**ACTUALIZACIÓN DE MEDIADOS DE AÑO**

# INFORME DE CIBERAMENAZAS 2020 DE SONICWALL


MID-YEAR UPDATE | JULY 2020

2020 SONICWALL
CYBER THREAT REPORT

Cyber threat intelligence for navigating the new business normal

SONICWALL

www.sonicwall.com | @SonicWall

**OBTENGA LA ACTUALIZACIÓN »**

**#Conocerlasamenazas**

## EN LOS ÚLTIMOS SEIS MESES,

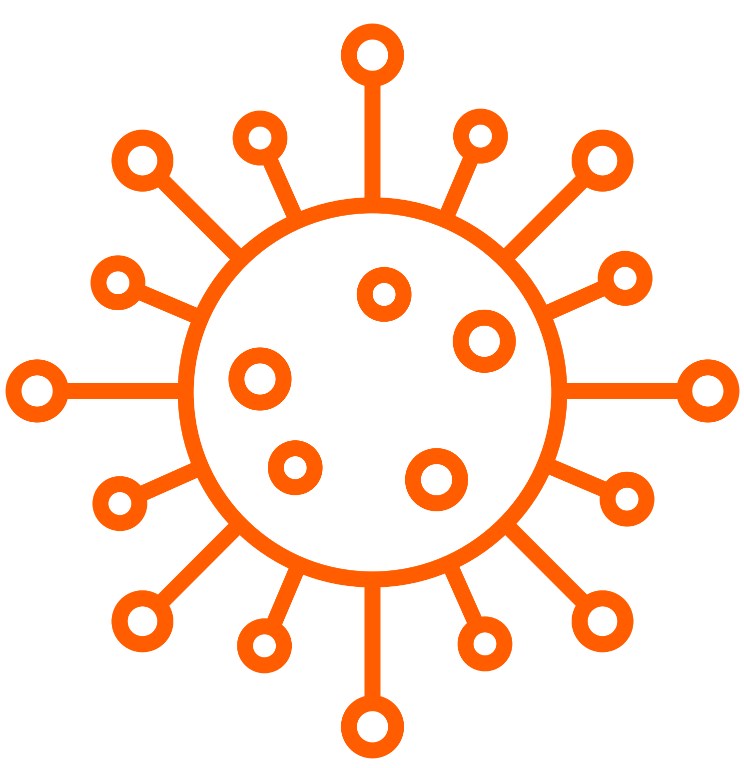
a medida que la pandemia de COVID-19 se extendía por todo el mundo, hemos sido testigos de cambios que pensábamos que tardarían décadas, pero que se han producido prácticamente de la noche a la mañana.

Si bien la perturbación histórica ha sido difícil para las empresas y los gobiernos, ha supuesto una oportunidad para los ciberdelincuentes.

**121,4 m**

## RANSOMWARE MÁS QUIRÚRGICO QUE NUNCA.

A pesar del descenso del *malware* total (-33 %), el *ransomware* sigue siendo la carga útil preferida por los ciberdelincuentes. **Los ataques de ransomware aumentaron un 20 % en la primera mitad de 2020 a nivel mundial** y se dispararon un 109 % en Estados Unidos.



## SACAR PROVECHO DE LA PANDEMIA.

SonicWall comenzó a detectar ataques, estafas y *exploits* basados específicamente en la COVID-19 el 4 de febrero y, desde entonces, ha identificado **al menos 20 tipos diferentes de ataques** en casi todas las categorías, como:

- ✓ MALWARE
- ✓ RANSOMWARE
- ✓ CRIPTOMINEROS
- ✓ TROYANOS
- ✓ RAT
- ✓ SPAM
- ✓ SCAREWARE Y OTROS

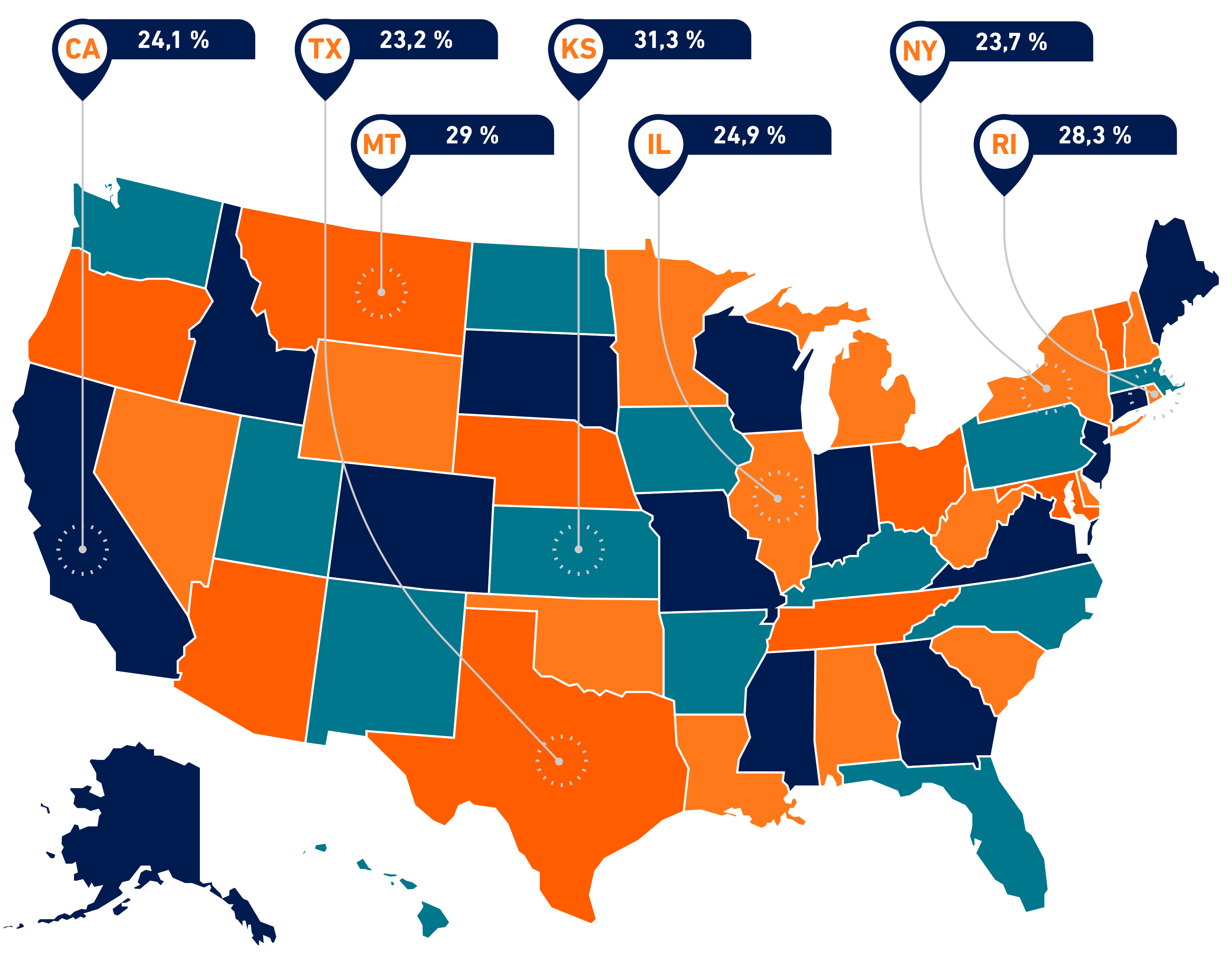
> **“Era solo cuestión de tiempo que un Estado nación recurriera a la ciberdelincuencia para influir o controlar la atención médica global durante un momento de gran necesidad.”**
>
> *BILL CONNER | PRESIDENTE Y CEO | SONICWALL | NEWSWEEK INTERNATIONAL, 16 DE JULIO DE 2020*

## ¿CORRE SU ESTADO EL RIESGO DE SUFRIR UN CIBERATAQUE?

En Estados Unidos, California tenía, con diferencia, el mayor número de ataques de *malware*, con 304,1 millones en total. Pero no es el estado con más riesgo, ni siquiera está en la primera mitad.

De hecho, es más probable que una organización encuentre *malware* en Kansas, donde casi un tercio (31,3 %) de los sensores de SonicWall registraron un ataque.

**% de sensores de SonicWall que registraron ataques de malware por estado**

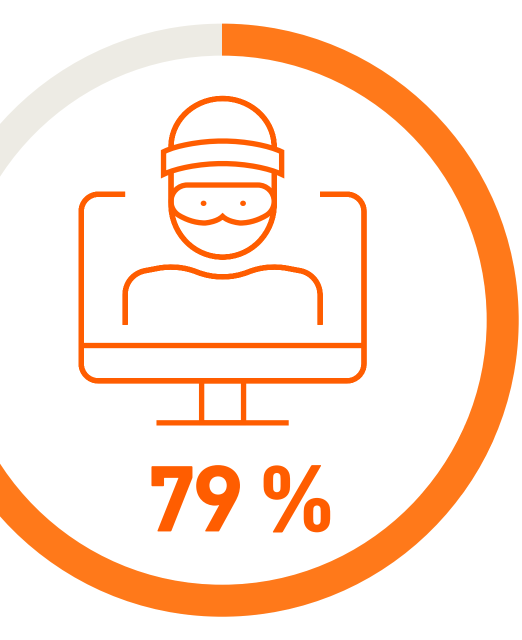


**IOWA** 28,1 %
**HAWAII** 27,7 %
**WEST VIRGINIA** 27,4 %
**VERMONT** 27,2 %

**IDAHO** 27,2 %
**LOUISIANA** 27,2 %
**FLORIDA** 26,7 %
**VIRGINIA** 26,6 %

**OREGON** 26,5 %
**NEW MEXICO** 26,4 %
**MICHIGAN** 26,3 %
**NEBRASKA** 26,3 %

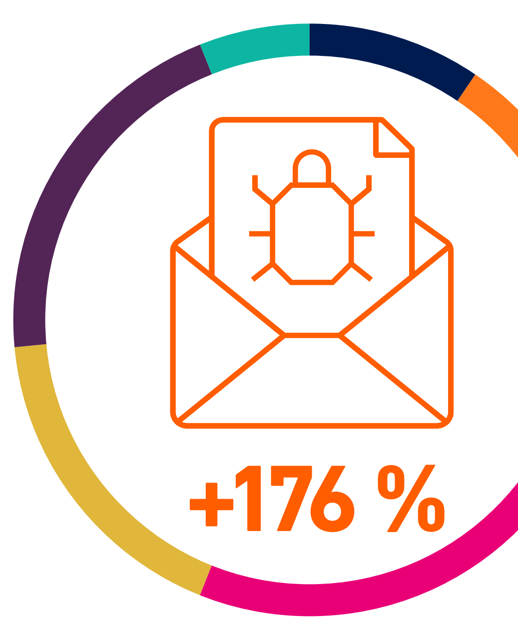
**NEW JERSEY** 26,3 %
**PENNSYLVANIA** 26,1 %
**NEVADA** 26 %
**MARYLAND** 26 %



## EL RANSOMWARE ES UNA PRIORIDAD.

Cuando se les preguntó qué tipo de ciberataques influyeron en su decisión de adquirir un firewall TZ de SonicWall, el **79 % de las organizaciones encuestadas** señalaron el «ransomware».

*FUENTE: ENCUESTA TECHVALIDATE A 250 CLIENTES SOBRE SEGURIDAD DE REDES DE SONICWALL*



## ¿QUÉ SE OCULTA EN LOS ARCHIVOS DE OFFICE?

Cada vez hay más malware oculto en archivos de confianza de Office. En la primera mitad de 2020, SonicWall registró un aumento del 176 % en nuevos archivos de Office maliciosos. **Consulte el informe completo para ver el análisis>**

## #Teletrabajo

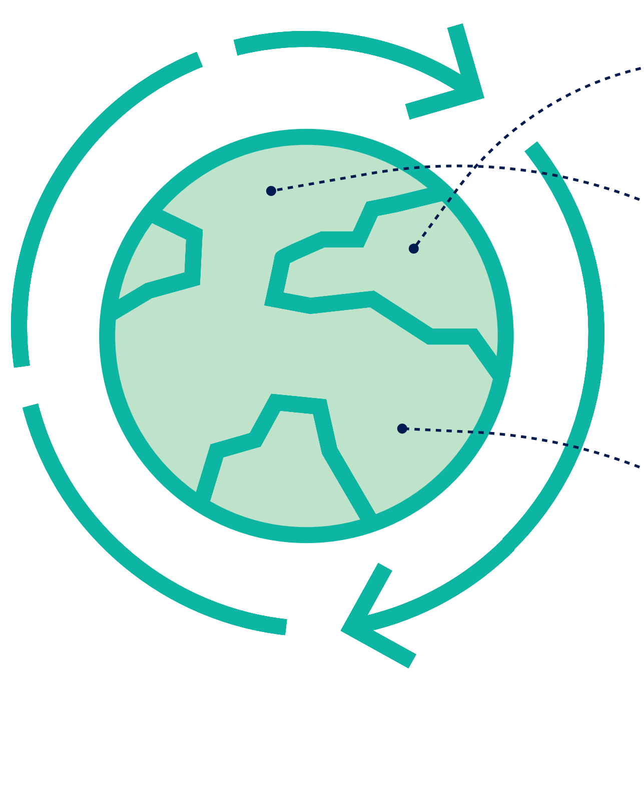
## AUMENTO DE LOS ATAQUES DE IoT

Desde enero, SonicWall ha registrado 20,2 millones de ataques de IoT, un aumento del 50 % en lo que va de año. Si el patrón actual se mantiene, los ataques de IoT totales superarán los niveles de 2018 y 2019. Si los dispositivos IoT no se controlan, pueden abrir las puertas a los ciberdelincuentes a lo que de otro modo podría ser una organización bien protegida.

**LOS ATAQUES DE IoT HAN AUMENTADO UN 50 %**

**EN LO QUE VA DE AÑO**

## TENDENCIAS MUNDIALES DE CIBERATAQUES



**41,4 m**

**Ataques de *cryptojacking***

**+19 %**

**Eventos de intrusión**

**1de cada12**

**Clientes sufrió un ataque cifrado**

## PROSPERE EN LA NUEVA NORMALIDAD EMPRESARIAL.


MID-YEAR UPDATE | JULY 2020

2020 SONICWALL
CYBER THREAT REPORT

Cyber threat intelligence for navigating the new business normal

SONICWALL

www.sonicwall.com | @SonicWall

Visite **SonicWall.com/ThreatReport** para descargar la actualización gratuita de mediados de año del Informe de ciberamenazas 2020 de SonicWall. Obtenga la información más reciente sobre ciberamenazas para abrirse camino en la nueva normalidad empresarial.

**OBTENGA LA ACTUALIZACIÓN »**

**#Conocerlasamenazas**

SONICWALL
CAPTURE LABS

SonicWall.com

*Como mejor práctica, SonicWall optimizó de manera rutinaria sus metodologías para la recopilación, el análisis y la generación de informes de datos. Esto incluye ajustes en la limpieza de datos, cambios en las fuentes de datos y una consolidación de la información sobre amenazas. Las cifras publicadas en informes previos pueden haberse ajustado para períodos de tiempo, regiones o industrias diferentes.

Infographic-2020ThreatReportMidYear-COG-2452