EL ESCENARIO DE CIBERGUERRA ACTUAL: TENDENCIAS 2024

Sergio Martínez
Country Manager Iberia

Company Overview

Cybersecurity for the hyper-distributed era

Global Footprint

500,000+ customers in 215 countries and territories

Industry Veteran

Trusted **30-year** veteran of the cybersecurity industry

End-to-End Portfolio

Comprehensive **cybersecurity** product and service **platform**

Global Threat Intelligence Network

Hundreds of terabytes, artifact **threat data**

100% Channel

17,000+ global Channel partners

Cybersecurity Innovation

More than **300 innovative patents** granted, including **RTDMI™**

Founded 1991

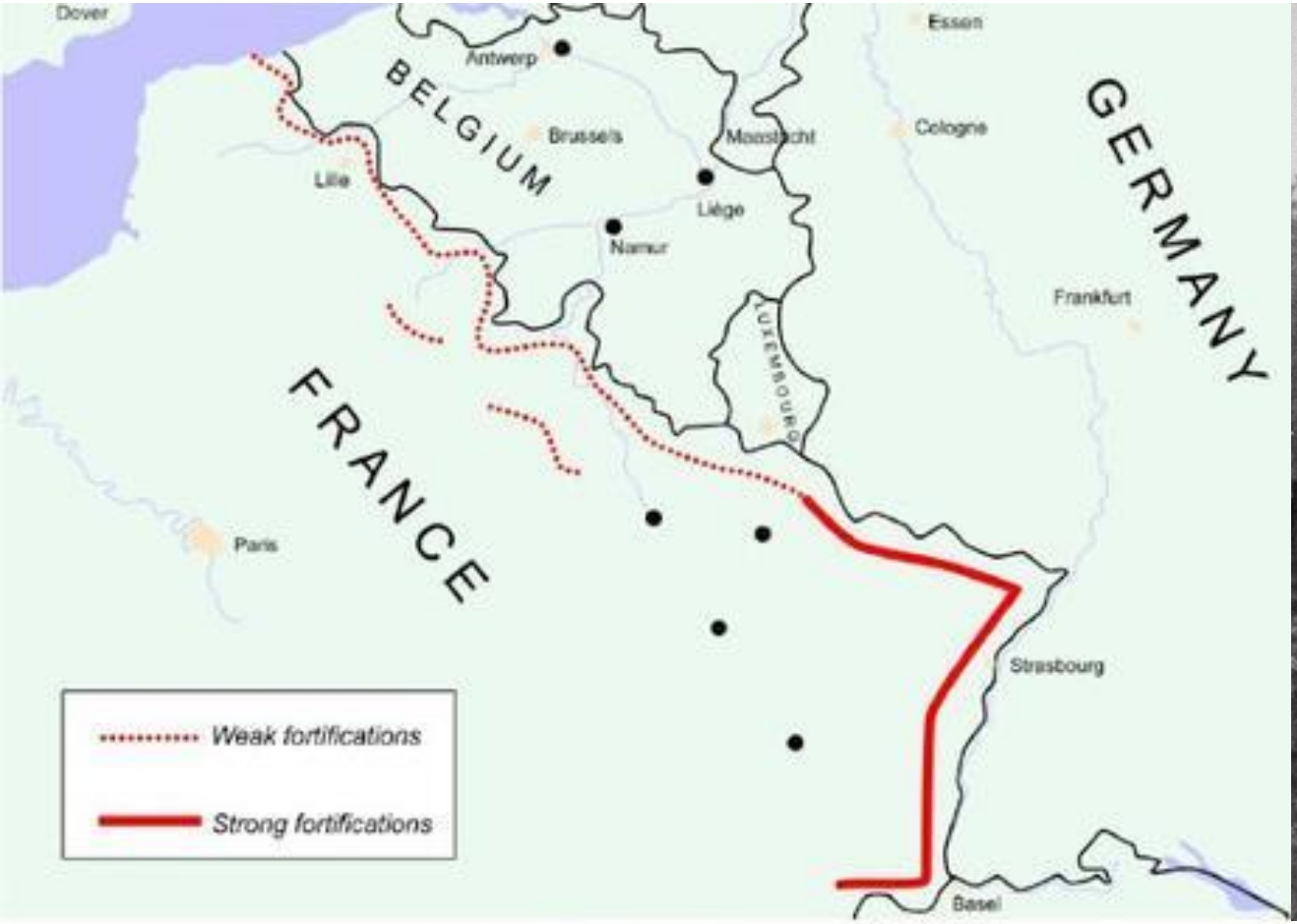
Headquarters
Milpitas, California

Employees 1,600+

www.sonicwall.com

SONICWALL®

Ejemplo: Linea Maginot (1940)

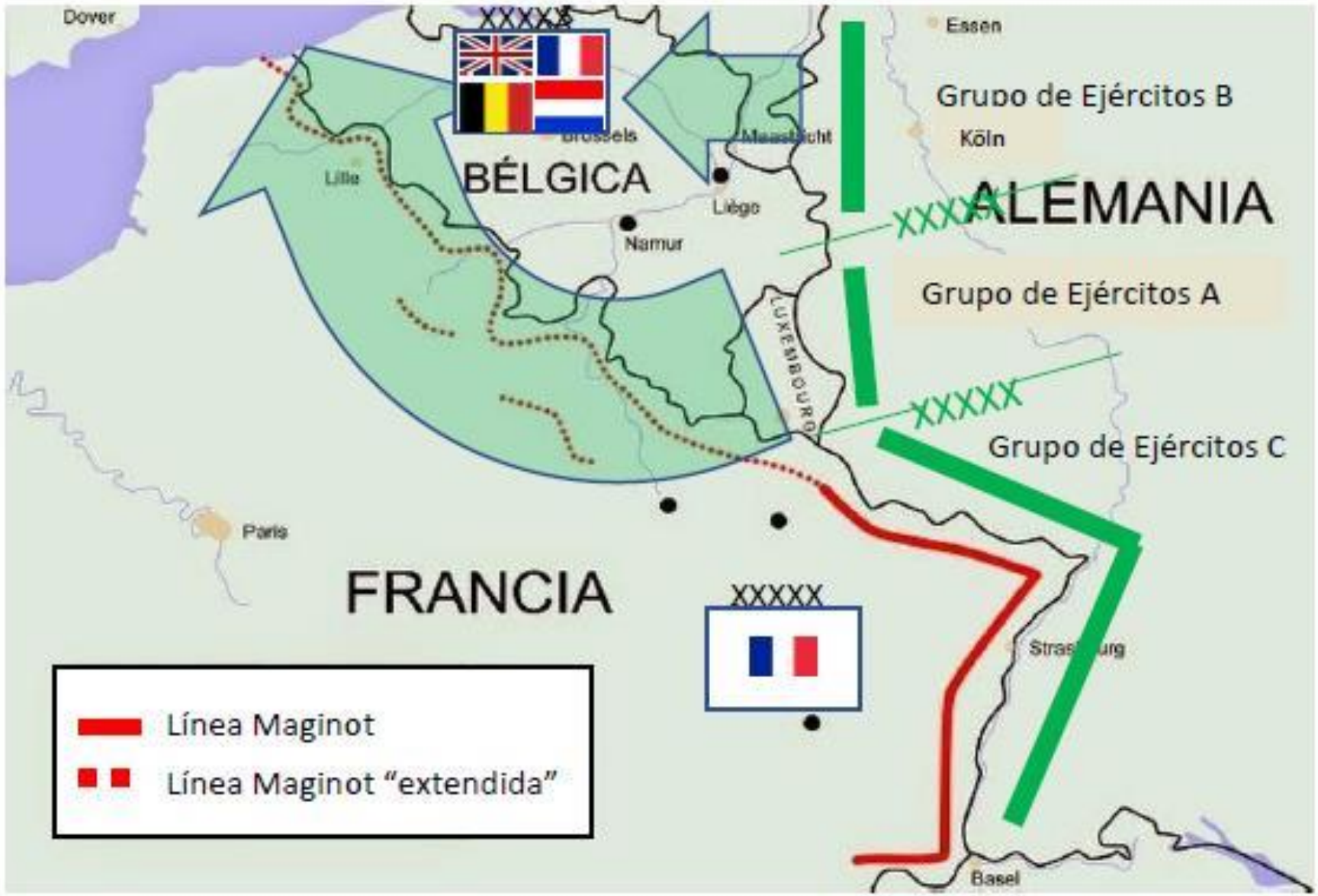


Línea Maginot

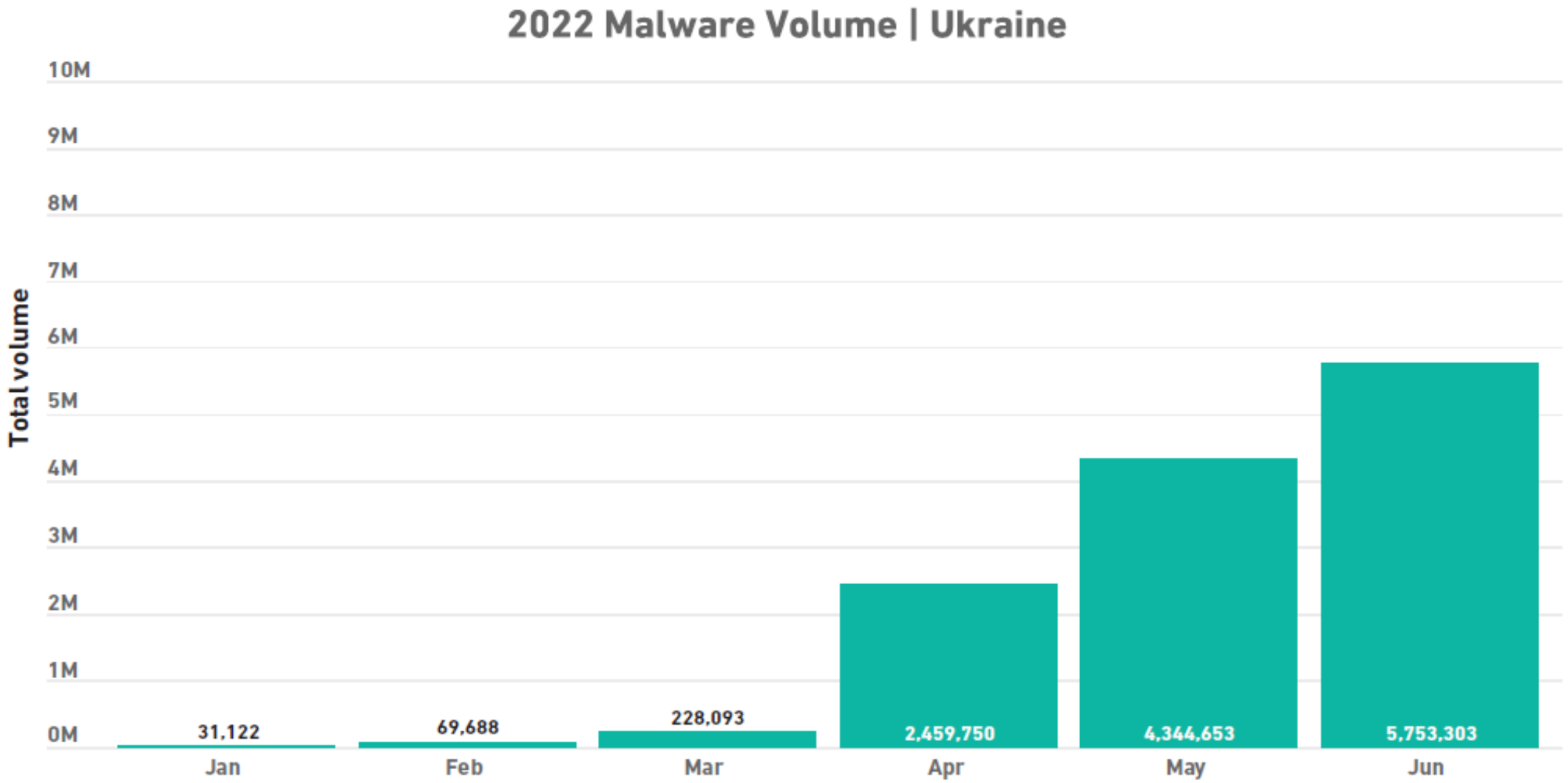
¿Qué sucedió? El ataque a Francia en 1940 se realizó por Bélgica y Luxemburgo. Por la parte "débil", la no vigilada: Los bosques de las Ardenas.

SONICWALL

Ejemplo: Linea Maginot (1940)



Y en Ucrania… x200. Ciberguerra!



SONICWALL

EL GRAN RETO ES…

La nueva IT distribuida de forma **masiva (…COVID)** está creando una **explosión de la superficie de exposición** (sin precedentes)

COVID: empleados en casa

Proliferación de apps, dispositivos

Organizaciones sin perímetro

Uso del Cloud

Sensores en todas partes

Virtualización de todo

Compliance

Entornos híbridos

SONICWALL®

Por otro lado... Nunca hemos invertido tanto en ciberseguridad...

Pero... Todo va a peor.

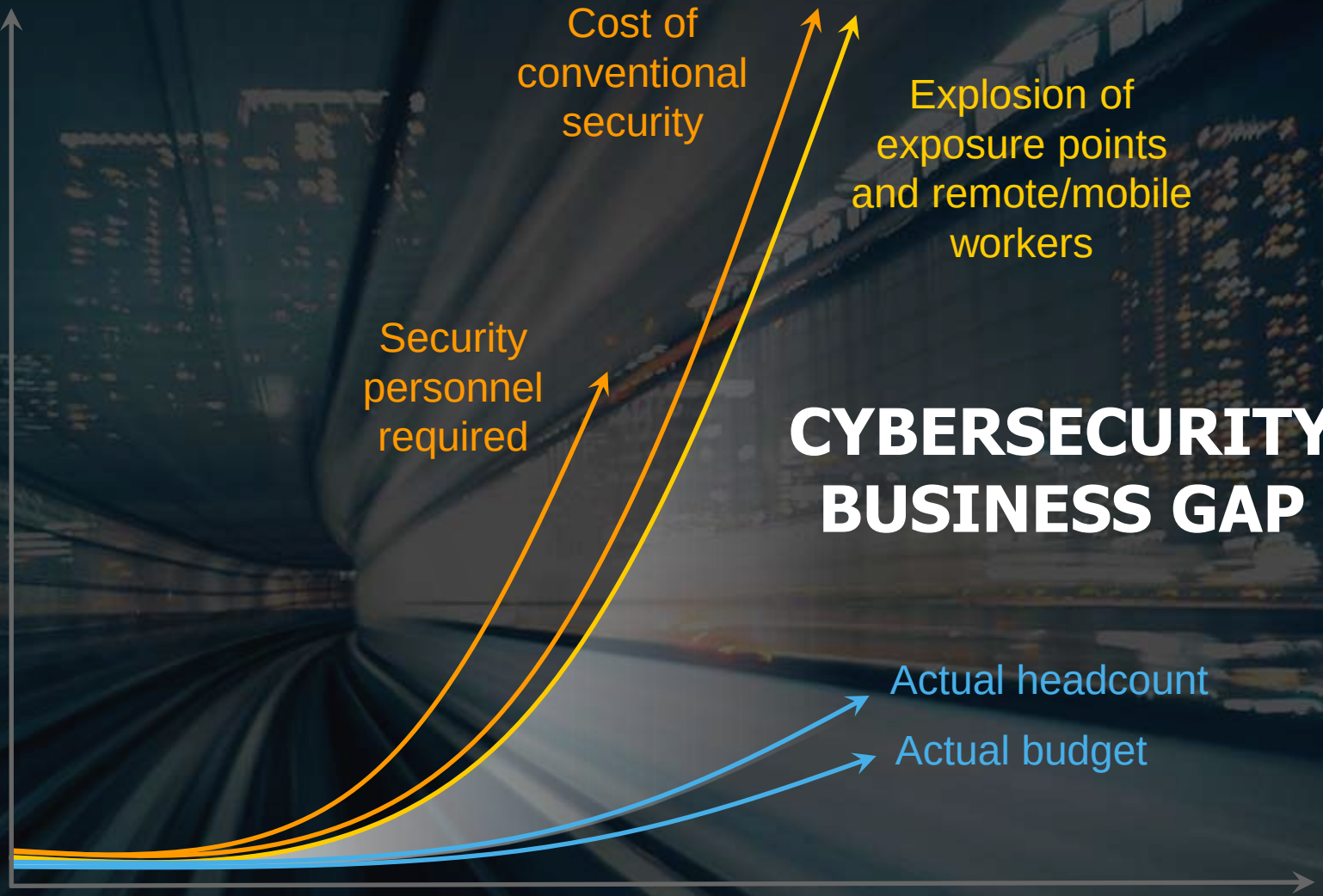
SONICWALL®

EL "GAP"…

Risk escalates with the explosion of exposure points and remote/mobile workers

Cost becomes prohibitive and the shortage of trained personnel becomes more acute

Constrained resources can't keep up

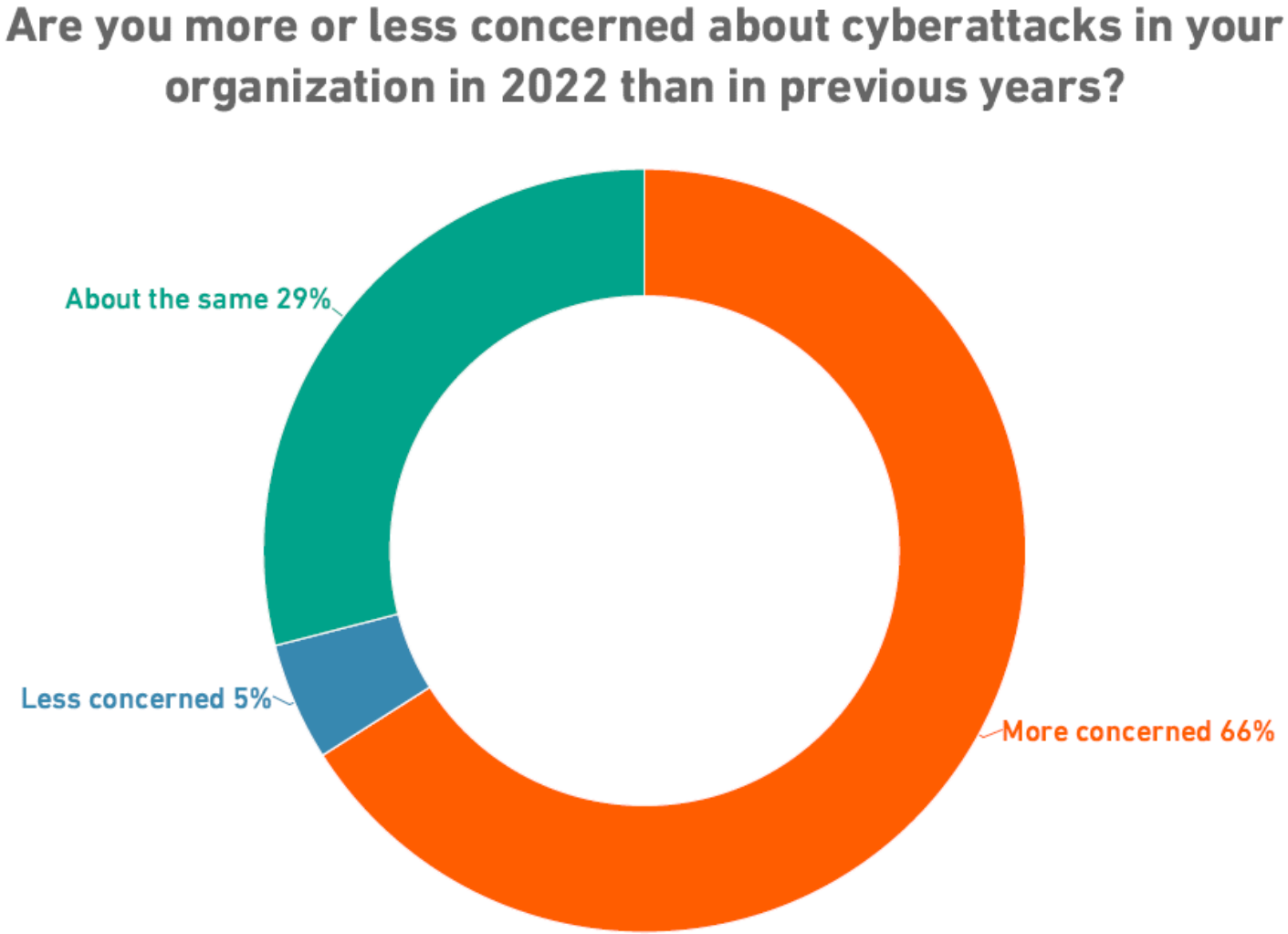


SONICWALL®

TODO VA A PEOR... ¿Qué piensan los CIOs?

66%

Todo va a peor… Y los CIOs así lo piensan…

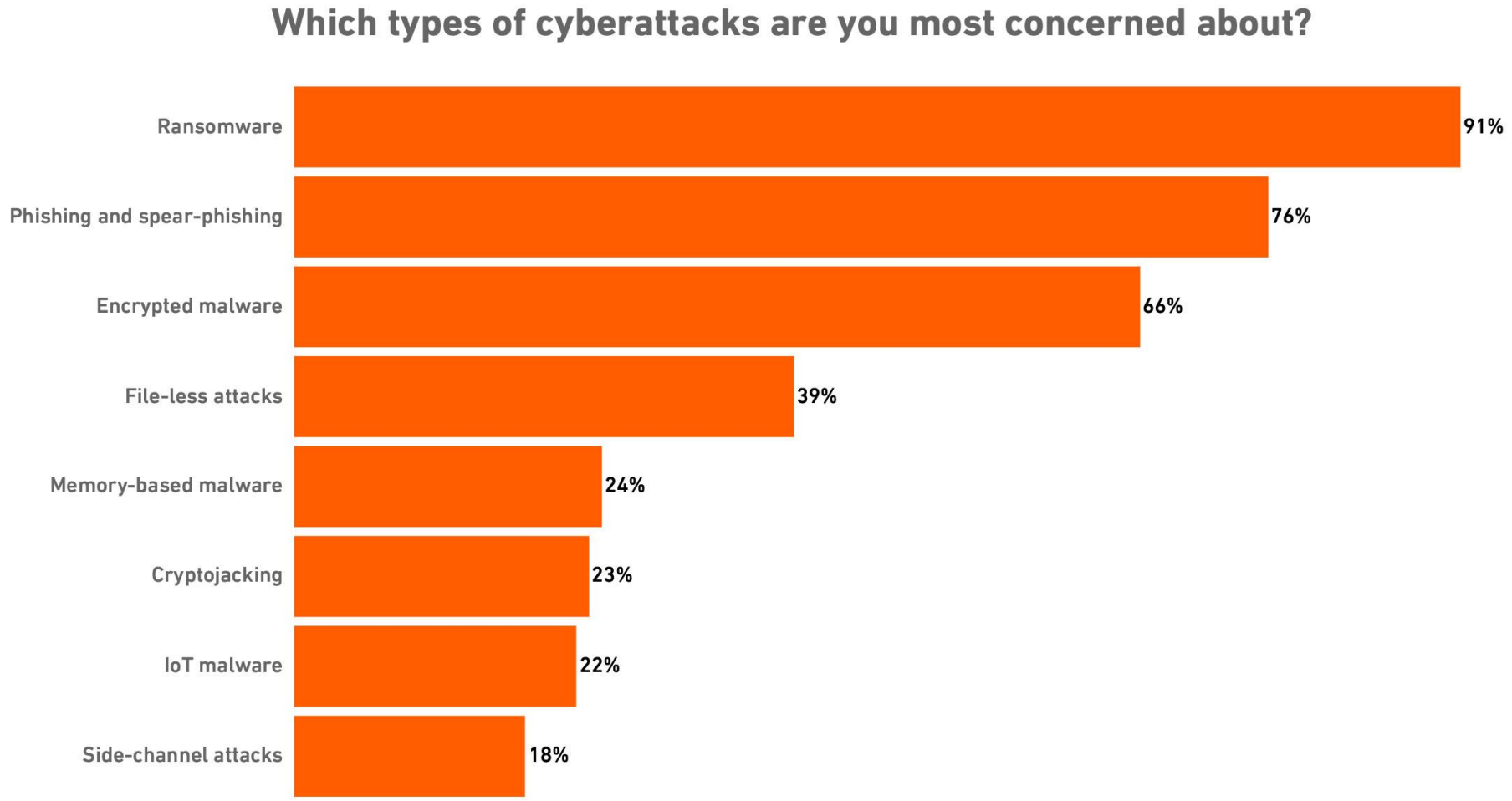


Source: 2022 SonicWall Threat Mindset Survey.

Y EL RANSOMWARE PREOCUPA A TODOS

91%

Despite a decline in overall volume in 2022, ransomware was chosen by **91%** of respondents as their top concern in 2022.



Durante los últimos 12 meses, el 57% de todas las organizaciones de 100 a 5.000 usuarios sufrieron uno o más ciberataques — y cada ataque costó de media unos $5,34 millones

Cambio de Paradigma

Modelo “Bastión” a uno más parecido a un “Aeropuerto”

SONICWALL

#KnowTheThreats

GET THE LATEST CYBER INTELLIGENCE

Download the mid-year update to the **2024 SonicWall Cyber Threat Report** to gain exclusive insight into cybercrime's shifting frontlines and how changing behaviors may impact your organization.

DOWNLOAD THE REPORT

SonicWall.com/ThreatReport

SONICWALL

SONICWALL CAPTURE LABS THREAT NETWORK

1.1m+
Global Sensors

215+
Countries & Territories

24x7x365
Monitoring

<24hrs
Threat Response

140k+
Malware Samples Collected Daily

28m+
Malware Attacks Blocked Daily

Estimulados por los acontecimientos geopolíticos y por un renovado cibercrimen, los protagonistas de las ciberamenazas en 2022/23 han mostrado una sutileza sin precedentes

Este informe de Ciberinteligencia elaborado por el equipo “SonicWall Capture Labs Threat Research” ofrece una información elaborada a partir de los cientos de miles de sensores distribuidos por todo el mundo.

SONICWALL®

2023 Trends and developments

▲11%

MALWARE

▲1BN

CRYPTOJACKING

MORE THAN DOUBLED

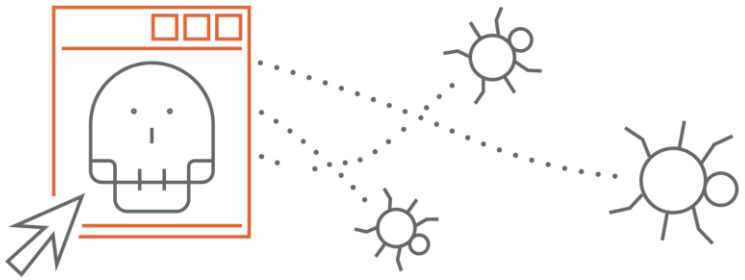
ENCRYPTED THREATS

APPROX 240K PER SECOND

INTRUSION ATTEMPTS

3RD HIGHEST YEAR ON RECORD

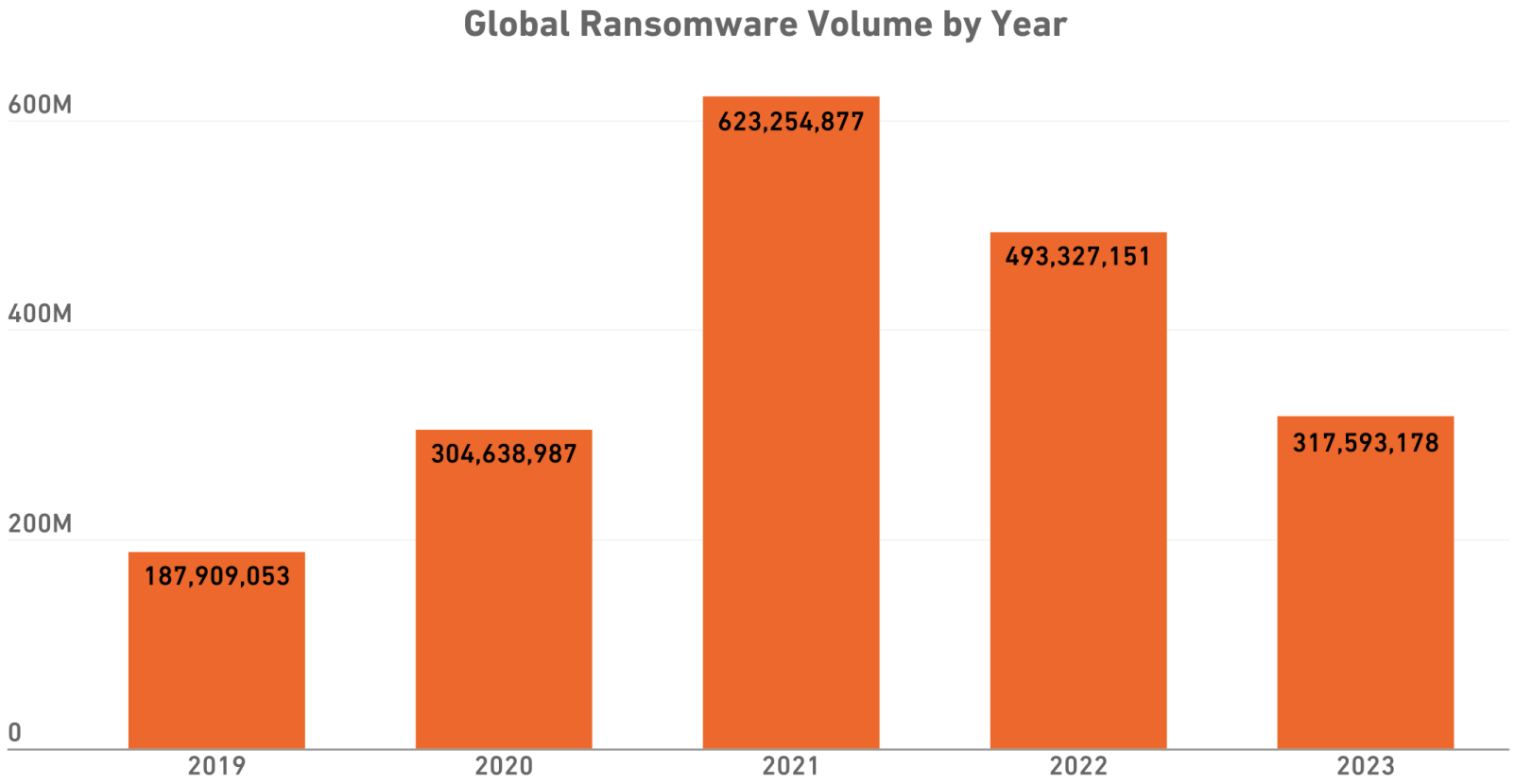
RANSOMWARE



SONICWALL®

Global ransomware volume per year

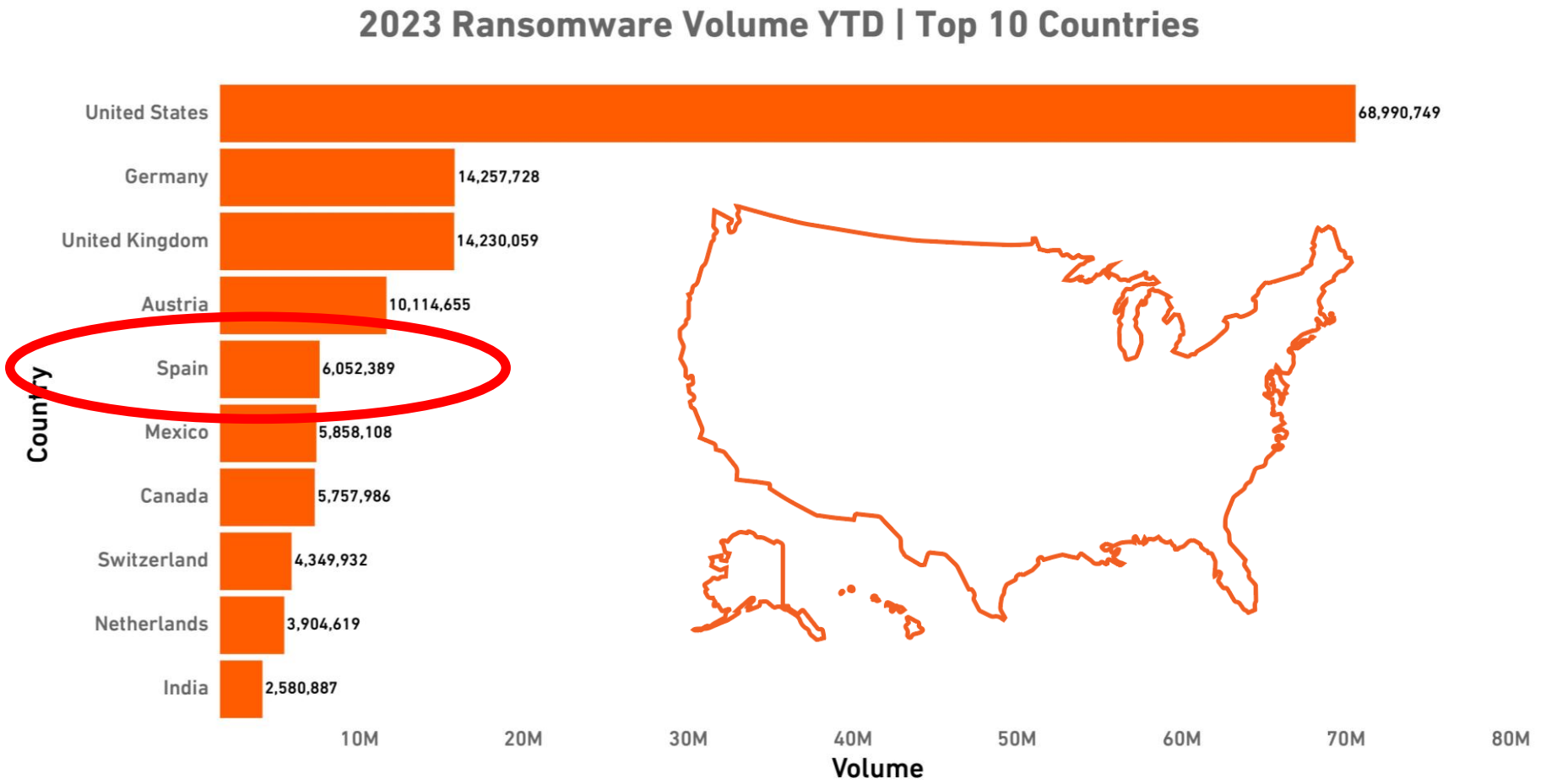
317.6 million ransomware attacks were recorded, a decrease of 36% year-over-year — but the third-highest total on record.



RANSOMWARE: TOP 10 COUNTRIES

While the U.S. still has the highest ransomware attack volume, other countries are continuing to catch up:

This year, the No. 2 country (Germany) saw 21% of the total ransomware recorded in the U.S. Last year, that percentage was 15%. And in 2021, it was just 6%.



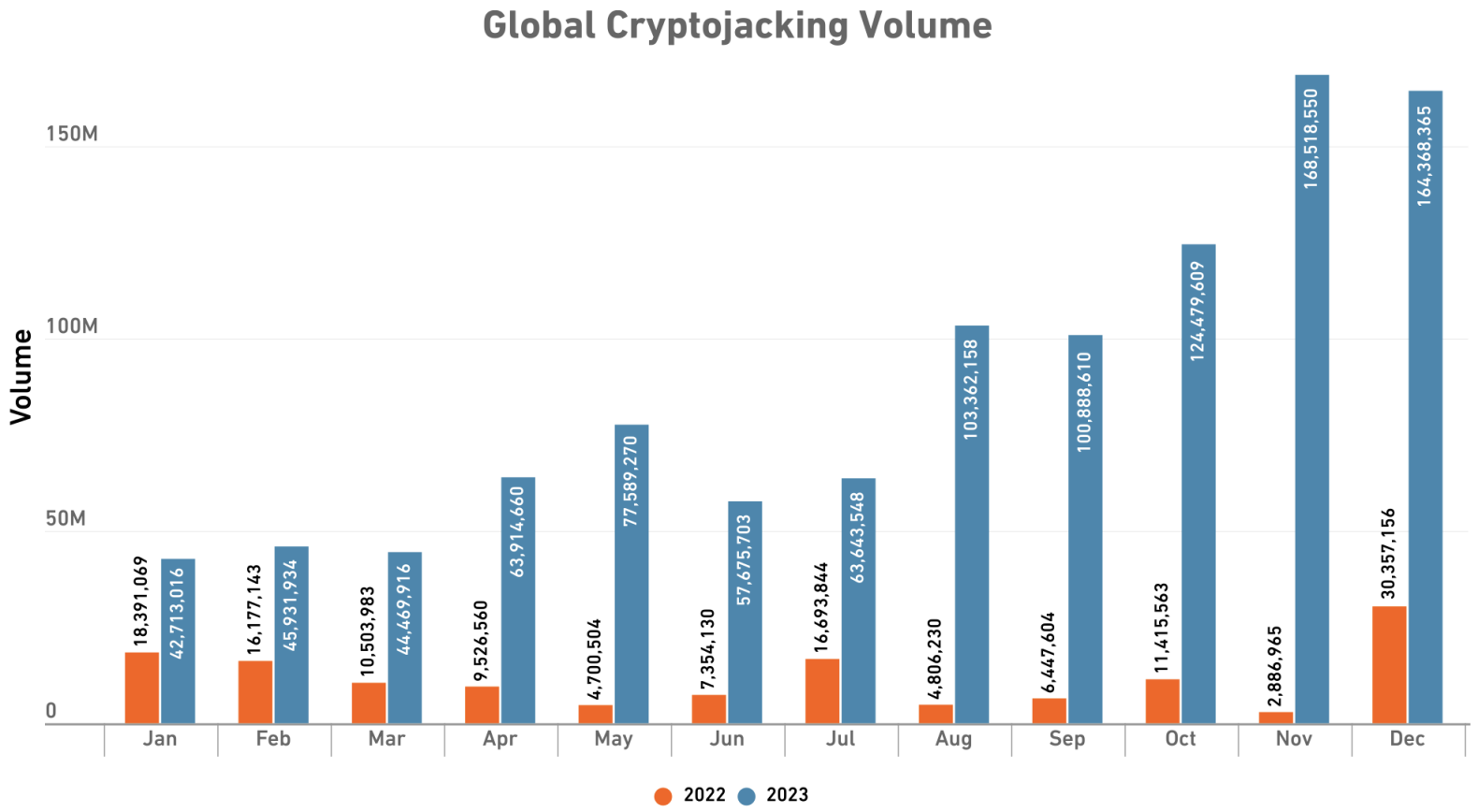
CRYPTOJACKING

Why It's Dangerous (And Why It's Climbing)

Cryptojacking hits had passed 2022's full-year total by early April. By the end of the year, SonicWall had recorded 1.1 billion cryptojacking hits—a 659% increase over 2022.

All regions showed an increase:

- APAC: +87%
- LATAM: 116%
- NOAM: +596%
- Europe: +1,046%



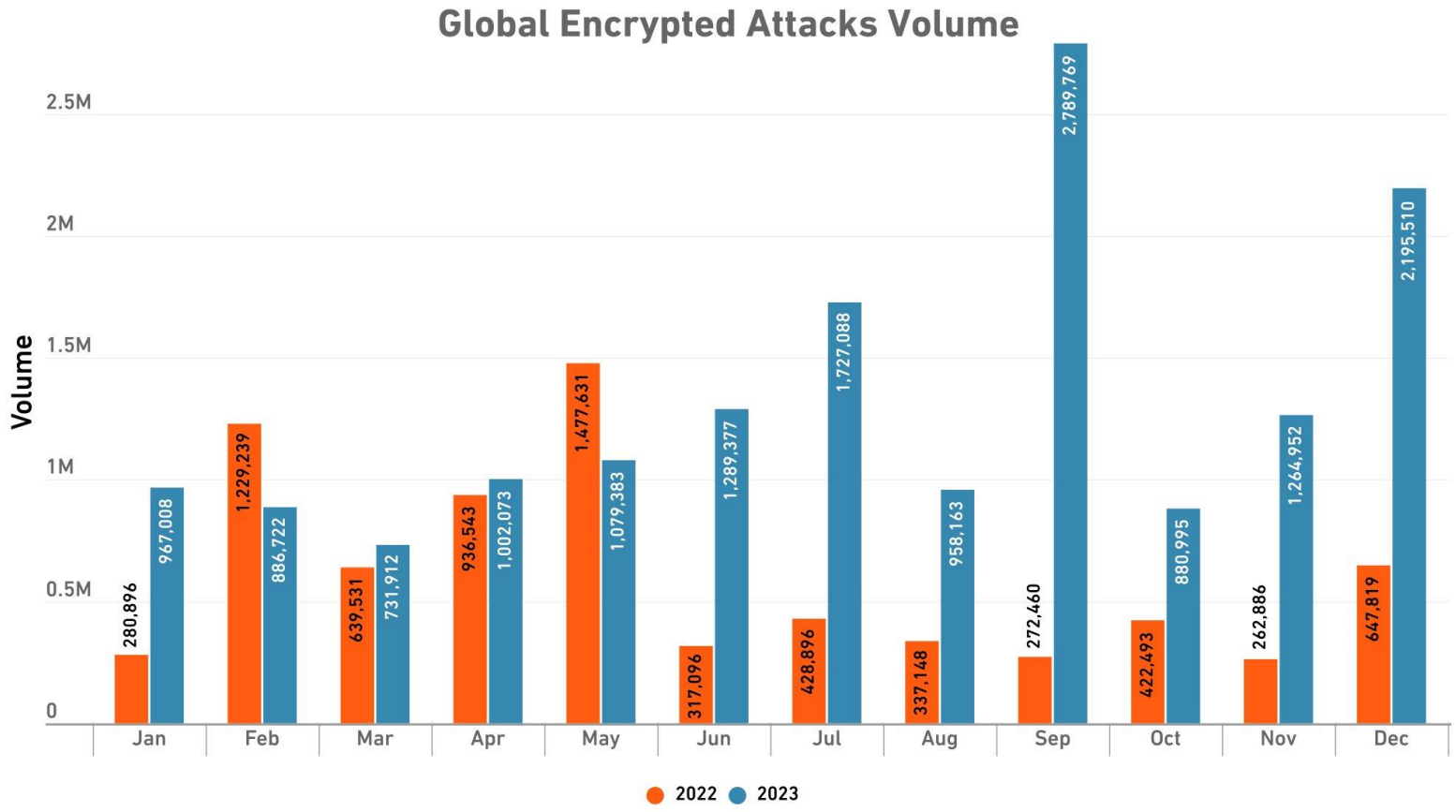
CRYPTOJACKING: ¿ES PELIGROSO?

- Es un **uso no autorizado** de los recursos de la empresa para otros fines externos.
- Normalmente se usa **software Open Source**: XMRing.
  - Este software es de fácil uso y suele estar "**troyanizado**"por malware, y ya no tiene tan buenas intenciones
- **Coste energético** y gran huella de carbono:
  - Entre 2020-21 se calculó el gasto enérgético del bitcoin con la producción de 190 centrales de gas
- No sólo eso, el sobrecalientamiento de los equipos reduce su **vida útil** –> Sobrecoste a las empresas.

ENCRYPTED THREATS

Encrypted Attacks More Than Double

SonicWall Capture Labs threat researchers observed 15.7 million encrypted attacks, a 117% increase year over year.



Tráfico encriptado

74% **Del tráfico en internet (2023) está cifrado (HTTPS)**

▲300%

EL AUMENTO DE LAS AMENAZAS CIFRADAS LLEGA A LOS TRES DÍGITOS

Julio 2022 contra julio de 2023, tiene un incremento de un 300%. Es el mayor incremento visto nunca en los laboratorios de SonicWall. El uso del tráfico TLS como túnel de entrada en las organizaciones se ha popularizado y el malware que lo utiliza crece exponencialmente.

HTTPS: Una avenida para el cibercrimen

Y otros cambios en camino...

UDP

QUIC

HTTPA

DNS over HTTPS (DoH)

Cambios que pueden ser también las “Ardenas” para el cibercrímen

Es el eterno dilema entre…

¿Privacidad o Ciberseguridad?

¿Cuál es el importante…? Lo dejo a cada uno

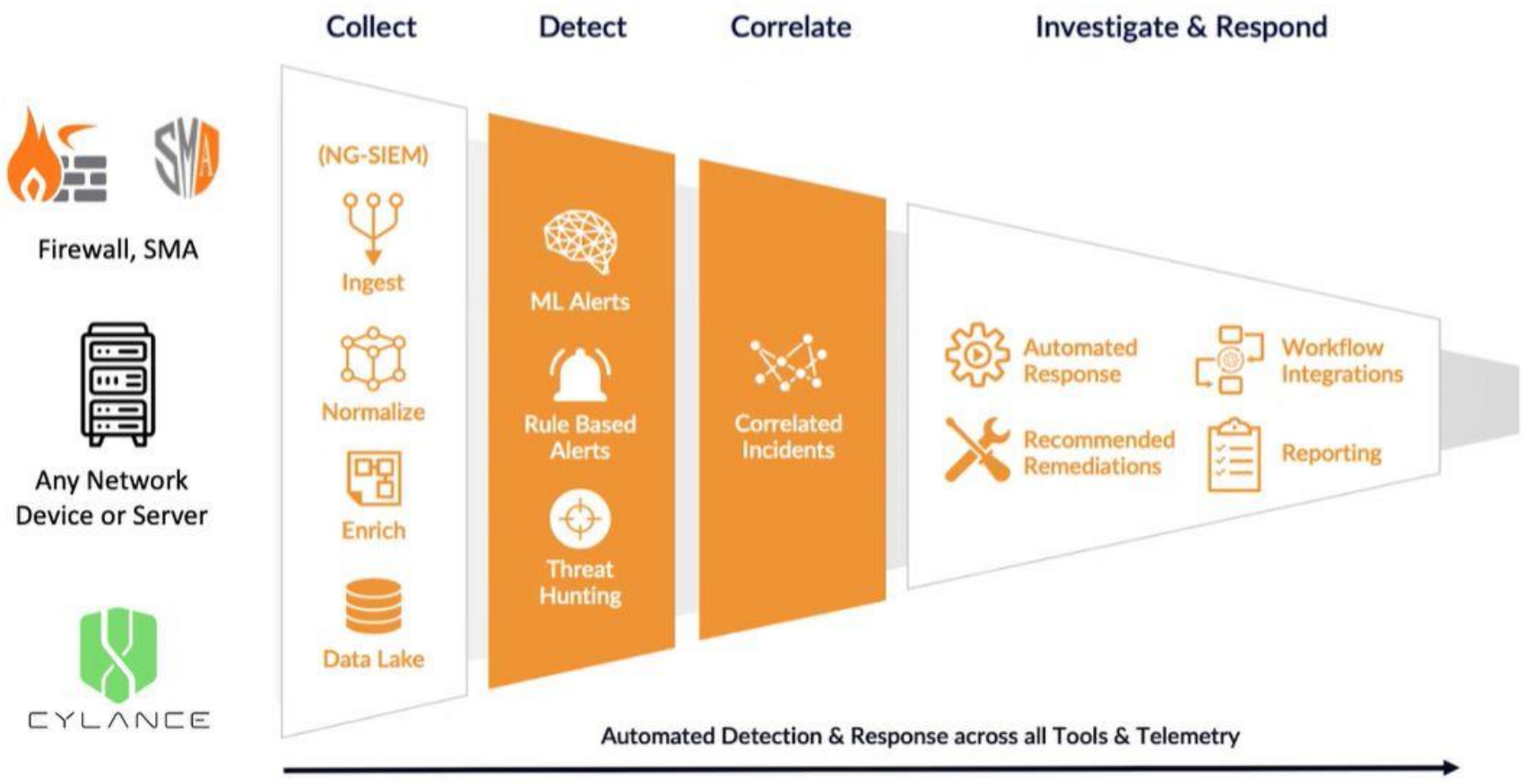
1 Defensa por capas

- Ataques cada vez más sofisticados
- Explosión del número de ataques
- Muchos de corte desconocido: Nunca ha habido tantas variantes desconocidas: 465K detectadas en 2022.
- Ransomware + focalizado
- No sabemos cómo ni cuándo nos van a atacar.
- La única solución: una defensa en profundidad, por capas, coordinada y **compartimentada**

SOC-aaS (Managed SIEM)

SIEM solution (backed by 24/7 SOC) provides protection and centralized visibility for greater control over your security

- Ingest logs from Firewall, SMA, Servers and other devices.
- Improve the accuracy of detecting security events, and mitigate the risk of data exfiltration
- Automatically piece together complex attacks across cloud, endpoint, network, user & applications



Visibilidad central para detectar y responder

2

- La defensa por capas precisa de coordinación
- El uso de la IA es una ayuda también para la detección en tiempo real.
- Hay que estar preparado para responder y aislar partes de la red.
- Monitorización para evitar Account Takeovers (robo de identidades) -> Identificar usuarios: ¿Eres quien dices ser? Uso de Zero-Trust

Consolidación en el mercado

Los clientes piden un "One Stop Shop" y los vendors estamos en fase de "consolidación"

Pasado

Explosión de vendors

Hoy

Empieza la integración

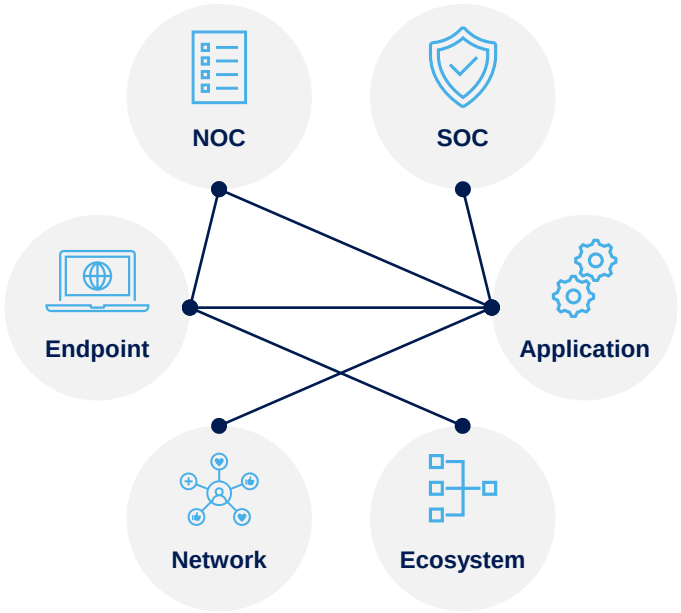
Futuro

Suites, AI y 3rd parties

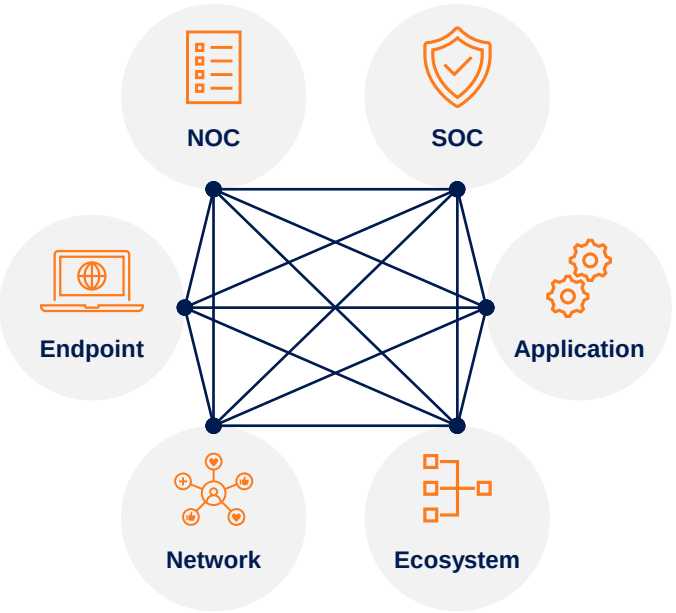
Journey to SOC Automation Maturity

3000+ Vendors

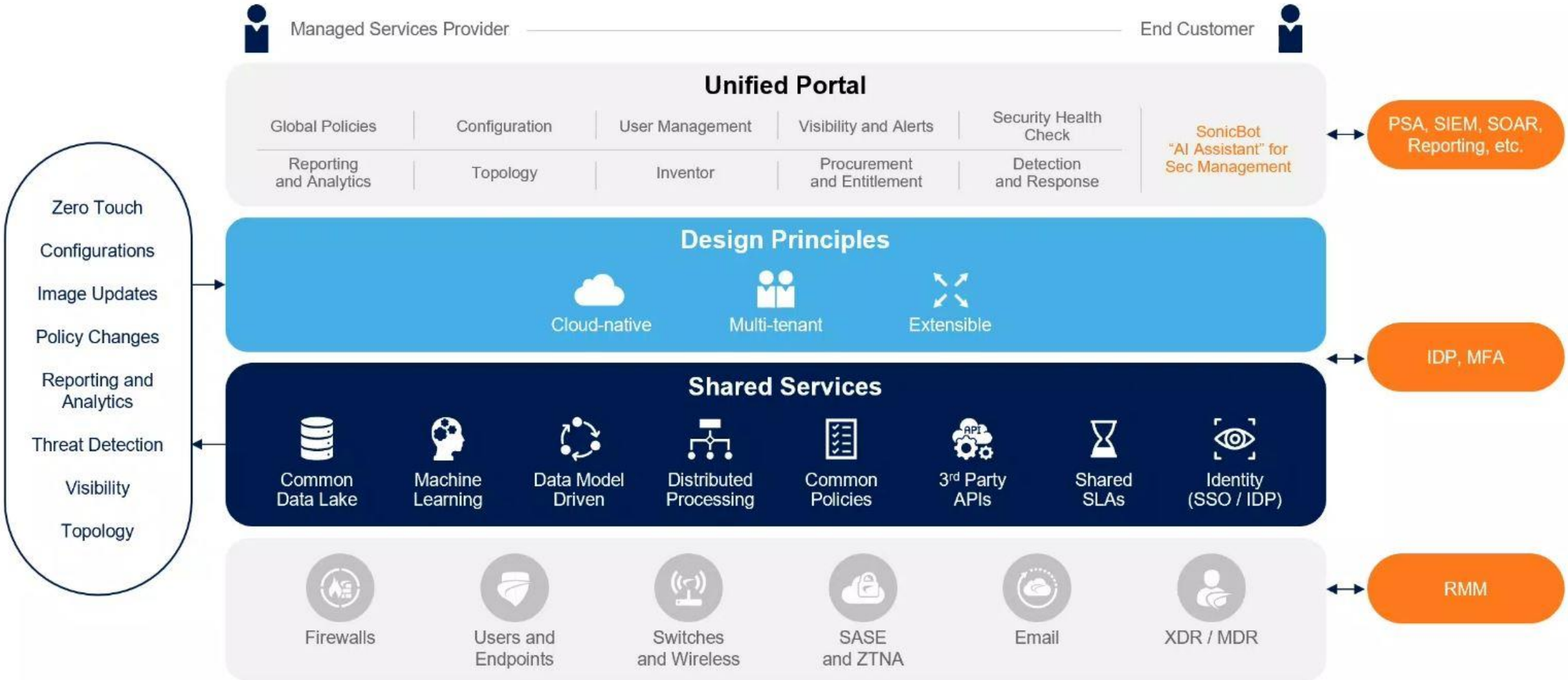
50+ Vendors



3 – 5 Platforms



SonicWall Unified Platform

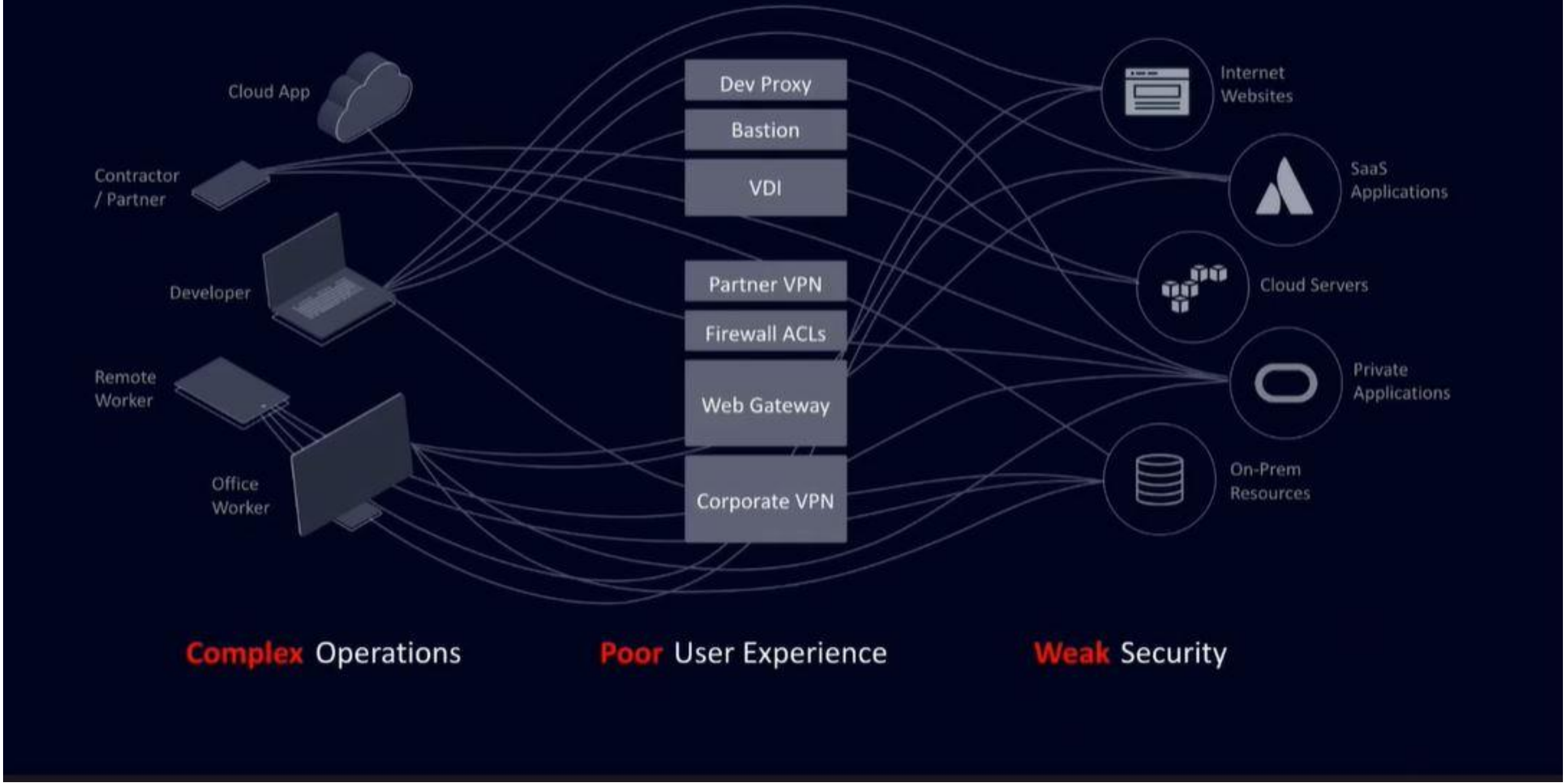


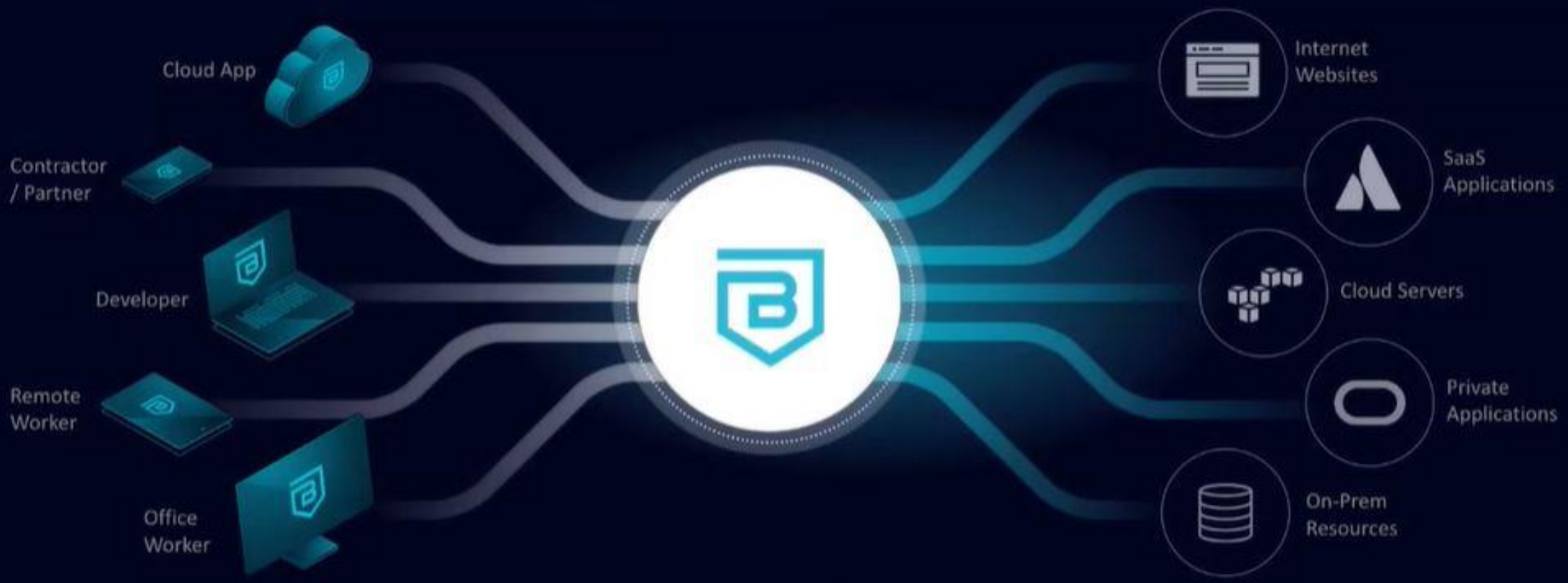
3 Detectar lo desconocido

- Uso de **Inteligencia artificial** para la detección desde hace décadas
- Miles de variantes de malware con y sin fichero (465K en 2022)
- Más del 70% tráfico encriptado
- El uso de sandbox Avanzado, con multiples estrategias, es fundamental

4 Acceso remoto seguro

- Doble autenticación (2FA):
  - Algo que sabes, algo que tienes, algo que eres
- Tunnel all Mode vs Split Tunnel.
- Always-on VPN
- Zero trust – Mínimo privilegio – Desconfianza máxima.
- Endpoint control: ¿Es de confianza?
- Acceso compartimentado


Cloud App
Contractor / Partner
Developer
Remote Worker
Office Worker
Dev Proxy
Bastion
VDI
Partner VPN
Firewall ACLs
Web Gateway
Corporate VPN
Internet Websites
SaaS Applications
Cloud Servers
Private Applications
On-Prem Resources
Complex Operations
Poor User Experience
Weak Security



Simplified Operations

Great User Experience

Robust Security

5 TCO y costes disruptivos

- Inspección de Gigabit a coste razonable
- Licenciamiento: cada uno del nodo HA o solo 1.
- Tecnología probada durante años en PYMES con IA y tecnología punta.

www.sonicwall.com

Email: smartinez@sonicwall.com
@smartinezh