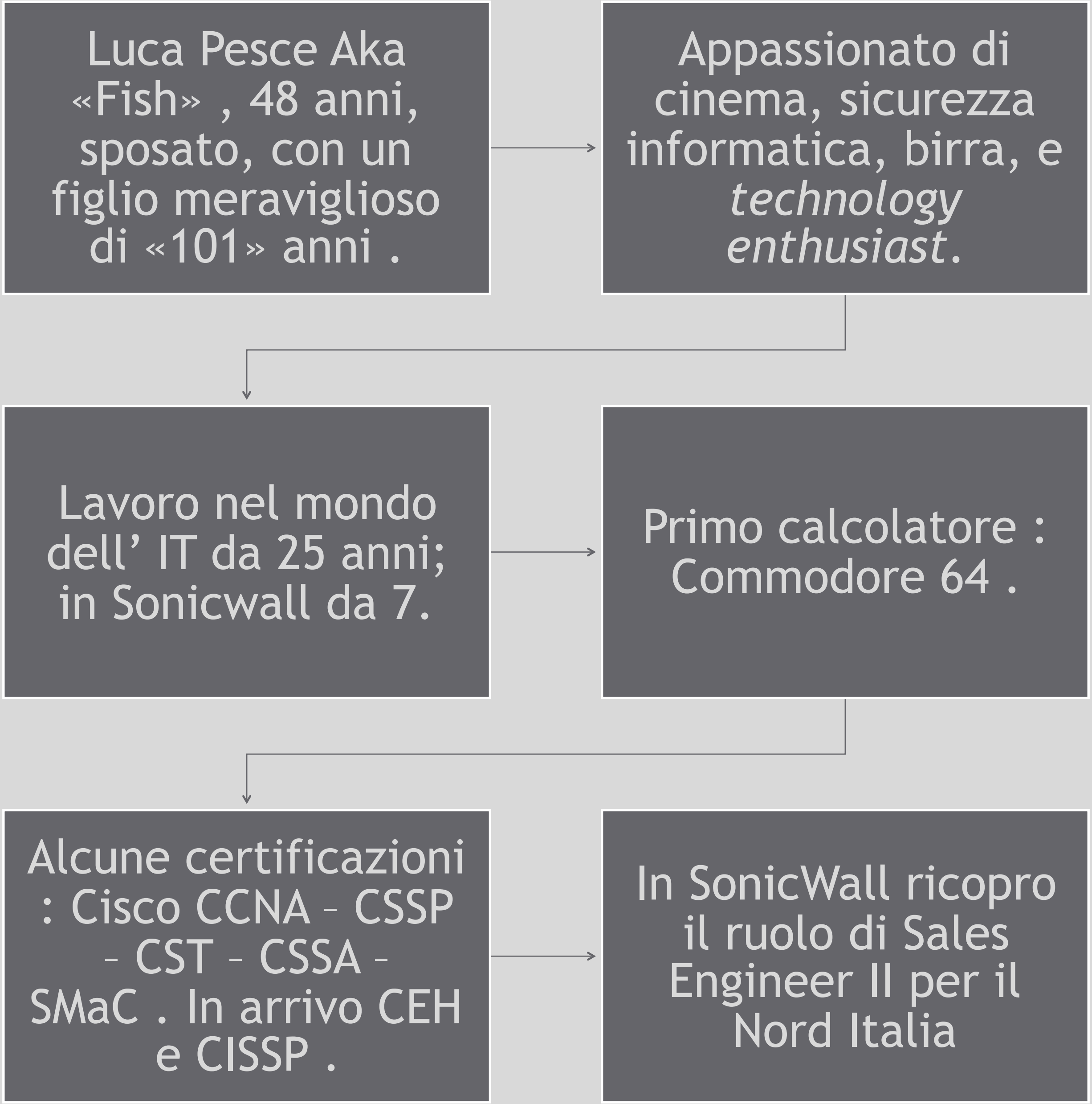
ntopConf Italia 2019

- **Padova, Maggio 2019**

Luca Pesce
System Engineer North Italy
lpesce@sonicwall.com
Mob: 3474770427

Chi Sono:



Luca Pesce Aka «Fish» , 48 anni, sposato, con un figlio meraviglioso di «101» anni .

Appassionato di cinema, sicurezza informatica, birra, e *technology enthusiast*.

Lavoro nel mondo dell’ IT da 25 anni; in Sonicwall da 7.

Primo calcolatore : Commodore 64 .

Alcune certificazioni : Cisco CCNA – CSSP – CST – CSSA – SMaC . In arrivo CEH e CISSP .

In SonicWall ricopro il ruolo di Sales Engineer II per il Nord Italia

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

SonicWall Leadership…

18,000+
global channel partners

1 million+
networks protected

215+
countries & territories

~500,000
organizations

290+
patents

3 million+
firewalls shipped

SonicWall History

Business Update

- Had the highest government quarter in our history
- New records across the business:
  - **92%** customer renewal rate
  - **54** new products and **~162 million** lines of code
  - **58%** of technical support cases resolve in first business day
  - **15:1** self-service score in 2018 (best in class)
  - **51** awards accumulated since February 2018
- Launched new Capture Cloud Platform and Capture Security Center

"Bill, just to let you know that Anonymous Italy declared an attack to various public administrations including Pisa University until Nov 5 2018. We resisted the attacks mainly on our mail thanks to the email security solution we recently deployed. We had peaks of 600,000 connections/day with only 100,000 legitimate and the system resisted under pressure. We are impressed by the system performance, in the month of October we received 12million connections and just over 2million were delivered as legitimate."

Antonio Cisternino – CIO University of Pisa, Italy

"As a Platinum SonicWall partner we have recently rolled out TZ 400 firewalls for one of our larger Enterprise Customers to over 2,500 locations across Germany and Austria to enable secure communications between retail kiosks and headquarters. The installation went extremely smoothly and the solution delivers exactly what our client required. During this Enterprise rollout we had no issues with the selected products, demonstrating the quality of the SonicWall Security Platform.

With this installation SonicWall has proven again to be the premier provider of high-class security solutions at an excellent price point.

At Axsos we are proud to continue and intensify our relationship with SonicWall in the future."

Peter Klien
Senior Account Manager IT-Security, AXSOS AG

SONICWALL

SonicWall Security Center: Did You Know?

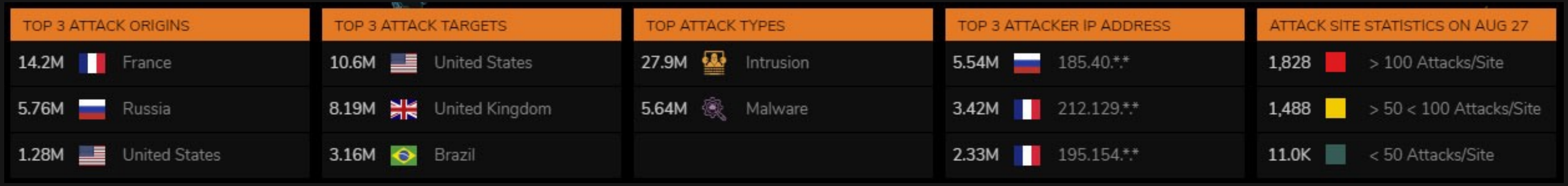
WORLDWIDE ATTACKS

In 2018, the average SonicWall customer faced:

- ~25,000 malware attacks (+22% over 2017)
- 490 ransomware attacks (+11%)
- 19% of malware using non-standard ports (+9%)
- 9.3 million intrusion attempts (+38%)
- 1,276 encrypted threats (+27%)
- 105K web app attacks (+79%)
- 5,488 phishing attacks
- 392K new attack variants (1,074/day) detected by Capture ATP
- 74K+ never-before-seen attack variants identified by RTDMI

In Jan-Feb 2019, the average SonicWall customer faced:

- 3,602 malware attacks (-26% over Jan-Feb 2018)
- 59 ransomware attacks (-25%)
- 12.6% of malware using non-standard ports (-26%)
- 1.6 million intrusion attempts (+11%)
- 368 encrypted threats (+20%)
- 15K web app attacks (-57%)
- 738 phishing attacks (+14%)
- 69.8K new attack variants (1,182/day) detected by Capture ATP (+97%)
- 89K+ 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

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)

SonicWall Capture Labs

Established in mid-90’s

Analyzed

12 billion malware attacks from January 2018 February 2019

Identified

164k+ never before seen threats from Jan. 2018-Feb. 2019

Dedicated

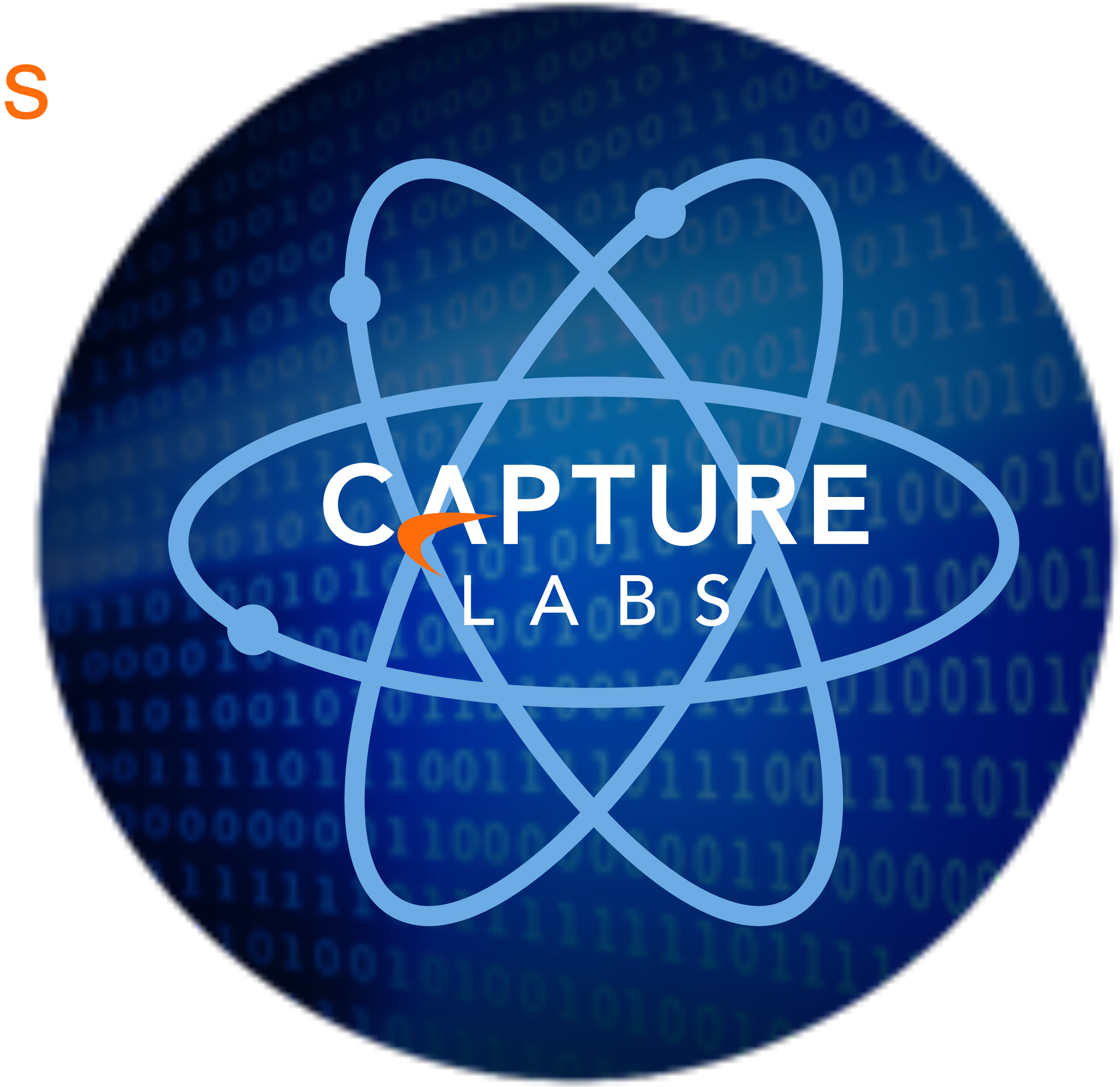
World-class threat and machine learning engineering team

Credited

Discovery of hundreds of unique variants every day

Extensive Malware Library

Hundreds of terabytes of data/artifacts



CAPTURE
THREAT NETWORK

50+
Industry research organizations in which intelligence is shared

1.0M+
Sensors

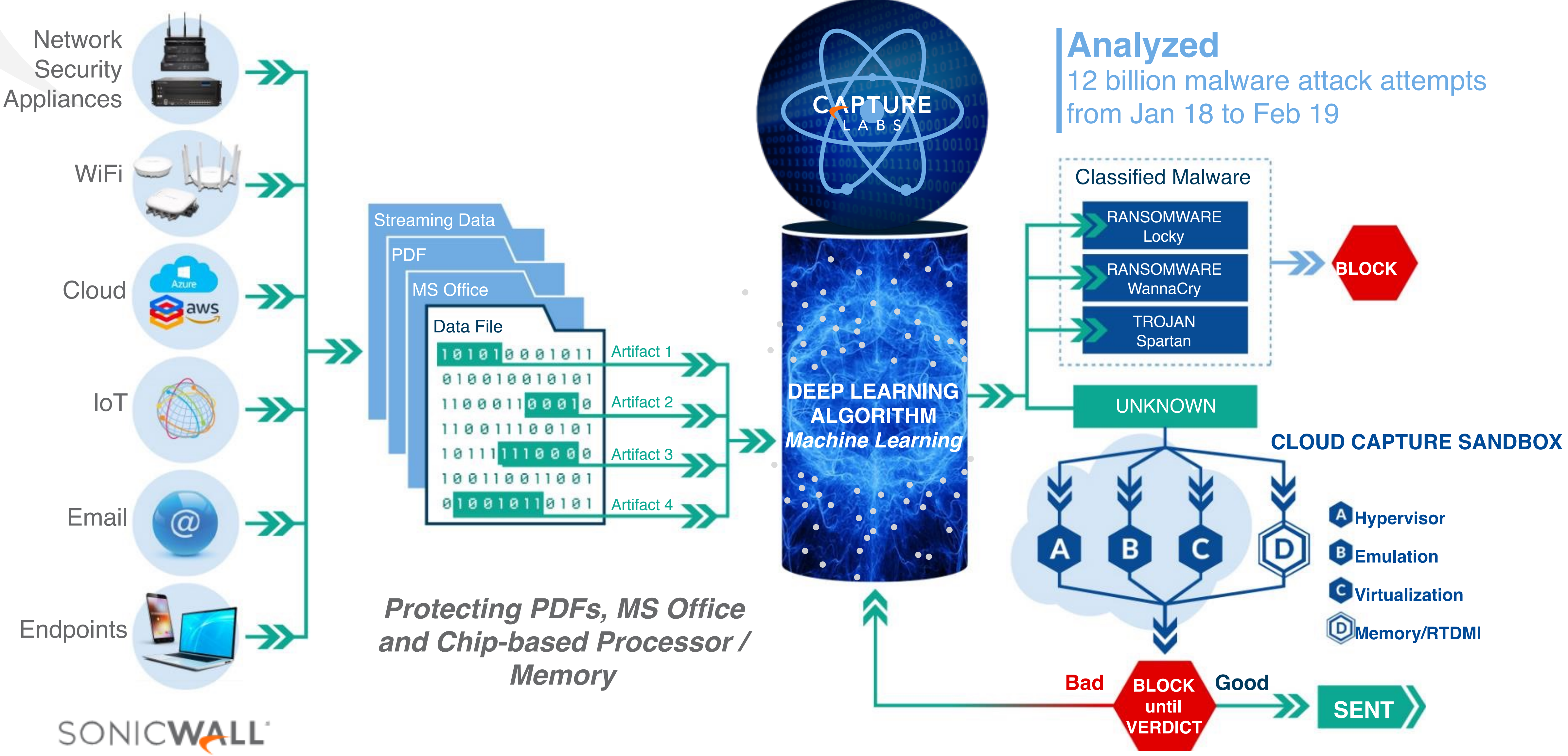
24x7x365
Monitoring

< 24 Hr.
Response to never seen before vulnerabilities

140K+
Malware samples collected daily

25M+
Malware attacks blocked daily

Automated Real-Time Breach Detection and Prevention Technology



Analyzed
12 billion malware attack attempts from Jan 18 to Feb 19

Network Security Appliances

WiFi

Cloud

IoT

Email

Endpoints

Streaming Data

PDF

MS Office

Data File

Artifact 1

Artifact 2

Artifact 3

Artifact 4

CAPTURE LABS

DEEP LEARNING ALGORITHM *Machine Learning*

Classified Malware

Classified Malware
RANSOMWARE Locky
RANSOMWARE WannaCry
TROJAN Spartan

BLOCK

UNKNOWN

CLOUD CAPTURE SANDBOX

- A Hypervisor
- B Emulation
- C Virtualization
- D Memory/RTDMI

Bad

BLOCK until VERDICT

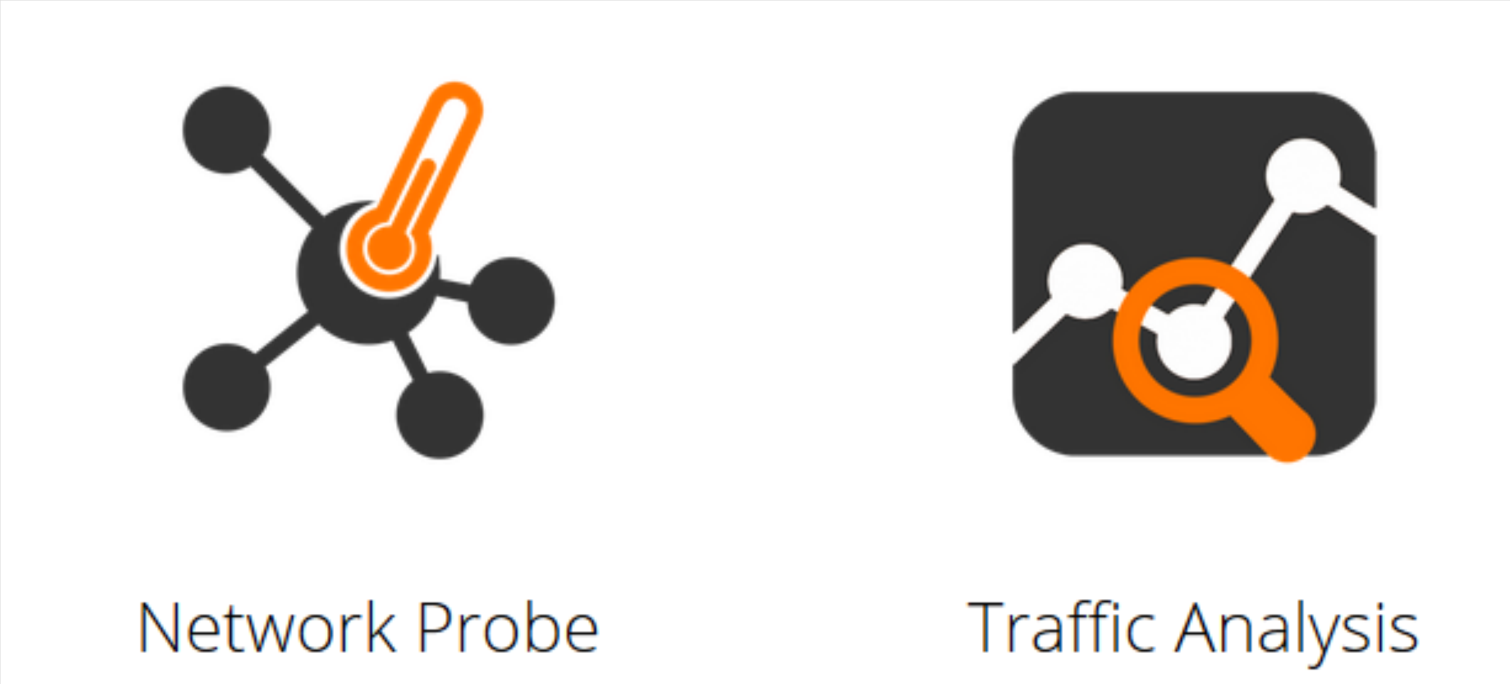
Good

SENT

Protecting PDFs, MS Office and Chip-based Processor / Memory

SONICWALL

SonicWALL e NTOP : declinare la security ed il monitoring con proattività



Due modalità di implementazione per ottenere il massimo della visibilità del traffico

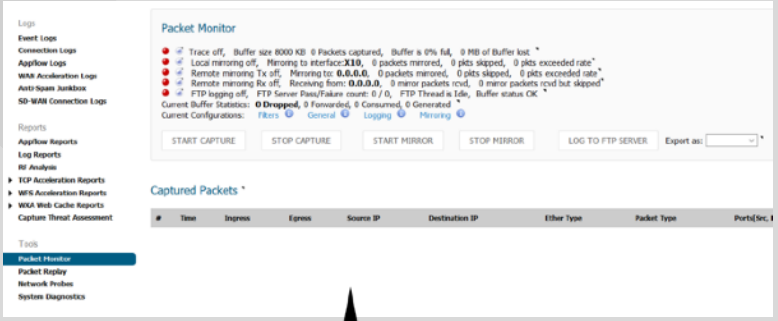
- Native:

Utilizzando la funzionalità di packet monitoring presente su tutti i nostri firewalls, si ottiene nativamente, in pochi secondi, la visibilità completa di tutti i flussi che attraversano il firewall ottenendo un dettaglio degli stessi prossimo all'ananalisi forense dei dati.

- Flow forwarding:

I nostri firewall permettono, con pochissimo tempo di configurazione, la possibilità di inviare i flussi che lo attraversano ad un collettore esterno tramite lo standard IPFIX with extension. Utilizzando Nprobe come collettore si può accedere immediatamente alla visualizzazione dei dati desiderati.

Native Mode



Packet Monitor

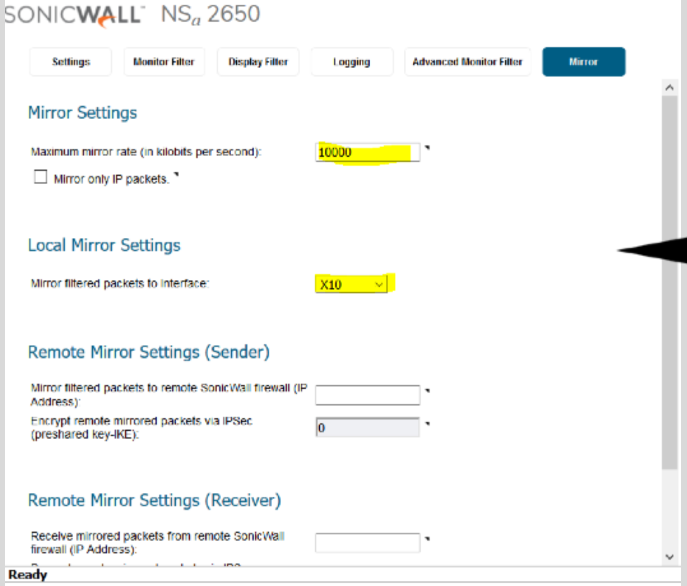
- Trace off, Buffer size 8000 KB 0 Packets captured, Buffer is 0% full, 0 MB of Buffer lost
- Local mirroring off, Mirroring to interface:**X10**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
- Remote mirroring Tx off, Mirroring to: **0.0.0.0**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
- Remote mirroring Rx off, Receiving from: **0.0.0.0**, 0 mirror packets rcvd, 0 mirror packets rcvd but skipped
- FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer status OK

Current Buffer Statistics: **0 Dropped**, 0 Forwarded, 0 Consumed, 0 Generated

Current Configurations: Filters General Logging Mirroring

Captured Packets

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src,



SONICWALL NS$_a$ 2650

Mirror Settings

Maximum mirror rate (in kilobits per second): 10000

□ Mirror only IP packets.

Local Mirror Settings

Mirror filtered packets to interface: X10

Remote Mirror Settings (Sender)

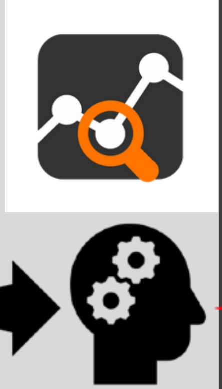
Mirror filtered packets to remote SonicWall firewall (IP Address):

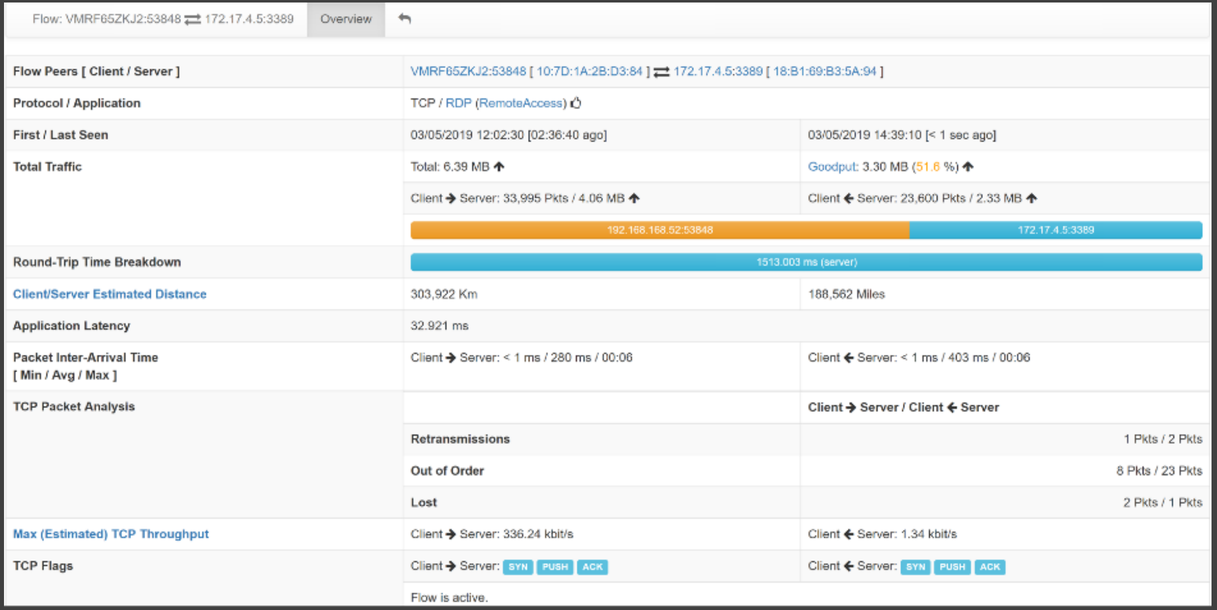
Encrypt remote mirrored packets via IPSec (preshared key-IKE): 0

Remote Mirror Settings (Receiver)

Receive mirrored packets from remote SonicWall firewall (IP Address):

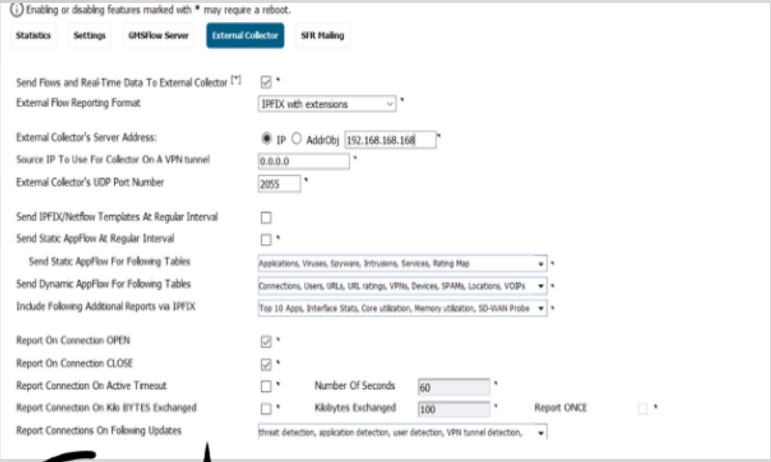
Ready





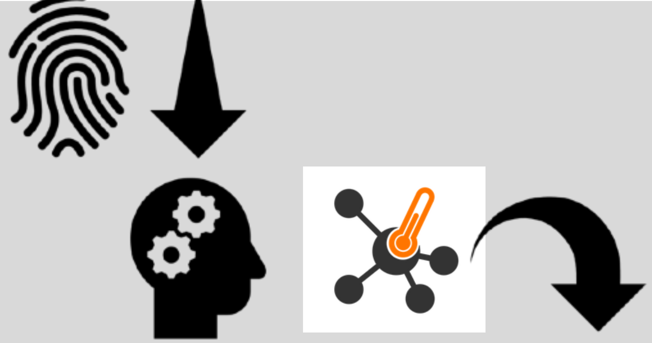
Flow Peers [Client / Server]	VMRF65ZKJ2:53848 [10:7D:1A:2B:D3:84] ⇄ 172.17.4.5:3389 [18:B1:69:B3:5A:94]	
Protocol / Application	TCP / RDP (RemoteAccess)	
First / Last Seen	03/05/2019 12:02:30 [02:36:40 ago]	03/05/2019 14:39:10 [< 1 sec ago]
Total Traffic	Total: 6.39 MB ↑	Goodput: 3.30 MB (51.6 %) ↑
	Client → Server: 33,995 Pkts / 4.06 MB ↑	Client ← Server: 23,600 Pkts / 2.33 MB ↑
	192.168.168.52:53848	172.17.4.5:3389
Round-Trip Time Breakdown	1513.003 ms (server)	
Client/Server Estimated Distance	303,922 Km	188,562 Miles
Application Latency	32.921 ms	
Packet Inter-Arrival Time [Min / Avg / Max]	Client → Server: < 1 ms / 280 ms / 00:06	Client ← Server: < 1 ms / 403 ms / 00:06
TCP Packet Analysis		Client → Server / Client ← Server
	Retransmissions	1 Pkts / 2 Pkts
	Out of Order	8 Pkts / 23 Pkts
	Lost	2 Pkts / 1 Pkts
Max (Estimated) TCP Throughput	Client → Server: 336.24 kbit/s	Client ← Server: 1.34 kbit/s
TCP Flags	Client → Server: SYN PUSH ACK	Client ← Server: SYN PUSH ACK
	Flow is active.	

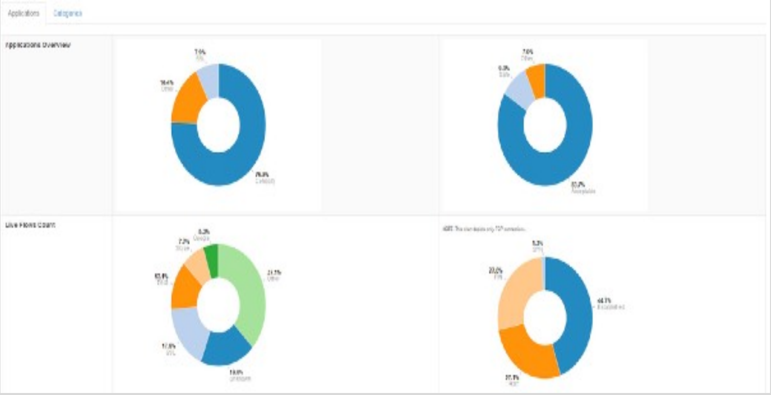
Flow Forwarding

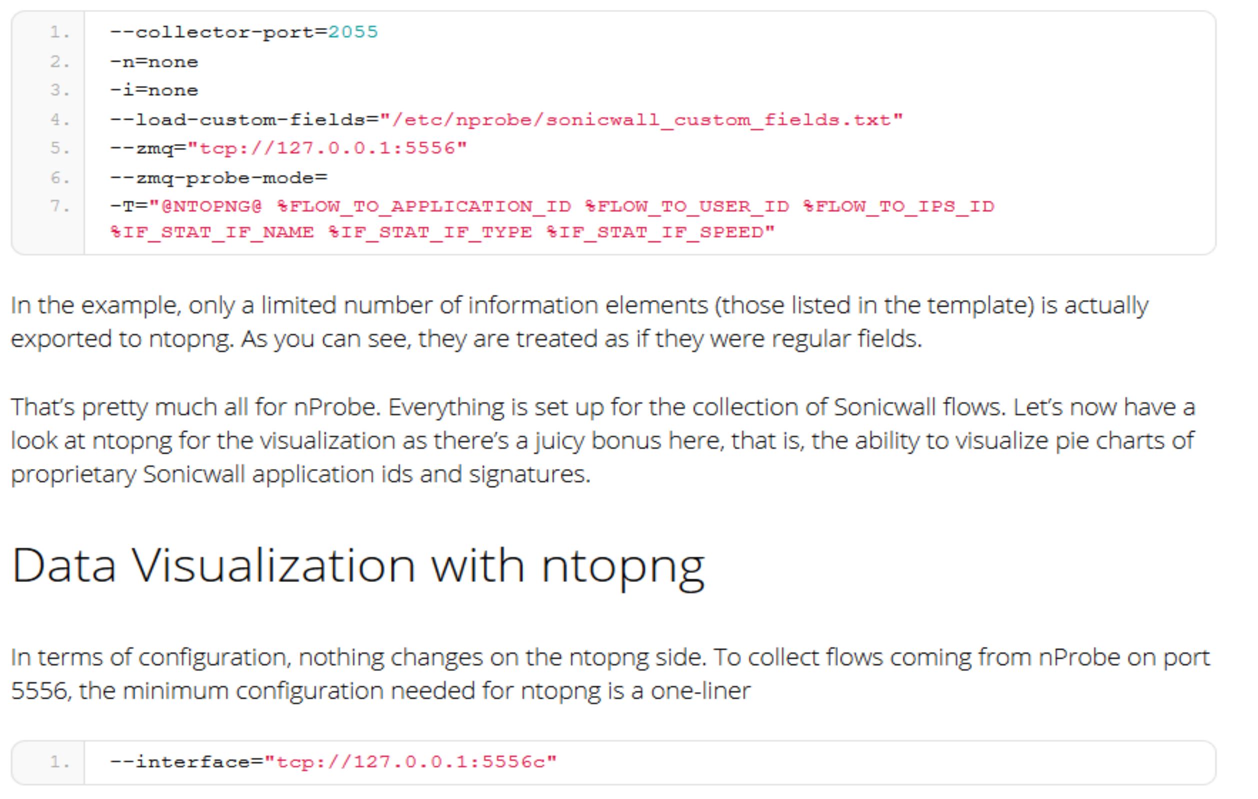


ⓘ Enabling or disabling features marked with * may require a reboot.

Send Flows and Real-Time Data To External Collector [*]	☑ *				
External Flow Reporting Format	IPFIX with extensions *				
External Collector's Server Address:	● IP ○ AddrObj 192.168.168.168 *				
Source IP To Use For Collector On A VPN tunnel	0.0.0.0 *				
External Collector's UDP Port Number	2055 *				
Send IPFIX/Netflow Templates At Regular Interval	□				
Send Static AppFlow At Regular Interval	□ *				
Send Static AppFlow For Following Tables	Applications, Viruses, Spyware, Intrusions, Services, Rating Map *				
Send Dynamic AppFlow For Following Tables	Connections, Users, URLs, URL ratings, VPNs, Devices, SPAMs, Locations, VOIPs *				
Include Following Additional Reports via IPFIX	Top 10 Apps, Interface Stats, Core utilization, Memory utilization, SD-WAN Probe *				
Report On Connection OPEN	☑ *				
Report On Connection CLOSE	☑ *				
Report Connection On Active Timeout	□ *	Number Of Seconds	60 *		
Report Connection On Kilo BYTES Exchanged	□ *	Kilobytes Exchanged	100 *	Report ONCE	□ *
Report Connections On Following Updates	threat detection, application detection, user detection, VPN tunnel detection,				







```
--collector-port=2055
-n=none
-i=none
--load-custom-fields="/etc/nprobe/sonicwall_custom_fields.txt"
--zmq="tcp://127.0.0.1:5556"
--zmq-probe-mode=
-T="@NTOPNG@ %FLOW_TO_APPLICATION_ID %FLOW_TO_USER_ID %FLOW_TO_IPS_ID
%IF_STAT_IF_NAME %IF_STAT_IF_TYPE %IF_STAT_IF_SPEED"
```

In the example, only a limited number of information elements (those listed in the template) is actually exported to ntopng. As you can see, they are treated as if they were regular fields.

That's pretty much all for nProbe. Everything is set up for the collection of Sonicwall flows. Let's now have a look at ntopng for the visualization as there's a juicy bonus here, that is, the ability to visualize pie charts of proprietary Sonicwall application ids and signatures.

Data Visualization with ntopng

In terms of configuration, nothing changes on the ntopng side. To collect flows coming from nProbe on port 5556, the minimum configuration needed for ntopng is a one-liner

```
--interface="tcp://127.0.0.1:5556c"
```

https://www.ntop.org/nprobe/using-nprobe-and-ntopng-for-collecting-and-visualizing-sonicwall-flows/

SONICWALL®

Thank You!