RANSOMWARE HAT VERHEERENDE FOLGEN FÜR UNTERNEHMEN

WARUM UNTERNEHMEN EINE NEXT-GENERATION-FIREWALL MIT DER SONICWALL-MULTI-ENGINE-SANDBOX CAPTURE ADVANCED THREAT PROTECTION (ATP) BRAUCHEN.

187 %ige

Zunahme der weltweiten Ransomware-Angriffe seit Jahresbeginn bis Juli 2018.

Quelle: SonicWall Capture Security Center

14 SEKUNDEN

Bis Ende 2019 wird alle 14 Sekunden ein Unternehmen einen Ransomware-Angriff erleiden.

Quelle: Cybersecurity Ventures

Jede 6.

Organisation musste nach einem Angriff Ausfallzeiten von 25 Stunden oder mehr hinnehmen.

Quelle: CNNMoney

11,5 MILLIARDEN $

Schaden wird Ransomware bis Ende 2019 weltweit voraussichtlich verursachen.

Quelle: Cybersecurity Ventures

31 %

der von einer Sicherheitslücke betroffenen Verbraucher meinten, dass sie ihre Beziehung zur gehackten Organisation beendet haben.

Quelle: Ponemon Institute

Die **Capture ATP-Sandbox** ist dank mehrerer Engines in der Lage, selbst schwer zu fassende Malware abzuwehren, einschließlich Ransomware-Angriffe, die Unternehmen teuer zu stehen kommen können.

Sandboxing: Eine Sandbox untersucht innerhalb kürzester Zeit verdächtige Dateien, um Malware und Ransomware zu stoppen, bevor sie in Ihr Netzwerk eindringen.

SonicWall Real-Time Deep Memory Inspection™ stoppt Zero-Day-Angriffe, bösartige PDFs und Microsoft-Office-Dateien und sogar chipbasierte Spectre-, Meltdown- und Foreshadow-Exploits.

Capture ATP mit RTDMI™ identifizierte 2018 bisher über 12.300 brandneue Angriffsvarianten.

Eine **SonicWall-Next-Generation-Firewall** erhielt im NSS Labs-Vergleichstest 2018 die Bewertung **„Recommended“**.

SONICWALL®