

# SONICWALL CYBER THREAT REPORT 2020



#KnowTheThreats

UPDATE ABRUFEN >>

## IN DEN VERGANGENEN SECHS MONATEN

haben wir infolge der weltweit verheerenden Auswirkungen der COVID-19-Pandemie schlagartig Veränderungen erlebt, die sich normalerweise erst über Jahrzehnte hinweg entwickeln würden.

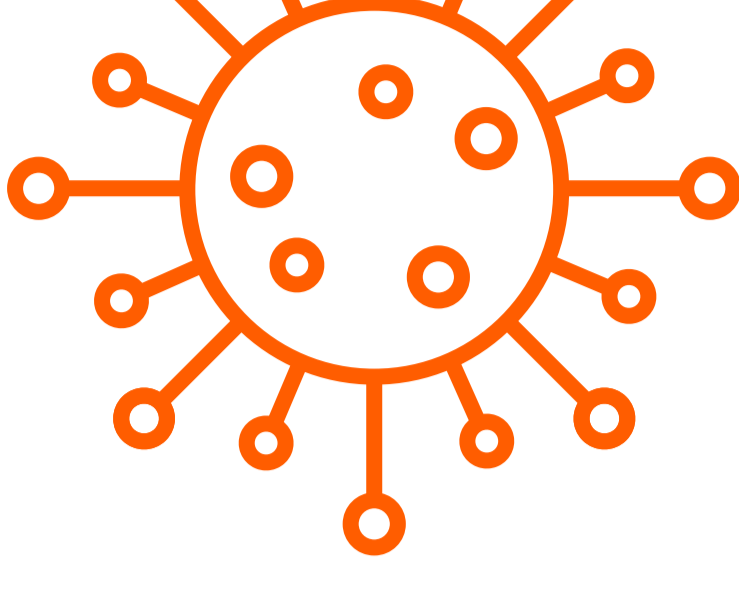
Während diese beispiellose Disruption Unternehmen und Regierungen vor große Herausforderung gestellt hat, erwies sich für Cyberkriminelle als Glücksfall.

# 121,4 Mio.

## RANSOMWARE-ANGRIFFE PRÄZISER ALS JE ZUVOR.



Trotz der insgesamt rückläufigen Malware-Aktivitäten (-33 %) ist Ransomware nach wie vor das bevorzugte Werkzeug von Cyberkriminellen. **Ransomware-Angriffe sind im ersten Halbjahr 2020 weltweit um 20 % gestiegen** und haben in den USA einen Höchststand von 109 % erreicht.



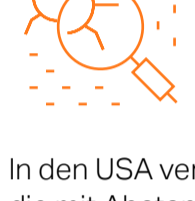
## PROFITIEREN VON DER PANDEMIE.

Bereits am 4. Februar 2020 sahen die Experten von SonicWall eine Flut von Angriffen, Scams und Exploits, die speziell auf COVID-19 gemünzt waren. Seither wurden **mindestens 20 verschiedene Arten von Angriffen** in fast jeder Kategorie verzeichnet, darunter:

- MALWARE
- RANSOMWARE
- CRYPTOMINERS
- TROJANER
- RATs
- SPAM
- SCAREWARE UND ANDERE

**„Es war damit nur eine Frage der Zeit, bis ein Nationalstaat in dieser schwierigen Zeit auf Cyberkriminalität zurückgreifen würde, um das globale Gesundheitswesen zu beeinflussen oder zu kontrollieren.“**

BILL CONNER | PRESIDENT UND CEO | SONICWALL | NEWSWEEK INTERNATIONAL, 16. JULI 2020

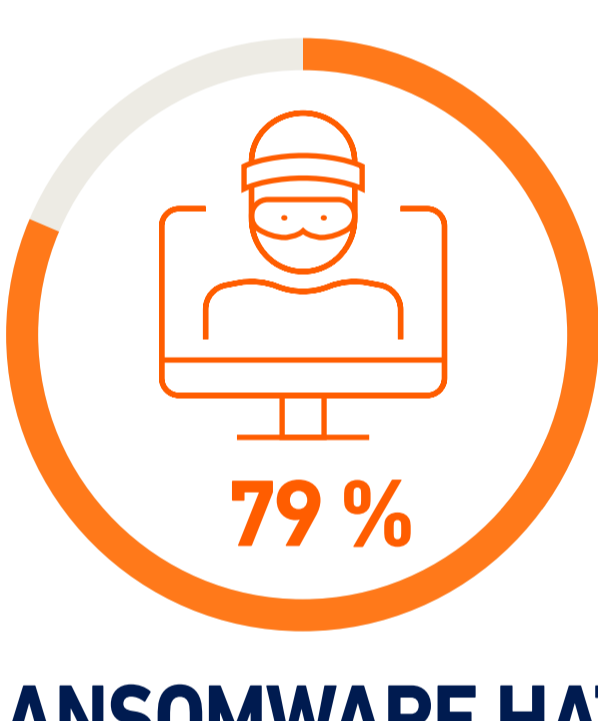
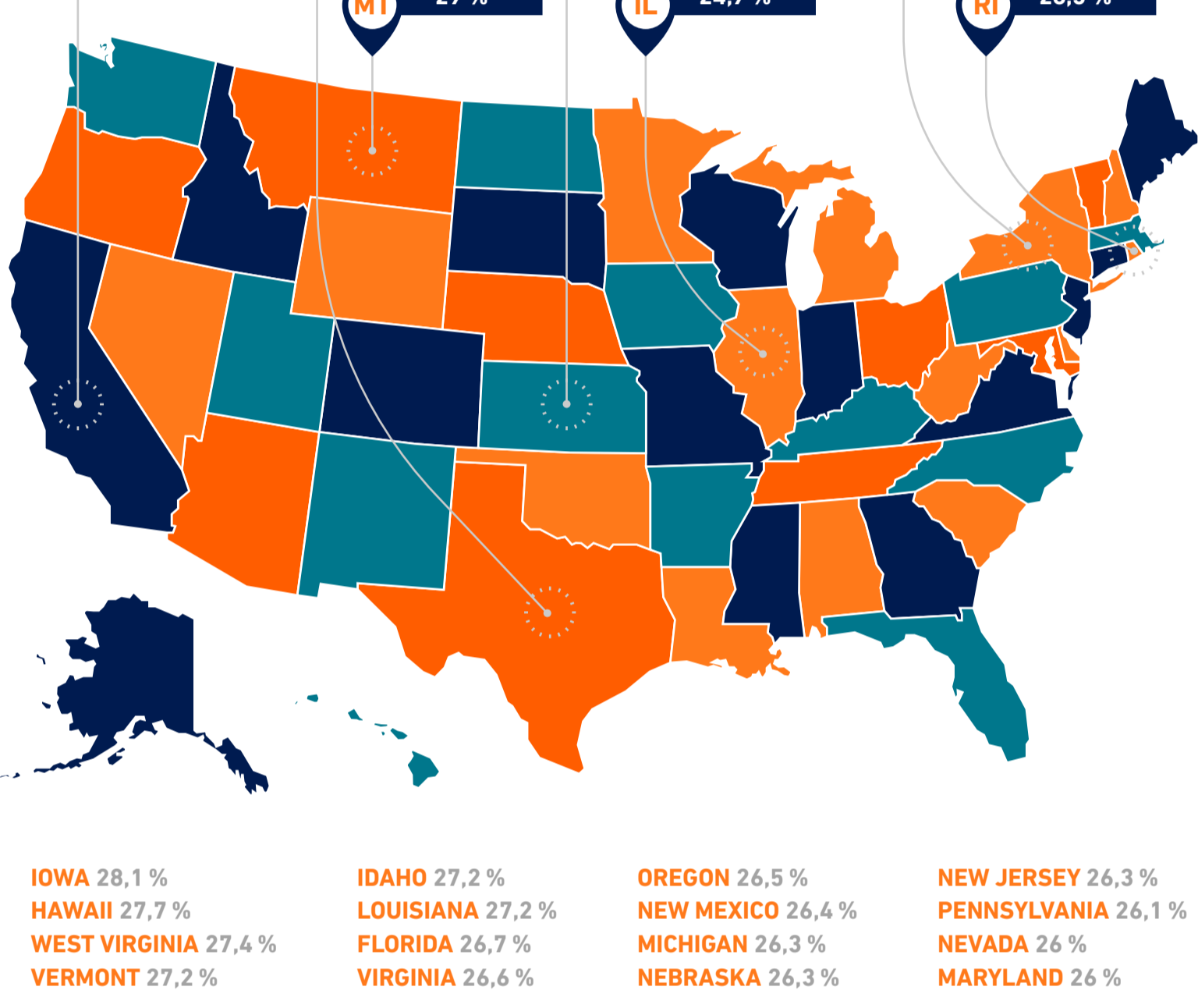


## IST IHR STAAT DURCH EINEN CYBERANGRIFF GEFÄHRDET?

In den USA verzeichnete Kalifornien mit **304,1 Millionen** die mit Abstand größte Anzahl an Malware-Treffern. Aber Kalifornien ist nicht der risikoreichste US-Bundesstaat und liegt auch nicht in der oberen Hälfte.

Tatsächlich sind Organisationen in Kansas eher Malware-Angriffen ausgesetzt, was sich darin zeigt, dass knapp ein Drittel (31,3 %) der SonicWall Sensoren einen Treffer registrierte.

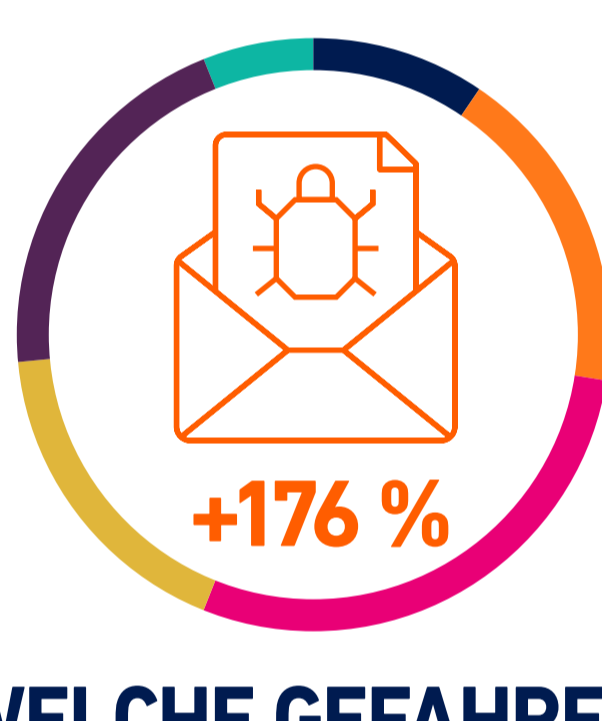
### Von SonicWall Sensoren registrierte Malware-Treffer nach US-Bundesstaat (%)



## RANSOMWARE HAT OBERSTE PRIORITÄT.

Auf die Frage, welche Art von Cyberangriffen ihre Entscheidung zum Kauf einer SonicWall TZ-Firewall beeinflusst hat, antworteten **79 % der befragten Organisationen** mit „Ransomware“.

QUELLE: TECHVALIDATE-UMFRAGE UNTER 250 KÄUFERN VON NETZWERKSICHERHEITSPRODUKTEN VON SONICWALL



## WELCHE GEFAHREN LAUERN IN IHREN OFFICE-DATEIEN?

Immer mehr Malware wird erfolgreich in vertrauenswürdigen Office-Dateien versteckt. Im ersten Halbjahr 2020 verzeichnete SonicWall einen Anstieg von 176 % bei völlig neuen bösartigen Office-Dateien.

[Siehe vollständigen Bericht für eine Aufschlüsselung >](#)

## #WFH DRASTISCHER ANSTIEG BEI IoT-ANGRIFFEN

Seit Januar verzeichnetet SonicWall 20,2 Millionen IoT-Angriffe, das entspricht einem Anstieg von 50 %. Wenn sich dieser Trend fortsetzt, werden die IoT-Attacks das Angriffsvolumen von 2018 und 2019 übertreffen. Unkontrollierte IoT-Geräte können Cyberkriminellen eine offene Tür in eine vielleicht ansonsten gut gesicherte Organisation bieten.



## Globale Trends bei Cyberangriffen



## ERFOLGREICH IN DER NEUEN GESCHÄFTSNORMALITÄT.



Besuchen Sie [SonicWall.com/ThreatReport](https://SonicWall.com/ThreatReport), um das kostenlose Halbjahres-Update zum SonicWall Cyber Threat Report 2020 herunterzuladen. Erhalten Sie Einblick in die neuesten Cyber Threat-Informationen, die Ihnen helfen, sich in der neuen Geschäftsnormalität zurechtzufinden.

UPDATE ABRUFEN >>

#KnowTheThreats