Check Point
SOFTWARE TECHNOLOGIES LTD

2018Q1 SE CLUB

Trust the process

Danny Yang | SE

WELCOME TO THE FUTURE OF
CYBER SECURITY
POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

Agenda

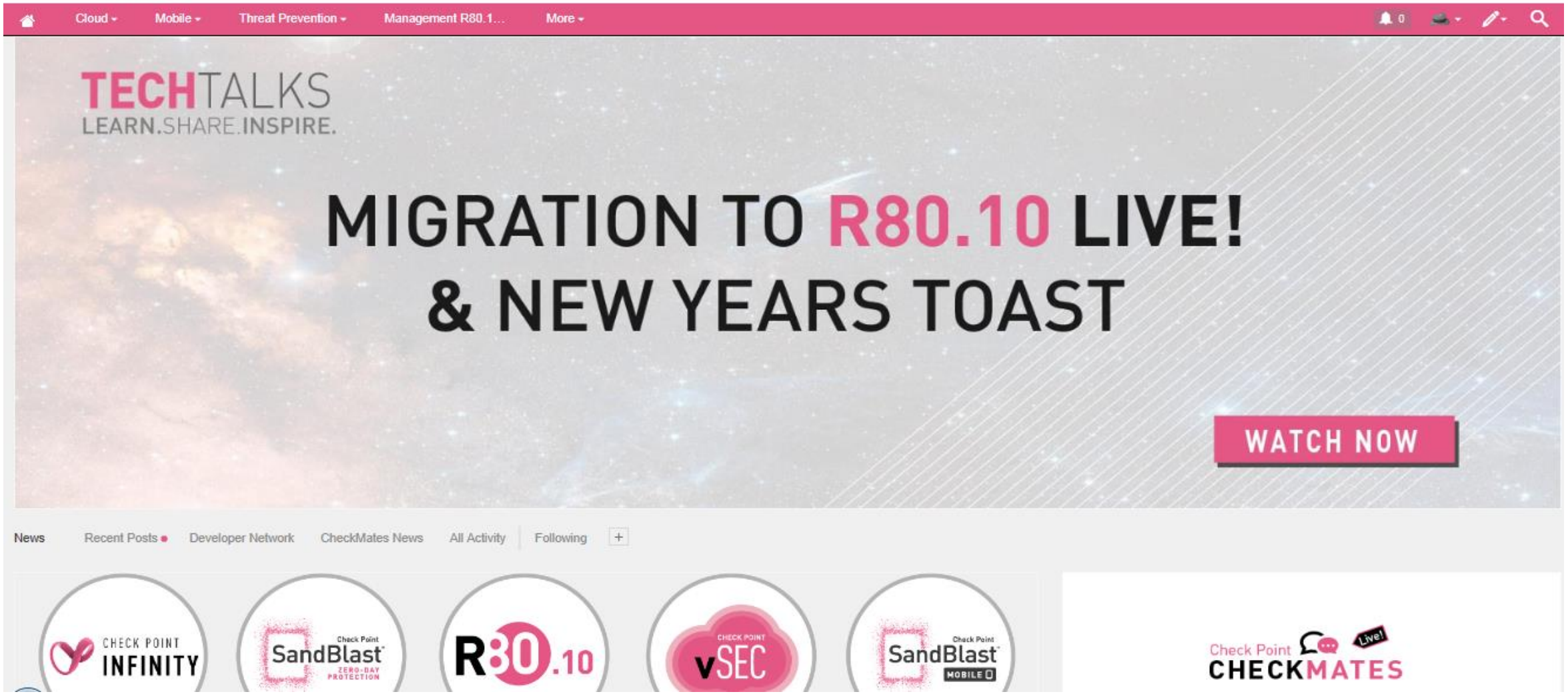
- 2017 Review
- 2018 Cyber Security Trend
- New Product Update & Competitive Information

- **2017 Review**

Join the CheckMate From Now!

Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point
CHECKMATES



Pro Support Free Trial (30 days)

See sk120332 for detailed information

Proactive Support service that monitors your system

Evaluates system parameters to assess the health of your devices

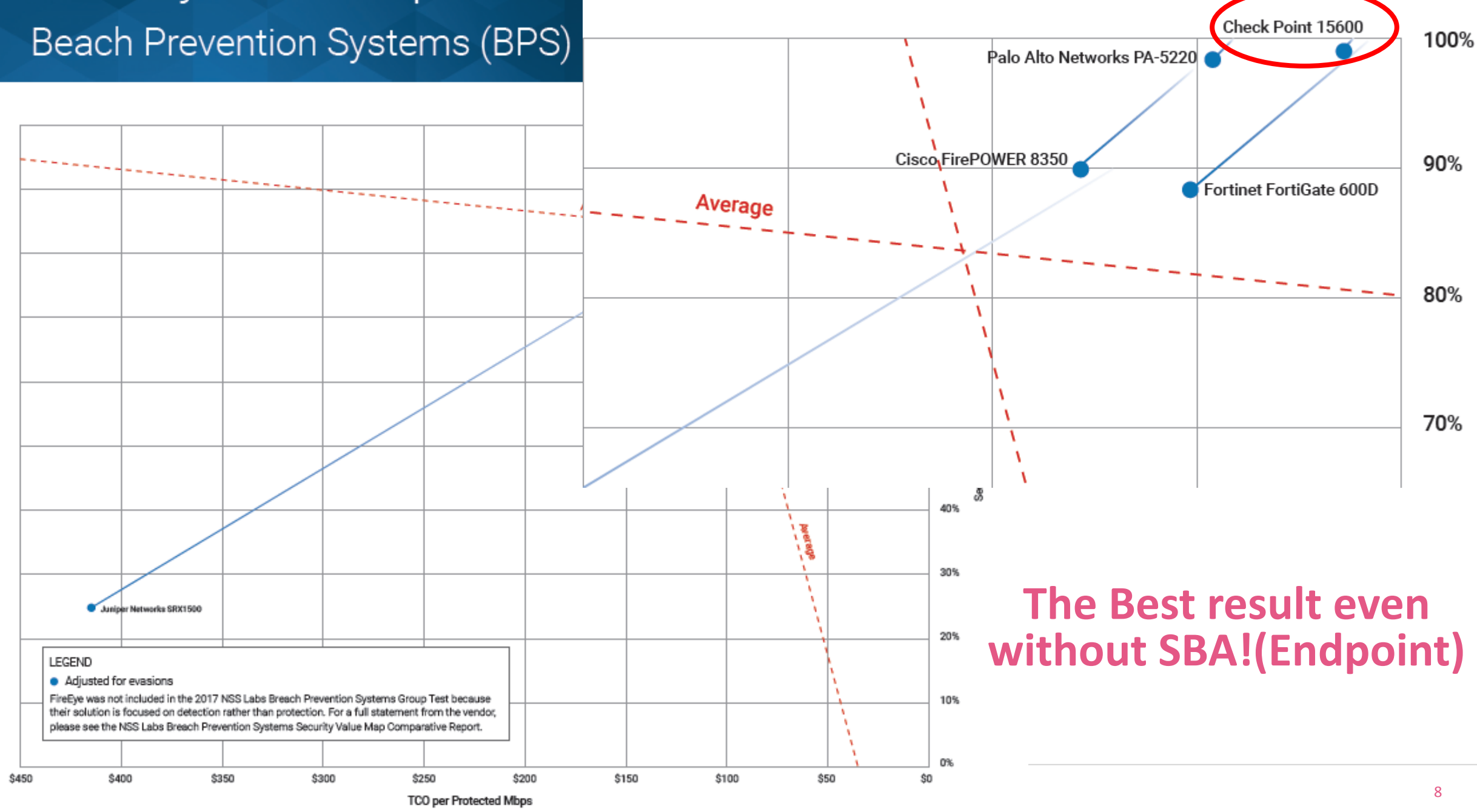
Proactively contacts you to resolve issues fast and efficiently

- **2018 Cyber Security Trend**


SandBlast
DLP
Anti-Bot
Bot
Backdoor
Stealing
Data
Variant
Threat
SandBlast
Mobile
NGFW
Phishing
Vul bility
Central
Management
& Event
Control &
Command
1 : 0
Endpoint
Security
Application
Control
Social
Engineering
Worm
Anti-
Ransomware
Anti-Virus
IPS
Exploit
Virus
Spy Eye
Spyware
Ransomware
2018 Cyber Security World Cup

Security Value Map™

Beach Prevention Systems (BPS)



The Best result even without SBA!(Endpoint)

Competitive Talking Point-1

- **Check Point**
  - Highest security effectiveness with single app[illegible]e! (N[illegible]
  - Full Threat Prevention throug[illegible]aX higher
  - The Best TCO of all vendors
- **FireEye**

Statement from FireEye

"At FireEye, we focus on the many real world securit[illegible]d that know[illegible]dge into our security solutions, products, and services. W[illegible] partici[illegible]ent N[illegible]s Breach Detection Systems (BDS) test but not the Breach Prevention Systems (BP[illegible]est, si[illegible]e current [illegible]eEye Network Security product's design priority was detection, not blocking/prevention."

We Do Prevention!

Competitive Talking Point-2

- **Palo Alto Networks**
  - Missed twice as many attacks & evasions as Check Point with over 3X the TCO
- **Cisco**
  - Suffered severe evasion failures with over 5X the TCO
- **Fortinet**
  - Low catch-rate, with multiple evasions bypassing and almost 4X the TCO
- **Juniper (Caution)**
  - Failed the test miserably and had TCO of $414 (**30X higher than Check Point!!!)**

All the testing result included their endpoint solution!(Expect Juniper)

Industrial BEST APT Solution: SandBlast

Real-Time Prevent Unknown Threat

Reduce Security Risk for Zero-Day Attack

CHECK POINT
SandBlast™
ZERO-DAY PROTECTION

Threat Emulation

OS Sandboxing
Anti-Evasion
Push Forward

CHECK POINT
SandBlast™
AGENT

Threat Extraction

Extract Malicious Content
Convert to PDF
Self-IT(User Check)

FACT

Protecting the enterprise from advanced threats requires security that covers

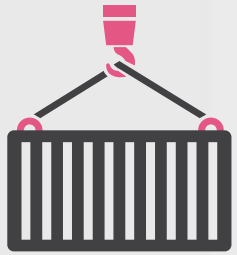
ALL ATTACK SURFACES

- When connected to corporate network
- Remote employees: At home using your endpoint
- Using cloud business services
- Inside or outside corporate network using mobile device

3 LINES OF DEFENSE FOR A SUCCESSFUL PROTECTION STRATEGY

DETECT & PREVENT

The only way to avoid the cost of an attack is to prevent it altogether

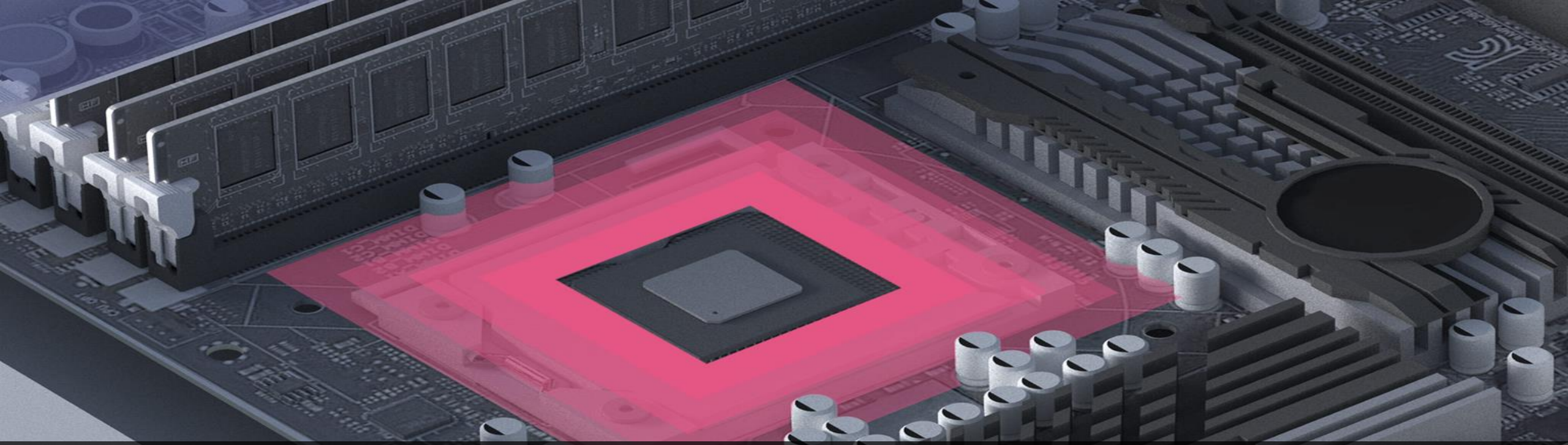


CONTAIN

Contain attacks as soon as possible. Once infected the cost of the attack will just keeps on rising

FORENSIC ANALYSIS

Effectively respond and remediate. Address the real business impact
Make sure the infection doesn’t come back



LEVERAGING THE HASWELL CPU

- Tracks the flow of branch operations
- Deterministic exploit detection
- Concept has been subject of academic research and recently endorsed by Intel Security

PATENTED TECHNOLOGY, EXCLUSIVE TO CHECK POINT

CPU-LEVEL DETECTION ENGINE

And Additional Static and Heuristic Engines

Vulnerability → Exploit → Shellcode → Malware

← Traditional Sandbox →

CPU DETECTION BLOCKS MALWARE

Before the malware is downloaded….

Before the evasion code can execute…

Landing Page

Research Blog

Corporate Blog

Where will the opportunities happen? (TW)

Check Point
SOFTWARE TECHNOLOGIES LTD

- GDPR

Global Compliance

- ICT Management Regulation

TW Compliance

- Segmentation
- APT
- FinTech

FSI

- IoT
- Cloud
- SCADA

Hi-Tech

Security Best Practices for GDPR

Check Point
SOFTWARE TECHNOLOGIES LTD

1 DATA CLASSIFICATION	2 CONFIGURATION CHANGE MANAGEMENT	3 ADMINISTRATOR CONTROLS AND SEPARATION OF DUTIES	4 SECURE SYSTEM CONFIGURATION
5 ACCESS CONTROL	6 NETWORK-BASED SEGMENTATION	7 ENCRYPTION AND PSEUDONYMISATION	8 DATA LEAK PREVENTION
9 DDOS PREVENTION	10 USER ACTIVITY MONITORING	11 VULNERABILITY MANAGEMENT	12 DISASTER RECOVERY

New technology focus

Check Point
SOFTWARE TECHNOLOGIES LTD

Network Security

THREATCLOUD

CHECK POINT PRO

Cloud & Mobile Security

CHECK POINT vSEC

CLOUD

SMB & Entry Level

- **New Product Update & Competitive Information**

New Smat-1 Series are available now!

Check Point
SOFTWARE TECHNOLOGIES LTD

5th Gen Smart-1 Security Appliances

Flexible and scalable five enterprise-grade Smart-1 dedicated management appliance

	405	410	525	5050	5150
		Enterprise Grade		Ultra High End	
Hardware Specifications					
Cores	2	2	4	16	24
Storage (HDD) Hot-Swapable	1 x 1 TB	1 x 2 TB	2 x 4 TB	4 x 4 TB	Up to 12x 4TB (default 6x 4TB)
RAID Type	-	-	1	5, 10	5, 6, 10, 50, 60
Memory (RAM) Default/Max	16GB	32GB	32/64 GB	64/128 GB	128/256 GB
Capacity and Performance					
Managed Gateways	5	10	25	50	150+[1]
Max Domains (Multi-Domain Mgmt)	-	-	-	50	200
Peak Logs per Sec	40,000	45,000	60,000	80,000[3]	100,000[3]
Peak Indexed Logs per Sec	6,000/400[2]	10.000/600[2]	14,000/1,600[2]	27,000[3]/7,500[2]	40,000[3]/12,000[2]
Sustained Indexed Logs per Sec	3,000/200[2]	5,000/300[2]	7,000/800[2]	15,000[3]/3,750[2]	22,000[3]/6,000[2]
GB per Day of Logs	53/1.7[2]	88/5.2[2]	150/17.1[2]	320/80[2]	470/128[2]

Top 5 FACTS to FOCUS on, in a COMPETITIVE situation vs PAN

Check Point
SOFTWARE TECHNOLOGIES LTD

1. Palo Alto is **susceptible to evasions.** simple obfuscation techniques will leave customers **vulnerable** to trivial **attacks**

2. Palo Alto only detects malware after the fact. **NO REAL-TIME PREVENTION**

3. Palo Alto uses **security shortcuts,** leaving customers **exposed** to malware

4. Palo Alto **own products** are not **secure**

5. **Sense of Urgency:** Palo Alto leaves its customers **exposed** to known **vulnerabilities**

1 PALO ALTO LEAVES YOU VULNERABLE. WANT TO TAKE THE RISK?

Check Point
SOFTWARE TECHNOLOGIES LTD

THIS CAN BE EASILY DEMONSTRATED:

- "HTTP Evader" – a very popular IPS / Next-Gen FW evasion tool that was developed 2 years ago by an independent security expert Steffen Ullrich.
- The movie below demonstrates the results when checked on Palo Alto gateways.
- Customers can realize similar results on their own:
  - Ask your customer to run this URL https://noxxi.de/research/http-evader.html from their desktop and **Follow this How-To Guide**

Test is done including Palo Alto security best practices configuration

Scan to Watch Full Video

http://tiny.cc/httpevader

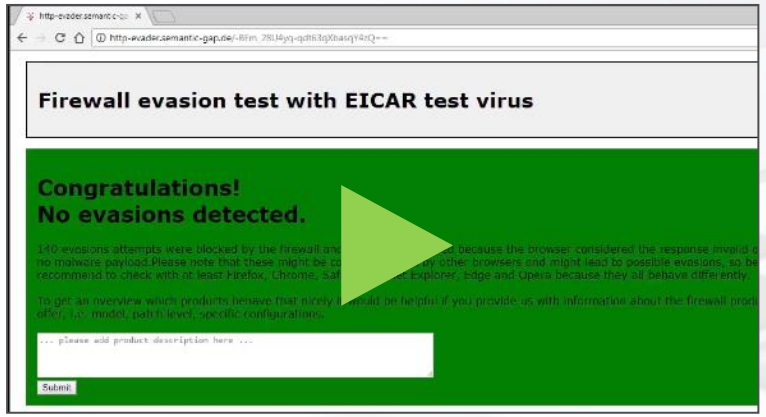
1 PALO ALTO LEAVES YOU VULNERABLE. WANT TO TAKE THE RISK?

Check Point
SOFTWARE TECHNOLOGIES LTD

WHAT ABOUT CHECK POINT?

- Do share the movie below, this time testing Check Point
- Alternatively customers can use the tool on their own, testing our IPS.

  Hint: no success in evading us.. ☺



Test is done including Check Point security best practices configuration.

2 PALO ALTO's IDEA OF "PREVENTION"

Check Point
SOFTWARE TECHNOLOGIES LTD

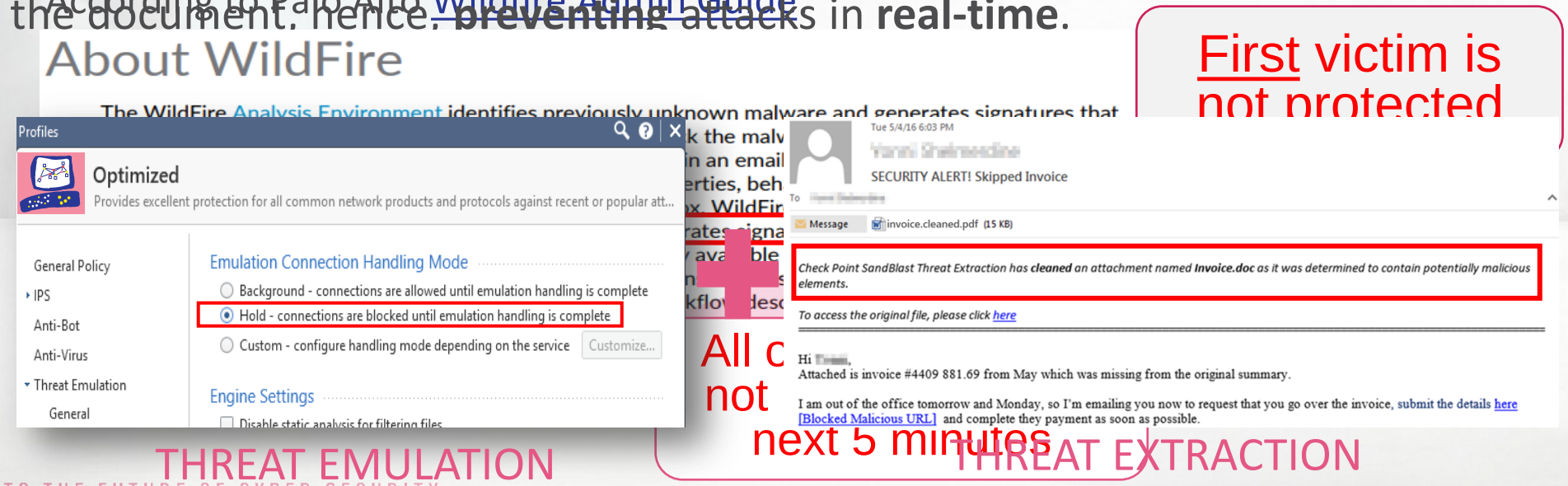
Palo Alto

- Wildfire (PAN Sandbox) CANNOT block threats from entering the network and infecting end point devices.
- Wildfire can only alert after the fact. Getting Infected is inevitable with Palo Alto's solution.

WHAT ABOUT CHECK POINT?

- Can **HOLD** connections **until emulation is complete**. Our Threat Extraction provides a sanitized copy of the document, hence **preventing** attacks in **real-time**.

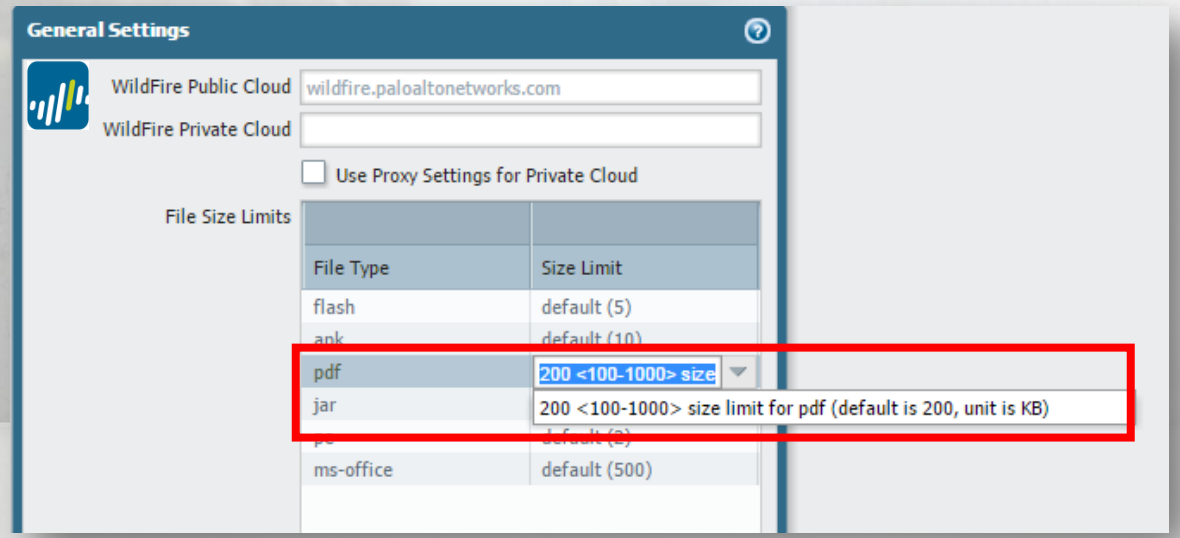
According to Palo Alto Wildfire Admin Guide:

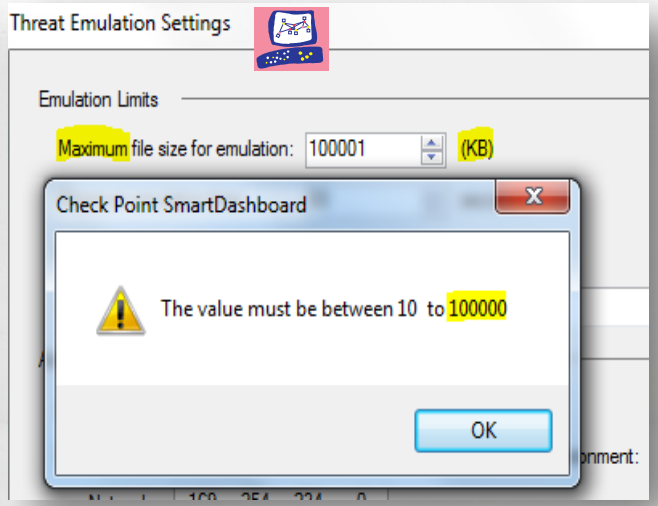


3 PALO ALTO SECURITY SHORTCUTS CAN COST YOU

Check Point
SOFTWARE TECHNOLOGIES LTD

- Example: Palo Alto Wildfire can only emulate PDF files smaller than 1MB
- As an attacker – do you need to be a genius to attack a customer using Wildfire?
- **Check Point SandBlast** emulates files up to 100MB





100X

Did You Know:
in the past 90 days:
out of **36K** malicious PDF files seen in Check Point Threat Cloud – **1,010 were above 1MB**

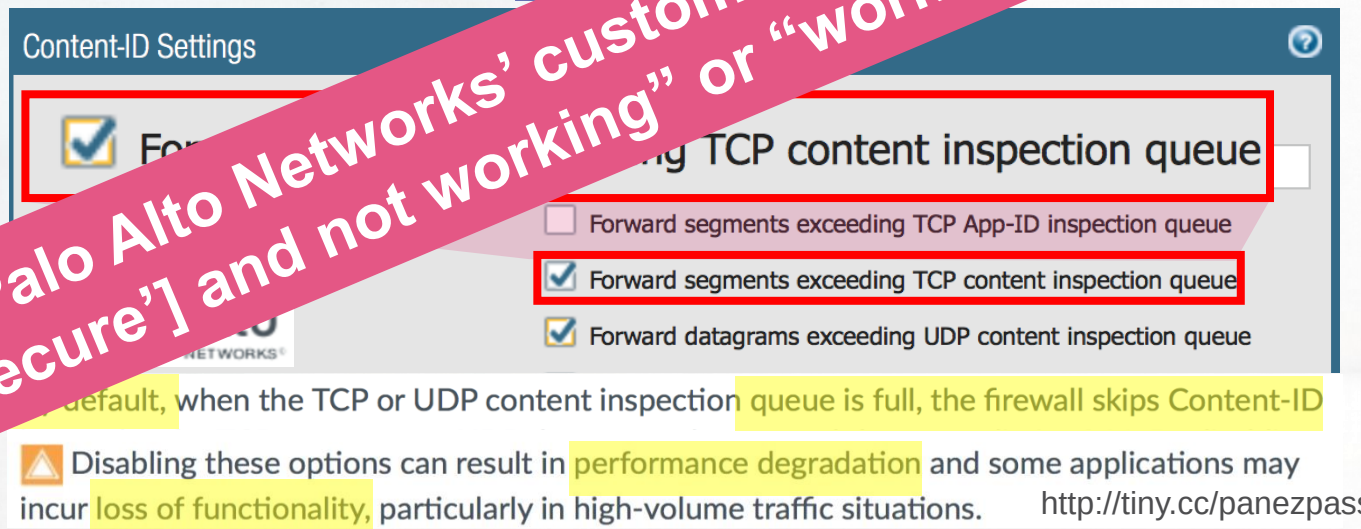
source: VirusTotal

3 PALO ALTO SECURITY SHORTCUTS CAN COST YOU

Check Point
SOFTWARE TECHNOLOGIES LTD

- **By Default**, when queue is full (high load), Palo Alto firewall **SKIPS INSPECTI** nce, **FORWARDS** the traffic inside the network **WITHOUT INSPECTING it**
- **Changing the default** behavior – results in performance **DEGR** e applications may incur **LOSS** of functionality

Source: PAN



Palo Alto Networks' customers have two choices: "['secure'] and not working" or "working and not secure"

http://tiny.cc/panezpass

4 PAN PRODUCTS ARE SEVERELY VULNERABLE! Using them will expose you to many backdoors

Check Point
SOFTWARE TECHNOLOGIES LTD

- Vulnerabilities on security products happen all the time. Once such vulnerability is disclosed, the vendor decide how to fix it and when.
- Let's compare the vulnerability status of Check Point and Palo Alto in 2016 & 2017 – we compared number of vulnerabilities and average time to fix.

	Check Point	Palo Alto
# Total of SW vulnerabilities(2016,2017)	2 Vulnerabilities	93 Vulnerabilities
Average Fix Time (days)	1 Day	183.6 Days

Source: relevant vendor's public security advisory web pages & http://tiny.cc/urgency

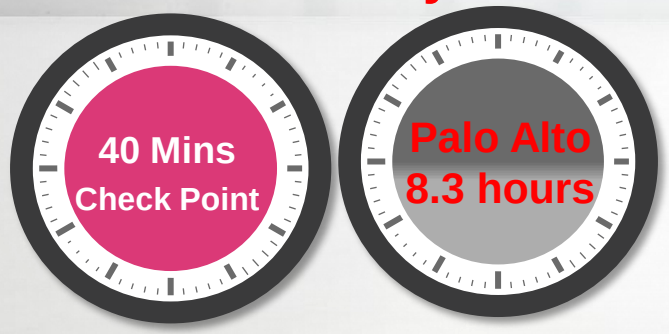
Palo Alto, with high number of vulnerabilities and **inexcusable** slow response time

5 PAN Sense of Urgency?

- Microsoft releases security patches regularly on Tuesdays. Security vendors write IPS signatures for it.
- Below you will find:
  - a comparison between the 2017 average time it took Check Point to release a signature to the time it took PAN – following a patch release by Microsoft
  - additional examples: **3 major vulnerabilities** exploited **in the wild** caused **massive damage** worldwide
    - WannaCry and Not-Petya – crypto lockers attacks that caused an estimated amount of $4 Billion in losses.
    - Meltdown & Spectre are **major widespread vulnerability** discovered on the most popular microprocessors (Intel, AMD, ARM)

Microsoft Patch Tuesday

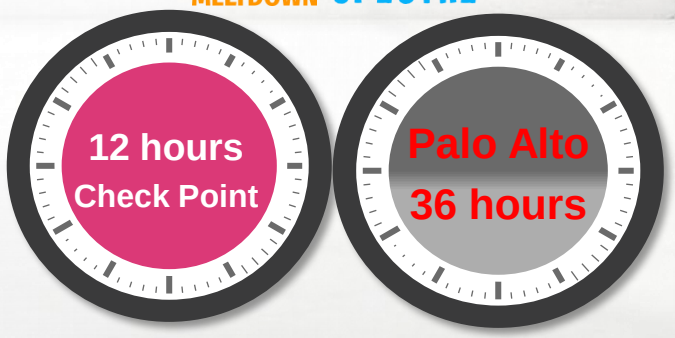
Patch Tuesday 2017



Wanna Cry NOTPETYA

WannaCry & Not-Petya

MELTDOWN SPECTRE



Reference: http://tiny.cc/urgency

Summary

paloalto NETWORKS®

1. Palo Alto security bypassed by simple evasion methods
2. PAN advanced threat prevention (Wildfire) cannot prevent patient zero in real-time
3. PAN uses unacceptable security shortcuts by default on expense of security
4. PAN is slow to address (the many) vulnerabilities in their products

Check Point® SOFTWARE TECHNOLOGIES LTD.

1. Check Point is secured. Period.
2. Check Point stops malware from getting into your network before it happens
3. Check Point puts security first
4. Security is the core of Check Point DNA. We respond swiftly

Application identify?

Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point AppWiki

The AppWiki is an easy to use tool that lets you search and filter Check Point's Web 2.0 Applications Database to find out information about internet applications, including social network widgets; filter by a category, tag, or risk level; and search for a keyword or application.

Resources | Sea

NEXT

solutions offer extensive
time through views,
malicious, risky, and
ıe perimeter, in the data
ts.

Careers Contact

Type to Search | 7,796 Applications

Include 255,736 Social Network Widgets

54 Applications (Clear filters)

RACTERISTIC

ndwidth
se

469 networking

63 encrypted-tunnel
48 erp-crm
304 file-sharing
63 gaming
151 general-business
80 infrastructure

359 4
138 5

1162 Transfers Files
368 Tunnels Other Apps
312 Used by Malware
1560 Vulnerabilities
1298 Widely Used

https://appwiki.checkpoint.com/appwikisdb/public.htm

https://fortiguard.com/learnmore#ac

https://applipedia.paloaltonetworks.com/

Check Point
SOFTWARE TECHNOLOGIES LTD

THANK YOU

2018Q1 SE Club

Danny Yang | SE

WELCOME TO THE FUTURE OF
CYBER SECURITY
POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION