

SonicWall de un vistazo:



28+ años de

experiencia



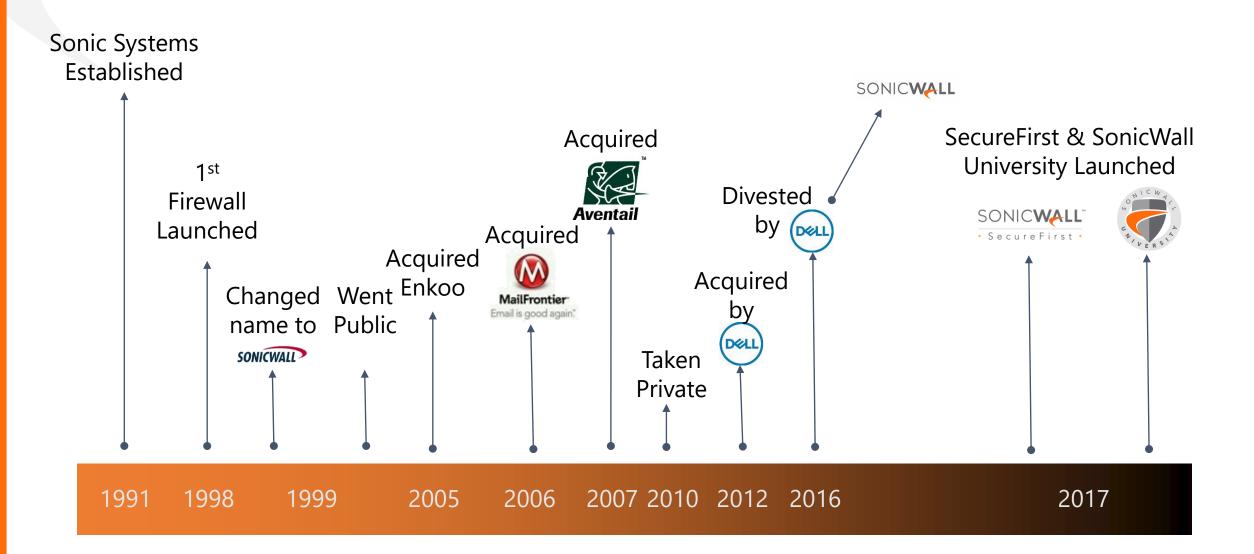




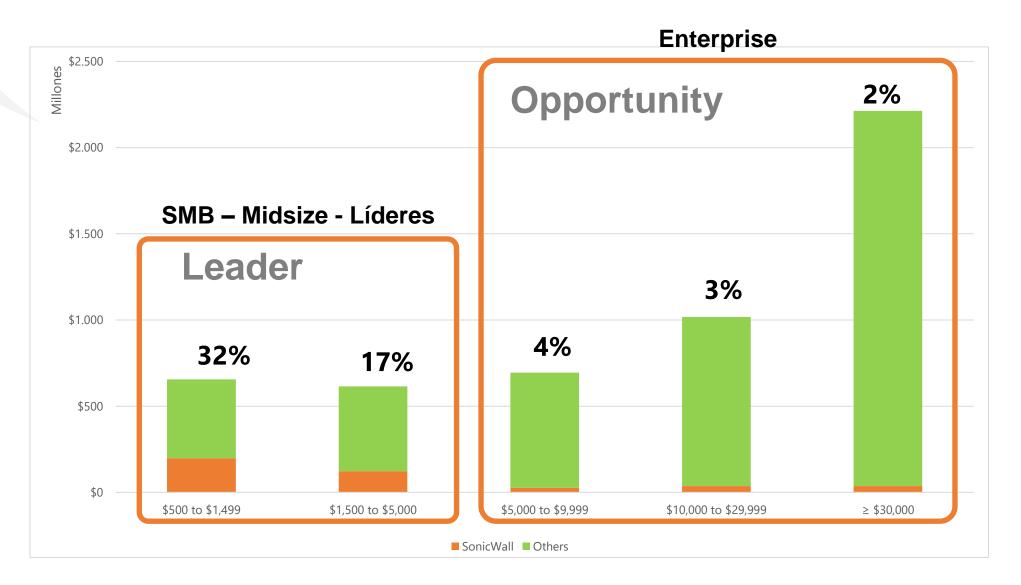




La historia de SonicWall...



SonicWall Market Share: Líder en Firewalls SMB - Midsize





^{*} Source: IHS Network Security Appliances & Software Market Tracker Q4 2017

SONICWALL CAPTURE LABS THREAT NETWORK









vulnerabilidades 0-Day





Nuestra plataforma
"SonicWall Capture
Labs" analiza los datos
recogidos por nuestra
red "Capture Threat
Network", que incluye
dispositivos en todo el
mundo.











WORLDWIDE ATTACKS - LAST 24 HOURS

https://securitycenter.sonicwall.com



Get the 2020 year full Threat Report.

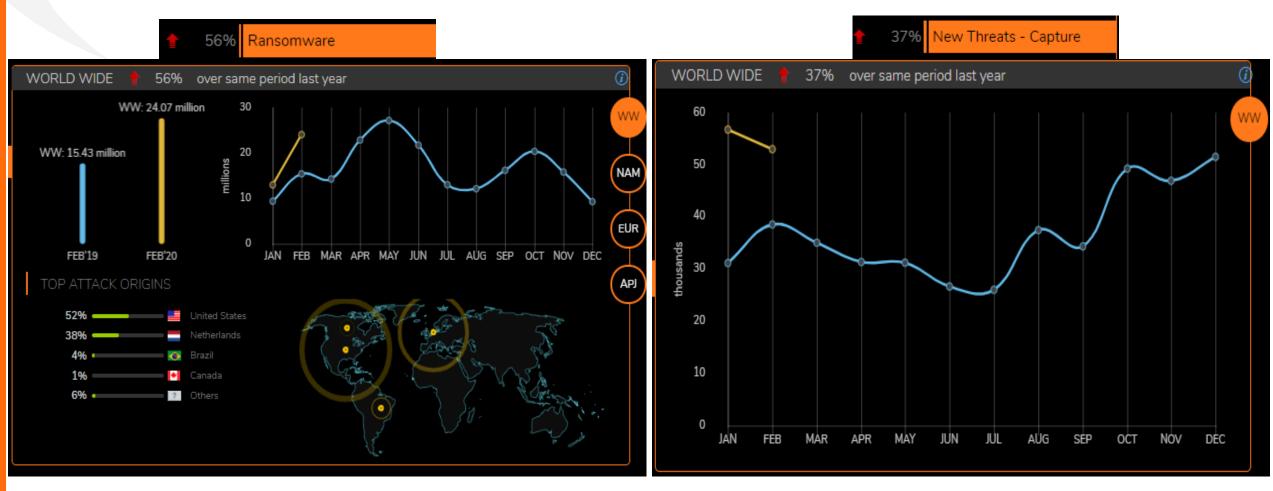
Exclusive cyber threat intelligence and analysis.
Only from SonicWall Capture Labs.

SonicWall.com/ThreatReport





Lo más significativo:



• Ransomware crece a un 56%

 Nueva amenazas en endpoint: Microsoft Office & PDF file breach



>70%

del tráfico de Internet está encriptado TLS/SSL

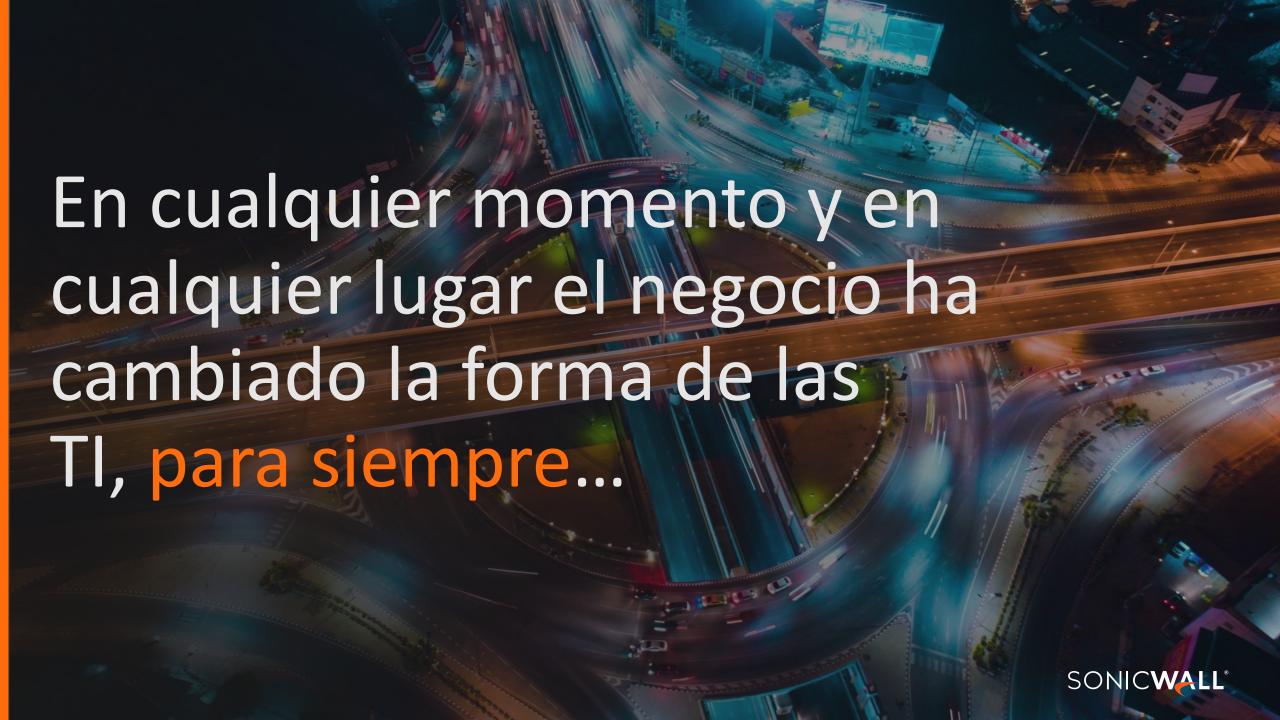


5%

De todo el malware usa encriptación TLS/SSL

Sólo el 5% de los clientes inspeccionan el tráfico TLS/SSL.





Pero nadie anticipó algo como esto, acelerando el lugar de trabajo digital, tan rápido...



COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)

Total Confirmed 6.418.078 Confirmed Cases by Country/Region/Sovereignty Brazil Russia United Kingdom Spain Italy India France Germany Peru Turkey Iran Chile Mexico Canada Admin2 Admin1

Last Updated at (M/D/YYYY)

6/3/2020 4:33:13 p. m.



Global Deaths US State Level 381.064 Deaths, Recovered 106.274 deaths 29.968 deaths. 66.262 recovered New York US 39.452 deaths 11.771 deaths, 26.815 recovered United Kingdom New Jersey US 33.530 deaths 7.085 deaths, recovered Italy Massachusetts US 31.199 deaths 5.667 deaths, 48.838 recovered Brazil Pennsylvania US 28.943 deaths 5.553 deaths, 38.099 recovered France Michigan US 27.127 deaths 5.525 deaths, recovered Spain Illinois US 10.637 deaths 4.320 deaths, recovered California US Mexico Global Deaths Global Recovered US Deaths, Recovered Daily Cases

188

Lead by JHU CSSE. Technical Support: Esri Living Atlas team and JHU APL. Financial Support: JHU and NSF. Click here to donate to the CSSE dashboard team, and other JHU COVID-19 Research Efforts. FAQ. Read more in this blog. Contact US.

Technology

Coronavirus Forces World's Largest Work-From-Home Experiment

By Shelly Banjo, Livia Yap, Colum Murphy, and Vinicy Chan February 2, 2020, 1:00 PM PST

- Co-working is out, video chat apps are in as offices close
- Startups that rely on Chinese manufacturing have no 'Plan B'

face of

El presentismo laboral se ha trasladado a los hogares con videoconferencias y mensajes frecuentes, avisan los expertos

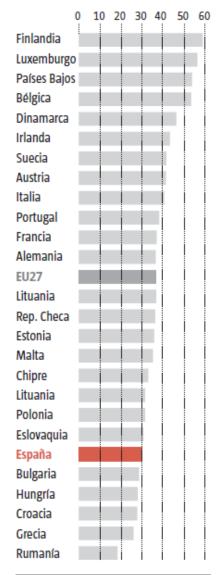
"El teletrabajo no era esto" Huge, Stressft

elerating in the U.S. But th



OCUPADOS QUE EMPEZARON A TELETRABAJAR POR LA COVID-19

% sobre el total de los trabajadores de cada país



FUENTE: Eurofound

LA VANGUARDIA

SONIC'

RETO DE NEGOCIO ACTUAL...

Esta nueva realidad de TI distribuida acelerada por el COVID-19, está creando una explosión de puntos de exposición sin precedentes

race to digitize

proliferation of apps, devices

borderless organizations

pervasive cloud

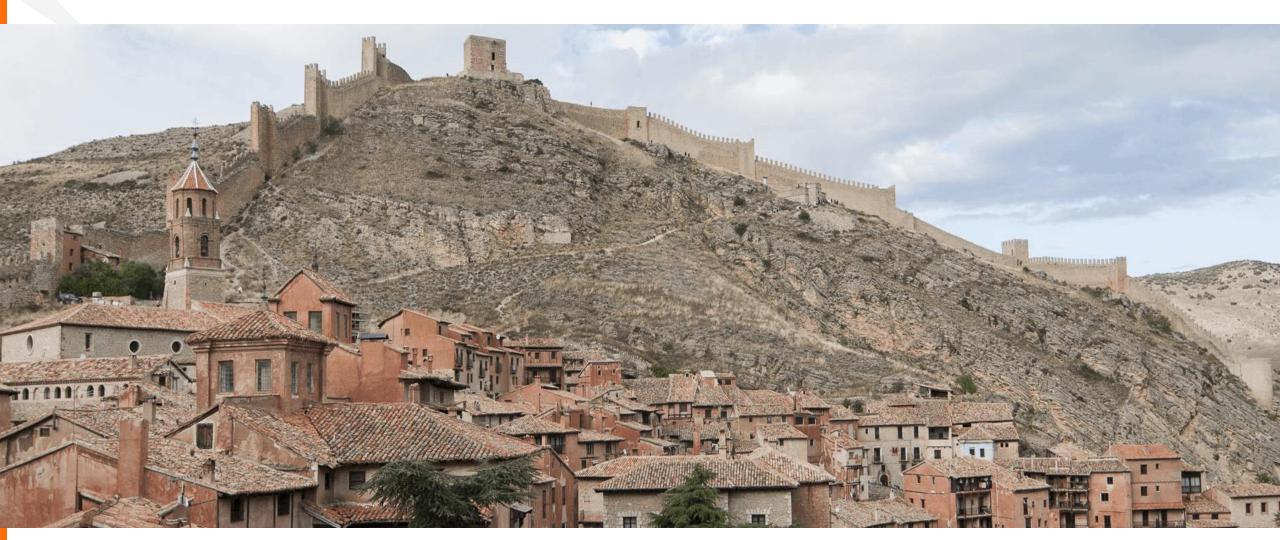
sensors everywhere

componentized, virtualized

evolving regulations



De un modelo bastión, con un perímetro definido a defender...





A un modelo parecido al de un aeropuerto, sin perímetro concreto y datos, usuarios distribuidos...

AL MISMO TIEMPO.

El panorama de ciberamenazas introduce nuevas e inteligentes tácticas de ataque

Hackers find new target as Russia Russia The Internet is drowning in COVID-19-

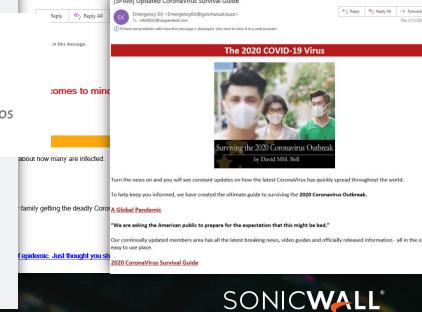
outbreak

Americans work for Decathlon España pirateada: filtrados los datos de trabajadores, tiendas y clientes

620 SHARES

La división española de la minorista deportiva ha sido hackeada y han expuesto los datos de sus trabajadores.

Un virus informático afecta al Hospital de Torrejón, que trabaja con papel desde el viernes



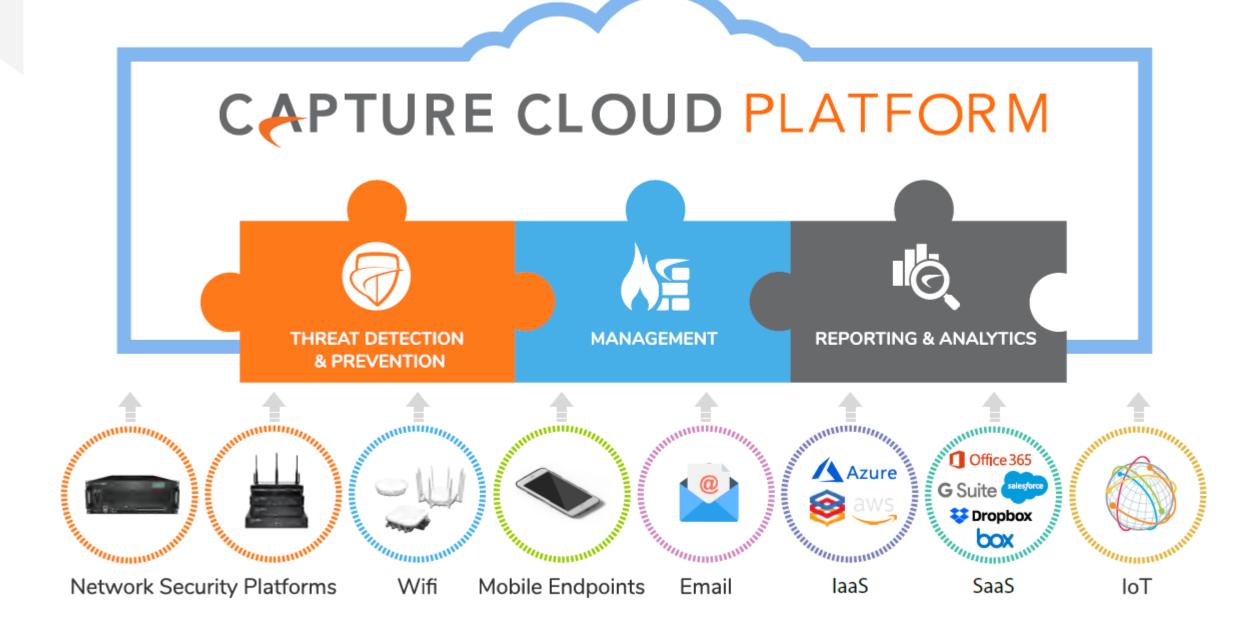
CUESTIÓN CLAVE...

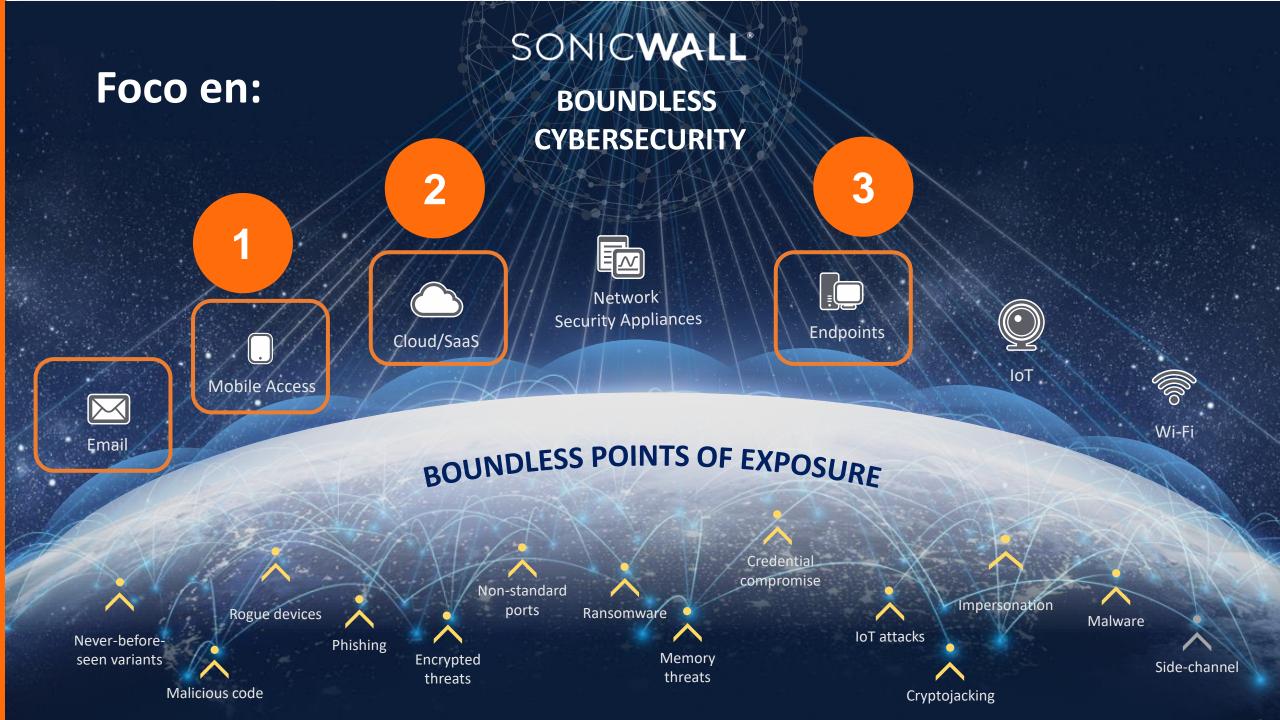
¿Cómo saber si quien se conecta es quién dice ser?

Todo está conectado, abierto y accesible
Las brechas son inevitables -> Robo identidad
La superficie de exposición aumenta...
El problema de la autenticación es otra pandemia



Porfolio soluciones SonicWall:





Acceso Remoto Seguro – autenticación segura



Situación Actual y Desafíos – Sin perímetro

- Teletrabajo y **reorganización de las empresas** en tiempo récord.
- Alternativa de acceso segura para que los trabajadores puedan seguir trabajando. Objetivo: intentar que la experiencia del usuario sea lo más parecida a estar físicamente en la oficina.
- Nuevos desafíos de seguridad. Los credenciales son el nuevo perímetro: acceso desde dispositivos personales (no corporativos), entorno hostil.
- Falta de soluciones y licencias necesarias para esta nuevo entorno.





Soluciones de SonicWall para conectividad remota segura

Firewall (SSL VPN & IPSec VPN)



SSL VPN Client

Principalmente TZ, o hasta 20 usuarios

IPSec Client

Escalabilidad (1000s) pero limitado a "tunnel mode"

SMA 100 Series

100-250 Users

SMA 1000 Series

Users



Enfoque principal de esta presentación:

- Esta es la mejor solución para la mayoría de los clientes
- Capacidad de oficina virtual vs tunelización

SonicWave Series



Capacidad: "Corp Wifi @ Home" Ability Aisle a los "high-target users" de su red corporative doméstica.

> **Puede complementar SMA** para usuarios seleccionados

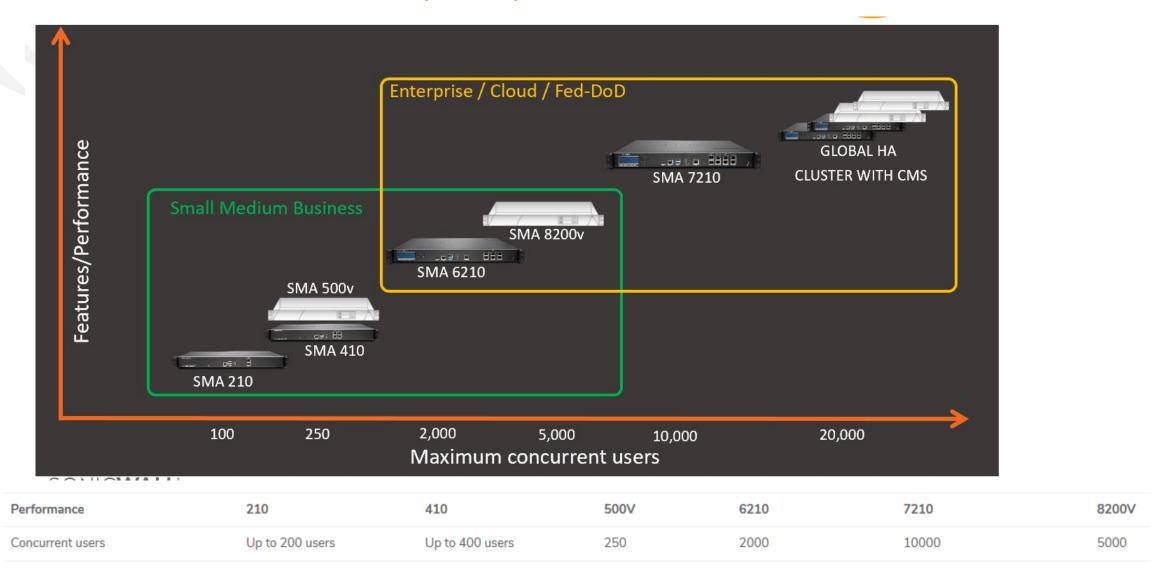


Recomendamos incluirlo con cada despliegue para garantizar la integridad del punto final



Control y protección del acceso SaaS directo

Secure Mobile Access (SMA) – Serie 100 & Serie 1000





Soluciones – Acceso Remoto Seguro







Google Authenticator



Microsoft Authenticator



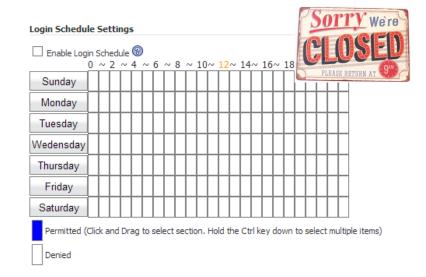
Duo Mobile

- Accesos <u>clientless</u> desde equipos no corporativos, sin necesidad de instalar ningún software para el acceso (portal SSL-VPN).
- Securización de la autenticación de los usuarios remotos (2FA).
- Licenciamiento flexible Incremento puntual de usuarios (Spike Licenses).
- Identificación y autorización de dispositivos (Device Management y EndPoint Control (EPC))



Soluciones – Acceso Remoto Seguro

- Restringir los accesos a determinadas horas del día (Login Schedules).
- Restringir los accesos en función de la IP de origen, por Reputación (AntiBotnet) o por ubicación geográfica (GeoIP) .
- Enrutar todo el tráfico del usuario por el Túnel SSL (incluido Internet) para tener un mayor control de su actividad (Tunnel All mode).
- Levantar la conexión VPN antes de que el usuario haga login en el equipo, y no permitir que desconecte la sesión (Always-On VPN).





Secure Mobile Access – Virtual Office

Secure Mobile Access SONICWALL



Classic mode ⓒ ♀





Welcome to the SonicWall Virtual Office

SonicWall's Virtual Office provides easy and secure remote access to the corporate network from anywhere on the Internet.

Click a pre-defined bookmark or create your own to securely access a corporate network resource.

Launch NetExtender to create a secure network connection to the corporate network for full network access.

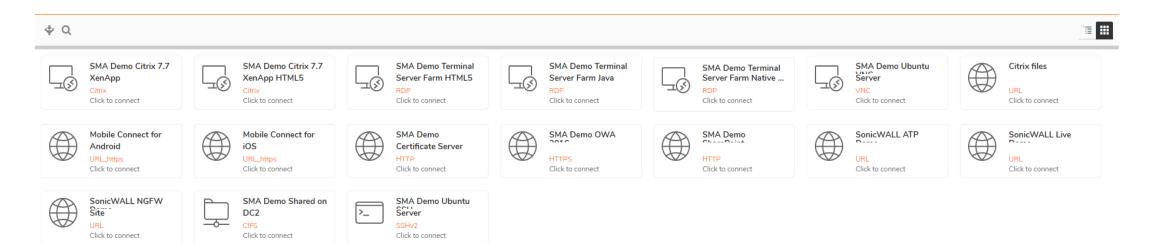


NetExtender



File Shares

Browse shared files on your corporate network



Showing 1-17 of 17 records | 24 per page ▼



Nuestra solución: Single Sign-on federado

SONICWALL Secure Mobile Access | WorkPlace

SONICWALL

Access: Web Zone: Default zone To access a resource, click its name from the list below. 4 HR Personal Bookmarks Concur (2) (X) FearLess Campaign tracker Travel and expense application Marketing program tracker Cloud and ADP - Pavroll Site Web Payroll for US Team members Sales applications Bamboo HR SFDC Salesforce SonicWall CRM instance SonicWall Benefits Benefits sign up and Info Portal Competitive Corner - Sales Competitive Comparison Materials Support MySonicWall.com Register products and manage product subscriptions Innerwall Public Training Pages SonicWall Intranet Customer facing product training info T Helpdesk Local SecureFirst Partner Portal Product Support Partner Program access and management portal applications Product Support Site SonicWall Live Demo site RFE Tracker Public demo access for partners and customers Request Feature Enhancements

La Solución de Sonicwall:

- Evento Single login
- Cualquier aplicación
- Cualquier dispositivo autorizado
- Múltiple factor de autenticación

Protección de Aplicaciones SaaS y Correo Electrónico (CAS)



Situación Actual y Desafíos – Protección Correo Electrónico

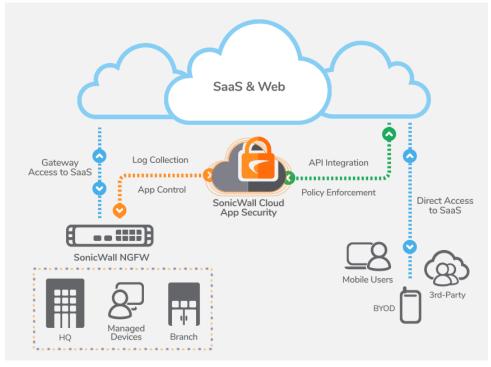
- Tradicionalmente ha sido uno de los vectores de ataque más habituales, pero ahora mismo lo es más.
- Los cibercriminales saben que en estos momentos la mayoría de las organizaciones son muy vulnerables. Mayor probabilidad de robo de datos y de credenciales.
- Incremento en el volumen de ataques de malware y phishing (temática Coronavirus).





Cloud App Security (CAS)





- Herramienta que permite monitorizar los logins de los usuarios (Account Takeover Protection) para evitar robo de credenciales.
- Inspección avanzada de phishing y antimalware (<u>múltiples motores</u>).
- Prevención de fugas de información (DLP).
- Integración con aplicaciones en la nube mediante API's.



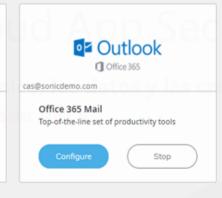
CONFIGURATION

Security Tool Exceptions

CLOUD STORE

Active Saas applications / 3



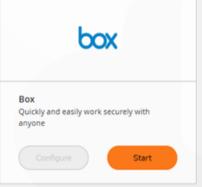


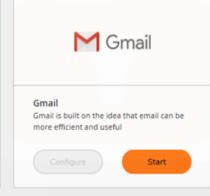


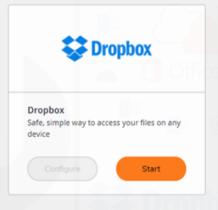
lacksquare

Inactive Saas applications / 8

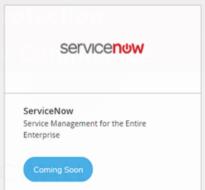


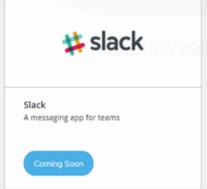








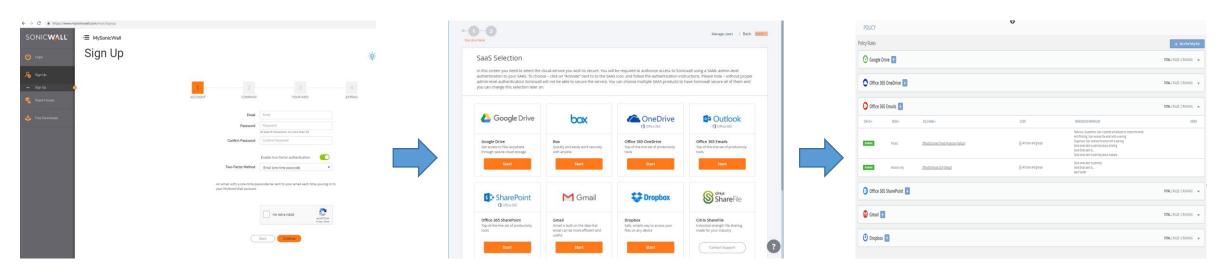






Cloud App Security (CAS)

Despliegue en pocos minutos



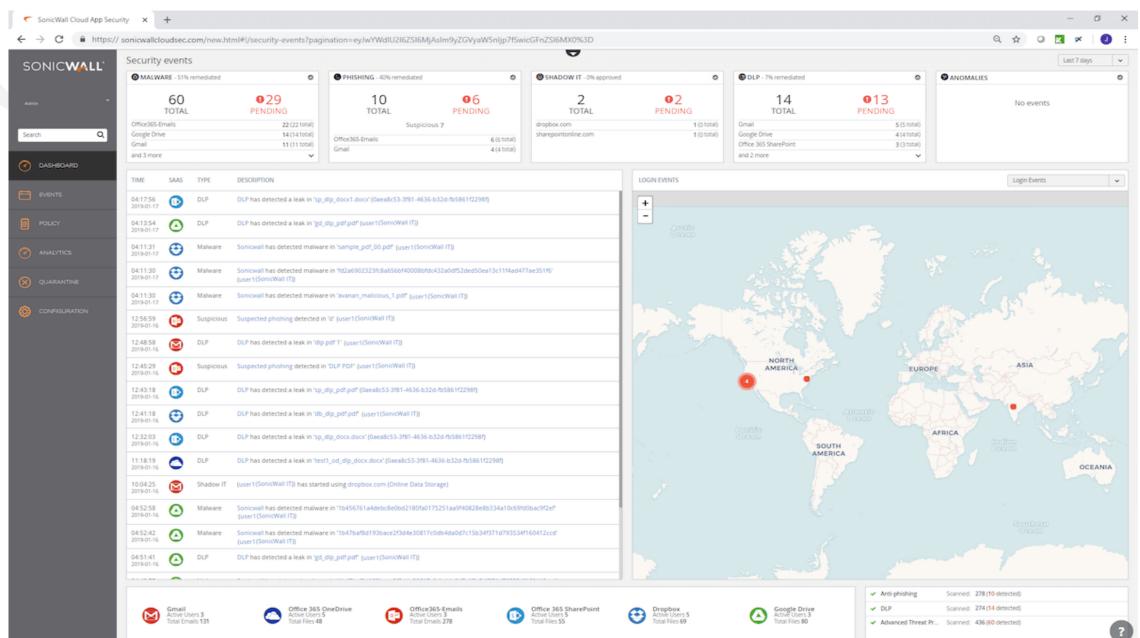
1. Activar y Aprovisionar

2. Seleccionar y Autorizar

3. Configurar y Monitorizar



Cloud App Security (CAS)



Cloud App Security (CAS) vs. O365

SonicWall Cloud App Security Closes O365 Security Gaps

	300 users limit		Unlimited users			300 users limit	
	O365 Business Essentials	O365 Business Premium	O365 Enterprise E1	O365 Enterprise E3	O365 Enterprise E5	Microsoft365 Business (0365+MDM+WIN10)	SonicWall (CAS Advanced)
Price (/user/month)	\$5.00	\$12.50	\$8.00	\$20.00	\$35.00	\$20.00	\$3.50
Anti-spam							
Anti-malware							
Anti-Spoofing							
Anti-Phishing (Reputation-based)							
Data Loss Prevention*							
ATP File Scanning							
ATP Anti-Phishing* (ML-based)							
ATP Attachment Analysis*							
URL Analysis*							
Account Takeover Protection*							





^{*} Optional Services that can be bought with extra cost

Protección EndPoint (Capture Client 3.0)



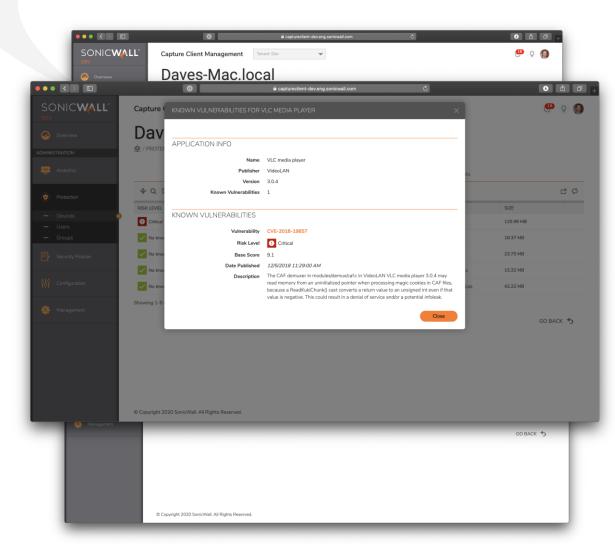
Situación Actual y Desafíos – Protección del EndPoint

- Las amenazas desconocidas (Zero Day) han aumentado desde que empezó la crisis del Coronavirus.
- Los PCs personales **no tienen el mismo nivel de seguridad que los corporativos**, por lo que es necesario protegerlos mejor.
- Es necesario tener cierto control (Filtrado Web, Análisis de Aplicaciones Vulnerables, Gestión Centralizada, etc.)sobre los equipos remotos (redes tipo BYOD).
- Medidas efectivas de desinfección, aislamiento o marcha atrás.





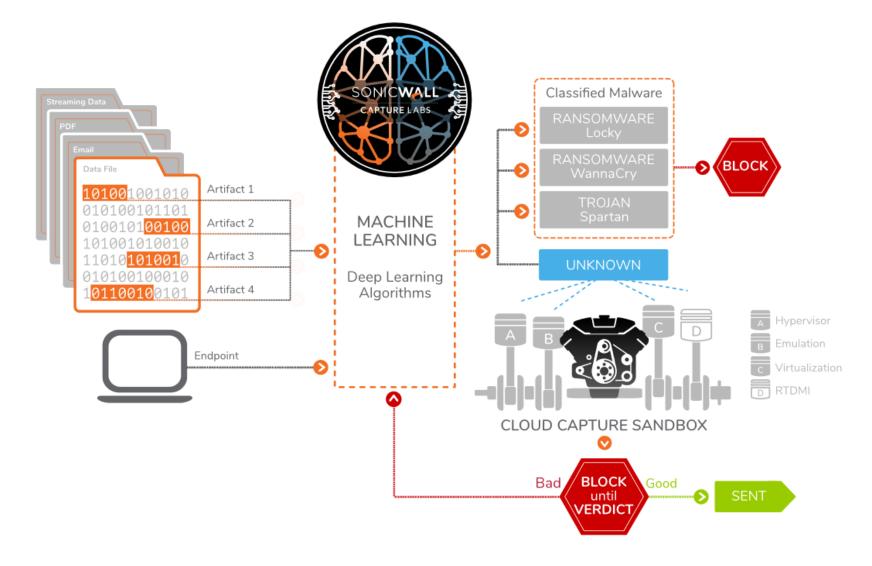




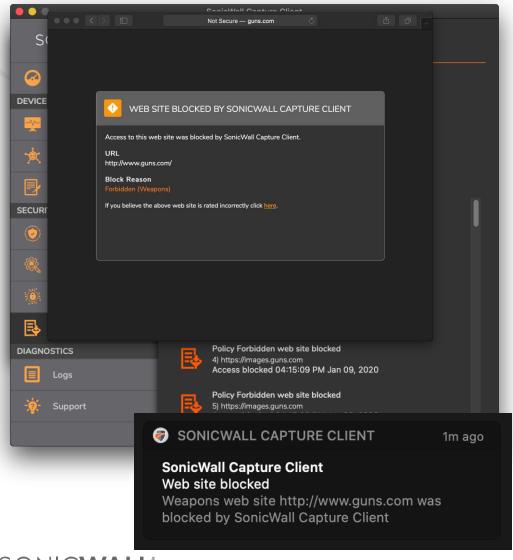
- Motor AV de nueva generación basado en Sentine One combinado con Sonicwall Capture ATP (SandBoxing Multimotor) para obtener múltiples veredictos y detectar malware de tipo desconocido.
- Posibilidad de aislar de forma "virtual" los equipos infectados.
- Análisis de aplicaciones vulnerables (Application Risk Management).
- Control de dispositivos USB y BlueTooth (Device Control).



Sonicwall Capture ATP – SandBoxing Multi-Motor

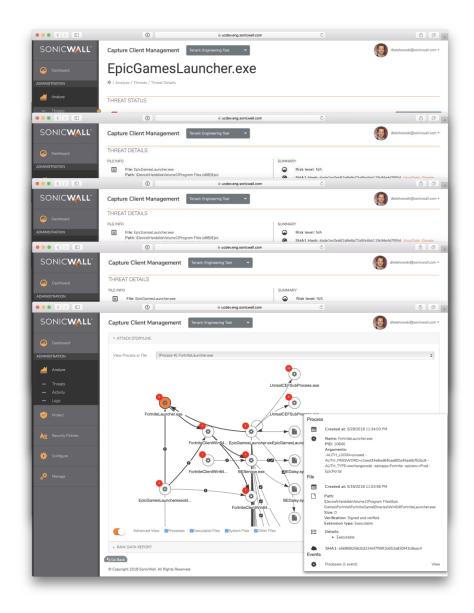




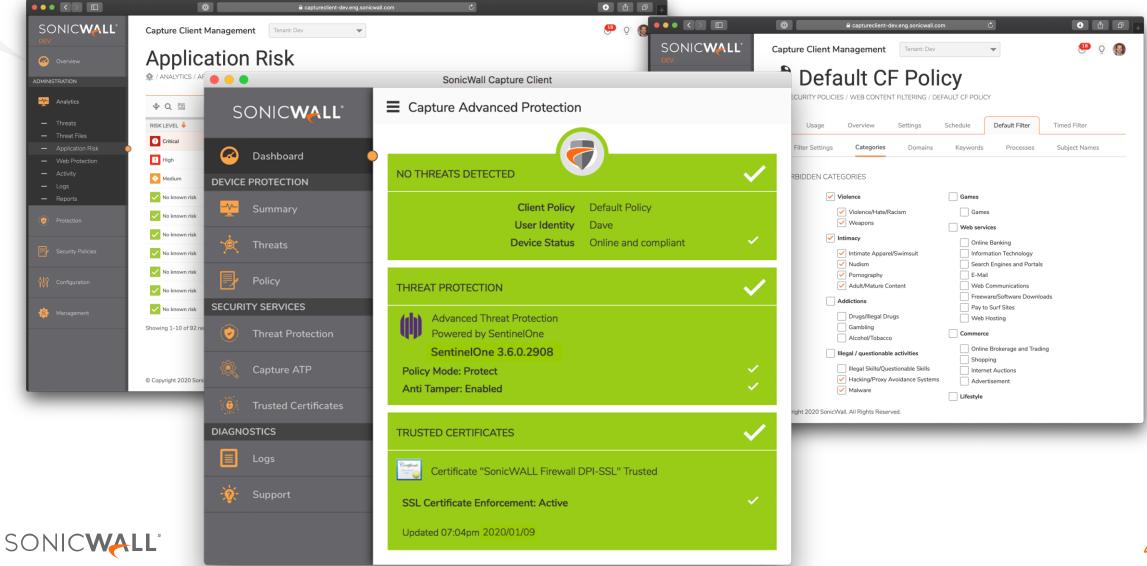


- Filtrado Web en el EndPoint.
- Múltiples Categorías (+56).
- Soporte de dominios permitidos/denegados (listas blancas/negras).
- Mismo servicio que el que ofrecemos en nuestros NGFW.
- Gestión de políticas personalizadas desde panel de gestión centralizado.

- Posibilidad de hacer roll-back en caso de infección.
- Funcionalidad EDR (EndPoint Detection and Response) para visualizar de forma gráfica la ejecución de las amenazas.
- Consola de gestión centralizada que aporte visibilidad sobre lo que ocurre en los endpoints.
- Soporte para Windows/Mac (próximamente Linux también).







Soluciones Virtuales vs. Físicas



Situación Actual y Desafíos

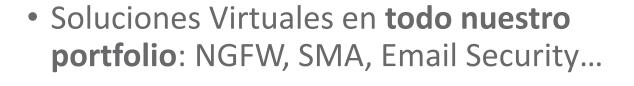
- Aceleración de la tendencia hacia el mundo virtual y servicios en nubes públicas (Azure/AWS).
- Reducción de costes de implementación y mantenimiento.
- Instalación y despliegue en remoto.
- Mayor flexibilidad y autonomía.





Soluciones Virtuales vs. Físicas





- Integración con nubes privadas
 (VMWare/Hyper-V) y nubes públicas
 (Azure/AWS).
- Licenciamiento flexible para Azure/AWS (PAYG vs. BYOL).
- Equivalencia a nivel funcional con las soluciones físicas.



Errores más communes en entornos de teletrabajo

Errores más comunes

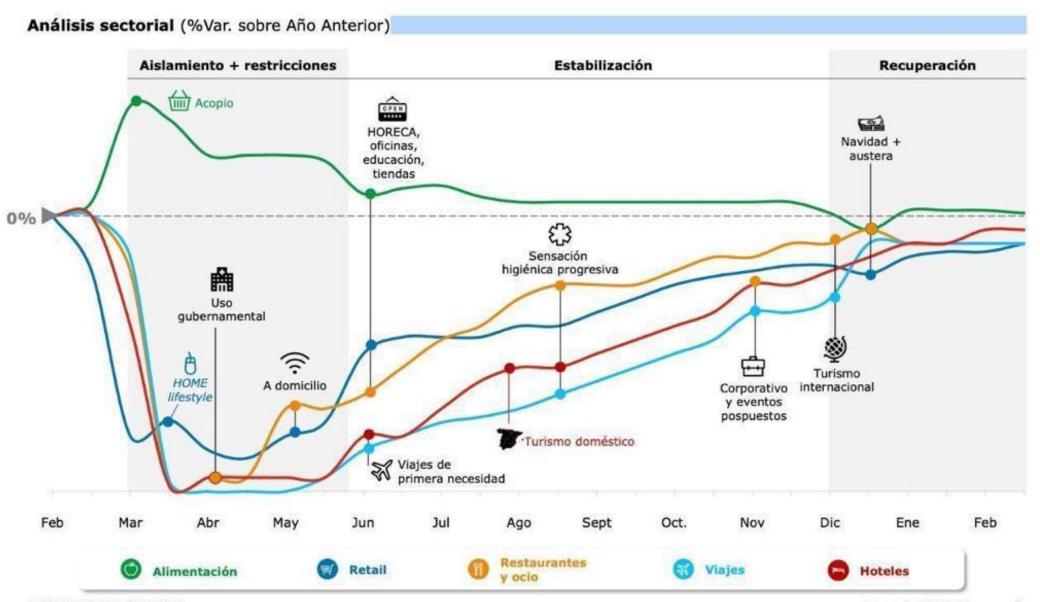
- Publicar directamente servidores RDP (BlueKeep).
- Dar a todos los usuarios el mismo nivel de acceso.
- Configuración de políticas muy permisivas (más prioridad al acceso que a la seguridad).
- No usar autenticación multifactor.
- Soluciones AV obsoletas o basadas en firmas (no Sandboxing).
- Control de usuarios, pero no de dispositivos.
- Errores de dimensionamiento. Entornos no preparados para la sobrecarga de conexiones remotas concurrentes.



¿Cómo va a ser el mundo Post-confinamiento?



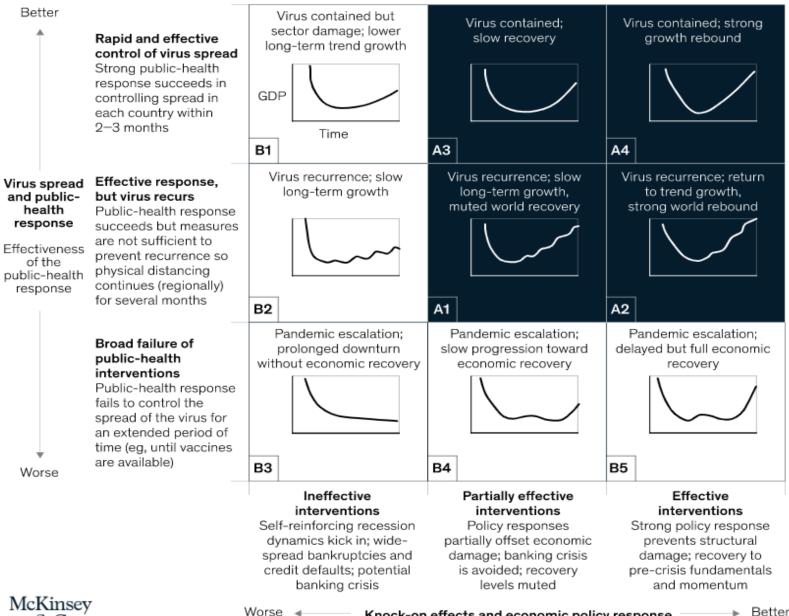
Racional de recuperación por sectores



48

Scenarios for the economic impact of the COVID-19 crisis.

GDP impact of COVID-19 spread, public-health response, and economic policies



RESUMIENDO, ESTOS DÍAS HEMOS PASADO A:



De un 20% de teletrabajo al 100% en pocos días



El perímetro ha desaparecido >
Usuarios en nuevo entorno hostil



Nuevas preocupaciones: credenciales, acceso remoto, encriptación, 100% offnet

Y EL MUNDO HA CAMBIADO PARA SIEMPRE:



Las oficinas ya no serán lo mismo... Teletrabajaremos mucho más



El perímetro ya ha desaparecido hace tiempo → Zero-Trust, SASE, etc.



Viajaremos menos. Nos veremos virtualmente mucho más → Nuevos riesgos



Volveremos en un tiempo. Seámos optimistas!

SONICWALL®

www.sonicwall.com





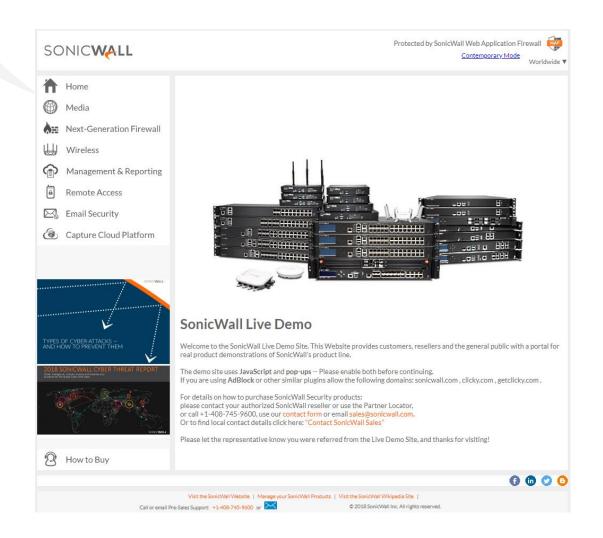


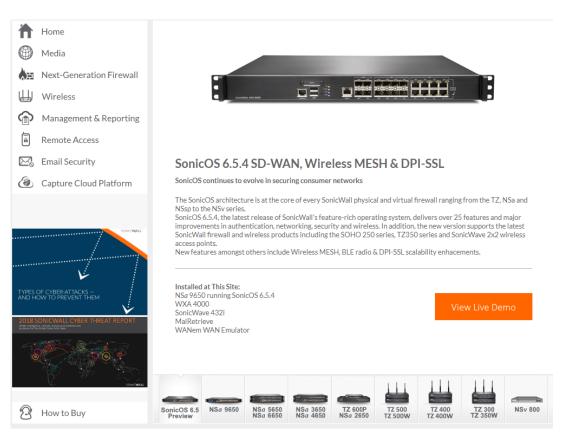


Recursos Útiles



Recursos Útiles - Livedemo







Recursos Útiles – Webs y Datasheets

- Portfolio Soluciones Sonicwall (Hot Sheet):
 https://www.linkedin.com/smart-links/AQF66NIxvAcDOQ
- <u>Seguridad por Capas (eBook)</u>: https://www.linkedin.com/smart-links/AQH3fvyzlikN9Q
- <u>NGFW Firewalls Físicos (TZ/Nsa)</u>: https://www.sonicwall.com/es-mx/products/firewalls
- <u>NGFW Firewalls Virtuales (NSv)</u>: https://www.sonicwall.com/products/firewalls/nsv-series/
- <u>SecureWiFi Sonicwall SonicWave</u>: https://www.linkedin.com/smart-links/AQEWUIefrLcmOA



Recursos Útiles – Webs y Datasheets

- <u>Secure Mobile Access (SMA)</u>: https://www.sonicwall.com/products/remote-access/remote-access-appliances/
- <u>Comparación SMA</u>: https://www.sonicwall.com/secure-mobile-access-sma-appliances-products-compare/
- <u>SMA Data Sheet</u>: https://www.linkedin.com/smart-links/AQEAzFJ8DKVKmQ
- <u>Solution Brief: "Best Practices for Secure Mobile Access":</u> https://brandfolder.com/s/q75j9h-enlp5c-5q1vzf
- Acceso Remoto Seguro Imperativo para las Organizaciones:
- https://www.linkedin.com/smart-links/AQGbcecrWXo6sw



Recursos Útiles – Webs y Datasheets

- Cloud App Security (CAS): https://www.linkedin.com/smart-links/AQGMSrkqXKG0FA
- <u>Capture Client (CC)</u>: https://www.linkedin.com/smart-links/AQGtK2MTbIF3ew
- <u>Capture Security Center (CSC)</u>: https://www.linkedin.com/smart-links/AQHZIHTLZV5rOQ

