

# Como trabajar desde la casa en forma segura en tiempos de COVID 19

## Practicas para empleados y para empresas

Fernando Patrito



covid19vodka.net	id-covid19.com	
covid-19weed.net	covid19.credit	
covid19weed.net	coronavirus.degre	
covid-19weed.net	coronavirus.degre	
covid19weed.net	thecoronavirus	
covid19qanda.net	coronavirus.s	
spokanecoronavirus.net	covid19.gifts	
coronaviruscura.online	covid-19loa	
coronaviruscura.online	covid19.inva	
aggiornamenticoronavirus.online	californiac	
covid19esp.online	coronavirusc	
sars-coronavirus.org	coronavirusil	
sars-coronavirus.org	covid19californ	
coronavirusargentina.org	newyorkcoronavir	
coronavirusbrazil.org	newyorkcovid19.law	
coronaviruscolombia.org	covid19michigan.lawyer	
coronavirusecuador.org	covid19live.life	
coronavirusgermany.org	curecoronavirus.life	covid-19.recipes
coronavirusguatemala.org	winovercoronavirus.life	covid-19.services
coronavirusiran.org	trackcovid19.live	fightcovid19.shop
coronavirusjapan.org	covid19ifo.live	nocovid19.shop
coronavirusnetherlands.org	covid19state.live	antivirus-covid19.site
coronavirusparaguay.org	sbacoronavirus.loan	antivirus-covid19.site
coronavirusperu.org	covid19sba.loans	chinacovid-19.site
coronavirusportugal.org	covid19.management	coronavirusnewsindia.site
coronavirusunitedstates.org	coronavirusofficecleaning.net	masques-coronavirus.store
coronavirusworldmap.org	covid-19cleaning.net	covid-19.support
covid19-world.org	covid19-cleaning.net	coronavirus-business.support
ctuwcovid19responsefund.org	covid19officecleaning.net	coronavirusinpakistan.today
www.coronavirus.org	survivethecoronavirus.net	coronavirusinpakistan.today
covid19surpport.org	covid-19weed.net	whereiscoronavirus.today
coronavirusargentina.org	covid19weed.net	whereiscoronavirus.today
coronavirusbrazil.org	covid19surpportgroup.net	coronavirus-treatment.today
coronaviruscolombia.org	covid19-vaccine.net	whatcoronavirusdid.today
coronavirusecuador.org	covid19surpport.net	covid19layoff.today
coronavirusgermany.org	thecoronavirusupdate.net	coronavirus-update.today
coronavirusguatemala.org	coronavirusv19.net	coronavirus19lawfor.trade
coronavirusiran.org	coronavirusv19.net	coronavirus-n95-mask.website
coronavirusjapan.org	coronavirusofficecleaning.net	coronavirus-covid19.world
coronavirusnetherlands.org	covid-19cleaning.net	coronavirus-covid19.world
coronavirusparaguay.org	covid19-cleaning.net	covid19virus.world
coronavirusperu.org	covid19officecleaning.net	2020coronavirus.world
coronavirusportugal.org	survivethecoronavirus.net	covid19antidote.world
coronavirusunitedstates.org	coronavid19.net	coronavirusaware.xyz
coronavirusworldmap.org	coronavirusofficecleaning.net	covid19safejob.xyz
coronavirusargentina.org	covid-19cleaning.net	coronavirus19.xyz
coronavirusbrazil.org	covid19-cleaning.net	covid19freejob.xyz
coronaviruscolombia.org	covid19officecleaning.net	viabcp-covid19.xyz
coronavirusecuador.org	survivethecoronavirus.net	anticovid19mask.xyz
coronavirusgermany.org	humancoronavirus.net	coronavirusuturkiye.xyz
coronavirusguatemala.org	covid-19vodka.net	coronavirus.zone

# Presentaciones

## McAfee Argentina

- Desarrolla productos de seguridad corporativa usados mundialmente
- 6 productos actualmente. Mas de 20 proyectos
- 280 empleados

## Objetivos de esta reunión

- Generar conciencia de los desafíos de seguridad en el contexto de trabajo remoto
- Proporcionar algunos tips y buenas practicas de seguridad

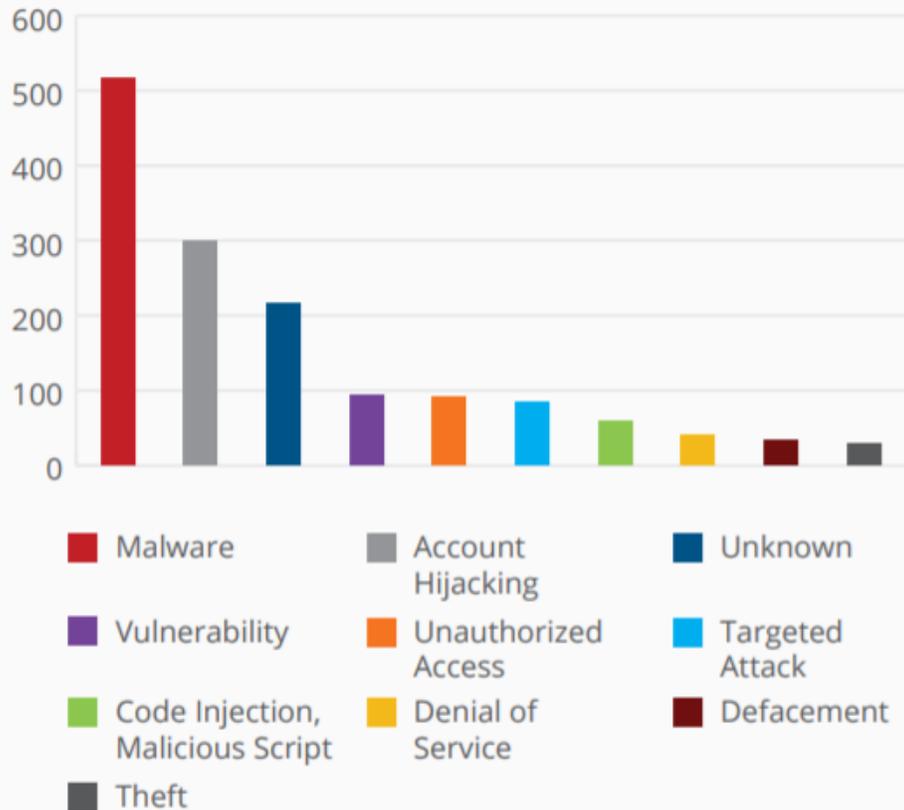


# Una nueva realidad. Oportunidad para los cambios ..pero cuidemos la seguridad



# Como nos atacan?

Top 10 Attack Vectors in 2018–2019  
(Number of reported breaches)



## Por donde entran?

- Correo Electrónico
  - Phishing y Spoofing (Covit 19)
- Conexión de USB
- Descarga de Archivos
- Paginas Web maliciosas
- Vulnerabilidades

## Malware

- Commodity que se customiza
- Ataques dirigidos
- Ransomware -> Sodinokibi REvil

Los Hackers saben que en epocas de cambios rápidos quedan huecos y aparecen oportunidades



# Como les impactaria?

- Si se les cae la red o los servidores por 3 dias?
- Si les encriptan los discos?
- Si la información privada de sus clientes o consumidores se publica para la venta?

# Parecen historias de Hollywood pero no...



Ingresa los datos de tu tarjeta de crédito, no se te cobrará ningún cargo.

Número de tarjeta



Expiración

01 **Segu.info**

2020

Código de seguridad

Continuar

## Your computer has been infected!



Your documents, photos, databases and other important files encrypted



To decrypt your files you need to buy our special software - 9781xsd4-Decryptor



You can do it right now. Follow the instructions below. But remember that you do not have much time

### 9781xsd4-Decryptor price

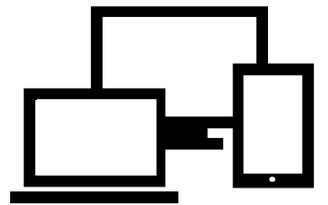
You have <b>3 days, 23:59:32</b>	Current price	0.20319454 BTC ≈ 2,500 USD
<ul style="list-style-type: none"><li>If you do not pay on time, <u>the price will be doubled</u></li><li>Time ends on Jul 12, 22:12:16</li></ul>	After time ends	0.40638908 BTC ≈ 5,000 USD

@AntiPhishing\_La

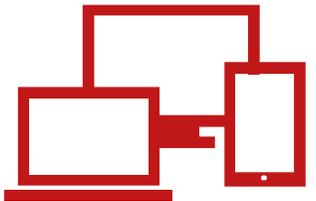
# Los desafíos para la seguridad

1 Vulnerabilidad de equipos personales y corporativos en el hogar

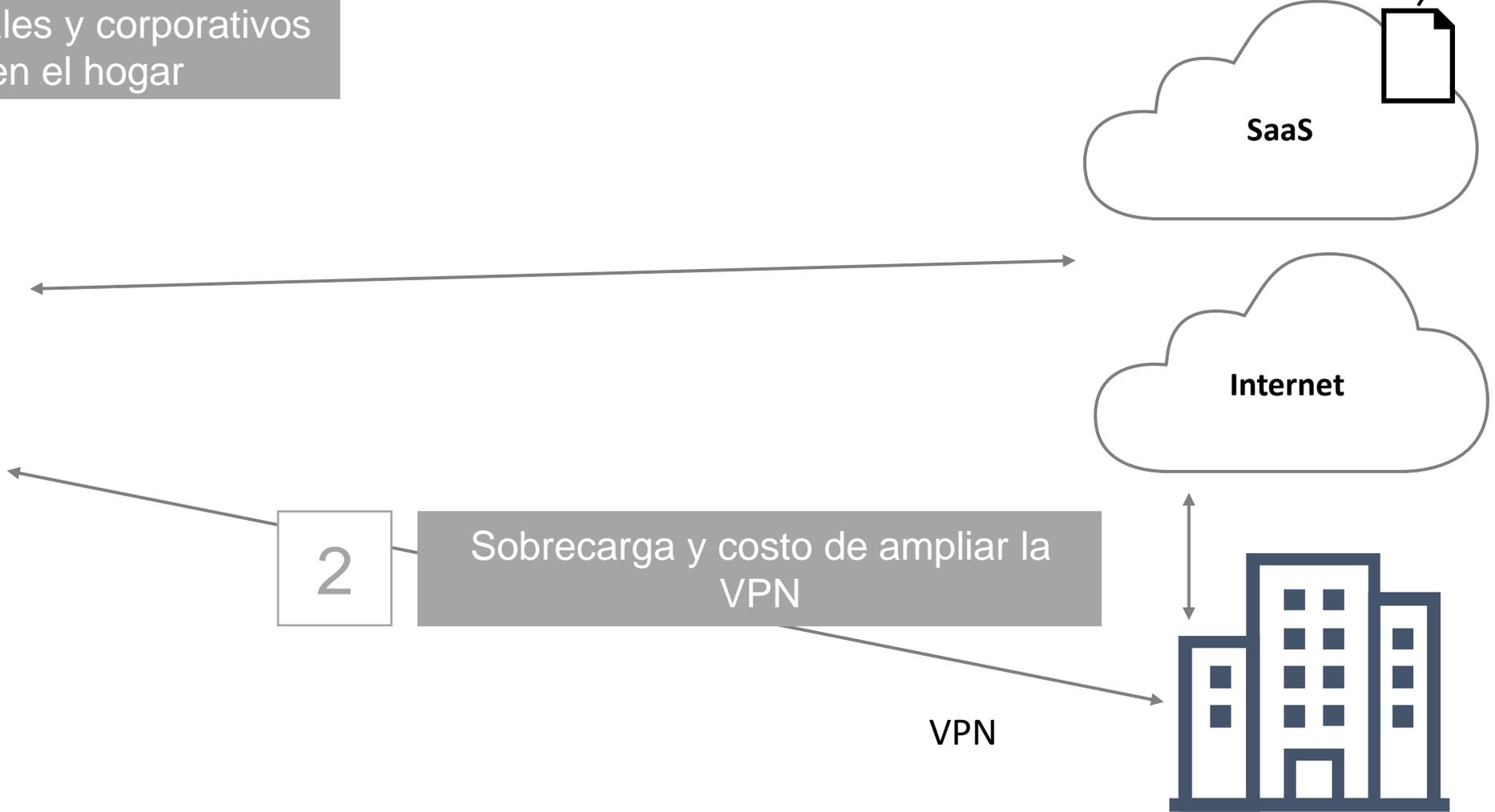
3 Filtración de datos del Cloud via Collab (Teams) y uso de SaaS fuera de la red corporativa



Personal  
No administrado



Administrados



# Recomendaciones para los usuarios y empleados

## Computadora provisto por la empresa

- Solo para uso laboral
- No modificar configuraciones
- Usar aplicaciones definidas

## Computadora Personal:

- Antivirus actualizado
- Sistema Operativo y navegadores actualizados
- Crear un usuario diferente para el trabajo

## Proteger los datos:

- Backups recurrentes - En otra maquina y otra red
- Encriptar archivos valiosos, disco duro, mails

## Redes Seguras

- No usar redes publicas
- Actualizar el router / Cambiar clave administración / WPA
- Utilizar VPN



# Recomendaciones para los usuarios y empleados

## Capacitarse y estar informado:

- Políticas de seguridad de la empresa
- Estar atento a los fraudes via email, redes sociales, etc
- Identificar y no propagar noticias falsas



# Y las organizaciones... como se preparan?

## Políticas de seguridad

- Entrenamiento / concientización
- Escritas para Homero Simpson
- Incorporar nuevos Procesos (ej colaboración, acceso, etc)
- Excepciones y evaluación de riesgos

## Identificar los sistemas críticos:

- Autenticación robustos (2FA)
- VPN para acceder

## Involucrar a todos los lideres: HR, IT, Operaciones

- Moverse rápido
- Planes de contingencia para toda la supply chain

## Información real time de ataques



# Y las organizaciones... como se preparan? ... Guia para CISOs

## Protegerse contra perdida de datos

- Encriptacion

## Sistemas de prevención de amenazas equivalente

- Antimalware con análisis de comportamiento (cloud)
- Web Security (cloud based)

## Colaboración Segura en el Cloud

- Definir herramienta (Teams, WebEx, ...)
- Aplicarle políticas de protección datos

## Acceso seguro a servicios Cloud

- Bloquear servicios riesgosos

## Plan de respuesta a Phishing

## Informacion real time de ataques



A si como buscamos aplanar la curva del COVID 19 – en el ámbito de la seguridad informática debemos mantener la “higiene” reduciendo la superficie de ataque de estos otros virus: 2FA, VPN y mucha seguridad en el endpoint.

# Recursos

---



INCIBE- Instituto Nacional CiberSeguridad de España **@INCIBE**

- Material y afiches listos para capacitación

Cordoba Hackerspace **@cbahackerspace**

- Publicaciones via twitter para practitioners

Chief Scientist McAfee Raj Samani **@Raj\_Samani**

**Fernando\_patrito@mcafee.com**

---

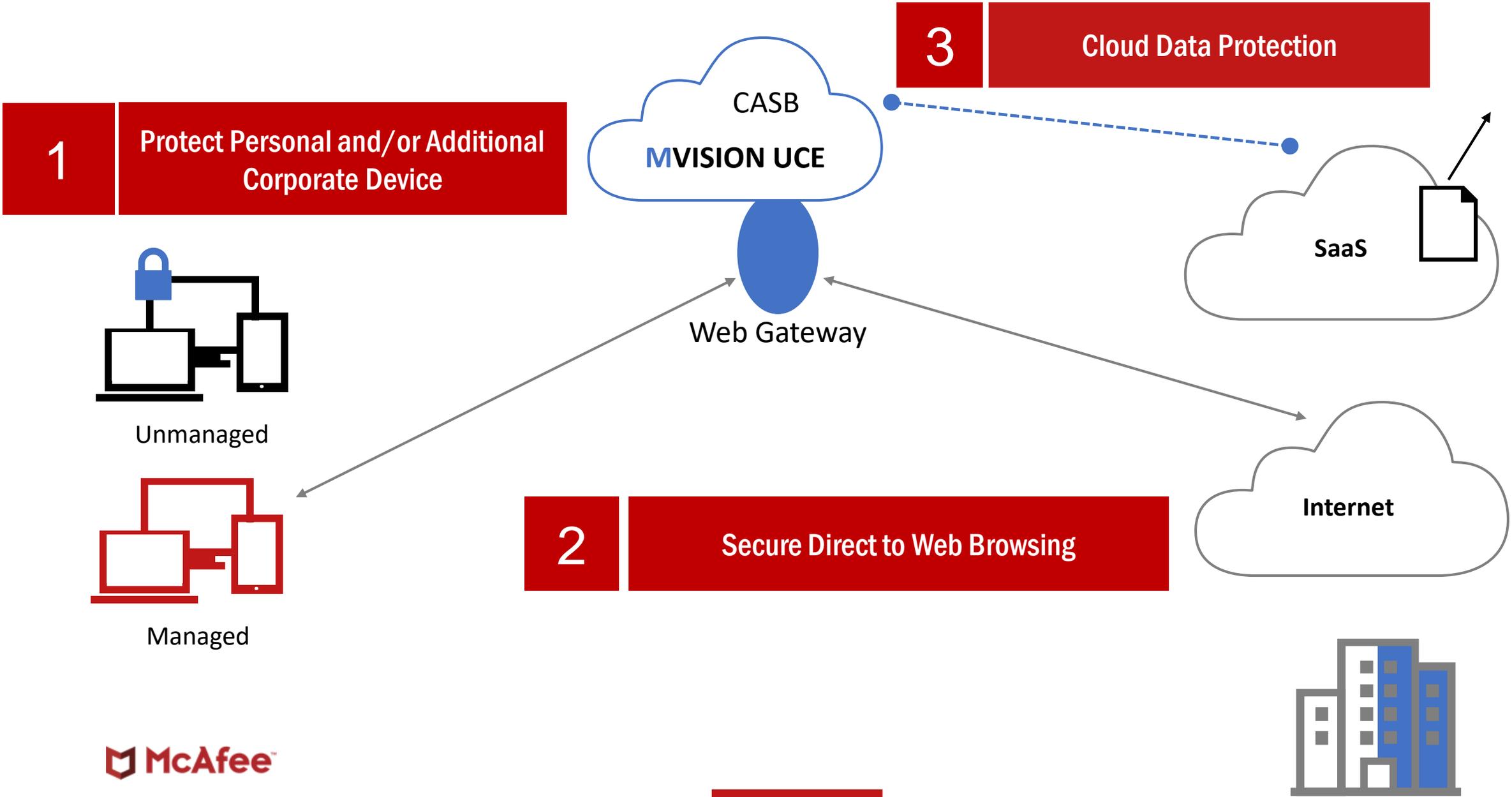
# Preguntas

# Soluciones McAfee

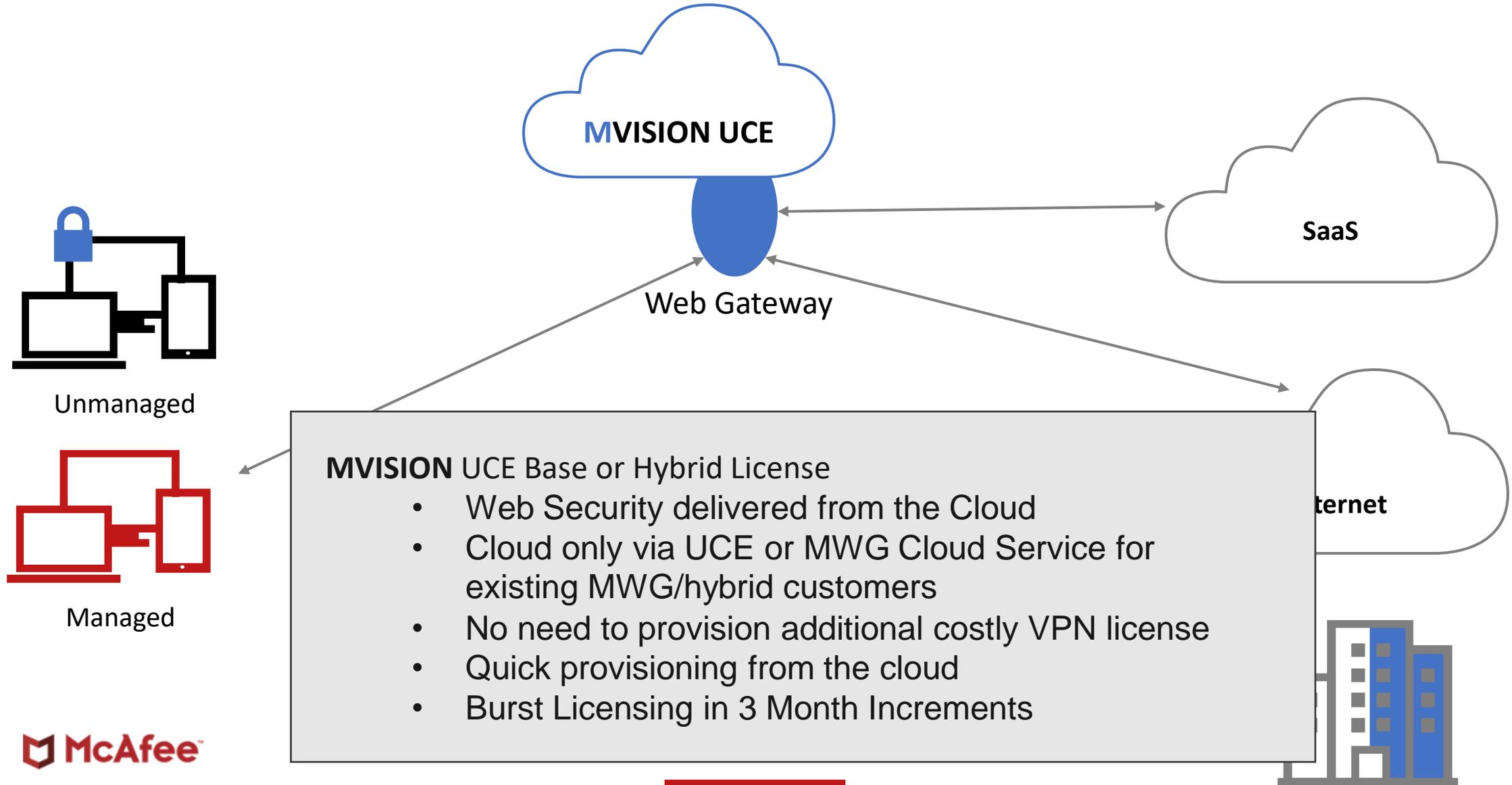
---



# The Solution



# Solution Details – MVISION UCE (Cloud SWG)



# The Solution

3

3

Cloud Data Protection

