



Cisco Security

Fran Pena

CyberSecurity Sales Specialist, CISSP, CCNP

frpena@cisco.com

Agenda

Problemas Seguridad
Cisco Cloud Security
Demos

Digitalización - Problemas Seguridad



TRANSFORMACION DIGITAL NUEVOS MODELOS DE NEGOCIO

*+Superficie Ataque
Movilidad, Nube, Perímetro
desaparece , 50B dispositivos
2020, IoT, BYOD, Visibilidad*



ENTORNO DE AMENAZAS DINÁMICO

*Nuevos vectores
Nuevos atacantes, Ransomware
IOT, Sofisticados I+D, IOT*



COMPLEJIDAD Y FRAGMENTACIÓN

*TTD+100 días, Falta personal
Muchos fabricantes
No integración/Automatización*



GDPR – Reglamento General de Protección de Datos

- **Organizations** which collect and **manage personal information**, purpose, where stored, who access.
- Must able to **Protect** it and **demonstrate** technical and organizational measures to ensure a level of security appropriate to the risk. (Processes and Technology).
- Obligation to **notify a breach 72h**. (Ways to detect a breach)
- is **NOT an option**. It becomes mandatory in May 2018
- Not being compliant may result in huge fines (up to 20M€ or **4% of the annual revenue**)

Un ataque informático masivo con 'ransomware' afecta a medio mundo

- En España, el virus ha llegado a grandes compañías como Telefónica, que han tenido que apagar ordenadores o desconectarlos de la red



- Most profitable malware in history
- Lucrative: Direct payment to attackers!
- Cyber-criminals collected **\$209 million in the first three months of 2016** by extorting businesses and institutions to unlock computer servers.
- At that rate, **ransomware** is on pace to be a **\$1 billion a year** crime this year.
- Let's take an example:
 - Looking only at the Angler exploit kit delivering ransomware
 - \$60 million dollars a year

► 27 Septiembre, 2017

El presidente de Equifax dimite tras el ciberataque

EFE, Madrid

La compañía de solvencia crediticia Equifax anunció ayer la salida de Richard Smith como máximo directivo de la compañía, semanas después de un pirateo informático que pudo haber expuesto datos privados de 143 millones de personas.

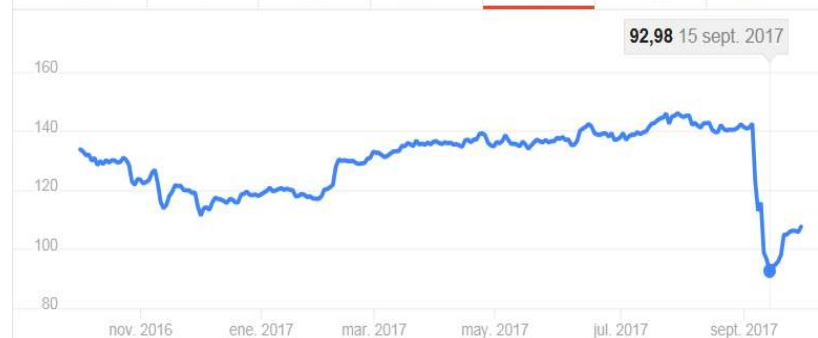
Equifax Inc.

NYSE: EFX - 2 oct. 19:29 GMT-4

107,81 USD ↑ 1,82 (1,72 %)

Tras el cierre de sesión: 107,30 +0,47 %

1 día 5 días 1 mes 3 meses 1 año 5 años máx.



SOLUCION INDUSTRIA - COMPLEJIDAD

The image displays a wide array of cybersecurity solutions organized into 15 distinct categories, each represented by a dark header bar and a collection of vendor logos. The categories and their associated vendors are as follows:

- Infrastructure Security:** Network Firewall (Cisco, Palo Alto, Fortinet, etc.), Network Monitoring (BlueCoat, XDR, etc.), Intrusion Prevention Systems (Cisco, Snort, etc.), Unified Threat Management (Cisco, Trend Micro, etc.).
- Endpoint Security:** Endpoint Protection & Anti-Virus (McAfee, Symantec, etc.), Endpoint Detection & Response (CrowdStrike, SentinelOne, etc.), Messaging Security (Microsoft, Cisco, etc.).
- Application Security:** WAF & Application Security (Akamai, Cloudflare, etc.), Vulnerability Assessment (Qualys, Rapid7, etc.), Web Security (Sophos, Trend Micro, etc.).
- IoT Security:** Solutions like MOCANA, Argus, and others.
- Security Operations & Incident Response:** SIEM (Splunk, IBM, etc.), Security Incident Response (Hexadite, etc.).
- Threat Intelligence:** Solutions like BrightPoint, ThreatMetrix, etc.
- Mobile Security:** Solutions like Lookout, Wandera, etc.
- Data Security:** Solutions like IBM, Veeva, etc.
- Transaction Security:** Solutions like Feedzai, Sift Science, etc.
- Risk & Compliance:** Solutions like RedSeal, IBM, etc.
- Specialized Threat Analysis & Protection:** Solutions like FortiScale, Invincea, etc.
- Identity & Access Management:** Solutions like Okta, PingIdentity, etc.
- Cloud Security:** Solutions like Palo Alto, CloudMatters, etc.

Source: Momentum Partners.

SOLUCION INDUSTRIA - COMPLEJIDAD



Gartner Advice

“By 2018, more than 50% of the cost of implementing systems will be spent on integration”

Peter Sondergaard
Senior VP and Global Head of Research
Gartner



The Most Complete Security Portfolio in Industry



Integrated Threat Defense

TALOS - Threat Intelligence



Network



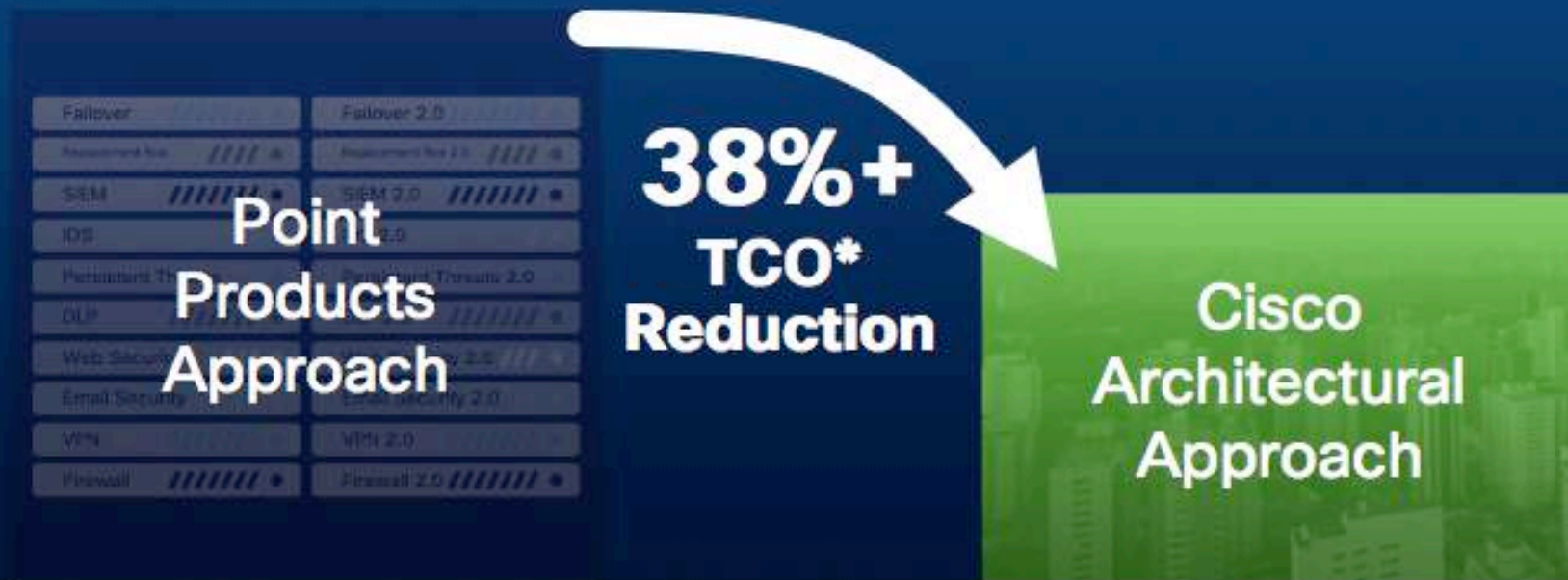
Endpoint



Cloud

Services

An integrated threat defense also saves money

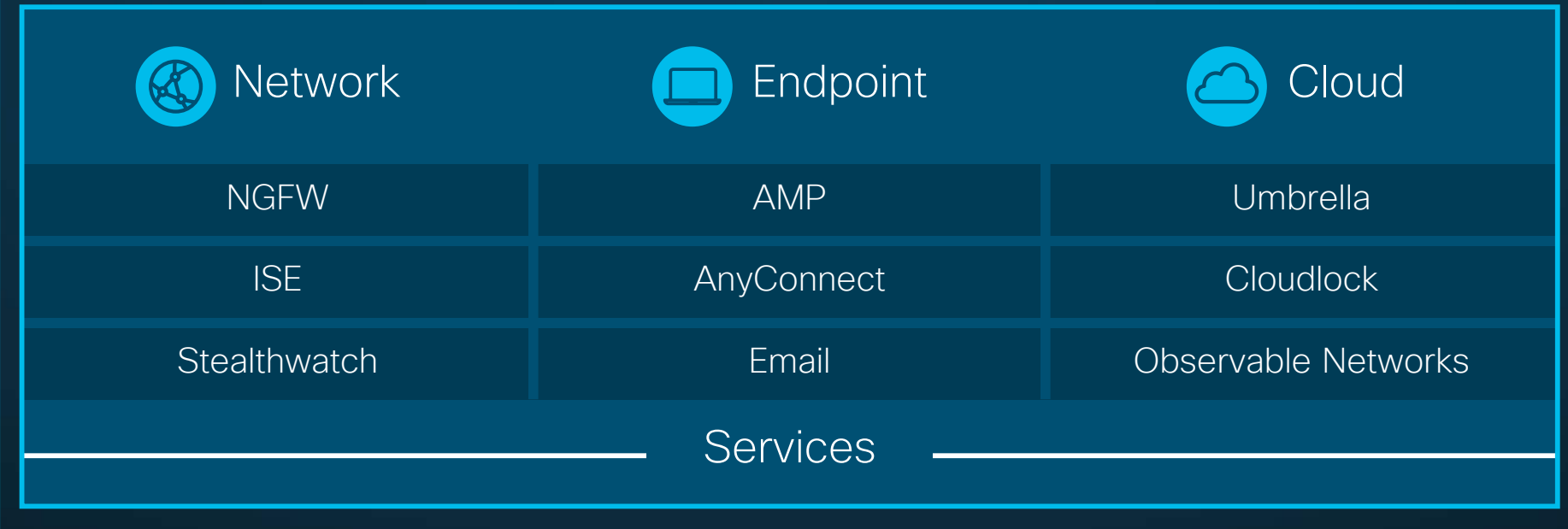


* Final Results

FORRESTER

Cisco Security Architecture – Security that works together

Threat intelligence – TALOS



The Most Complete Security Portfolio in Industry

ANTES

Política y Control

Control
Cumplimiento
Endurecimiento

DURANTE

Identificación y Bloqueo

Detección
Bloqueo
Defensa

DESPUÉS

Análisis y Remediación

Alcance
Contención
Remediación

Visibilidad Local

Cisco **PMGRID**



NGFW - Cisco Firepower



NGIPS - Cisco Firepower



APT - Cisco AMP



NAC - Cisco ISE



Web - Cisco WSA



CASB - Cisco CloudLock



Email - Cisco ESA/CES



Analítica - Cisco CTA

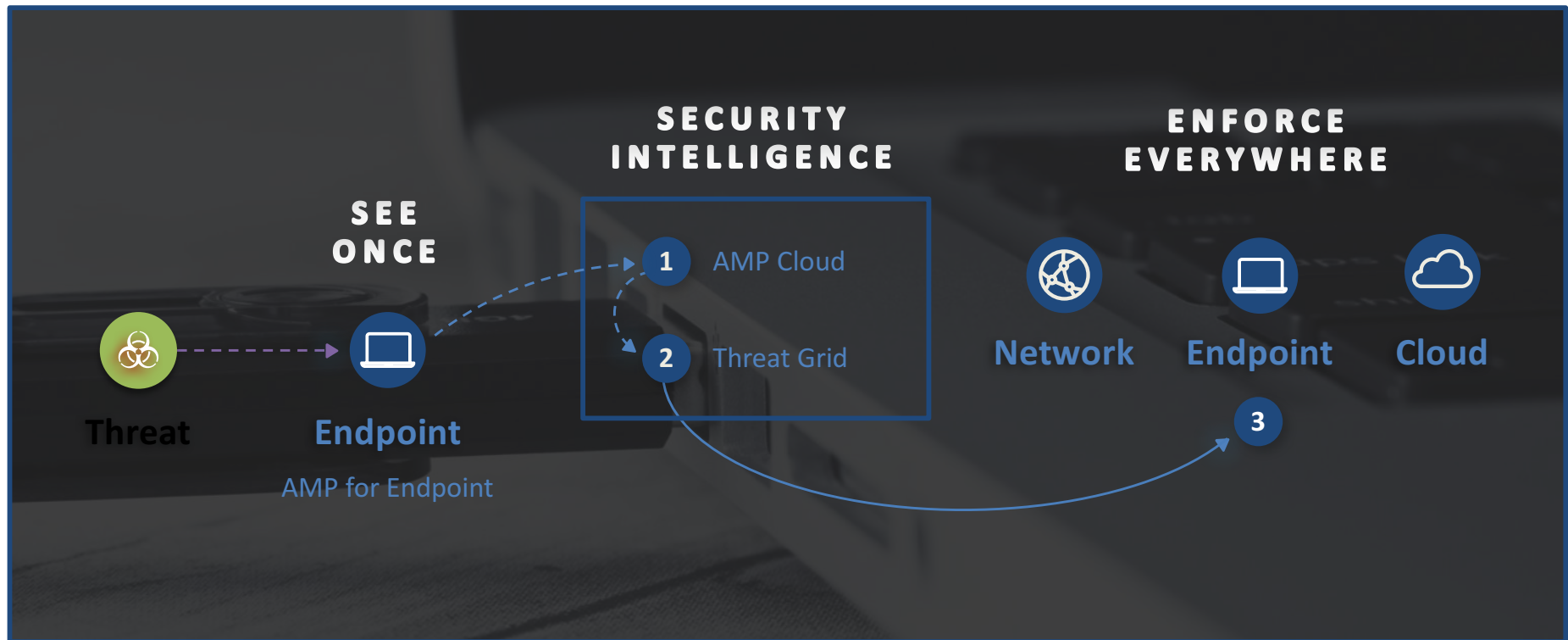


La Red - Cisco StealthWatch NBA y Cisco Umbrella SIG

Visibilidad Global

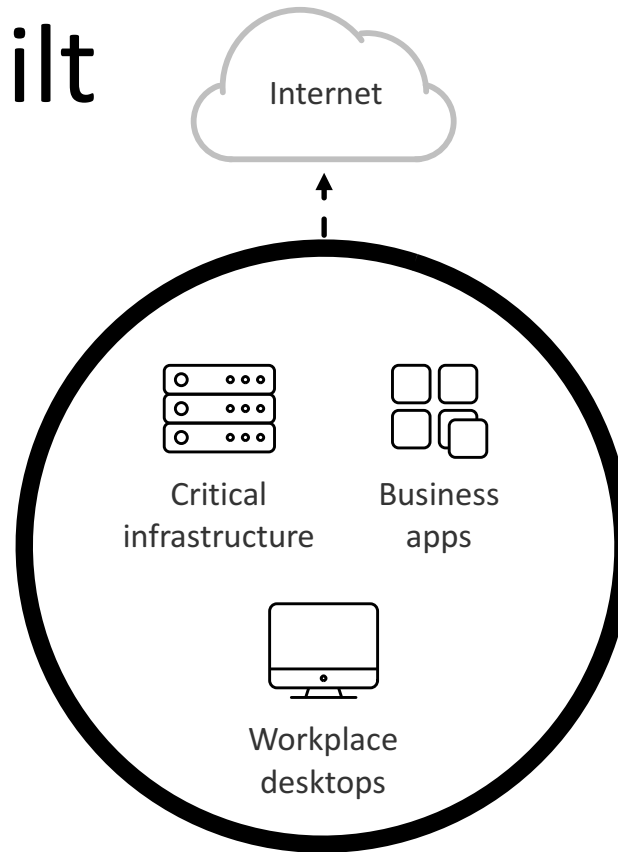
Cisco **TALOS**

The Architectural Advantage in Action

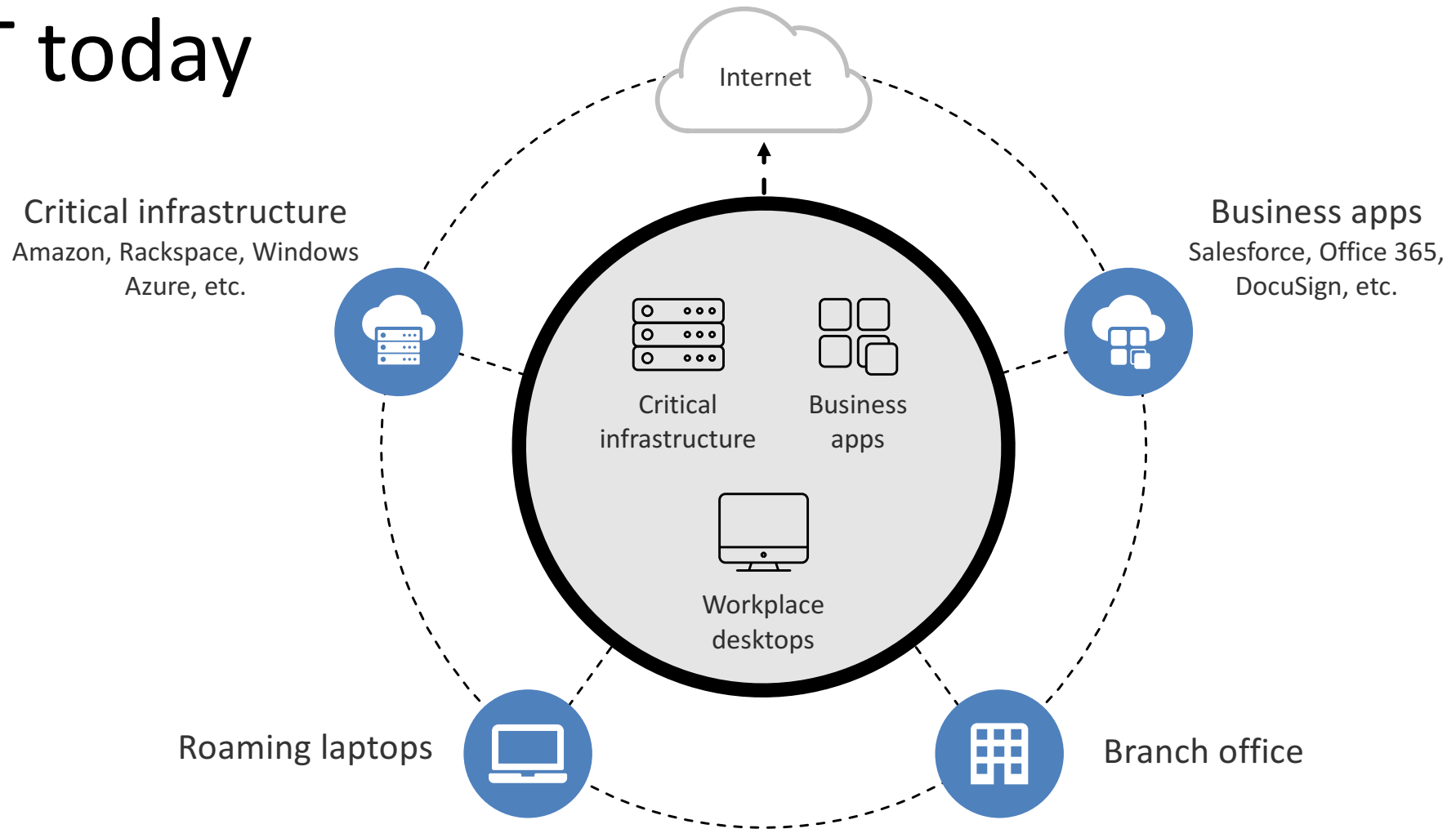


Primera linea Defensa Umbrella

How IT was built



IT today



By 2018, Gartner estimates:

25% of corporate
data traffic will bypass
perimeter security.

Umbrella



Malware and
ransomware



Gaps in visibility
and coverage



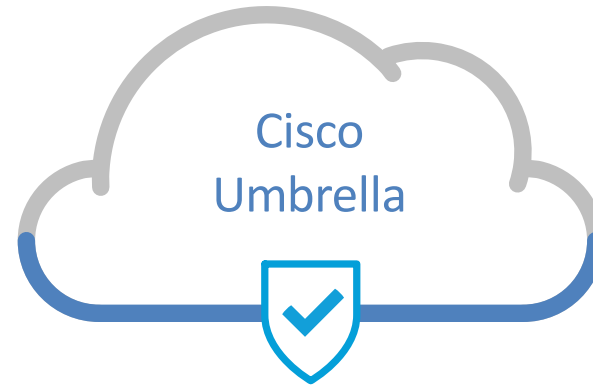
Cloud apps
and shadow IT



Difficult to
manage security

Easiest security product you'll ever deploy

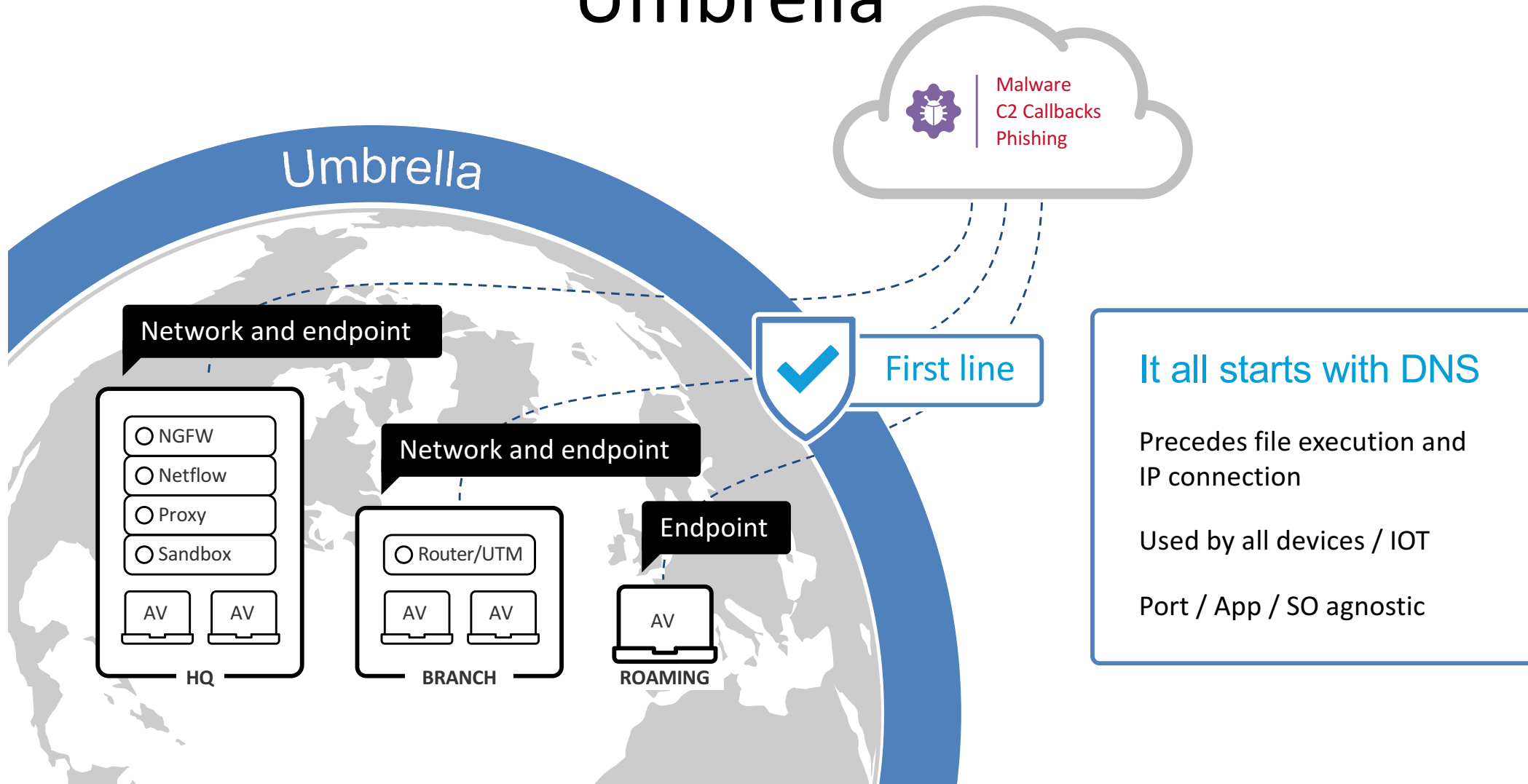
- 1 Signup
- 2 Point your DNS
- 3 Done



208.67.222.222



Umbrella



It all starts with DNS

Precedes file execution and IP connection

Used by all devices / IOT

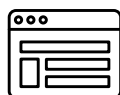
Port / App / SO agnostic

ENFORCEMENT

Built into foundation of the internet

Destinations

Original destination or block page



Safe
Original destinations



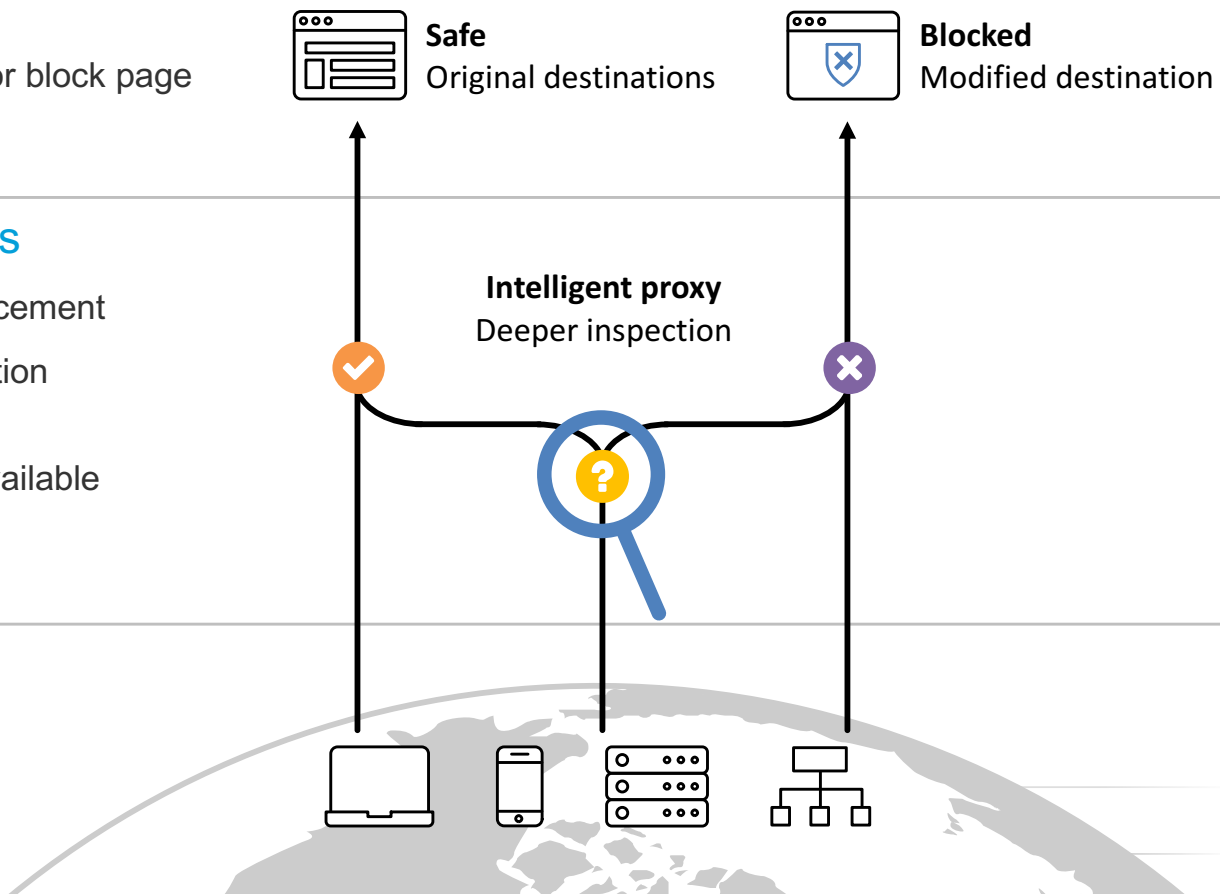
Blocked
Modified destination

Security controls

- DNS and IP enforcement
- Risky URL inspection through proxy
- SSL decryption available

Internet traffic

On and off-network

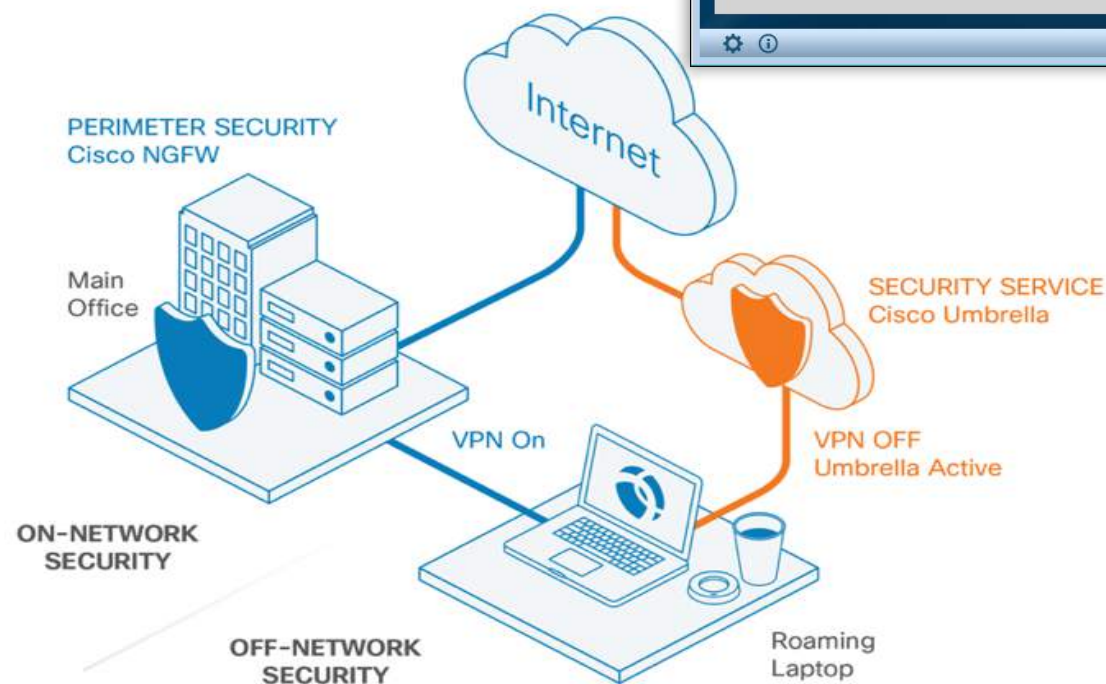


Simplificación OpenDNS

AnyConnect + Umbrella

Key Features

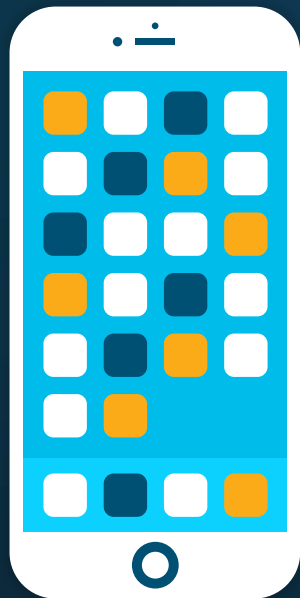
- Malware, botnets, phishing
- Protection when VPN is off or split-tunnel is configured
- Set a single security policy for all roaming laptops
- Customize 1 block page
- Basic reporting available by hostname





Cisco Security Connector

The first ever security application for iOS



Cisco Umbrella



Advanced Malware Protection (AMP)

Resumen Umbrella



BENEFITS

Simple to point
DNS

No hardware to
install No
software to
maintain

Provision globally
in **under 30**
minutes

PROTECTION

Threat Prevention

Protects on & off
Network

Always Up to
Date, not need
VPN

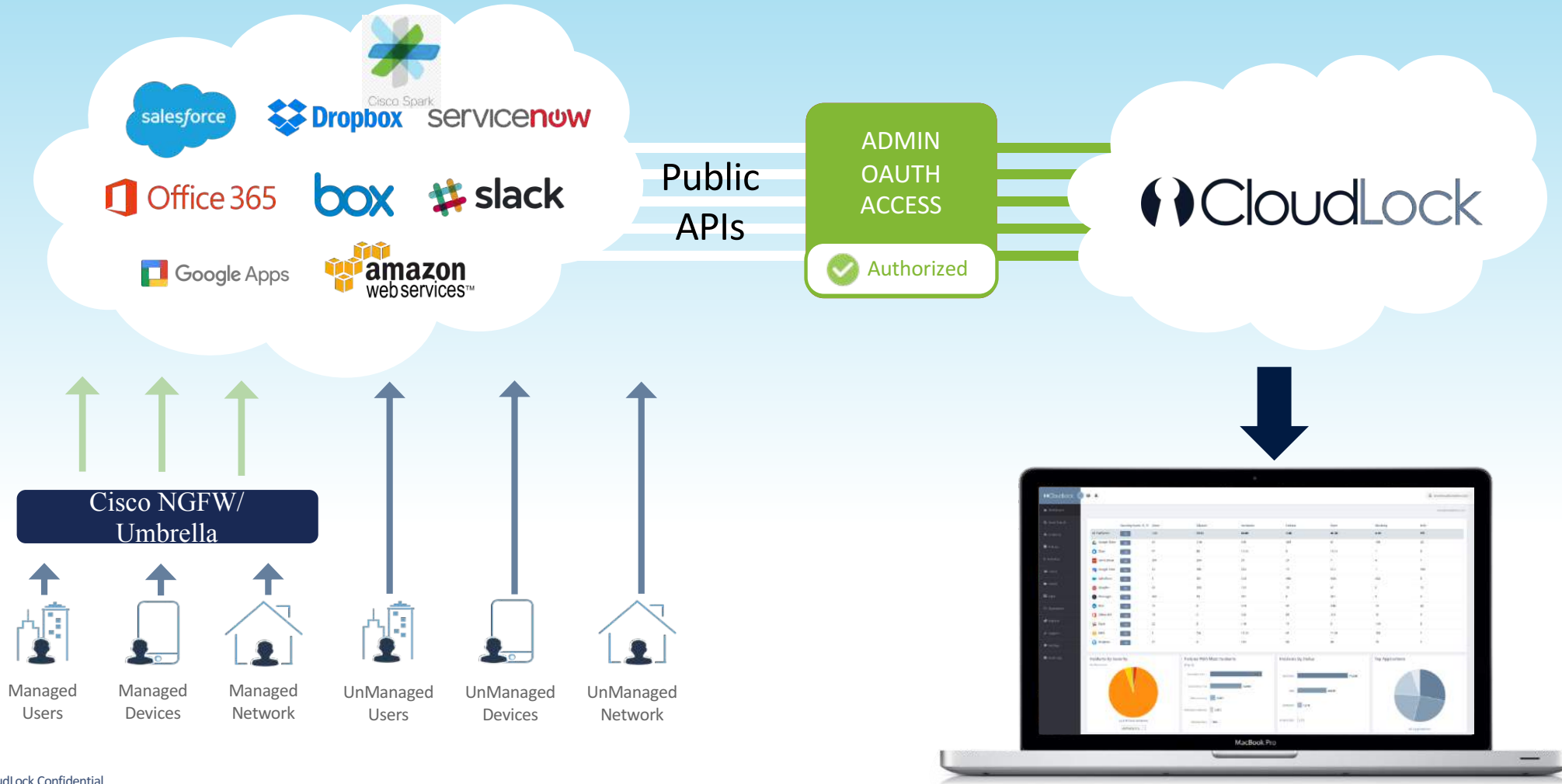
Block domains,
IPS & URLs all
Ports (not only
80/443)



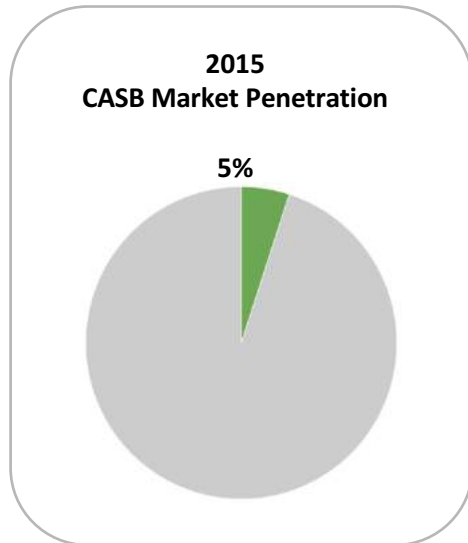
Demo Umbrella

By 2020, 92% of global
data center traffic will come
from the cloud.

CASB - API Access (Cloud to Cloud)



Market Opportunity

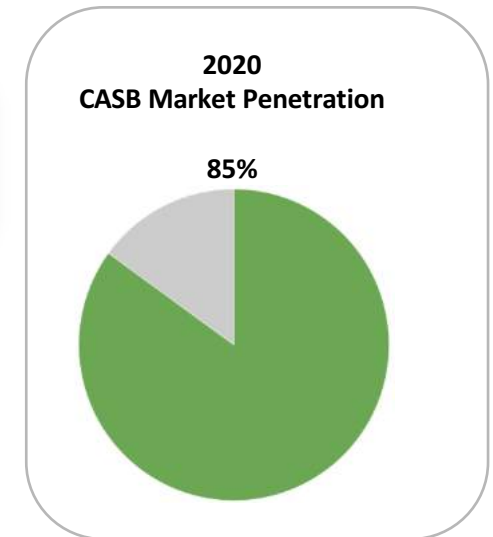


#1

**Technology for Information Security in
2016**

CASB
Cloud Access Security

Broker
Source: Gartner, 2016

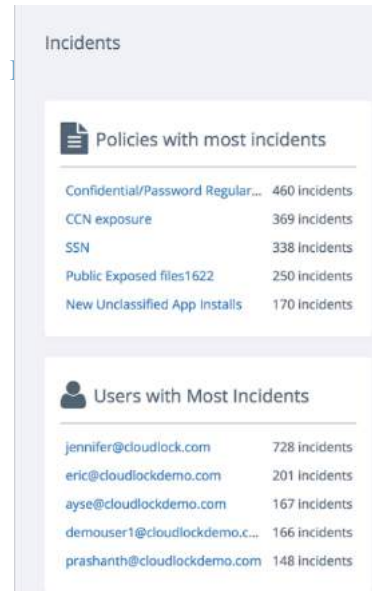
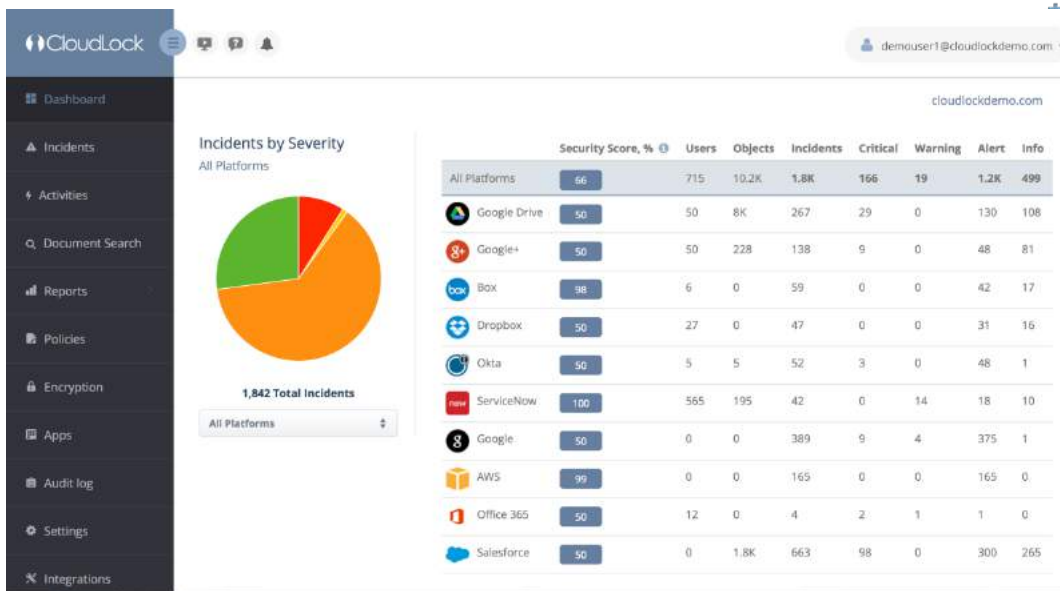


Cloud Shared Responsibility - SaaS/PaaS/IaaS

	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	SaaS
	People	People	People
	Data	Data	Data
	Applications	Applications	Applications
	Runtime	Runtime	Runtime
	Middleware	Middleware	Middleware
	Operating System	Operating System	Operating System
	Virtual Network	Virtual Network	Virtual Network
	Hypervisor	Hypervisor	Hypervisor
	Servers	Servers	Servers
	Storage	Storage	Storage
	Physical Network	Physical Network	Physical Network
	CSR Responsibility	Customer Responsibility	Customer Responsibility

*Gartner Research Paper: Mind the SaaS Security Gaps Published: 19 May 2016

CASB - Key Cloud Security Questions



Who does what?

Where is my sensitive data?

What Shadow Apps are my users using?

PaaS and IaaS




SaaS

IDaaS



Casos de uso criticos en nubes públicas




Discover and Control:

-  Compromised Accounts
-  Insider Threats
-  User and Entity Behavior Analytics

Discover and Control:

-  Unintended Exposures & Leakages
-  Privacy Compliance Violations
-  Cloud Data Loss Prevention (DLP)

Discover and Control:

-  Cloud Malware
-  Shadow IT/OAuth Discovery & Control
-  Apps Firewall

NEWS

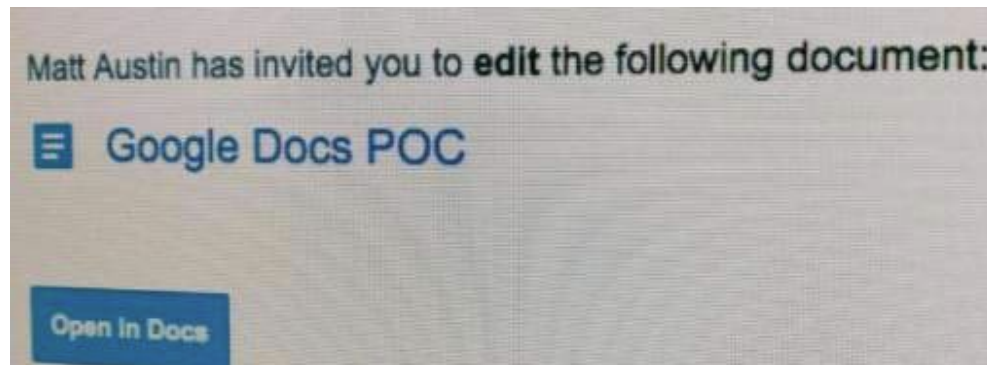
Google Docs phishing attack underscores OAuth security risks

One security researcher easily managed to replicate Wednesday's phishing attack.



By [Michael Kan](#)

U.S. Correspondent, [IDG News Service](#) | MAY 5, 2017 4:30 AM PT



Google Docs would like to:

- Read, send, delete, and manage your email
- Manage your contacts

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other [Account Permissions](#) at any time.

Over 700 organizations in all segments use Cisco Cloudlock



Demo

Cisco Cloudlock