

Innovate more. Fear less!

SonicWall Corporate & Security Solutions Overview

Cosmin Vilcu

ASBIS

Sarajevo

October, 2018

SONICWALL®



FEARLESS.

Achieve more than just breach detection.

We can help you achieve automated real-time breach prevention that protects your organization from today's most pervasive cyber threats.

Securing your journey to the cloud, software as a service and digital business future.

Want to learn more?



With 27 years of experience,
SonicWall is recognized as the
Network Security leader
in the Cyber Arms race.

SonicWall Leadership...



SonicWall Security Center



Did you know?

From January to August, the average SonicWall customer faced:

- 18,474 malware attacks (+70% over 2017)
- 567 ransomware attacks (+108%)
- 6.1 million intrusion attempts (+54%)
- 811 encrypted threats (+73%)
- 2,668 phishing attacks
- 235K new attack variants (980/day) detected by Capture ATP
- 27,600 + never-before-seen attack variants identified by RTDMI

TOP 3 ATTACK ORIGINS	TOP 3 ATTACK TARGETS	TOP ATTACK TYPES	TOP 3 ATTACKER IP ADDRESS	ATTACK SITE STATISTICS ON AUG 27
14.2M France	10.6M United States	27.9M Intrusion	5.54M 185.40.**	1,828 > 100 Attacks/Site
5.76M Russia	8.19M United Kingdom	5.64M Malware	3.42M 212.129.**	1,488 > 50 < 100 Attacks/Site
1.28M United States	3.16M Brazil		2.33M 195.154.**	11.0K < 50 Attacks/Site

Business Impact



\$75B

Total cost of ransomware to businesses each year¹



\$3.6M

Average total cost of a data breach²



22%

Businesses that had a stoppage because of malware last year³



\$5B

Global losses due to business email compromise scams as of December 2016⁴

Our Vision: Automated Real-time Breach Detection and Prevention

ADVANCED THREATS



Ransomware
Fileless Malware
Encrypted Malware
Cryptojacking
Malvertising
Phishing

THE CHALLENGE



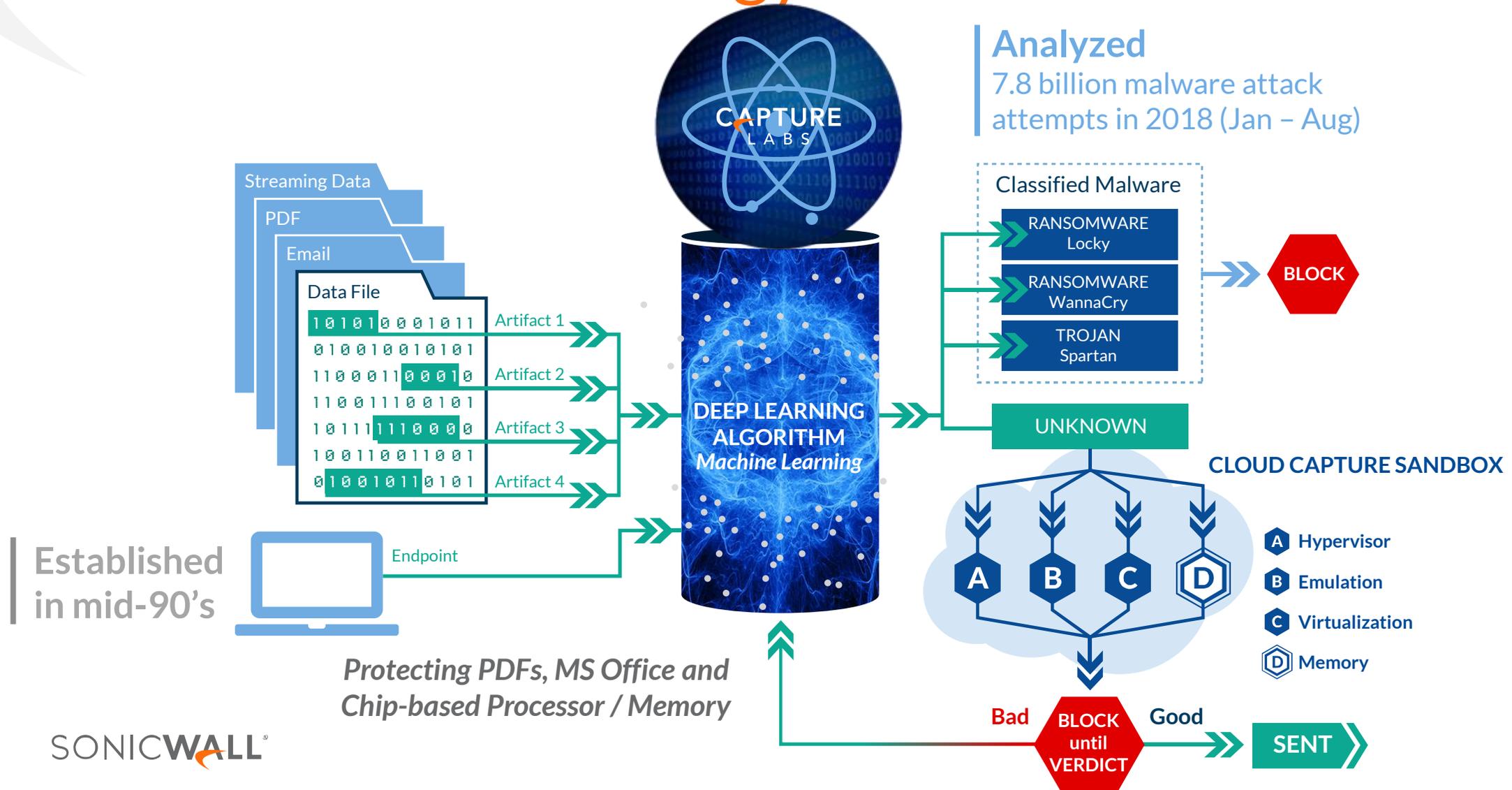
Any Vehicle
Email, Browser, Apps, Files
Any Traffic
Encrypted, Unencrypted
Any Network
Wired, Wireless, Mobile, Cloud
Any Device
PC, Tablet, Phone, IoT

CRITICAL COMPONENTS



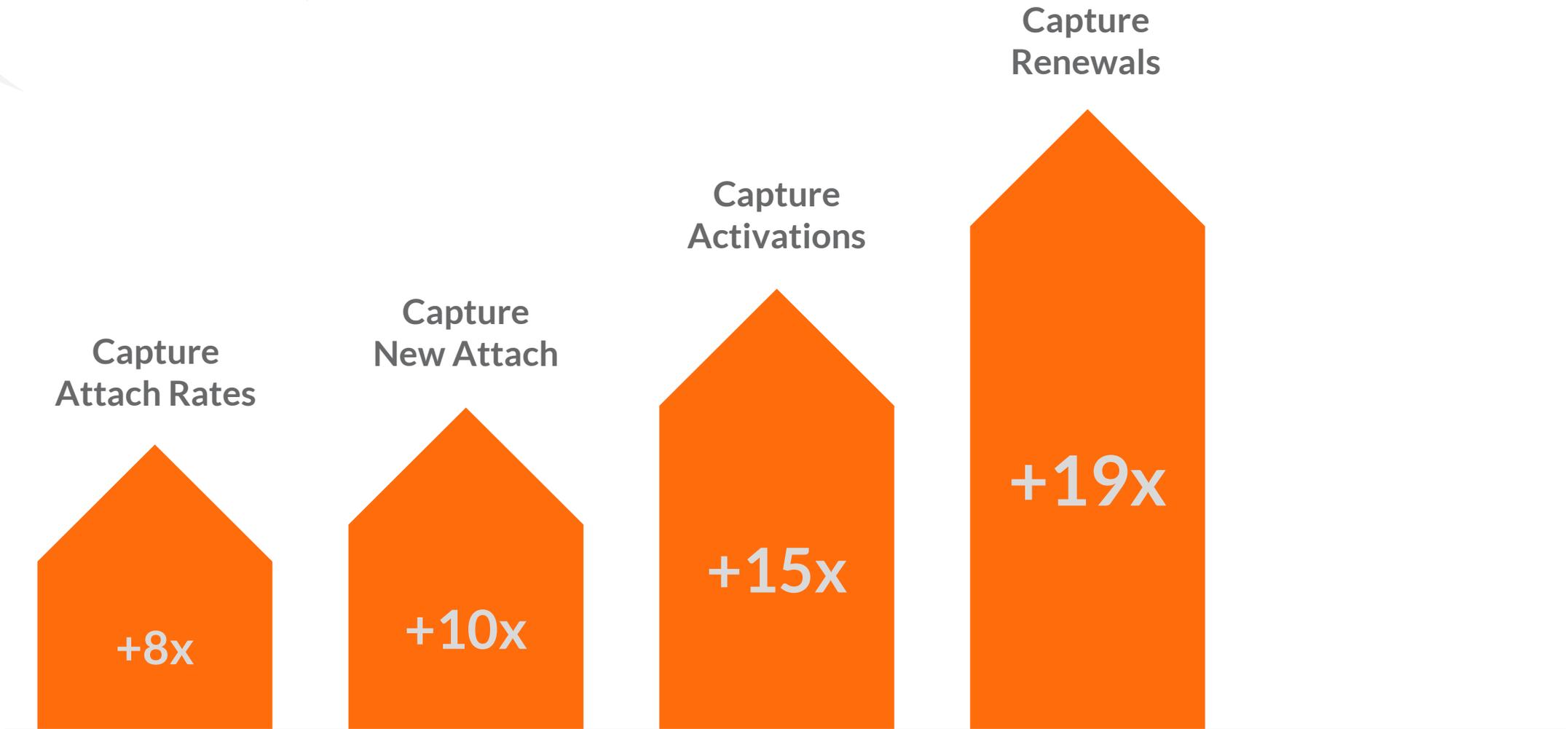
Inspect all SSL/encrypted traffic
Machine learning
Multi-engine, CPU-tracking cloud sandbox
Block files until a verdict is rendered
Integrated security platform (firewall, endpoint, wireless, email, CASB, Wi-Fi)
Security center (SOC)

Automated Real-Time Breach Detection and Prevention Technology



Capture ATP Momentum

Since November, 2016



Accelerating Product Innovation

Capture Security Center



Virtual Firewall



SonicWave APs



Cloud-Based Analytics



Capture Client 1.0



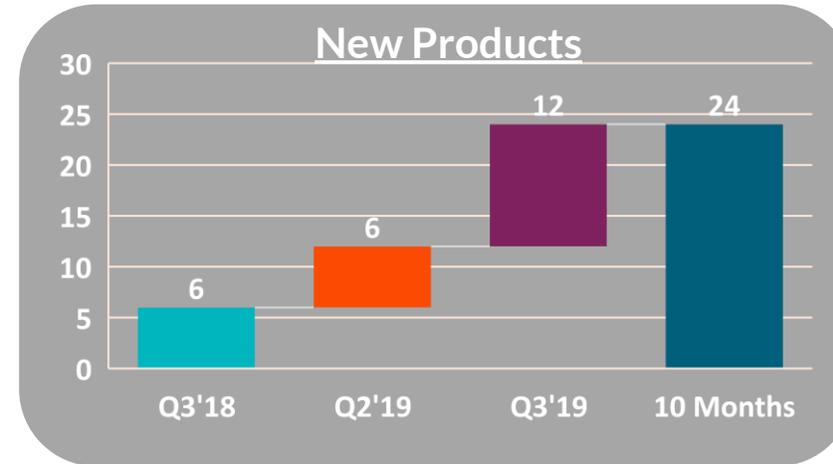
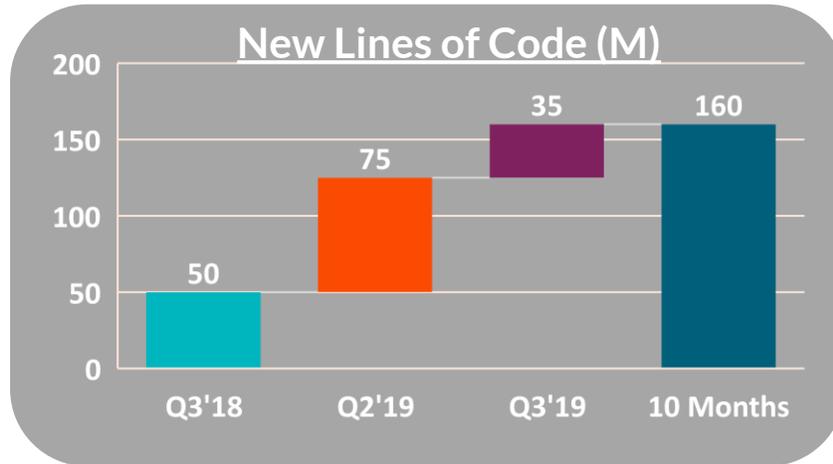
Cloud Analytics



High-end Network Security Appliances



Mid-Range Network Security Appliances



SonicOS 6.5.2



Analyzer 2.0



Cloud App Security



Sonic OS 6.5.1



Email Security 9.2



SMA 12.1



GMS 8.4



Secure Mobile Access



Capture Client 1.5



NSA 2650



SONICWALL

CAPTURE SECURITY CENTER

Login with your MySonicWall account credentials

Username or email address

cgms1@sonicwall.com

Password

••••••••

[Forgot Password?](#)

SONICWALL

Overview

Status

Dashboard

Live Monitor

Summary

Analytics

Dashboard

/ SonicWall Products /

Total Connections [40]

SYSTEM HEALTH

BANDWIDTH (Kbps)



TRAFFIC MAP



PRIVATE IP

SONICWALL

Overview

Status

Dashboard

Live Monitor

Summary

Analytics

Live Monitor

/ SonicWall Products /

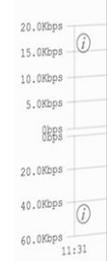
APPLICATIONS



Show Legends

- ICMP-5193
- Service Echo

BANDWIDTH



Show Legends

- X0
- X6
- X12
- X18

SONICWALL

DEVICE MANAGER

GlobalView

- 0011A-Engg-FW ID...
- 18B16952BE88
- 18B16977D18C (Aut...
- COEAE4C55DEA
- Justin NSA3600
- Justin NSA4600
- Justin NSA4600_1
- Justin NSA4650
- Justin NSA6500
- Justin SM9400
- Justin TZ300W
- Justin TZ400
- Justin TZ500W
- Nachiket TZ500
- Om-FW
- Pratap 3600
- Pratap TZ500W
- Test-FW-1 (DM)

SONICWALL

Overview

Status

Dashboard

Live Monitor

Summary

Applications

Users

Viruses

Intrusions

Spyware

Web Categories

Sources

Destinations

Source Locations

Destination Locations

BW Queues

Botnet

Blocked

Threats

Analytics

Source

/ SonicWall Products /

TOP INITIATOR

- 10.11.2...
- 10.21.3...
- 10.11.8...
- 10.11.8...
- 10.11.2...
- 10.21.5...
- 10.204...
- 10.21.1...
- 10.11.2...
- 10.11.9...

TOP INITIATOR

INITIATOR IPS NAME	TOTAL DATA TRANSFERRED	PERCENTAGE
10.21.82.14	28.1 GB	72.90%
10.11.25.10	2.2 GB	5.83%
10.11.95.66	1.9 GB	4.97%
10.11.95.58	1.4 GB	3.56%
10.11.99.300	1.1 GB	2.83%
10.21.62.5	1.1 GB	2.80%
10.21.77.203	884.4 MB	2.24%
10.11.59.85	718.2 MB	1.85%
10.11.93.207	566.7 MB	1.44%

SONICWALL

CAPTURE SECURITY CENTER

/ SonicWall Products /

SERVICES

TENANTS / GROUPS (3)

CLOUD SERVICES (7)

- DT Corp
Central Nervous System specialists
- PM CaptureCloud
PM Capture Cloud units
- SecDynamic
Security Dynamic Enterprise

Please select a service to launch.

Management

Reports

Analytics

Capture Client

CAS

Wireless

Licensing

Enrollment

28.1 GB

72.90%

10.21.82.14

28.1 GB

72.90%

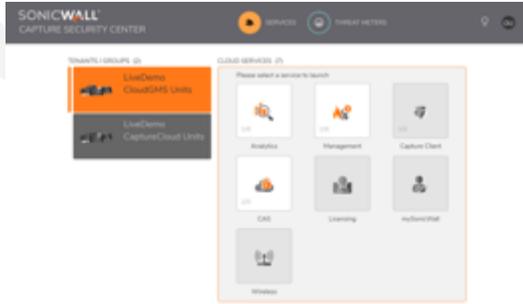
10.21.82.14

28.1 GB

72.90%

10.21.82.14

Accelerating Product Innovation



Capture Security Center

- Delivers centralized management for TZ, NSA and Supermassive Security Appliances
- Serves as a single pane of glass for product and services portfolio.
- MSSP Enabling for mid-tier enterprise focus



Cloud-Based Analytics

- Delivers centralized analytics for TZ, NSA series solutions
- Deep visibility into threats
- Enables threat hunting and analysis of east-west traffic and lateral threat movement
- Graph analysis of threats



Network Security virtual firewall

- Fully featured virtual version of SonicWall NGFW
- Automated breach prevention for public, private or hybrid cloud
- Common management through GUI, CLI, GMS, Capture Security Center or API



SonicWave APs

- Wave2ac (Wireless Modernization)
- 2.5Gig (Interface Modernization)
- 3rd scanning radio
- New hybrid AP & Service pricing model



Web Application Firewall

- Web application threat management
- Data leak prevention
- SSL inspection for web traffic
- Application delivery acceleration and load balancing
- DOS/DDOS attack prevention on web servers

Accelerating Product Innovation



Network Security appliances

- NSa offers enterprises highest security efficacy and lowest TCO in the industry
- NSsp supports large enterprises, data centers and service providers
- Leverages intelligence from Capture Cloud Platform
- Adds high-performance TLS/SSL inspection
- Can be centrally managed with GMS 8.6



Cloud App Security

- Reduces shadow IT by discovering usage of sanctioned and unsanctioned IT applications
- Offers real-time visibility into cloud application traffic and usage patterns
- Improves security posture by enforcing access policies to block risky applications



Capture Client: Better NGAV

- Highly accurate protection
- Endpoint remediation/rollback
- Integrates with Capture ATP
- Enforced by SonicWall firewall
- DPI-SSL certificate management
- Shares threat intelligence
- Adds attack visualization
- Supports Windows Servers 12 and upwards



Sonic OS 6.5.2

- Common OS across NSa and TZ appliances
- Increases Capture ATP BUY and DPI-SSL controls
- Adds Application-Based Routing
- Supports SonicWave wireless Fast Roaming (802.11k/r/v)
- Enhancements to DNS Security



Email Security 9.2

- Utilizes Capture ATP for dynamic URL analysis to block malicious URLs
- Adds Advanced Threat Protection support for G Suite mailboxes
- Enhances anti-phishing effectiveness



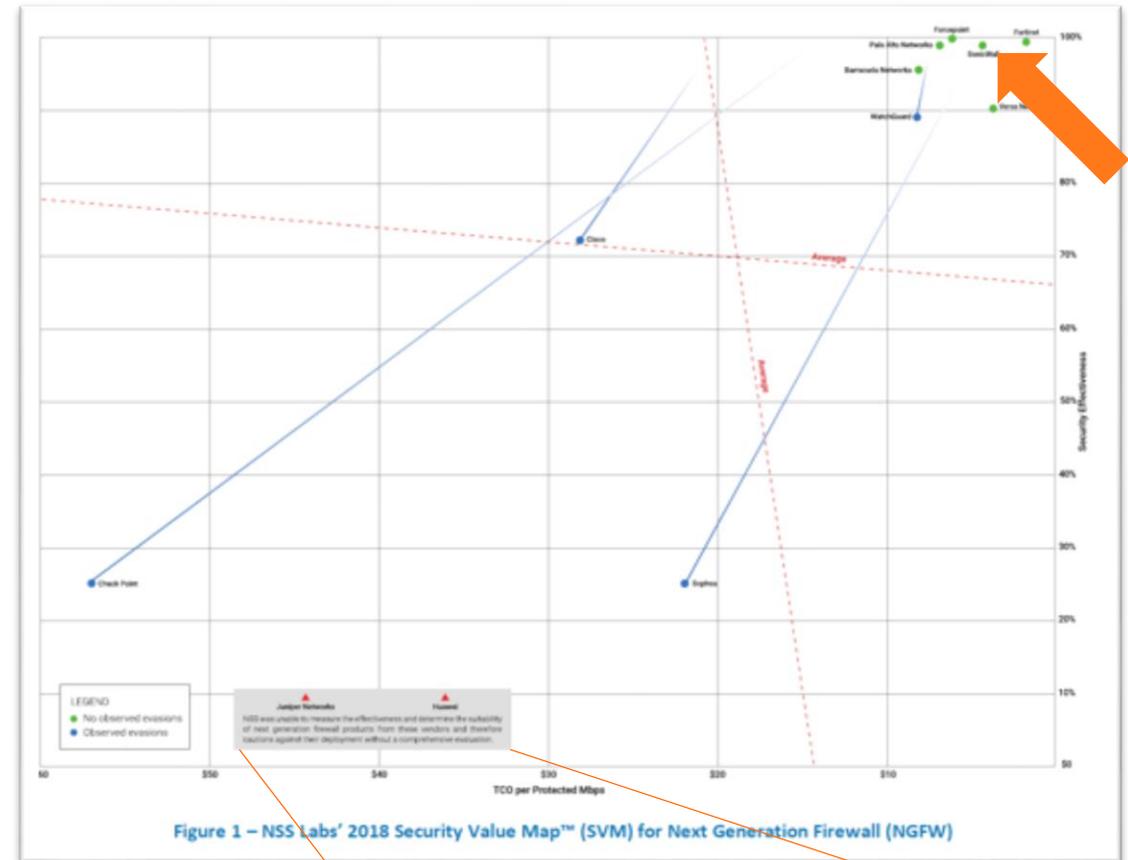
Secure Mobile Access

- Delivers seamless secure access over untrusted networks with Always On VPN
- Supports time-based one-time password (TOTP)
- Unifies secure access for hybrid IT using SAML 2.0 authentication
- Adds Secure File Share with Capture ATP on SMA 100 series

2018 NSS NGFW Report

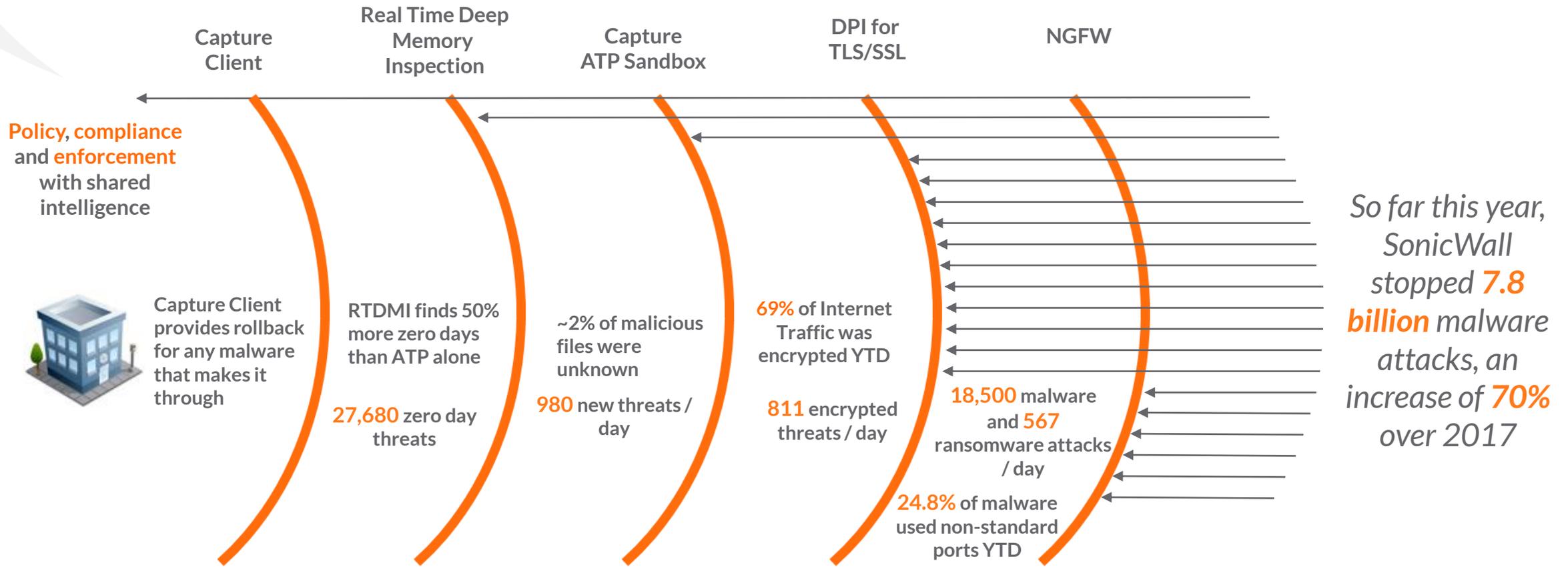
- In July 2018, NSS Labs published its 6th annual NGFW report
- For the 5th time, SonicWall is strongly positioned in the upper right “Recommended” quadrant
- NSa 2650 achieved a security effectiveness score of 98.8%
- 100% effectiveness against all evasions (190/190)
- 100% pass rate for all stability & reliability tests
- Achieved security effectiveness with a low TCO of \$4/Mbps (2nd best in value vs. all the models tested)

2018 NSS Labs Security Value Map for NGFW



Juniper Networks **Huawei**
NSS was unable to measure the security effectiveness and determine the suitability of next generation firewall products from these vendors and therefore cautions against their deployment without a comprehensive evaluation.

SonicWall Automated Real-Time Threat Detection & Prevention: JAN-AUG '18



Why we are different:

Shared intelligence, rollback

Ultra-fast, catches never-before-seen attacks

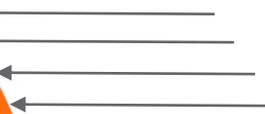
Multi-technology, block until verdict, deep learning

High performance patented RFDPI

High security efficacy, machine learning algorithms

Protection Outside the Enterprise...

Capture Client



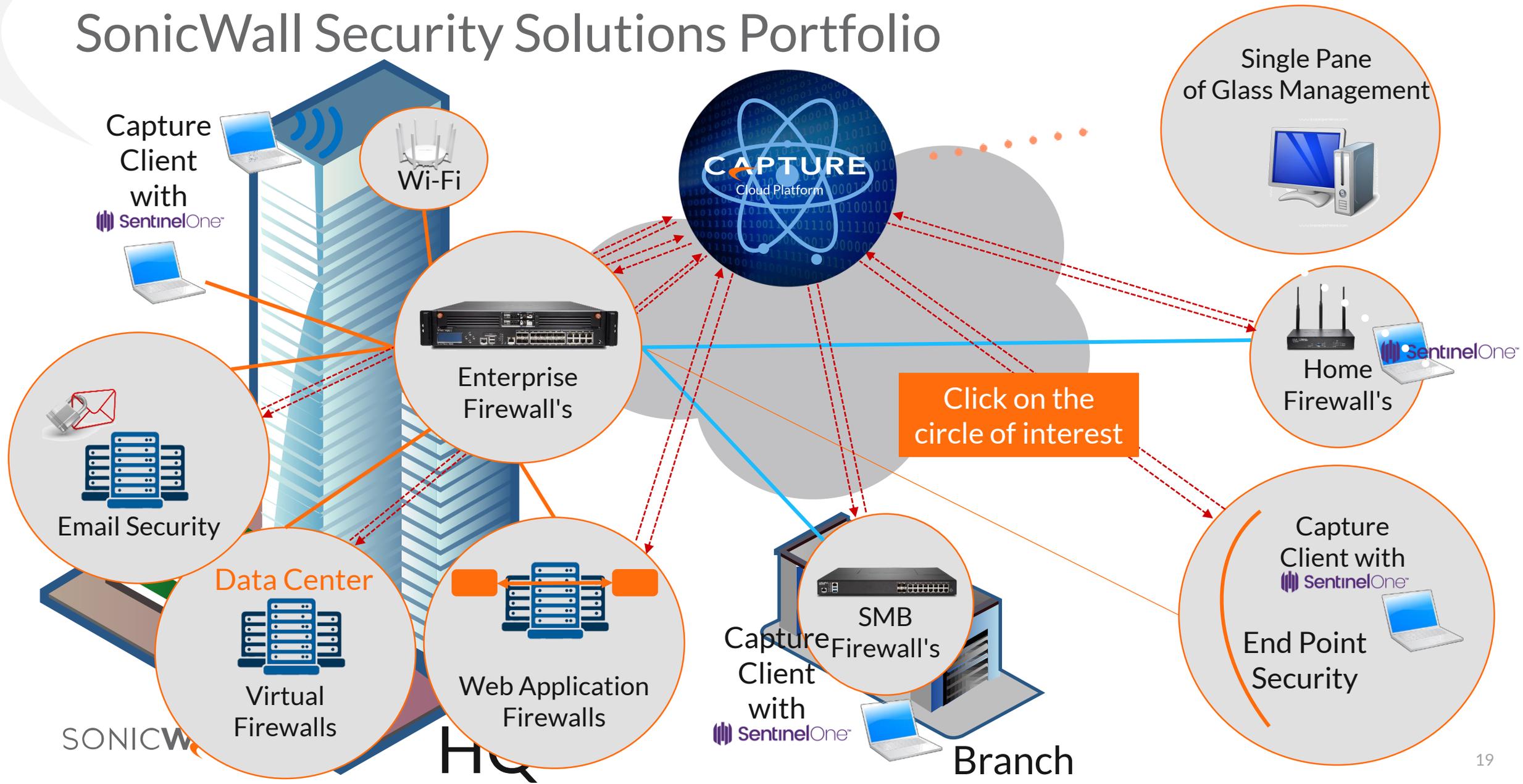
Capture Client provides next-gen protection for mobile and remote users

Administrator or end-user
rollback to a good state for
any attack outside the
enterprise

Why we are
different:

Shared
intelligence,
rollback

SonicWall Security Solutions Portfolio



Thank you!



Questions?