Enterprise Security with Expanded Network Boundaries

Dr. Zhijun (William) Zhang
Lead Security Architect at The World Bank Group

Data Breaches in the News

Large-scale breaches are now a regular occurrence across industry and geography

Strategic Risk

Financial Risk

Operational Risk

Reputation Risk

Consequences

- Erosion of client confidence
- Financial loss
- Damage to Brand
- Poor publicity
- Delays in strategically competitive initiative
- Regulatory fines

Cybersecurity is an enterprise-wide business issue requiring a risk management approach.

Information Security Threats

External Threats

- Organized Crime
- Hacktivist Group
- State or Business Sponsored Entity
- Vendor/Third-Party

Internal Threats

- Careless/Unaware User
- Malicious Privileged Insider
- Nonprivileged Insider

Attack Patterns

Crimeware

Cyber Espionage

Distributed Denial of Service

Insider and Privilege Misuse

Web Application Attacks

Business Email Impersonation (CEO Fraud)

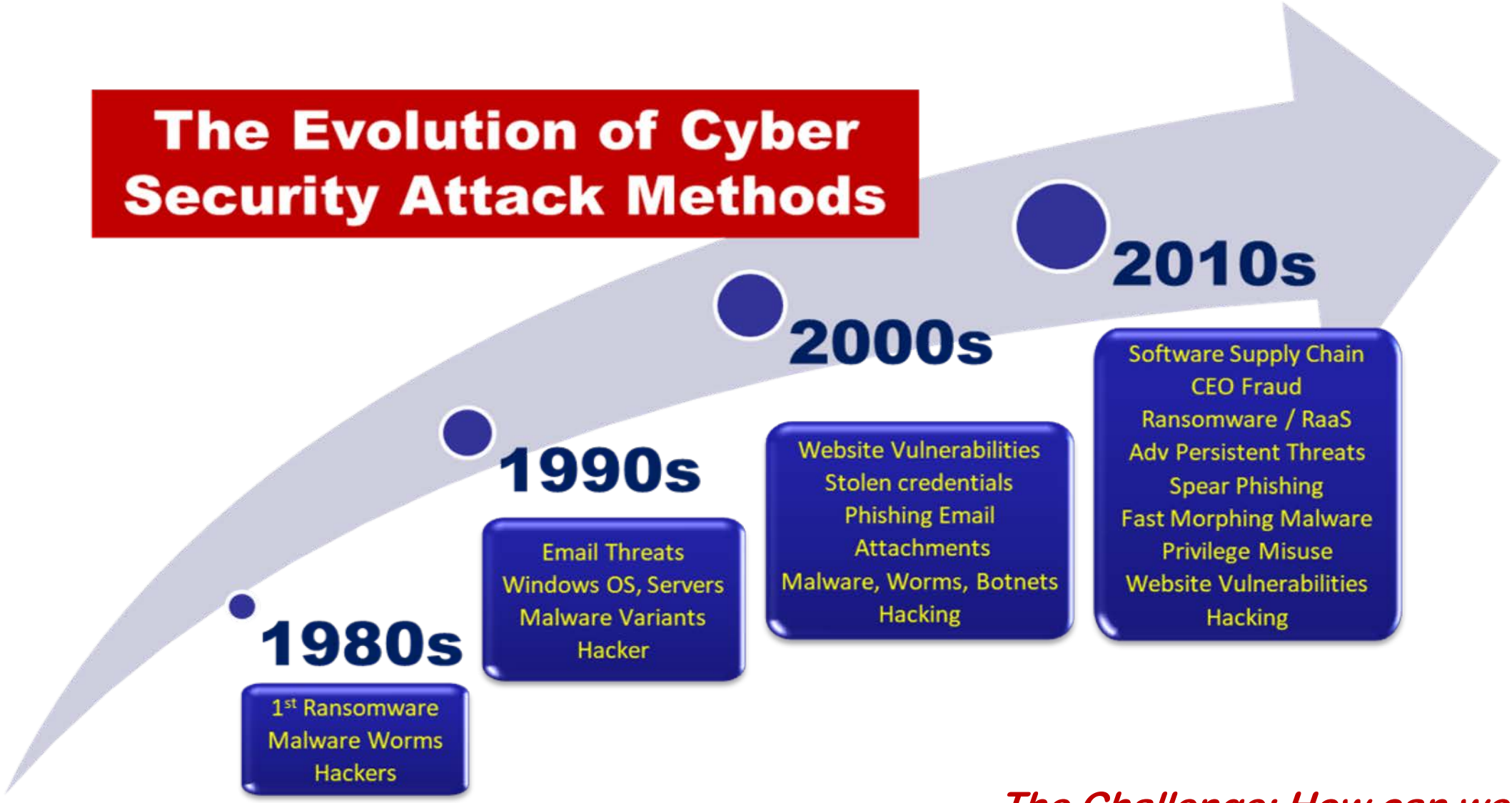
Spear Phishing

Information Leakage

Unauthorized Use

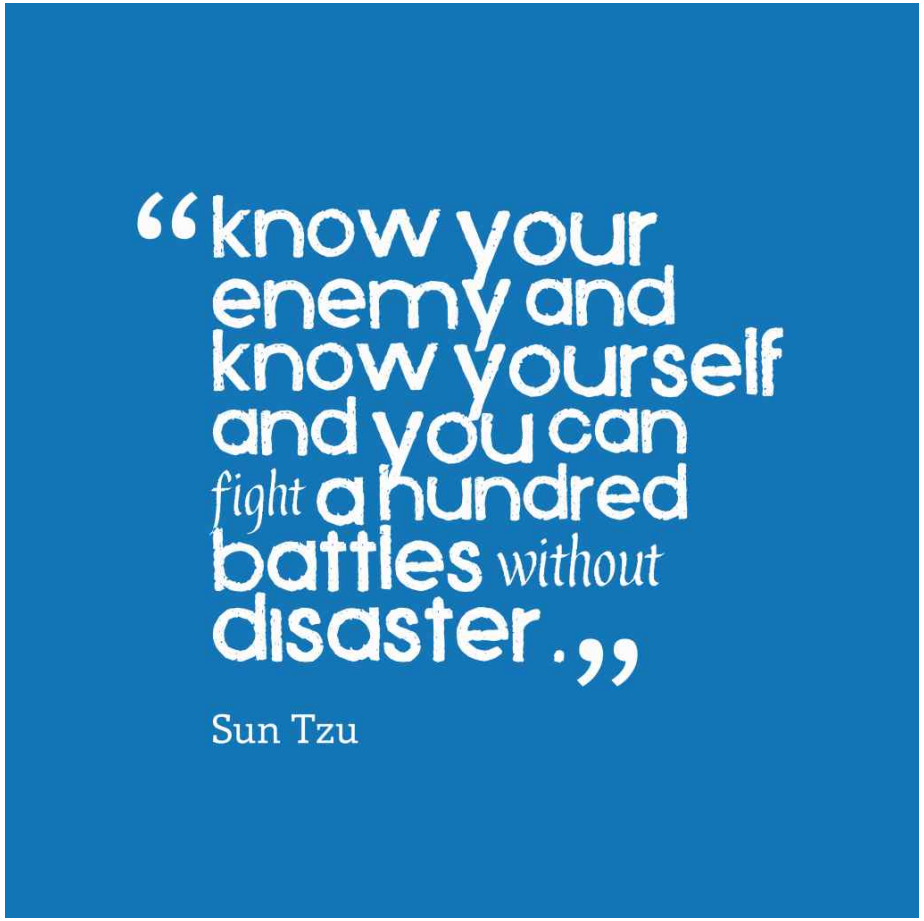
Ransomware

The Evolution of Cyber Security Attack Methods



The Challenge: How can we fight a set of ever-moving targets?

The Answer: Know Your Enemies



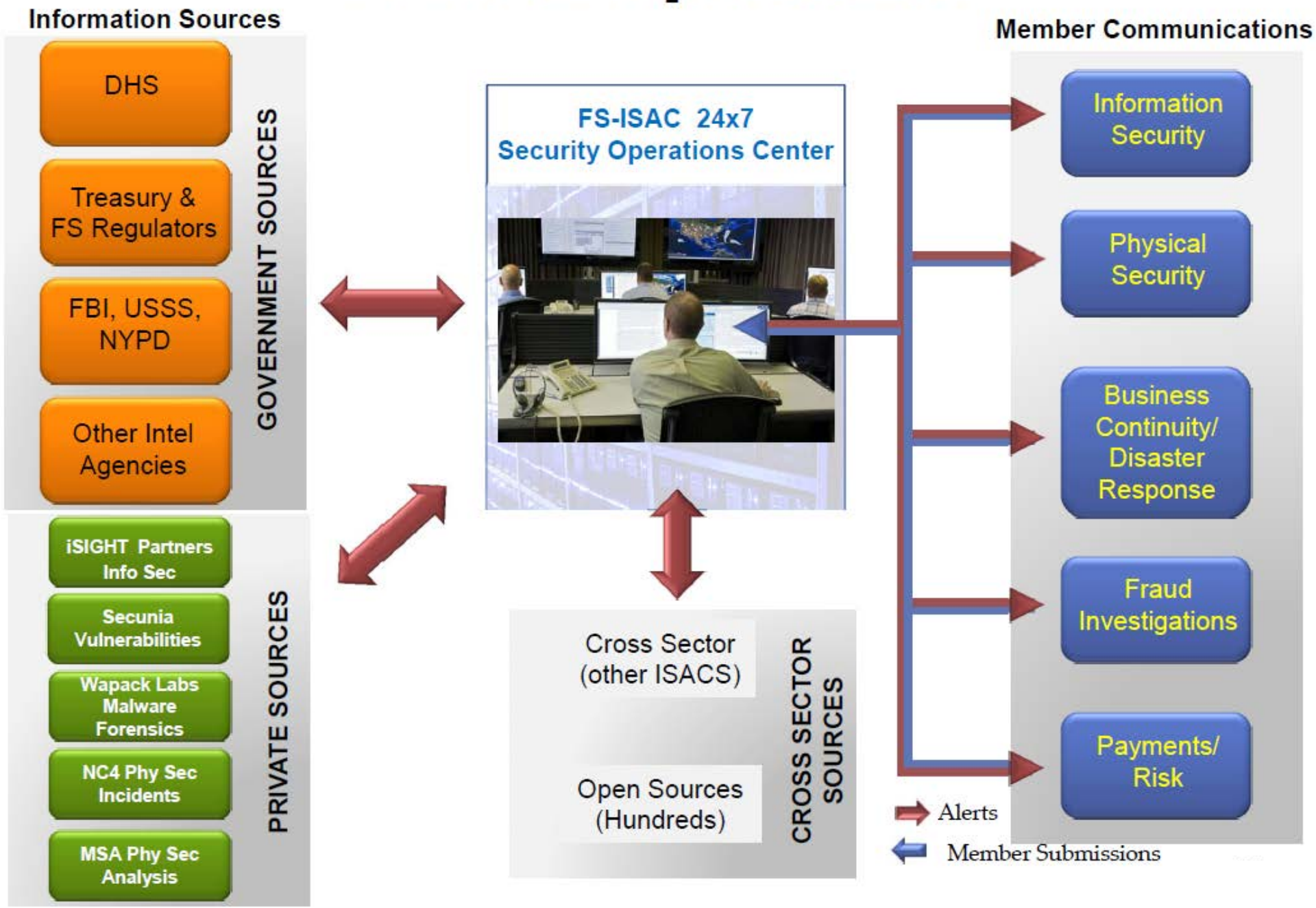
We need threat intelligence

- Vulnerability reports
- New attacks and IOCs
- New malware and signatures
- Suspicious domains
- IP addresses associated with malicious activity
- Enterprise information shared on pastebins

We need to automate threat intelligence actions

- Structured Threat Information eXpression (STIX)
- TAXII (Trusted Automated eXchange of Indicator Information)

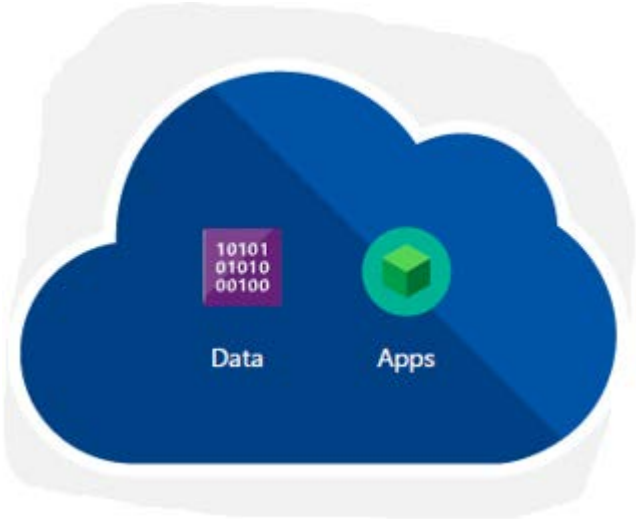
FS-ISAC Operations



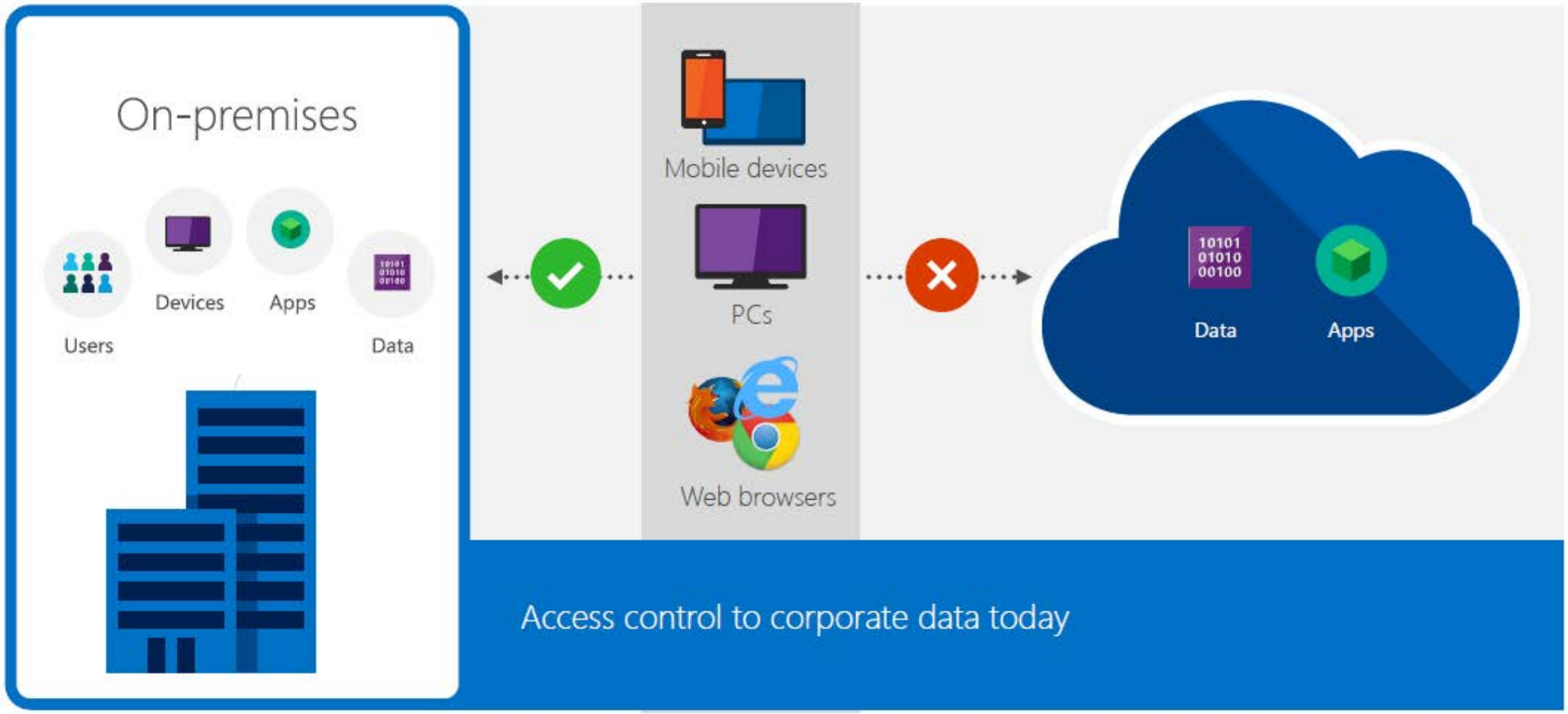
But Information Security is NOT the Goal

- Business wants mobility
  - Traveling staff
  - Consumerization
  - Convenience and productivity

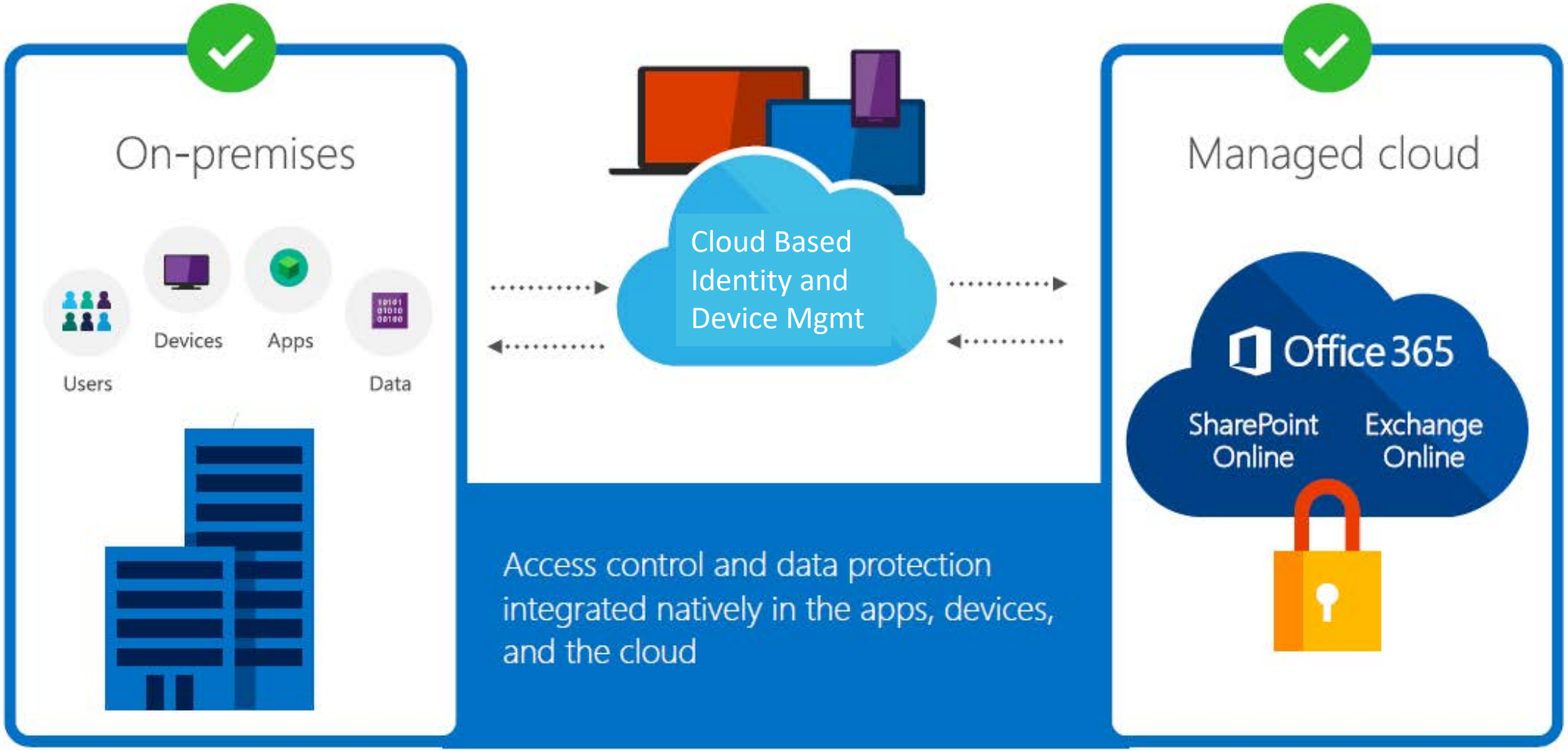
- Business wants cloud
  - Agility
  - Up-to-date capabilities
  - Service level guarantee



Control Access to Enterprise Data - Traditional



Controlling Access to Data in Mobile-first and Cloud-first Context



Cloud-based Security is an Industry Strategy

The Promise by Microsoft

- Leverage its massive customer base to collect and analyze data
- Centrally manage security to benefit all customers
- Manage security across all Microsoft services
- Much more frequent updates and upgrades

The Pre-requisite

- “Deep adoption” of Azure AD and other cloud services
- Constantly feeding data to Microsoft cloud

Key Microsoft Cloud Services

Azure AD (positioned to be the IDaaS)

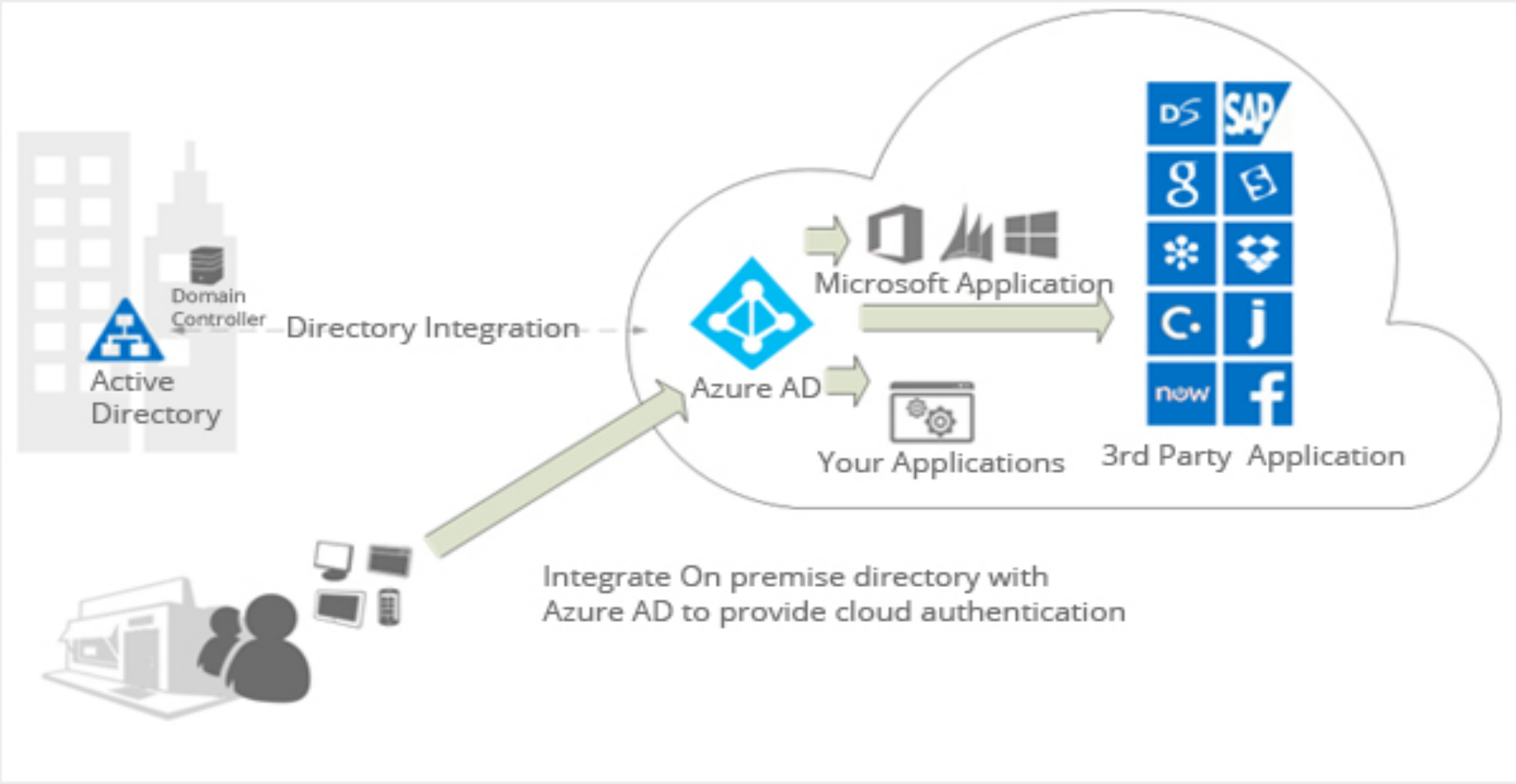
- WBG currently uses as part of Office 365
- Windows 10 devices will “domain join”
- Will become the preferred federation engine for SaaS
- Will be a central authentication/authorization engine for applications (OpenID Connect & Oauth)

Intune

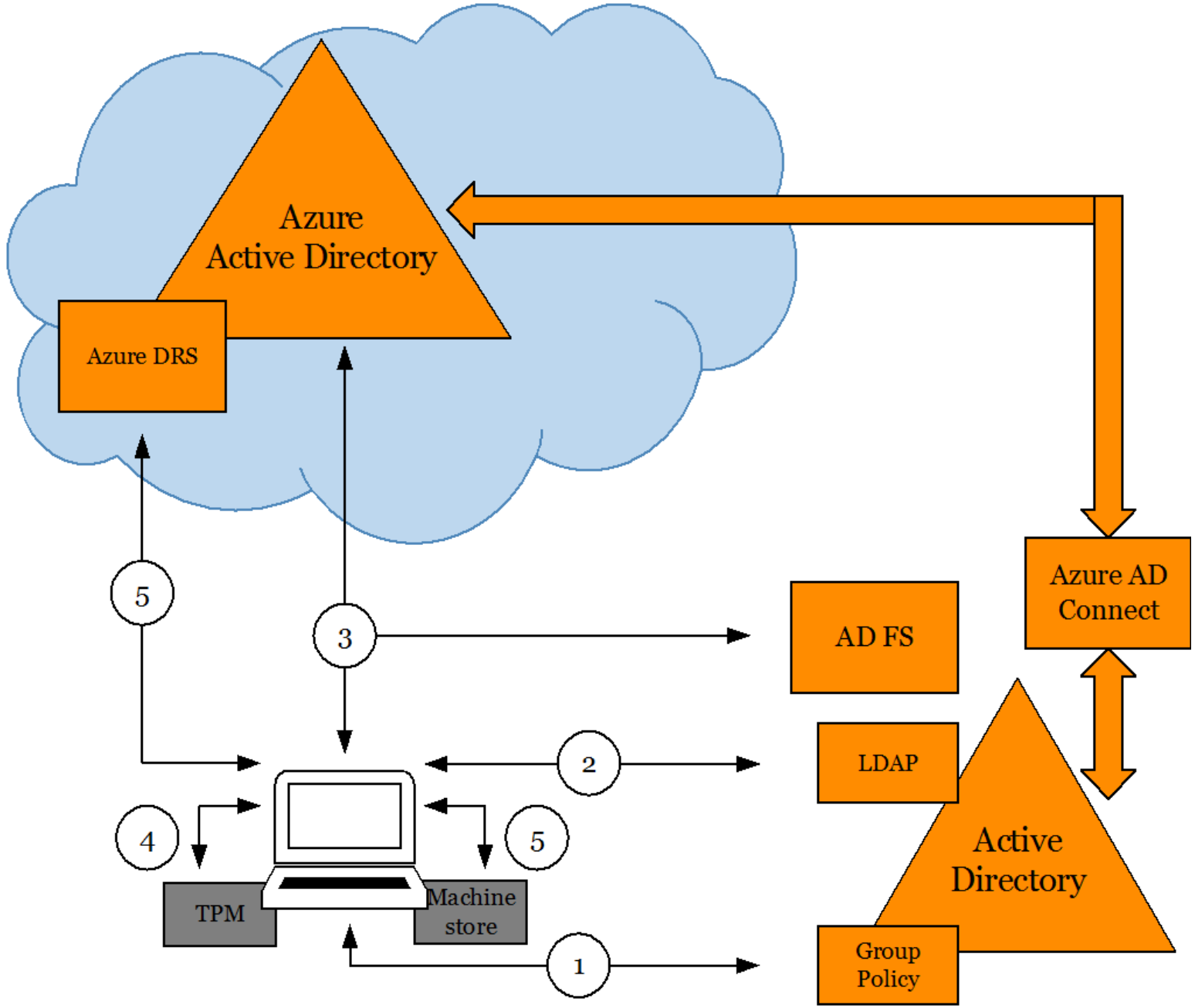
- For MAM and MDM
- On-going security such as DLP

Cloud engine behind Defender, ATP, Information Protection, etc.

Windows Devices Can/Will Join Azure AD

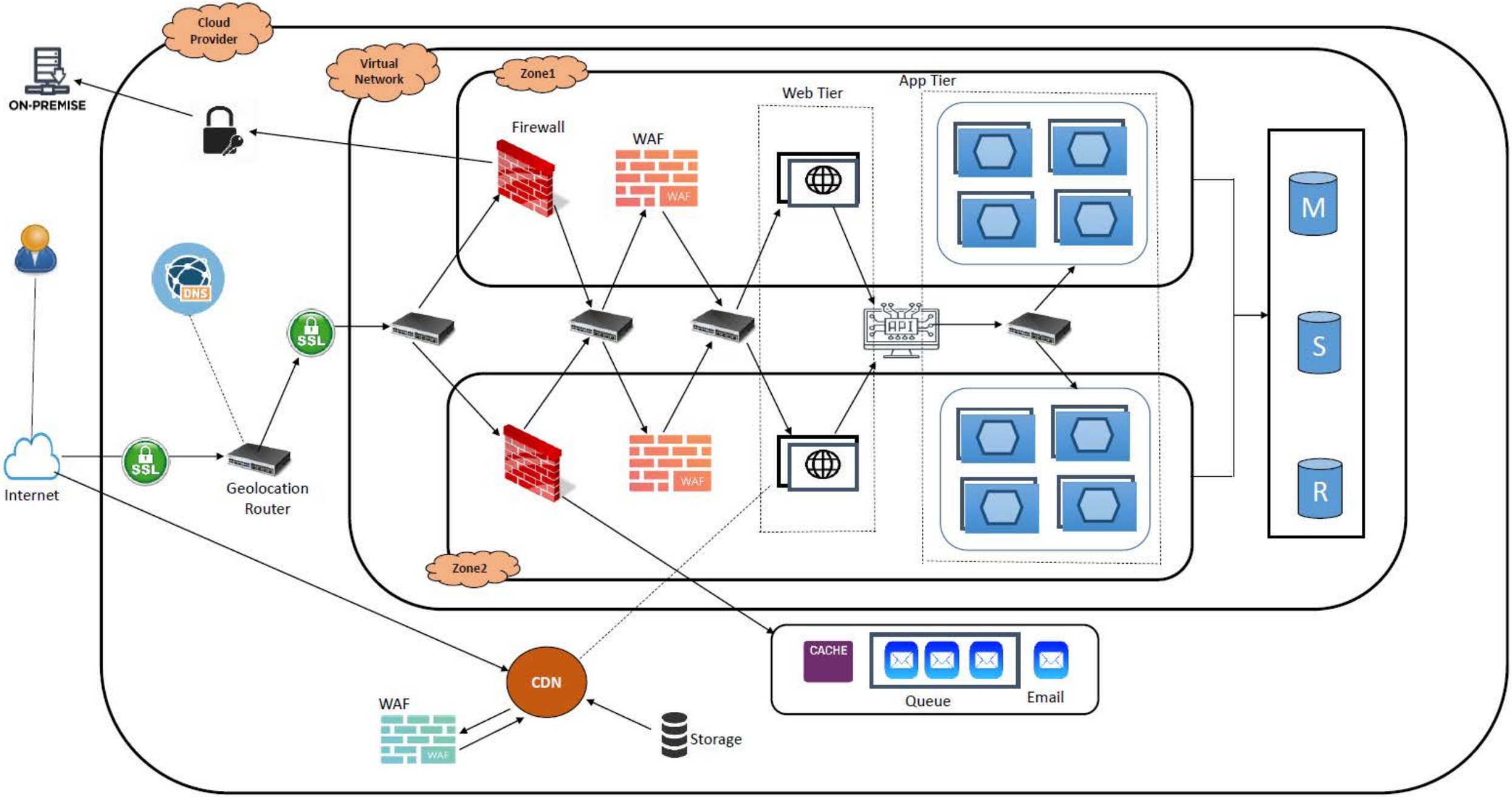


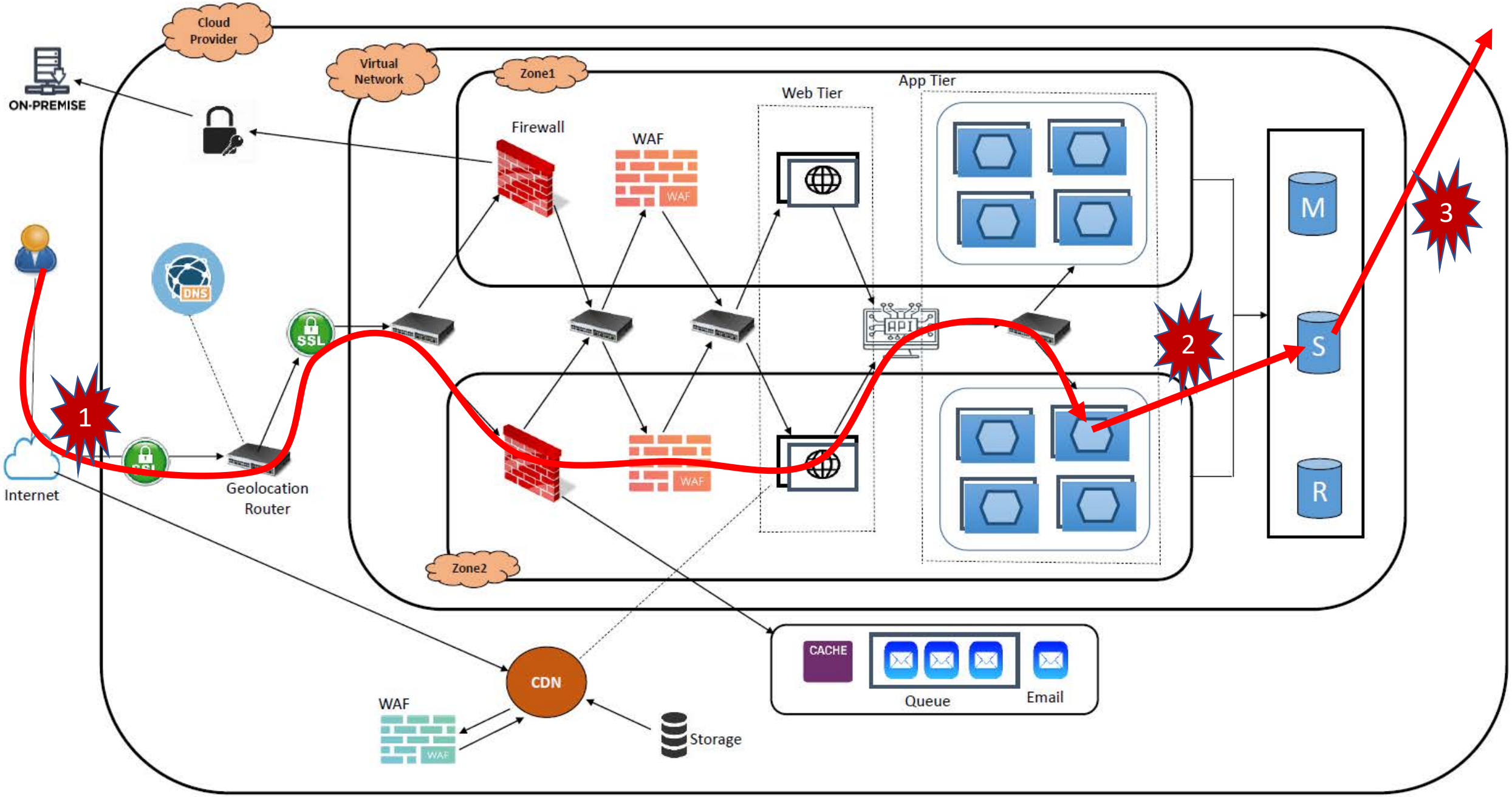
Such devices will have much less dependency on on-premises infrastructure when accessing cloud resources.

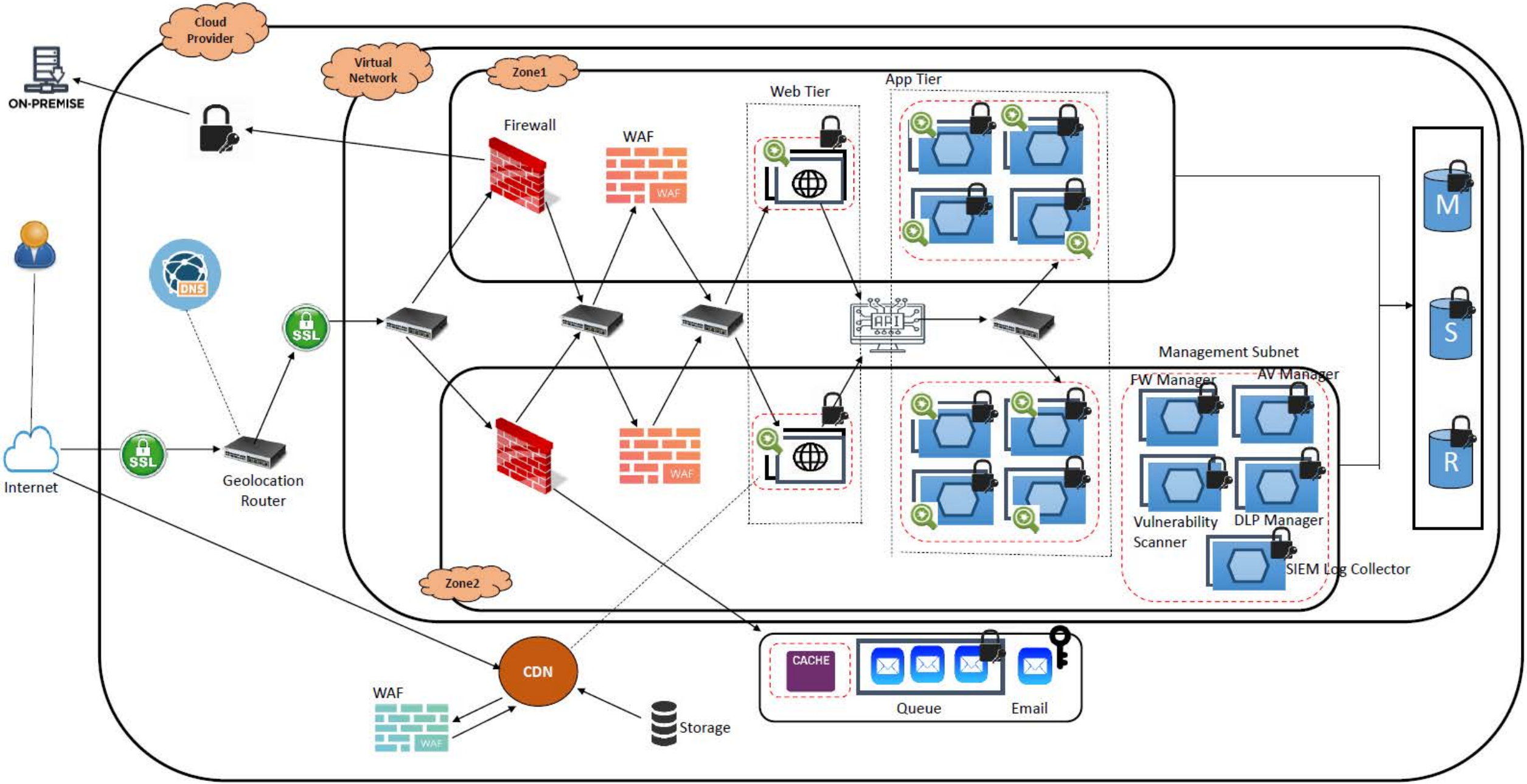

Azure
Active Directory
Azure DRS
Azure AD
Connect
AD FS
LDAP
Active
Directory
Group
Policy
5
3
2
4
5
1
TPM
Machine
store

What about Moving Your Own Apps to the Cloud?

- Enterprises focus on their own business app logic
- Cloud service providers manages compute, storage, and networking
- It can be more secure
  - Keeping humans (employees) away from systems
  - Leverage dedicated resources to take care of foundational security
  - Overall security is a shared responsibility


Cloud Provider
Virtual Network
ON-PREMISE
Zone1
Web Tier
App Tier
Firewall
WAF
WAF
DNS
SSL
SSL
API
M
S
R
Internet
Geolocation Router
Zone2
CDN
CACHE
Queue
Email
WAF
WAF
Storage


Cloud Provider
Virtual Network
ON-PREMISE
Zone1
Web Tier
App Tier
Firewall
WAF
DNS
SSL
API
M
S
R
1
2
3
Internet
Geolocation Router
Zone2
CDN
WAF
Storage
CACHE
Queue
Email


Cloud Provider
Virtual Network
ON-PREMISE
Zone1
Web Tier
App Tier
Firewall
WAF
DNS
SSL
Internet
SSL
Geolocation Router
API
Management Subnet
FW Manager
AV Manager
Vulnerability Scanner
DLP Manager
SIEM Log Collector
M
S
R
Zone2
CDN
WAF
Storage
CACHE
Queue
Email

Summary

Leverage the power of the cloud

Leverage the intelligence of the community

Automate security controls

- Security-as-code: baselined, version controlled, and monitored

Re-validate what you trust periodically

- Your cloud service providers
- You threat intelligence sources
- Your software suppliers
- Your employees and contractors

Re-validate your technical controls

- Are your security baseline code still valid?