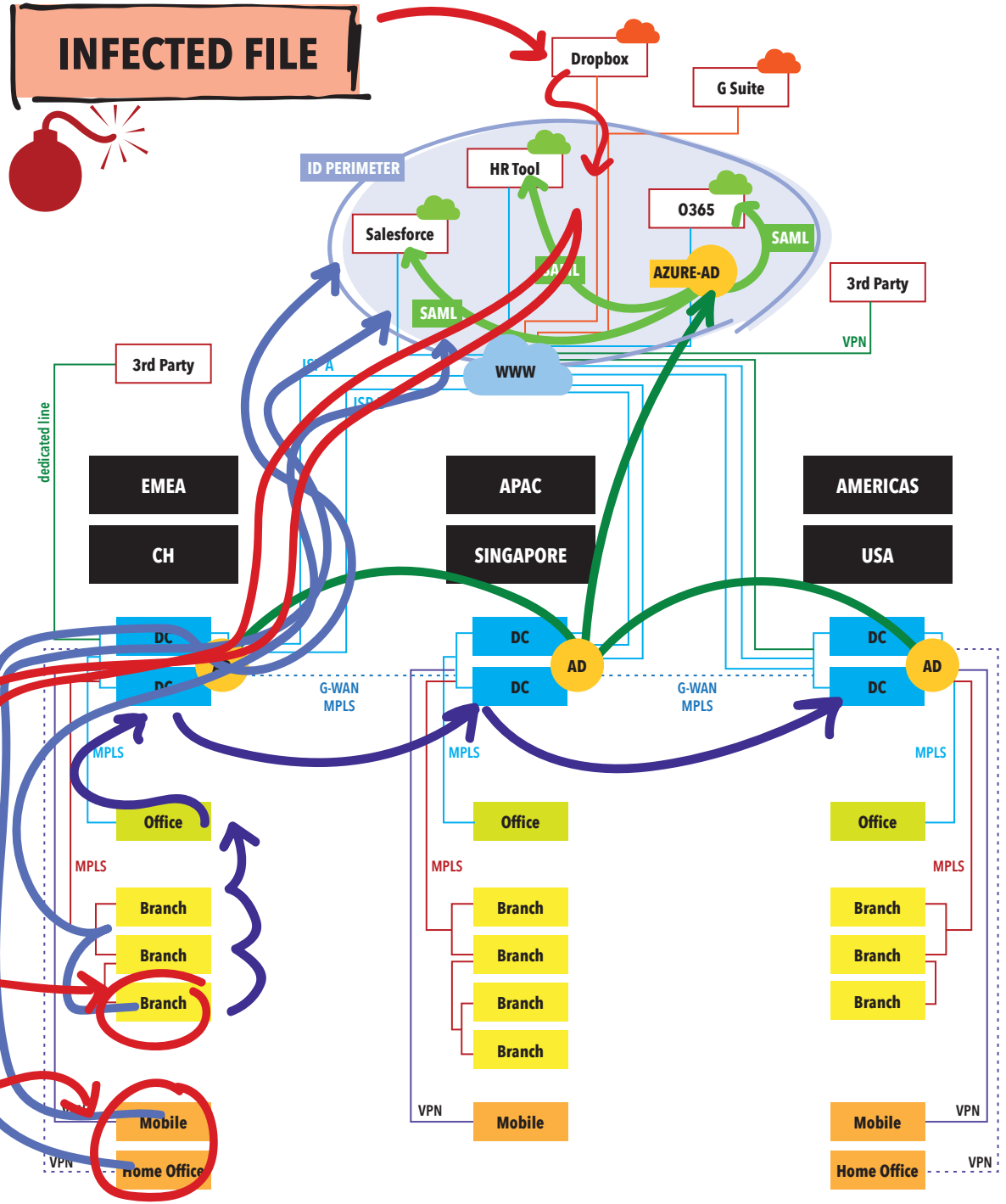
Companies are leaking sensitive files via Box accounts

Leaks discovered at Apple, the Discovery Channel, Herbalife, Schneider Electric, and even Box itself.

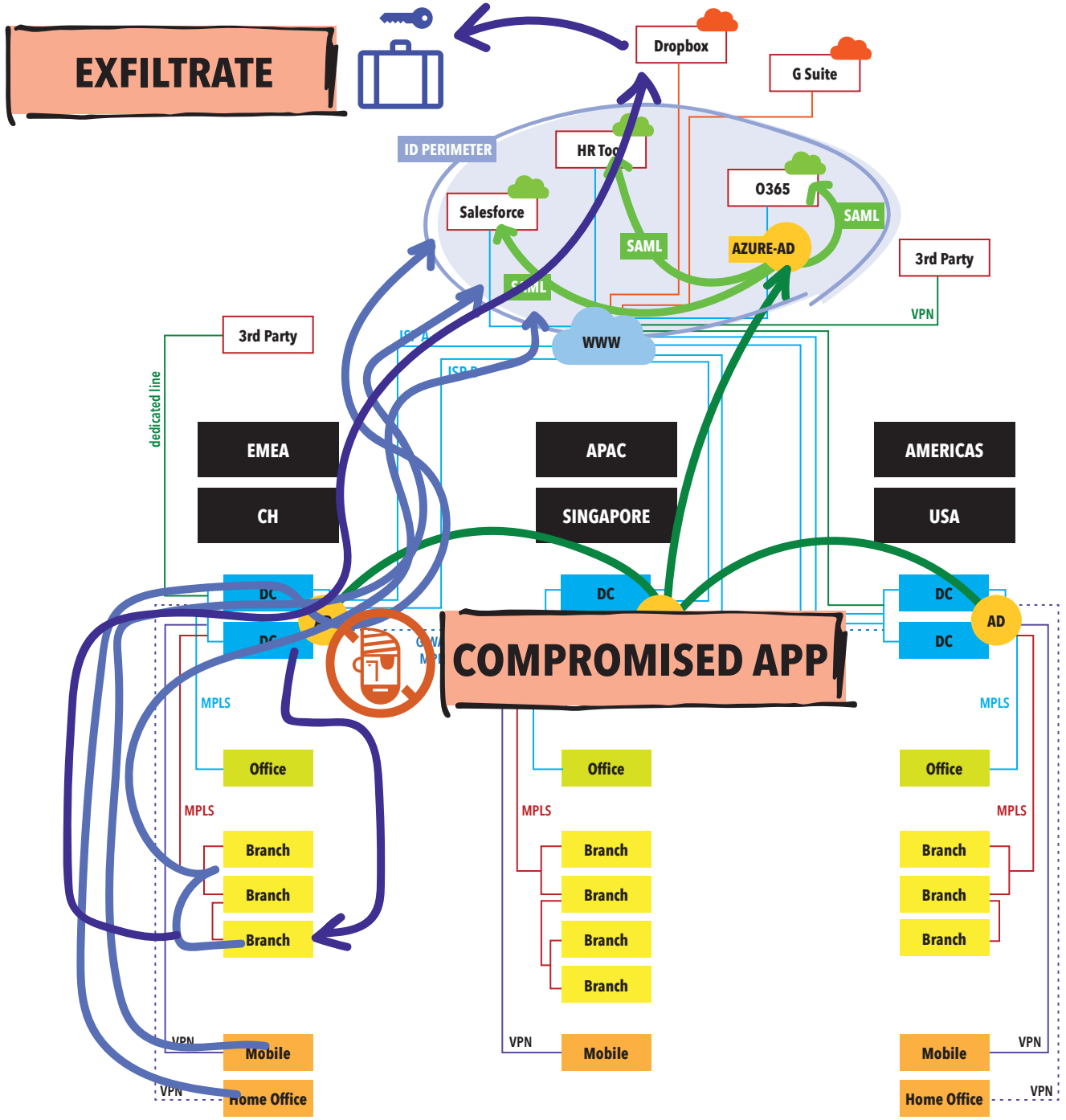
By Catalin Cimpanu for Zero Day | March 11, 2019 -- 19:54 GMT (19:54 GMT) | Topic: Security

11.3.2019

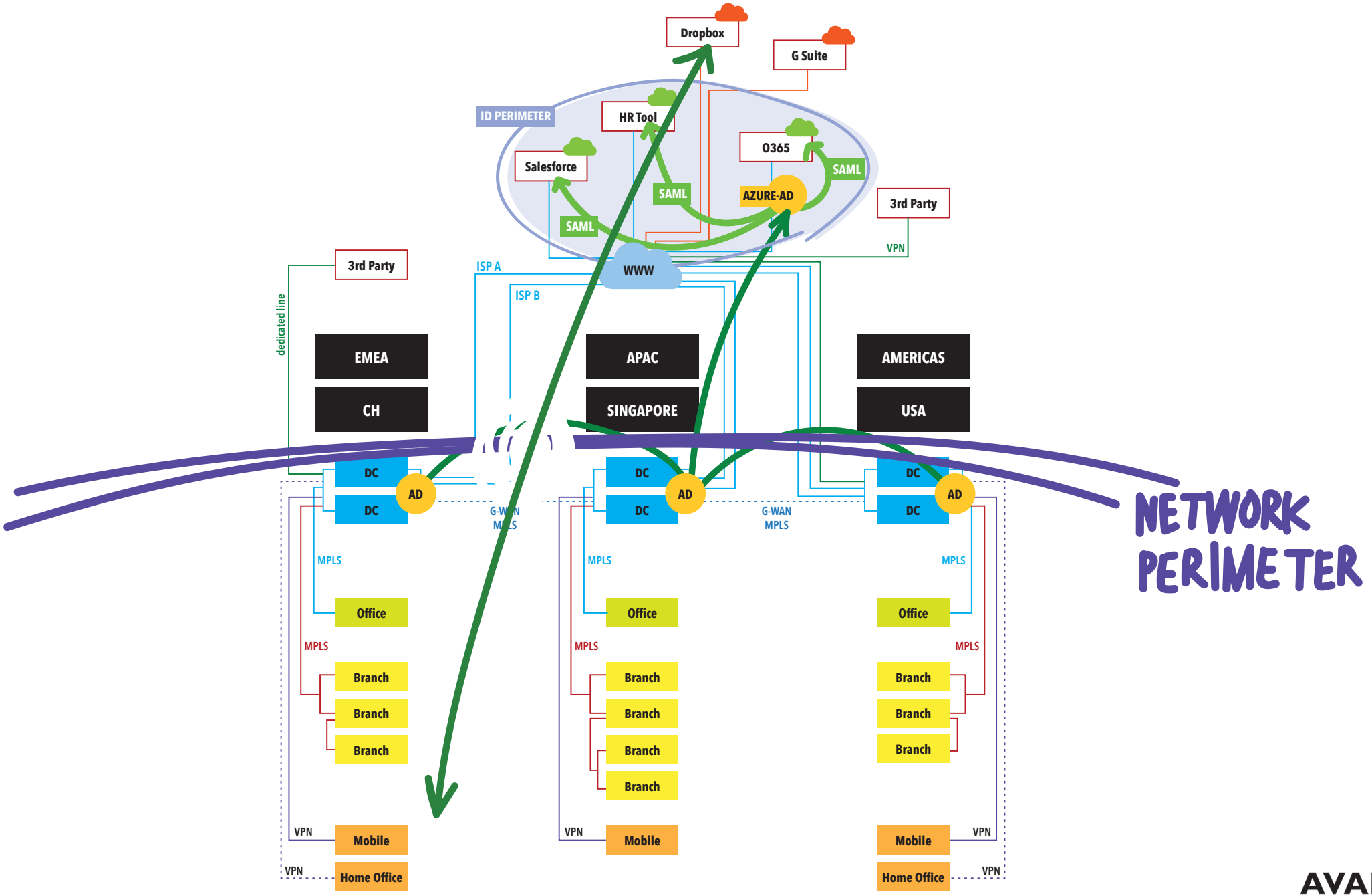
0



AVANTEC
Competence. Security. Trust.



AVANTEC
Competence. Security. Trust.



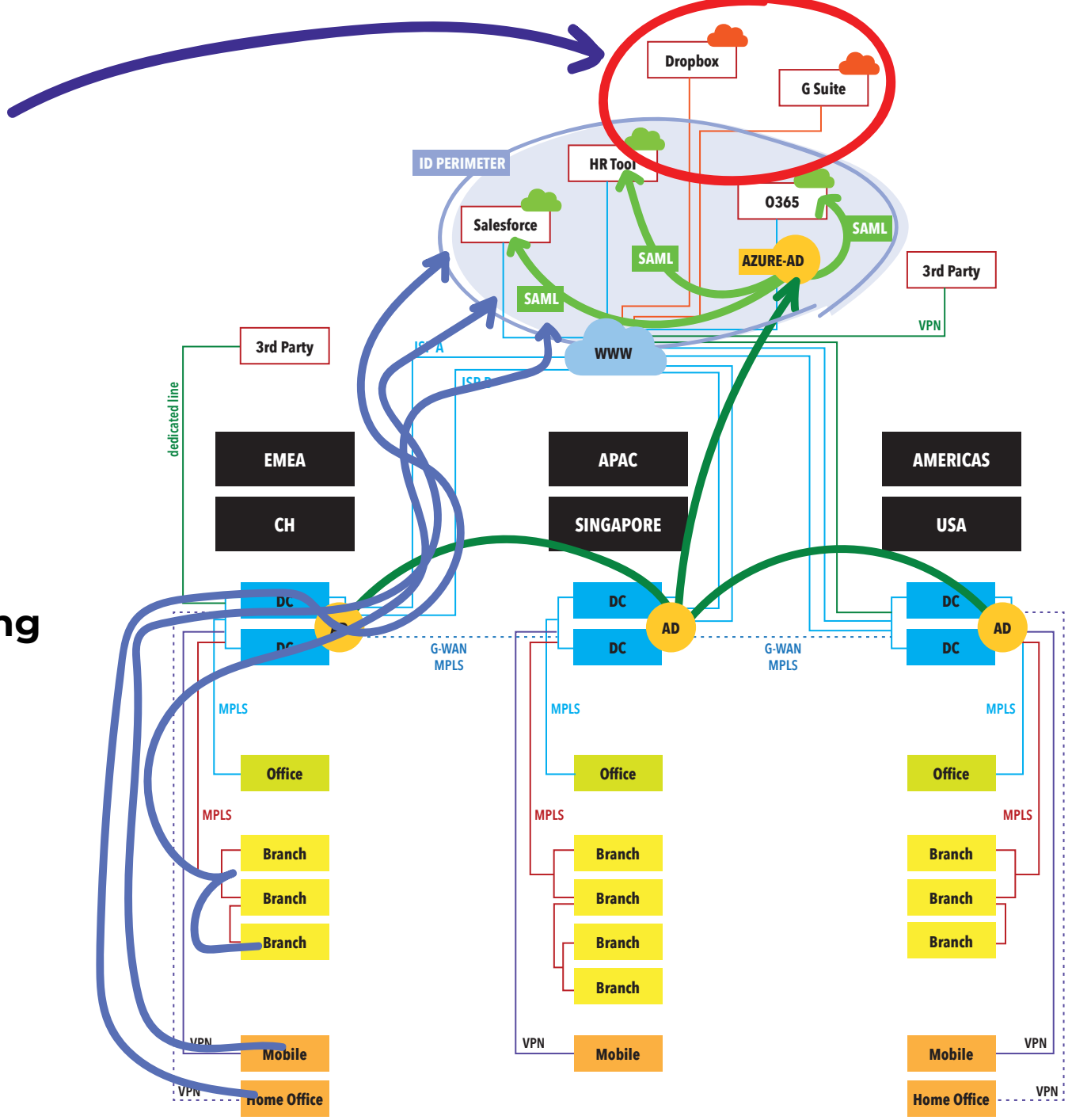
AVANTEC
Competence. Security. Trust.

1 IDENTIFY

- CASB connects to cloud services via API
- Using CASB Gateway “inline”

2 ENFORCE

- DLP
- Prevent unauthorised sharing
- Detect compromised accounts
- Detect risky users
- Detect malware
- Detect insider threats
- Limit long sessions
- Identify location change
- Identify privilege escalation
- Log everything



AVANTEC
Competence. Security. Trust.

We have multiple perimeters now:

- Identity Perimeter
- Messaging Perimeter
- Data Perimeter
- Compute Perimeter
- App Perimeter

Identity & CASB have similar concepts:

Who is accessing what, when, how?
Can he/she?
Does he/she usually?
Incoming or outgoing?
Privileged data or account?
Then act accordingly.

AVANTEC
Competence. Security. Trust.

At the end of the day:

Visibility on what Cloud Apps are being used.

Control access adequately.

AVANTEC
Competence. Security. Trust.

Thank you

AVANTEC
Competence. Security. Trust.