# LOS SIETE PECADOS CAPITALES DE LA CIBERSEGURIDAD

Sergio Martínez
Country manager Italia, España y Portugal
Sonicwall

SONICWALL

# WE ARE SONICWALL

Never alone. Relentless security.

**Fundada en 1991, Headquarters en Milpitas (California), 1700+ empleados, https://www.sonicwall.com**

**SonicWall defiende a centenares de miles de empresas en todo el mundo**

**3.5 millones**
Firewalls instalados

**1.1 millones**
Sensores activos

**~30%**
Market share de PYMES en NOAM

**17,000+**
Partners en +215 países y territorios

**Porque somos un aliado del canal:**

ZENXEON TECHNOLOGIES

Logically

InterVision

**En retail…**

ACE The helpful place.

Chick-fil-A

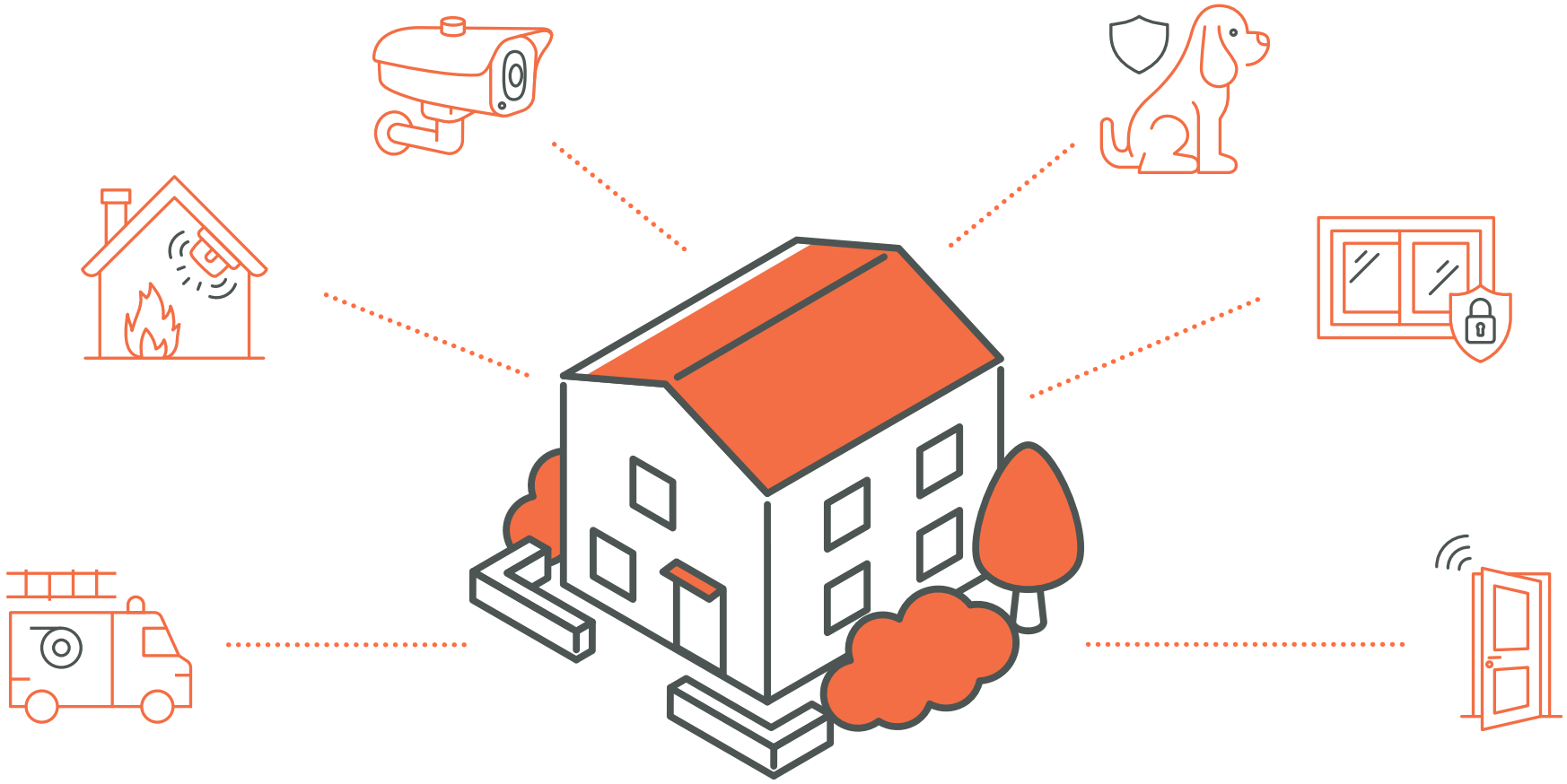
**En universidades e incluso en un F-35…**

Università di Pisa

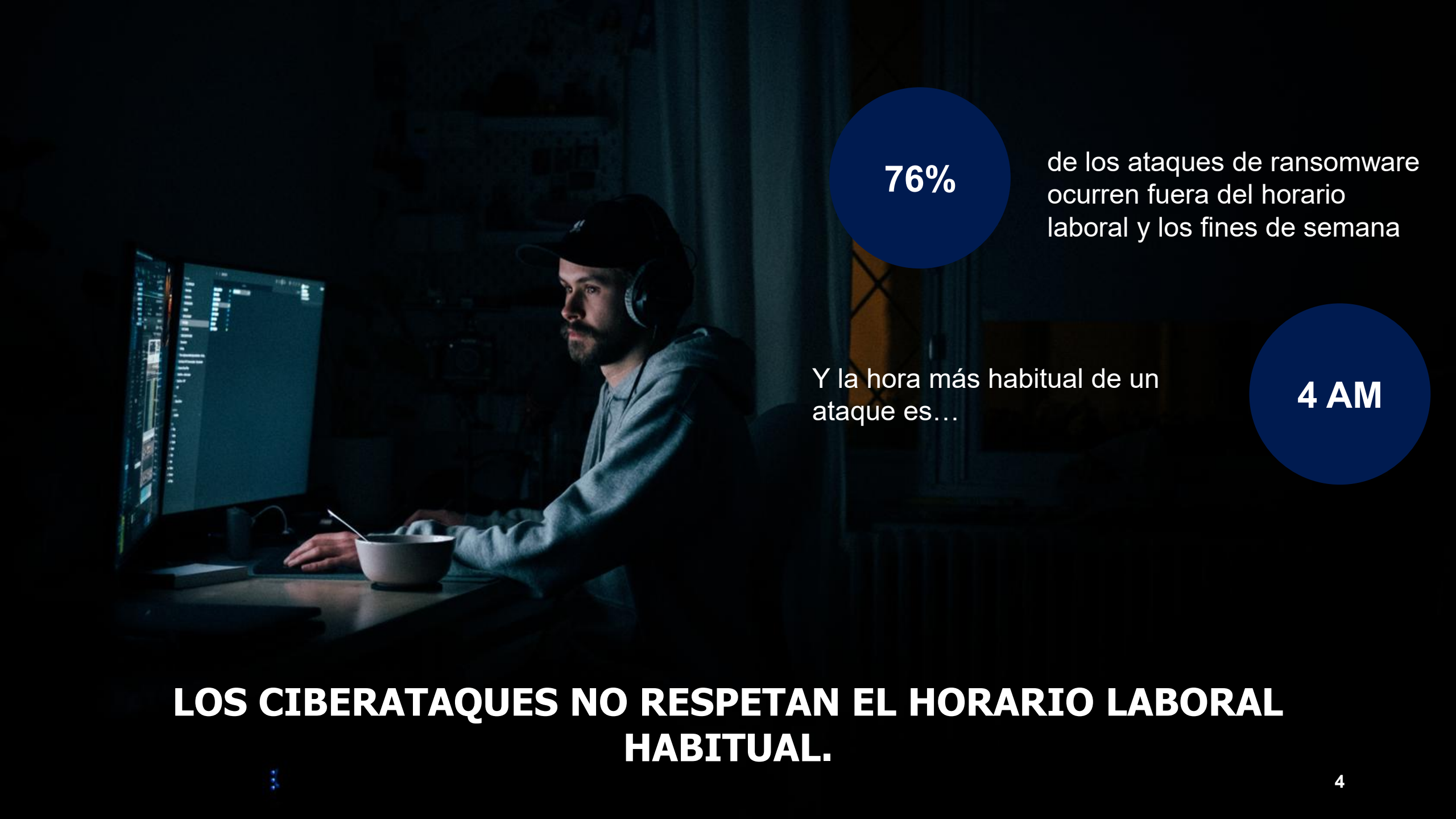
Joint Strike Fighter — JSF F-35 — Lethal Survivable Supportable Affordable

| HIGHER EDU | GOVERNMENT | K-12 | RETAIL |
|---|---|---|---|
| **Docenas de Universidades** | **10+** Ministerios defensa | **Cientos** de colegios | **100+** Marcas |
| **500,000+** estudiantes | **1M+** tropas | **2M+** estudiantes | **200,000** Tiendas |

# SE NECESITA:
# PREVENCIÓN – DETECCIÓN – RESPUESTA



# "EL PERRO LADRA"



**76%**

de los ataques de ransomware ocurren fuera del horario laboral y los fines de semana

Y la hora más habitual de un ataque es…

**4 AM**

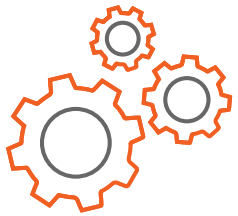
# LOS CIBERATAQUES NO RESPETAN EL HORARIO LABORAL HABITUAL.

# PROBLEMAS CON...

| | |
|---|---|
| **Tiempo de respuesta** | Las alertas a gestionar se producen en horas **intempestivas**, proporcionando un tiempo valioso a los atacantes ante la falta de respuesta en tiempo. |
| **Fatiga de alertas** | Muchas alertas son falsos positivos.<br>El constante flujo de alertas puede enmascarar las de carácter **crítico** |
| **Faltan expertos** | Los MSPs ayudan a los clientes en todos los servicios de IT, hasta para la instalación de impresoras<br>Es difícil captar y retener **talento** de Ciberseguridad para poder gestionar correctamente estas alertas. |

SONICWALL®

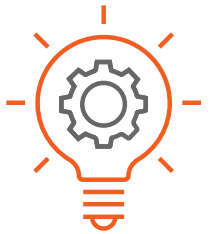
# EL CAMPO DE BATALLA ESTÁ CAMBIANDO



Las redes son más **complejas**

Las amenazas crecen en volumen y **sofisticación (IA)**

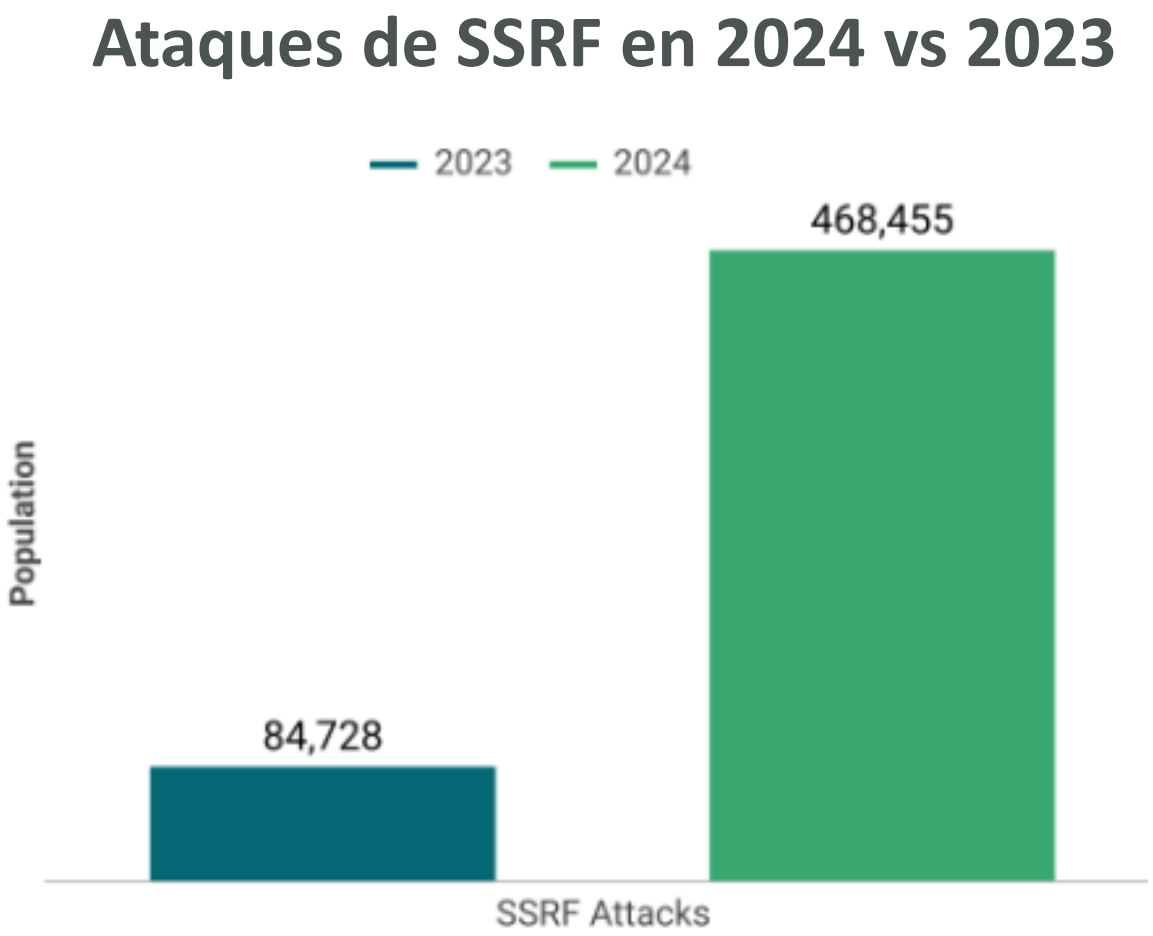
Los empleados están distribuidos y **fuera del perímetro**



Hay que estar preparado para responder 24x7x365

# IA: FACILITA LOS ATAQUES E INCREMENTA SU COMPLEJIDAD

## Viejas amenazas revitalizadas por la IA




SONICWALL

SSRF: Server Side Request Forgery

La introducción de las herramientas potenciadas por **IA generativa y agéntica**, ha reducido las barreras de entrada. Algunos de los ataques que ha potenciado son:

- **Phishing muy convincente y Deepfakes avanzados.**
- **Localización de sistemas no parcheados** o anticuados: Los escaners basados en IA identifican los sistemas “legacy” con vulnerabilidades no parcheadas.
- **Automatización de encadenamiento de Exploits**. La IA diseña procesos de encadenamiento de malware con vulnerabilidades para el escalado de privilegios y movimientos laterales.
- **Evasión de detección**. La IA proporciona técnicas de ofuscación para evadir la detección, haciendo más efectivos los ataques.

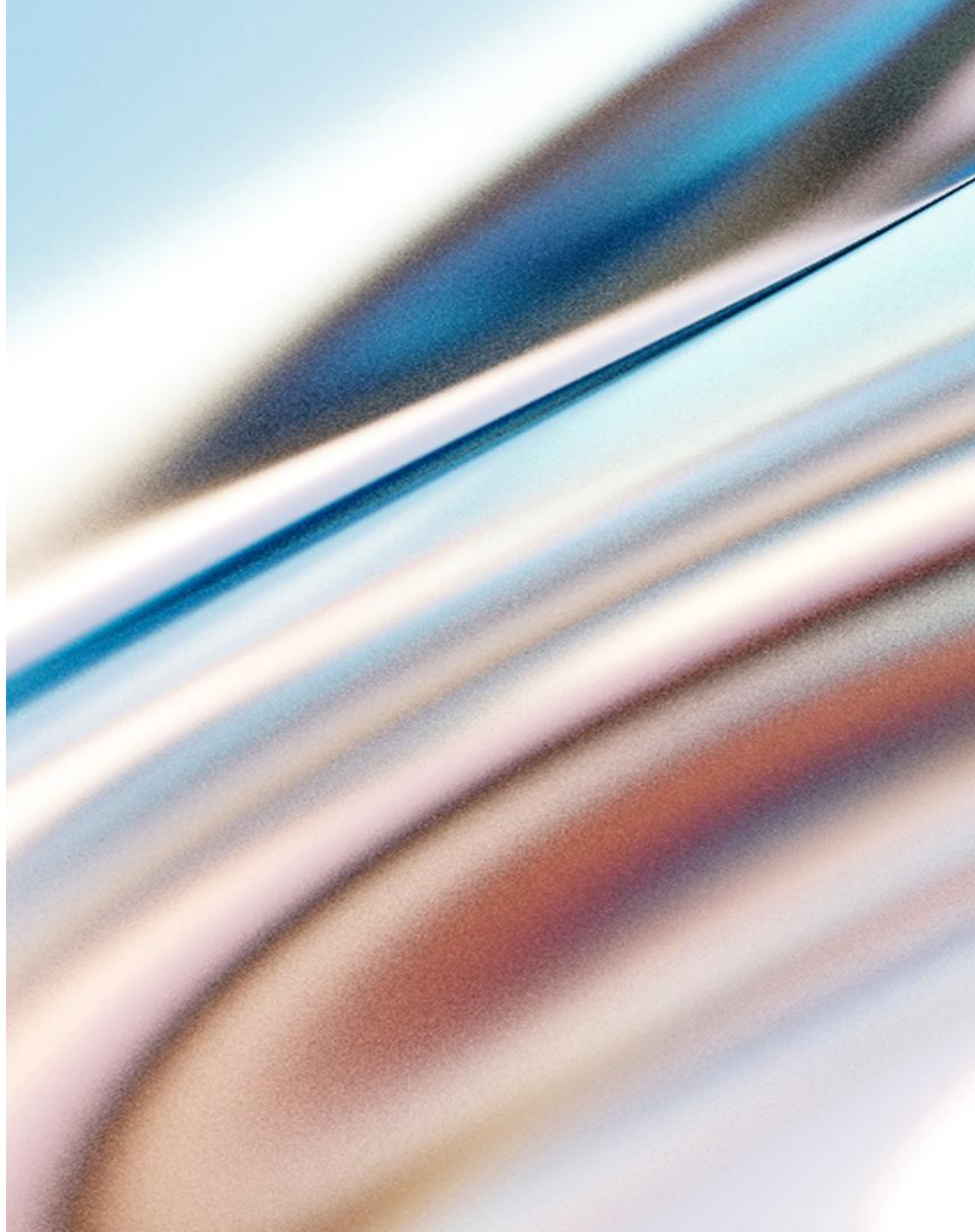
**NOTA**: SSRF es la falsificación de peticiones en lado del servidor, el atacante lo manipula para realizar peticiones a recursos internos o externos.

SONICWALL®

MARCH 31, 2026

# SonicWall 2026 Cyber Protect Report.

## Los siete pecados capitales de la ciberseguridad



# Cada año, esperamos descubrir algo nuevo.

Un ataque innovador. Una nueva técnica. Algo que nos sorprenda…

Sin embargo, año tras año encontramos lo mismo. Los ataques siguen siendo

**Predecibles. Evitables. Conocidos.**

LO QUE ESTÁ EN JUEGO

# 85 %

de las alertas de seguridad de 2025 tenía su origen en el robo de credenciales / identidades.

**Los atacantes no utilizan herramientas sofisticadas.**

**Usan simplemente la ventana que se dejó abierta.**

*— Informe Cyber Protect 2026 de SonicWall*

# Los 7 pecados capitales de la ciberseguridad.

PECADO 01

**Ignorar aspectos básicos**

85 % de las alertas: credenciales

PECADO 02

**Falsa confianza**

El 88 % de las pymes fueron víctimas de ataques ransomware

PECADO 03

**Acceso excesivo**

48 % de las filtraciones: credenciales de VPN

PECADO 04

**Enfoque reactivo**

El 44 % de las alertas no se investigan

PECADO 05

**Decisiones motivadas por los costes**

Coste medio de las filtraciones en pymes: $4,91 M

PECADO 06

**Modelos de acceso antiguos**

CVEs de las VPNs +82,5 % en 2025

PECADO 07

**Persiguiendo la moda**

El 90 % carece de madurez de IA

PECADO 01

# Ignorar aspectos básicos

**El principal vector de ataque no son las amenazas de día cero.**
**Son las contraseñas robadas de una puerta no vigilada**

*La mayoría de las filtraciones no empiezan con técnicas avanzadas. Empiezan con una brecha que debería haberse cerrado.*

**85 %**

de las alertas: compromiso de credenciales e identidades

**61 %**

de los exploits se producen en las 48 horas tras la publicación de la vulnerabilidad

**102**

días de promedio para aplicar parches en el sector de la banca

PECADO 02

# "Somos demasiado pequeños para ser el blanco de un ataque."

**88 %**

de las filtraciones en pymes están relacionadas con ransomware frente al 39 % en empresas grandes

**181**

días de promedio que los atacantes pasan desapercibidos. El 80 % de los directores de TI afirman que lo descubrirían en 8 horas

***Las meras suposiciones no son una buena base para la seguridad. Lo que cuenta son los hechos.***

PECADO 03

# Acceso VPN excesivo

**El acceso no es más que la mitad del problema.**

Lo que ocurre después viene determinado casi totalmente por la amplitud del acceso que el atacante encuentra al otro lado.

**0 min.**

Credenciales comprometidas vía VPN

**18 min.**

Propagación por toda la red

**48 min.**

Movimiento lateral a todos los sistemas (promedio)

***El 48 % de las filtraciones empiezan con credenciales de VPN comprometidas.***

PECADO 04

# 44 %

## de las alertas de seguridad no se investigan.

No porque a los equipos no les importe, sino porque el volumen de ruido ha superado el nivel que el ser humano es capaz de procesar.

# El tiempo del atacante ya está en marcha.


*Tiempo promedio de permanencia del atacante antes de ser detectado*

**En las revisiones posteriores al incidente, las señales siempre estaban en los logs. Nadie las revisó**

PECADO 05

# Decisiones de seguridad motivadas por los costes

## Coste vs. resultados

Posponer pruebas de penetración, saltarse la capacitación, elegir la herramienta más barata: aunque todas estas acciones pueden parecer prudentes, combinadas aumentan el riesgo.

Las organizaciones con planes exhaustivos de IR se ahorran $1,23 M por filtración. Tener un plan cuesta tan solo una fracción de ese importe. No tenerlo se nota cuando ya es demasiado tarde.

## Herramientas vs. estrategia

Actualmente, las empresas utilizan una media de 45 herramientas de seguridad. Casi la mitad de los profesionales de seguridad dedican más tiempo al mantenimiento de herramientas que a defender contra ataques.

El 74 % de las organizaciones que han sufrido múltiples incidentes de ransomware afirman que compaginan demasiadas herramientas que no se integran. Visibilidad fragmentada = brechas explotables.

## Brechas en el personal y los procesos

El error humano es la principal causa de las filtraciones. Se aprueban los presupuestos para las herramientas porque aparecen en facturas - las mejoras en el personal y los procesos son más difíciles de cuantificar y más fáciles de posponer.

El resultado: las herramientas se implementan, pero nadie sabe cómo utilizarlas, y nadie se hace responsable.

**$1,23 M**

ahorrados por filtración con un plan de respuesta a incidentes

**45 herram.**

de promedio por empresa – la mitad no se integran

**$4,91 M**

coste potencial de una filtración para una pyme

PECADO 06

# Uso de modelos de acceso legacy

**El perímetro que usted defiende ya no existe.**

**Los atacantes no están atravesando los firewalls. Están iniciando sesión.**

**La identidad es el nuevo perímetro**

**82,5 %**
de aumento en las CVEs de las VPNs

**90 %**
de las organizaciones actualmente tienen problemas con las VPNs

**48 %**
de las filtraciones: VPN como vector inicial

PECADO 07

# Las herramientas no generan resultados. La ejecución sí.

*"La gran mayoría de los ataques que investigamos se deben a aspectos básicos que siguen pasándose por alto. Nos hemos enfocado tanto en la **IA** que estamos permitiendo que sobrecompense las cosas que probablemente sigan siendo las más importantes."*

— Michael Crean, SonicWall

# Qué hacen las organizaciones protegidas de manera diferente.

01 Aplican la MFA en todas las cuentas — sin excepciones

02 Aceleran la aplicación de parches en los sistemas conectados a Internet

03 Segmentan las redes para limitar el alcance en caso de incidente

04 Monitorizan 24/7 — no solo en horario laboral

05 Ponen a prueba la respuesta a incidentes antes de que se produzca uno

06 Cambian del acceso a toda la red al acceso basado en la identidad

07 Ejecutan las medidas básicas completamente antes de buscar nuevas herramientas

# Las pymes no fracasan por falta de herramientas de seguridad.

## Las herramientas ya las tienen.

El reto reside en la disciplina operativa, la implementación consistente de las medidas básicas, la evaluación honesta de lo que realmente funciona y en contar con un partner que vigile su sistema cuando usted no puede.

*Los 7 pecados no son inevitables. Son una elección.*

# ¿NOS PODEMOS PERMITIR UN SOC?

# VIGILANCIA EN TODA LA SUPERFICIE

## SonicSentry Managed XDR

Alert Management · Threat Hunting · Threat Mitigation
Log Retention · Reporting

## 1 MDR for Endpoint

***Protection and response for endpoints***

CROWDSTRIKE

Capture Client

SentinelOne

Microsoft Defender

SOPHOS

## 2 MDR for Cloud

***Protection and response for cloud apps and email***

**Cloud Email Security**

Microsoft 365

Google Workspace

**Cloud Threat Analytics**

slack

Dropbox

salesforce

## 3 MDR for Network

***Protection and response at the perimeter***

***Any network device from any maker***

# CLOUD SECURE EDGE.

La solución creada por **Sonicwall** para la oficina híbrida actual.

**SWG**

Protege contra las amenazas de internet, concluyendo Phishing, sitios maliciosos y ransomware.

**CASB**

Controla el acceso y proporcionada Seguridad añadida a las aplicaciones SaaS

**ZTNA**

Permite a los empleados y 3rd parties acceso a las aplicaciones Cloud, híbridas, On-premises y multiCloud, estén dónde estén.

**VPNaaS**

Crea un acceso seguro y encriptado en internet entre el usuario y el recurso requerido (“túnel”)

Modernize VPN/ ZTNA & Firewall

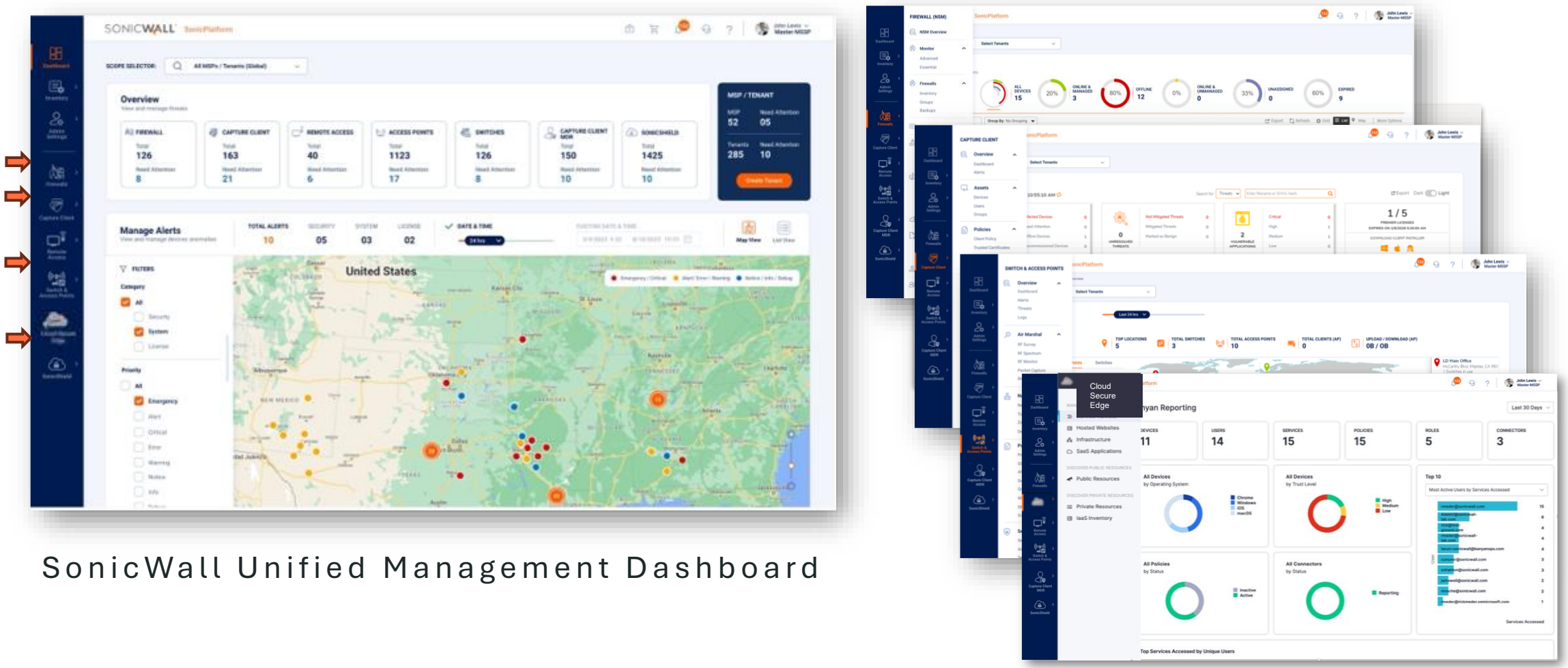
3rd Party Access / BYOD / M&A

Device Trust & Internet Threat Protection

SONICWALL

SONICWALL UNIFIED MANAGEMENT + SAMI

# UNA PLATAFORMA PARA CONTROLARLOS A TODOS

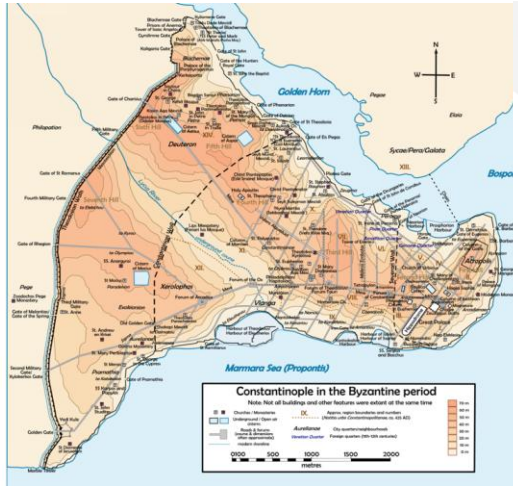



SonicWall Unified Management Dashboard

# SE NECESITA UNA NUEVA CIBERSEGURIDAD.

## 1 DEFENSA POR CAPAS

- Compartimentar
- **Añadir Servicios MSSP: MXDR**




## 2 VISIBILIDAD CENTRAL PARA DETECTAR Y RESPONDER

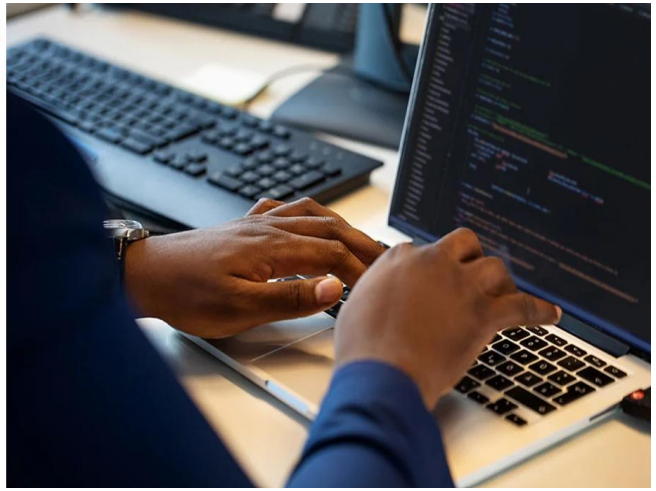
- SOC as a Service (MSS)
- SonicSentry.
- Unified Management

## 3 DETECTAR LO DESCONOCIDO

- IA
- Sandboxes avanzados
- SOCas a Service (MSS)

## 4 ACCESO REMOTO SEGURO Y MODERNO

- MFA – Zero Trust
- Cloud Secure Edge: Modernizar la VPN.



## 5 TCO Y COSTES DISRUPTIVOS

- Desde PIMES hacia cualquier tamaño
- Siempre Canal
- Empujamos el negocio MSP


**Sergio Martínez**
Country Manager Italy, Spain & Portugal
@smartinezh
smartinez@sonicwall.com