

Applied Cybersecurity Fundamentals

Brendan McGowan

Chief Technology Officer



Key points

- Threat landscape
- Top threat payloads of 2018
- Tools you need to defend
- Evolving philosophy on security preparedness and investment
- Cloud services implications

How do the
bad guys
attack?

Top 3 Infection Vectors

Email



Website



USB



Email



Infected
Attachments



Phishing

Phishing

Puddle

Your Bank

Spear

Specific Staff

Whale

C-Level

Web



Drive-by
Downloads



Malvertising

USB



What payloads do
bad guys
deliver in 2018?





Ransomware

Data Theft



The background is a dark blue circuit board with glowing blue traces and components. A network of orange lines with Bitcoin symbols (B with a vertical line) connects various points across the image. A large Bitcoin symbol is centered behind the text.

crypto Mining

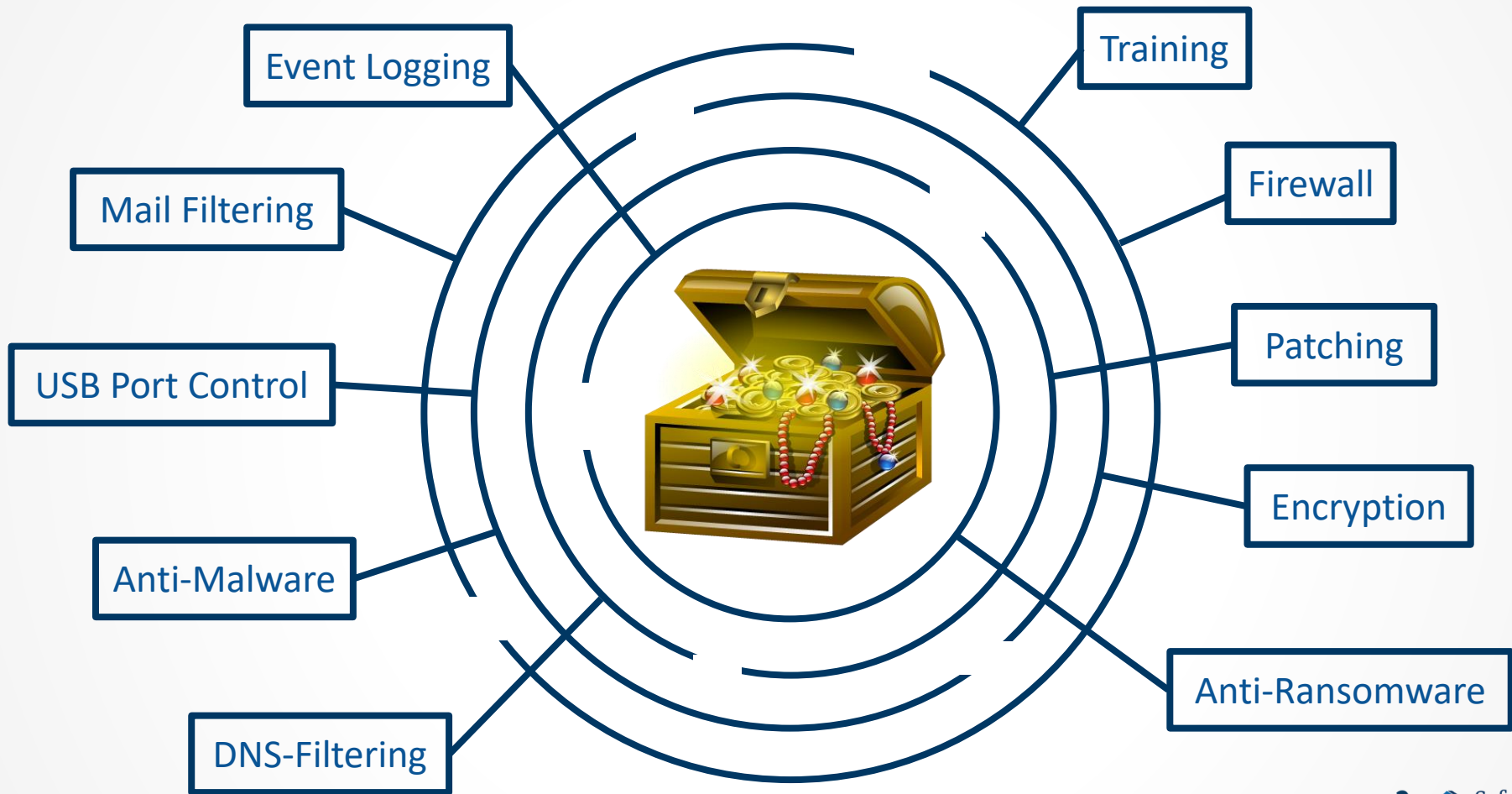
Botnet



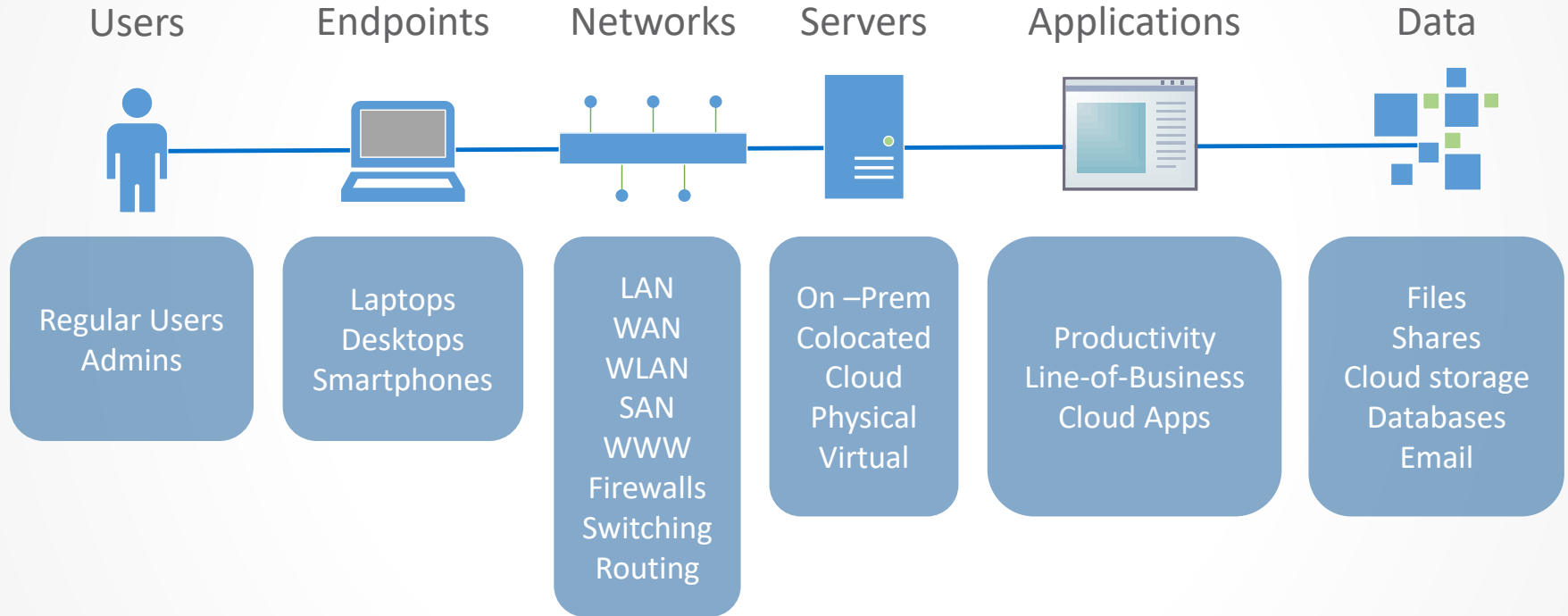
How do **we** defend?

Defense in Depth



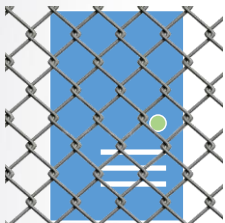


Surface Area



Network Edge

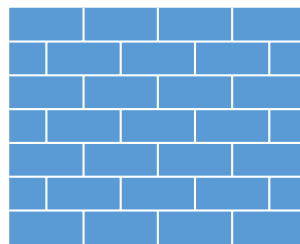
Server
Hardening



Sandboxing



SSL Break-Inspect



Firewall
IPS
Content Filter

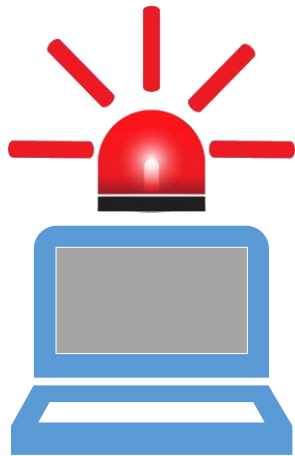
Content Filtering



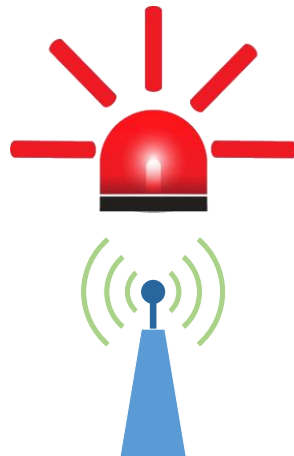
Network Interior



Vulnerability
Scanning



Rogue
Device
Detection

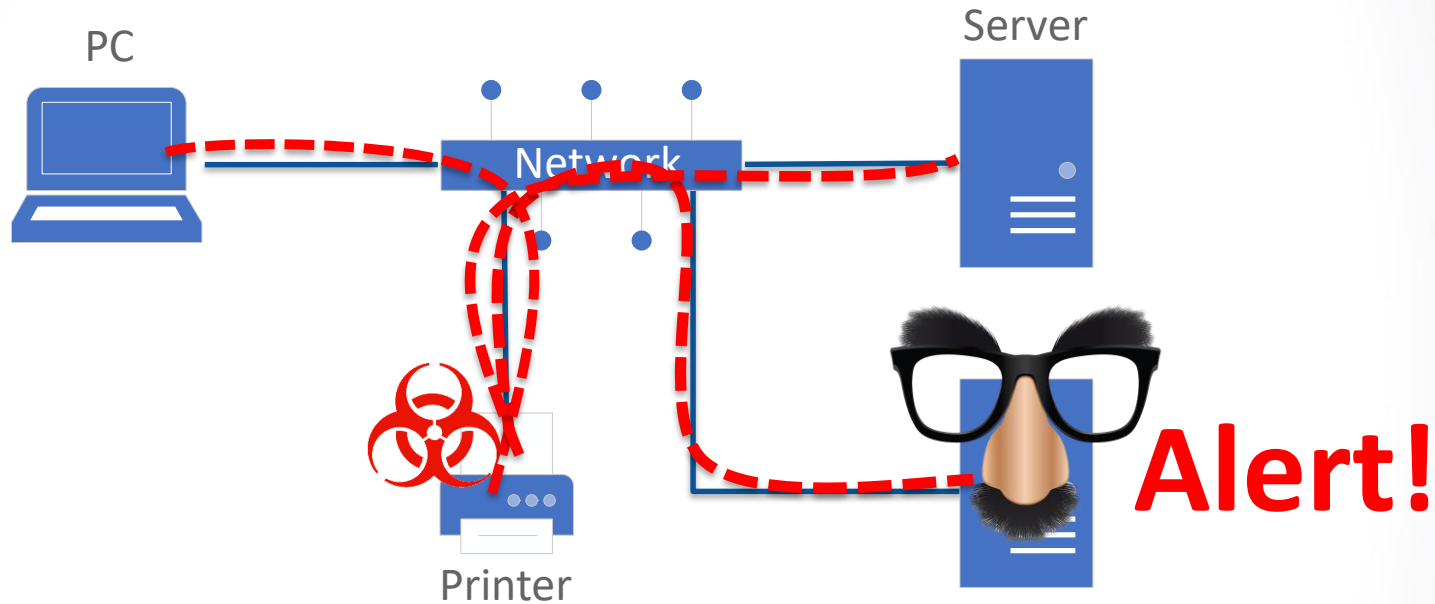


Rogue
AP
Detection



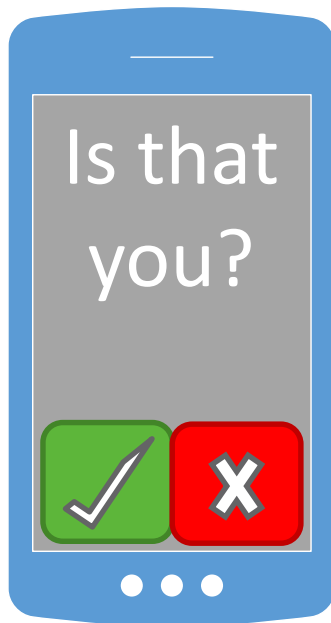
Rogue
Actor
Detection

Rogue Actor Detection



Users

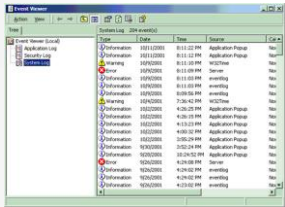
Multifactor Authentication



Security Awareness Training



Server and Workstations



Event Log
Monitoring



Process
Journaling



Anti-
Ransomware

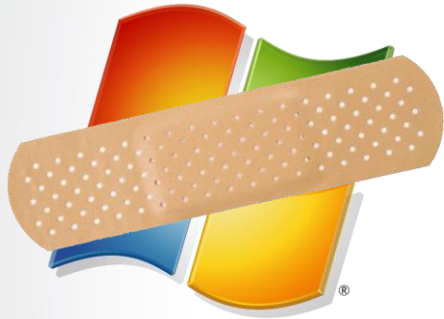


Anti-
Malware

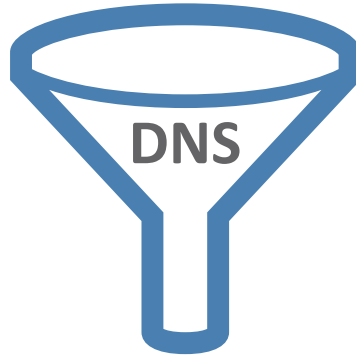
Anti-Malware



Server and Workstations



Patching



DNS Filtering



Disk
Encryption



USB Port
Control



explorer.exe



BLOCKED BUT NOT DELETED
c:\users\...\installer.exe
88fc6051...9cb2a4f9



ROOT CAUSE

Existed before agent



VIRUS TOTAL

Detection Ratio: 40/56

[Go to Virustotal](#)



SIGNATURE

Unsigned



PREVALENCE

Found on 1 host

Secd...ing2 | c:...er.exe

Secd...ing2 | ...\csrss.exe

Security Awareness Training



Data



Email
Filtering



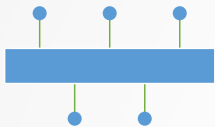
Email
Encryption



Data Loss
Prevention

Security

Networks



LAN

Vulnerability Scanning
Rogue Actor Detection
Switch/Router Patching
Rogue Device Detection
Network Access Control

WAN IPS

WWW IPS

DDoS Prevention
Content Filtering

WLAN

Multi-Factor Auth
Rogue AP Detection

Users



Security Testing

Servers



IPS

Anti-Malware
Anti-Ransomware
Patching
Event Log Monitoring

Endpoints



Anti-Malware
USB Port Control
Anti-Ransomware
DNS Filtering
Patching
Content Filtering
Configuration Enforcement
Event Log Monitoring

Applications

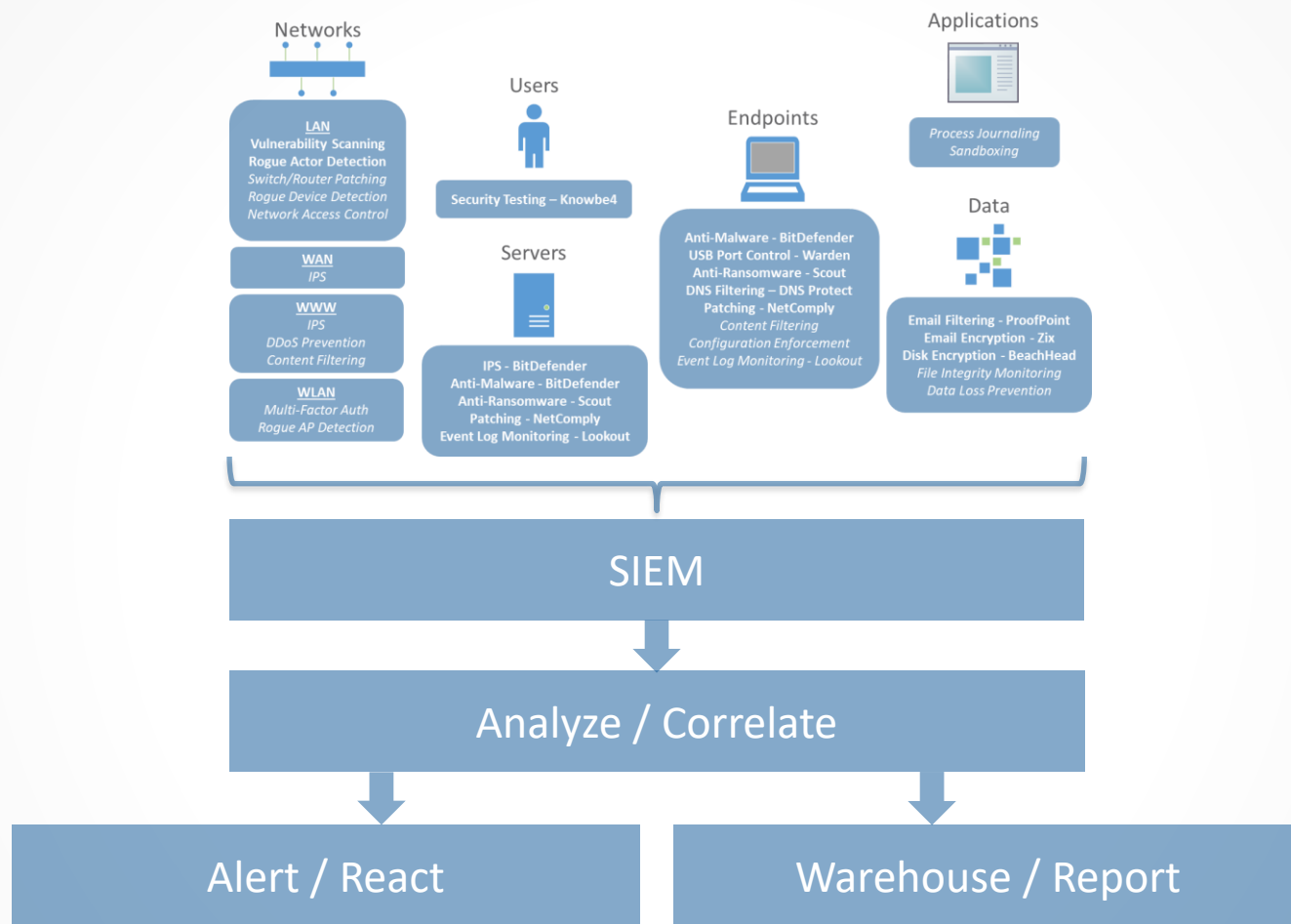


Process Journaling
Sandboxing

Data



Email Filtering
Email Encryption
Disk Encryption
File Integrity Monitoring
Data Loss Prevention



How it all comes together: 3 Prevention Stories

Vector: Email
Goal: Credential Theft

Vector: Web

Payload: Ransomware

Vector: USB
Goal: Data Theft

Evolving Security Philosophy

Investment Mentality

October 2016: Attack on Dyn

Attack Name: Mirai

Attack Type: DDoS



DNS

IP



9.83

 Safe Systems™



4 Security Truths

Attack is easier than defense

- Complexity is the worst enemy of security
- Attackers have the advantage

There are new vulnerabilities in the interconnections

- We keep finding new vulnerabilities as we continue connecting everything to everything else

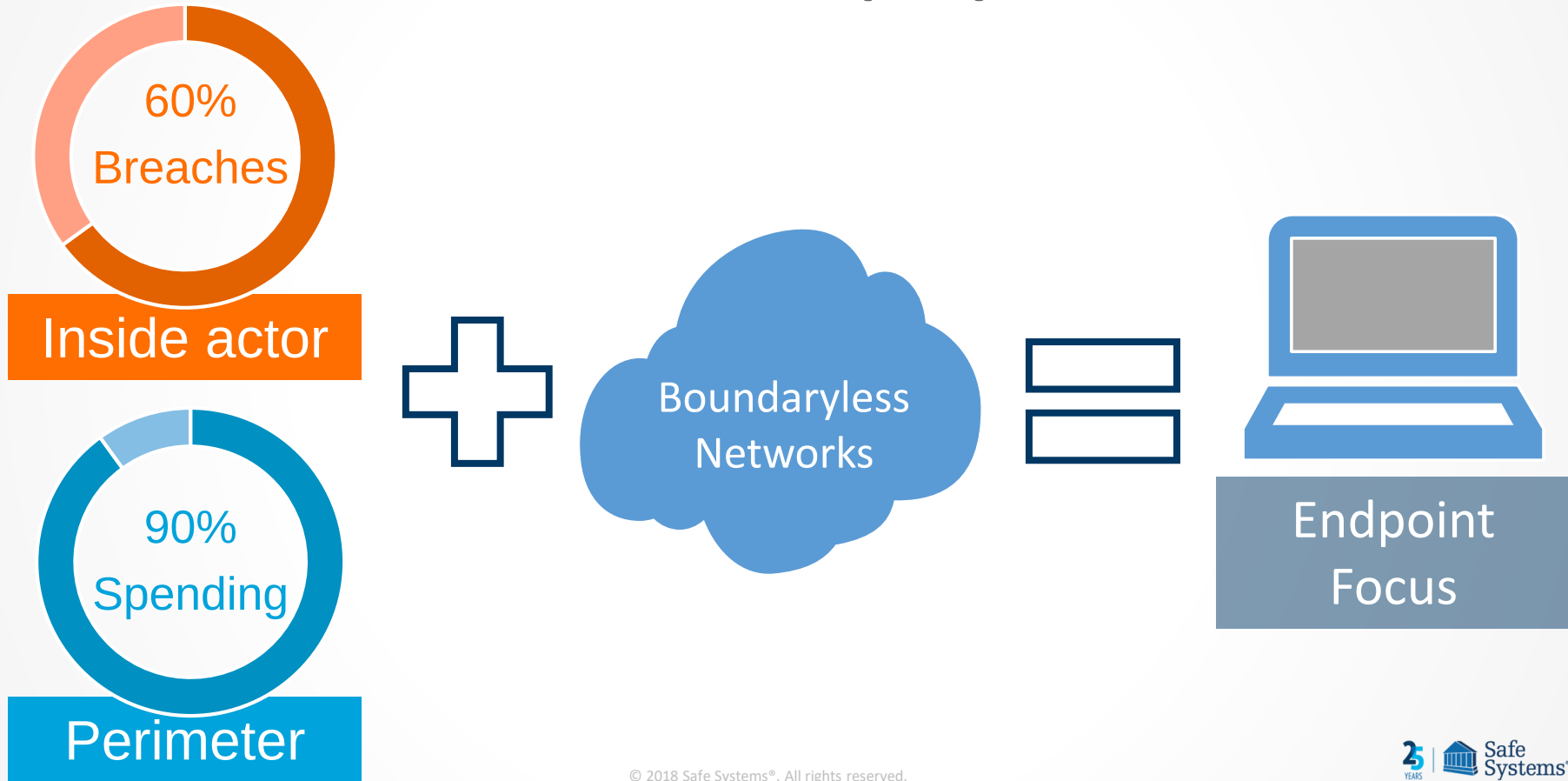
The Internet empowers attackers

- It is the most powerful efficiency enabler
- Attacks can scale

The economics don't trickle down

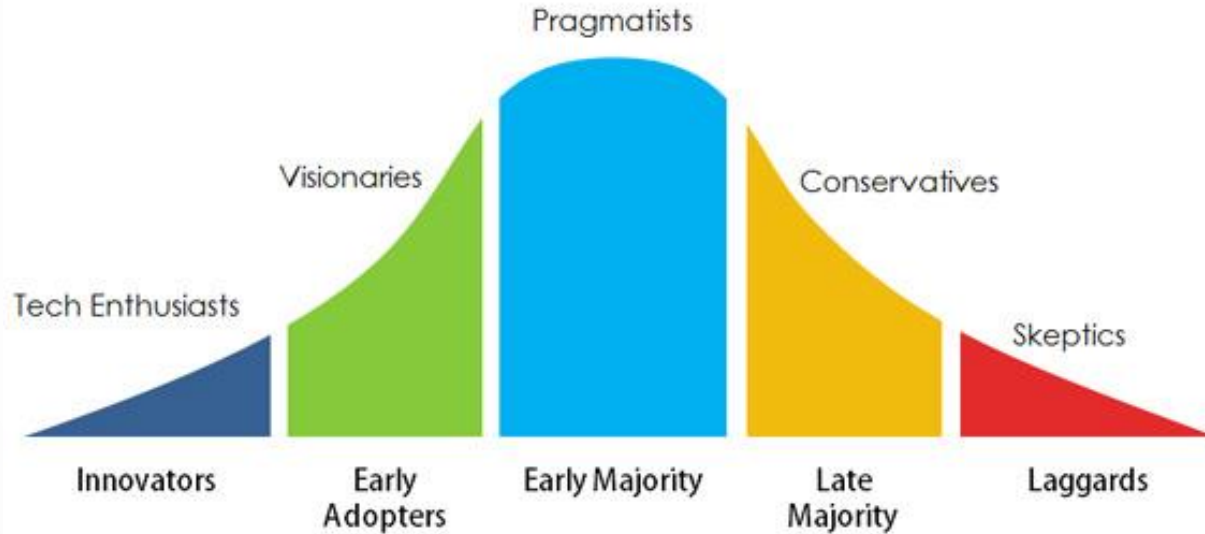
- Microsoft/Google/Apple work hard at security
- Vendors of DVR's/IP cameras/printers/consumer devices do not

Philosophy

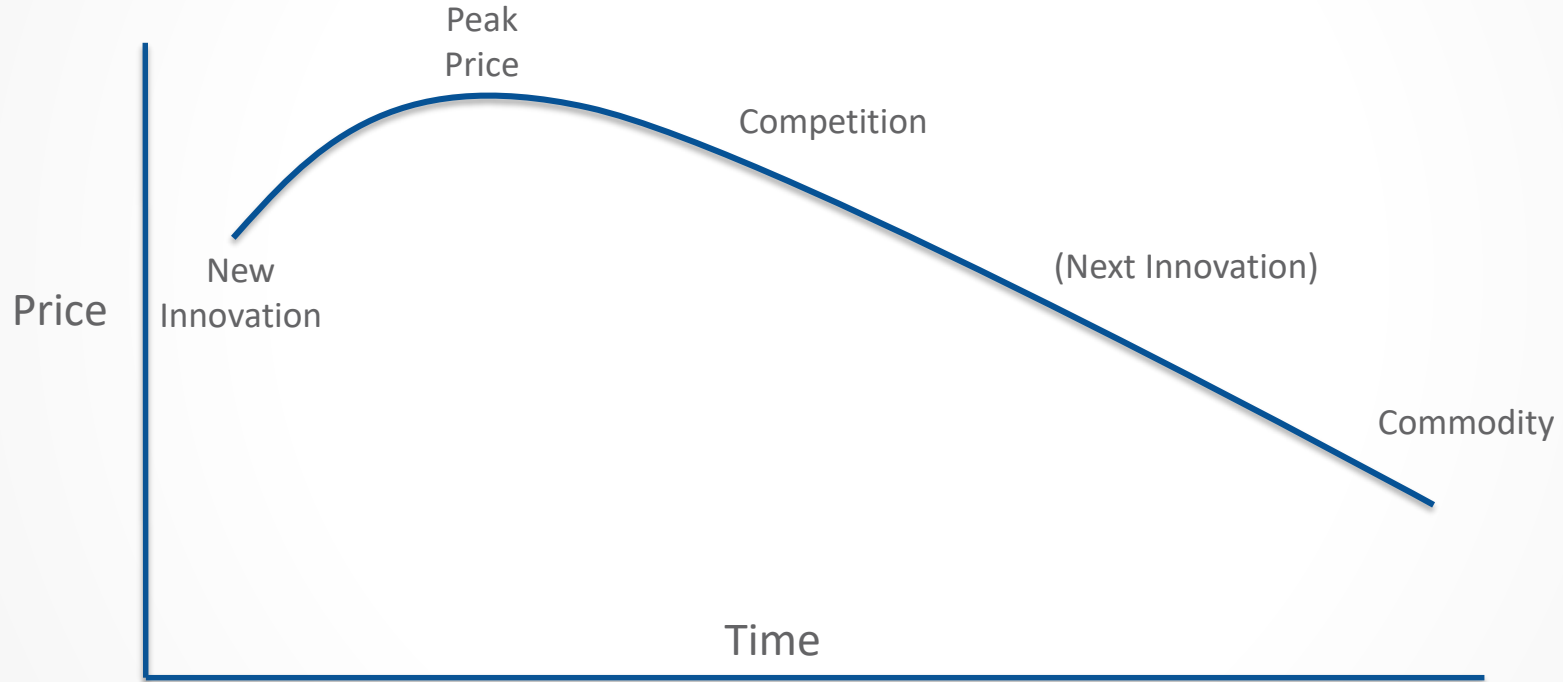




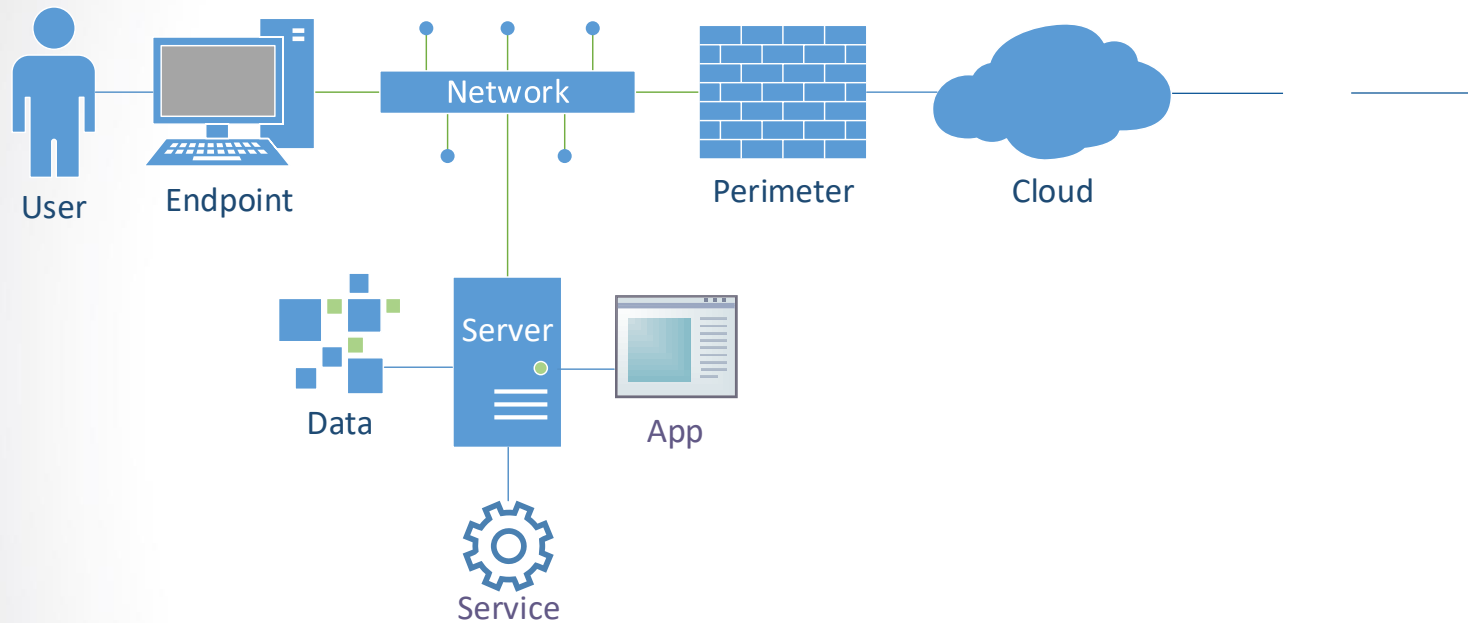
Product Adoption Curve

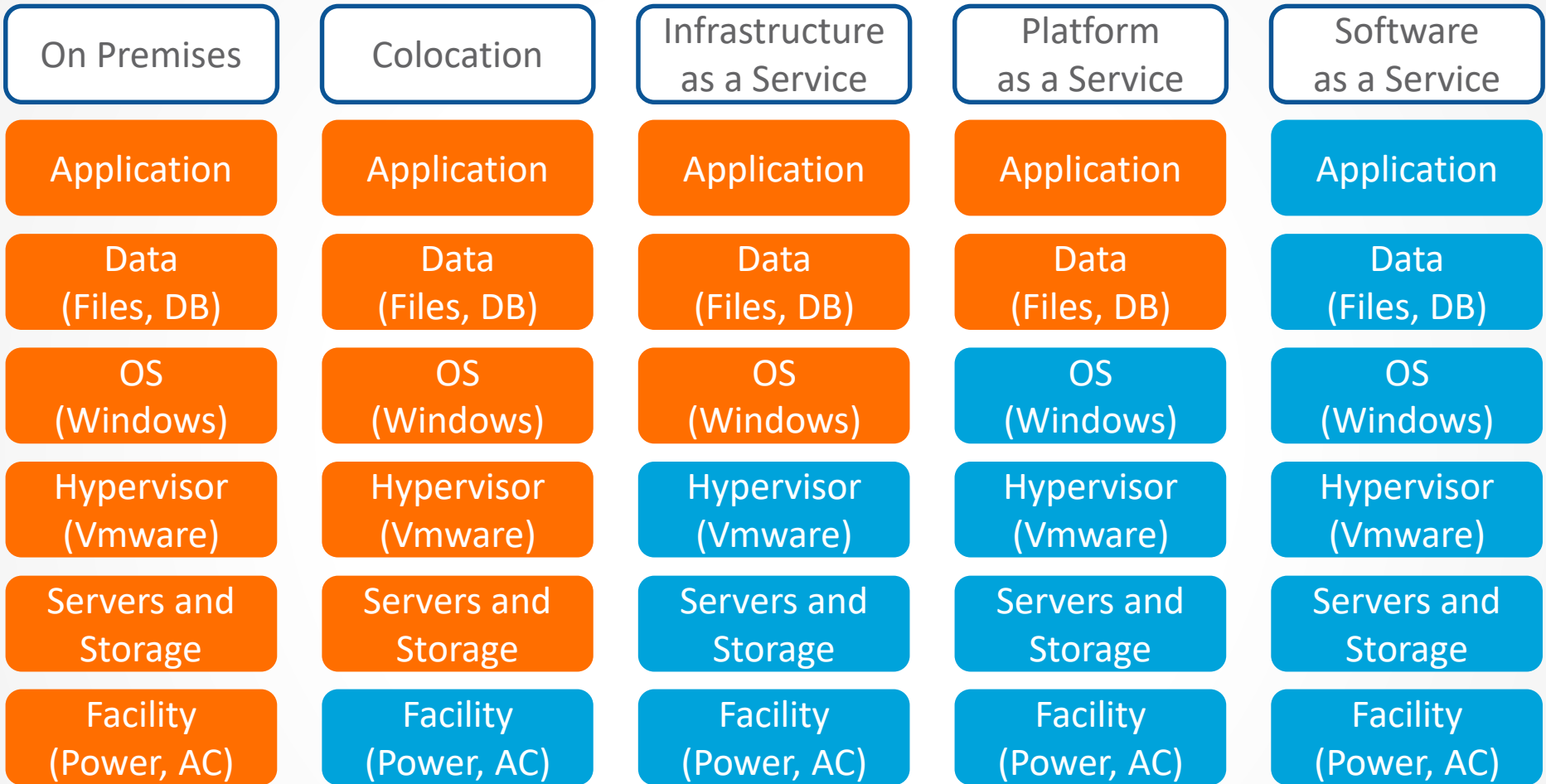


Commoditization



Cloud shift



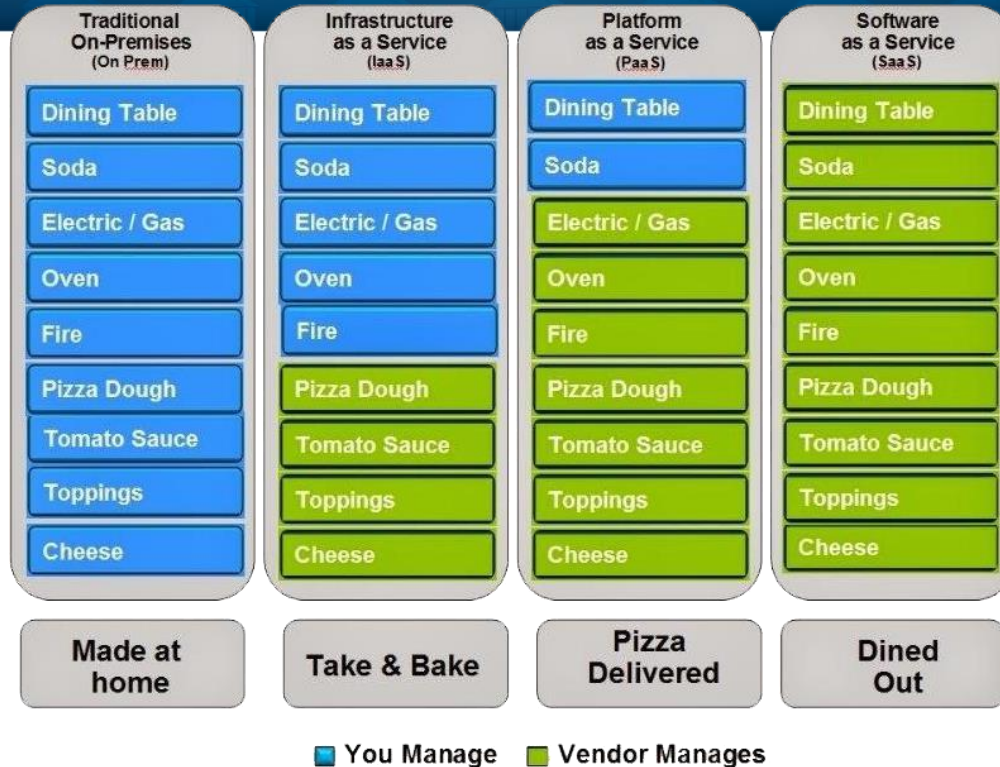


Managed by:

You

Vendor

Pizza as a Service



4 Cloud Truths

Cloud does not have a lower price tag

- The value is in the strategic agility

Spending moves to OPEX

- Cloud services are subscriptions

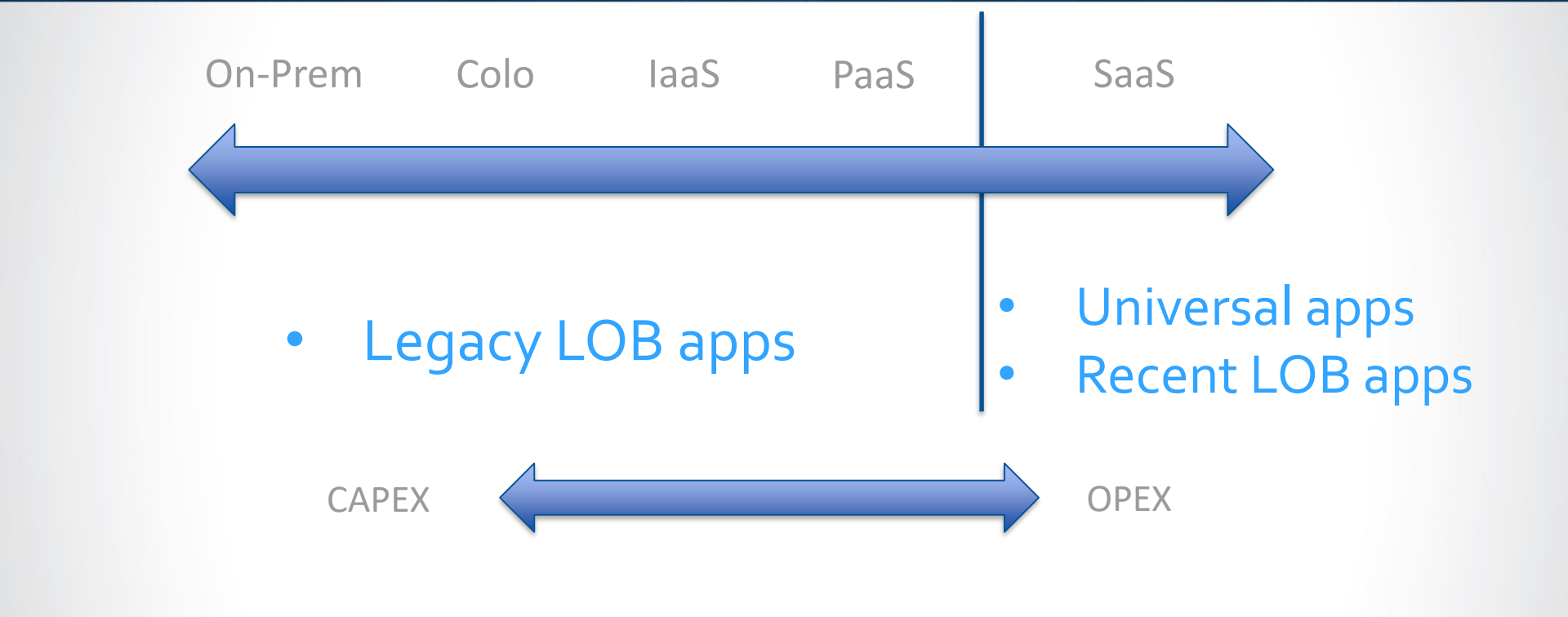
There is no path you are supposed to follow

- Ignore the hype

Cloud choices follow strategic decisions

- Corporate strategy first, then IT strategy

Cloud Destinations



How to win?



Partnership between CFO and ~CTO

25
YEARS



Safe
Systems®