



**Check Point**  
SOFTWARE TECHNOLOGIES LTD

**SKO2017**  
ONE STEP > AHEAD

# THE **DIFFERENCE** AND WHY IT **MATTERS**

Moti Sagey | Head of Strategic Marketing & Intelligence



Check Point®  
SOFTWARE TECHNOLOGIES LTD

**“IN GOD WE TRUST  
ALL OTHERS  
MUST BRING DATA”**

*W. Edwards Deming*

# WHAT DOES IT TAKE TO GAIN YOUR TRUST ?



Check Point<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD

**1** UNCOMPROMISED  
SECURITY

**2**

EVERYWHERE  
ARCHITECTURE

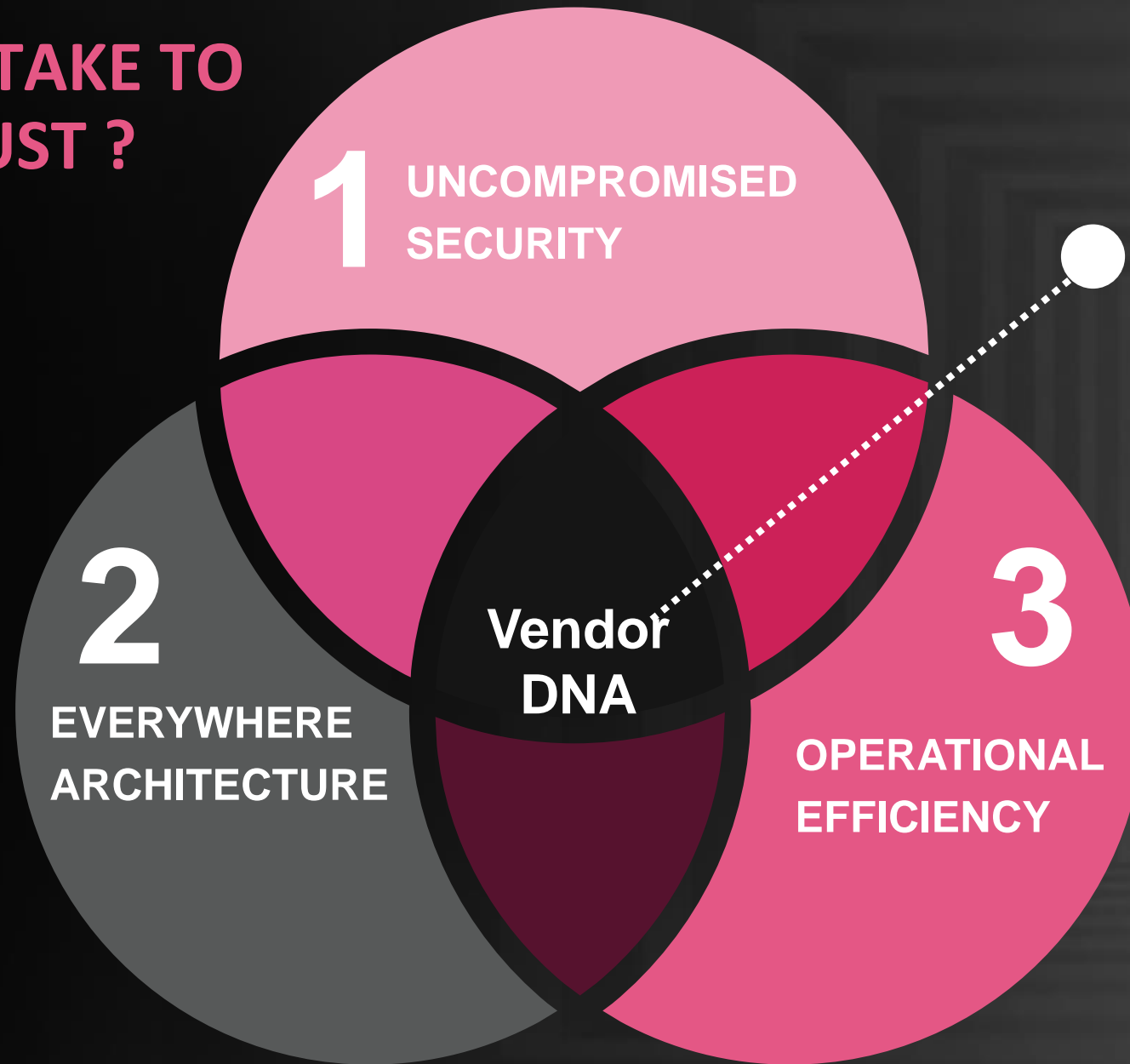
**3**

OPERATIONAL  
EFFICIENCY

# WHAT DOES IT TAKE TO GAIN YOUR TRUST ?



Check Point®  
SOFTWARE TECHNOLOGIES LTD



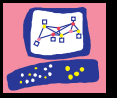
The CORE of  
Vendor DNA:  
COMMITMENT  
TO CUSTOMER  
SUCCESS



Commitment to customer success, what does it mean?

IT ALL STARTS WITH  
THE RIGHT FOCUS..

# ... TO KEEP CUSTOMERS PROTECTED



Check Point<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD

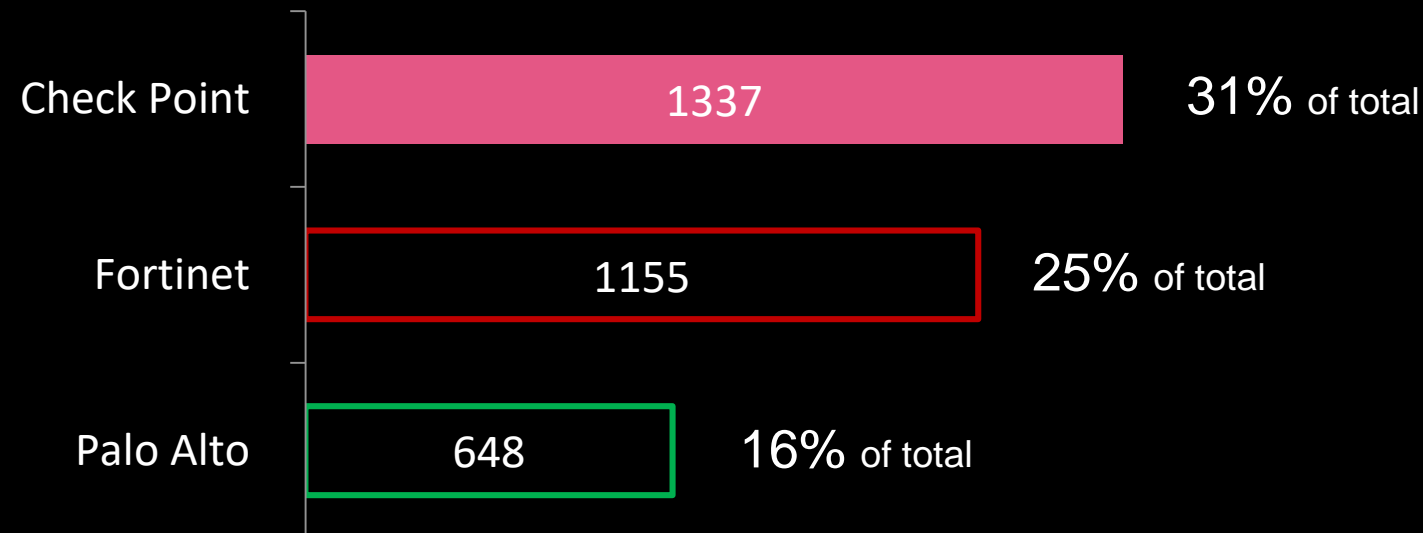
1337

R&D Engineers

31% of Employees

2X more than Palo Alto

“Do they put their  
Headcount where their  
MOUTH is???”



Source: Palo Alto's Form 10-Q for the quarterly period ended October 31, 2016  
Fortinet Q3 2016 Financial Results October 27, 2016



Commitment to customer success, what does it mean?

# WITH THE RIGHT PHILOSOPHY: **PREVENTION**

# THE IMPORTANCE OF REAL-TIME PREVENTION





# THE IMPORTANCE OF REAL-TIME PREVENTION



Check Point  
SOFTWARE TECHNOLOGIES LTD

5. Select the update frequency from the **Update Frequency** drop-down list.

You can select the following update frequencies:

- daily
- **hourly**

## About WildFire

The WildFire **Virtual Sandbox** identifies previously unknown malware and generates signatures that Palo Alto Networks firewalls can use to then detect and block the malware. When a Palo Alto Networks firewall detects an unknown sample (a file or a link included in an email), the firewall can automatically forward the sample for WildFire analysis. Based on the proWildFire Administrator's Guide properties, behaviors, and activities the sample displays when analyzed and executed in the WildFire sandbox, WildFire determines the sample to be benign, grayware, or malicious. **WildFire then generates signatures** to recognize the newly-discovered malware, and makes the latest signatures globally available every **five minutes**. All Palo Alto Networks firewalls can then compare incoming samples against these signatures to automatically block the malware first detected by a single firewall.

Cloud **does not block** files that it uploads. Instead they are used to improve how  
red and signatures created for them and added to the FortiGuard antivirus

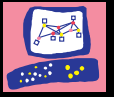
FortiOS™ Handbook - FortiOS Handbook for FortiOS 5.4.0



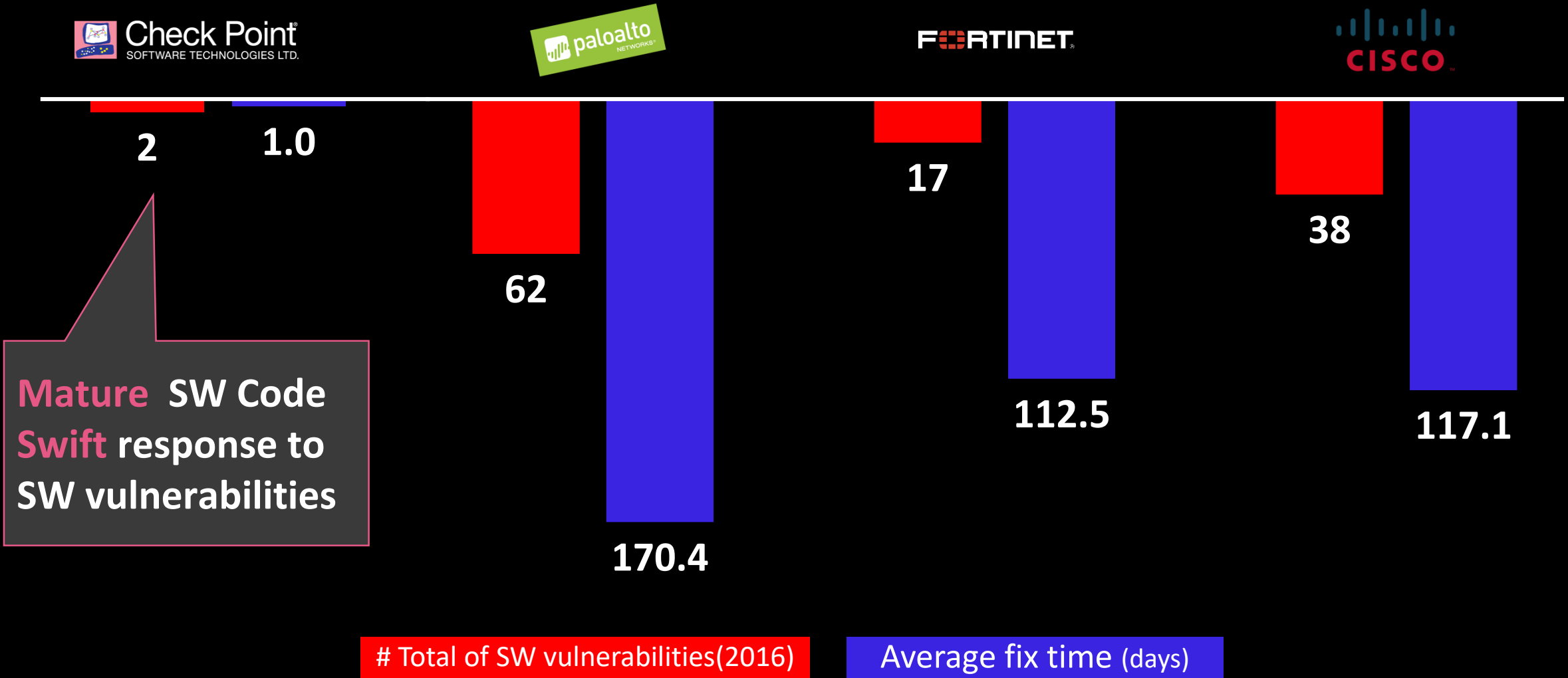
Commitment to customer success, what does it mean?

# WITH AN UNPARALLELED SENSE OF URGENCY

# TO MAKE SURE CUSTOMERS ARE NOT EXPOSED...



Check Point  
SOFTWARE TECHNOLOGIES LTD

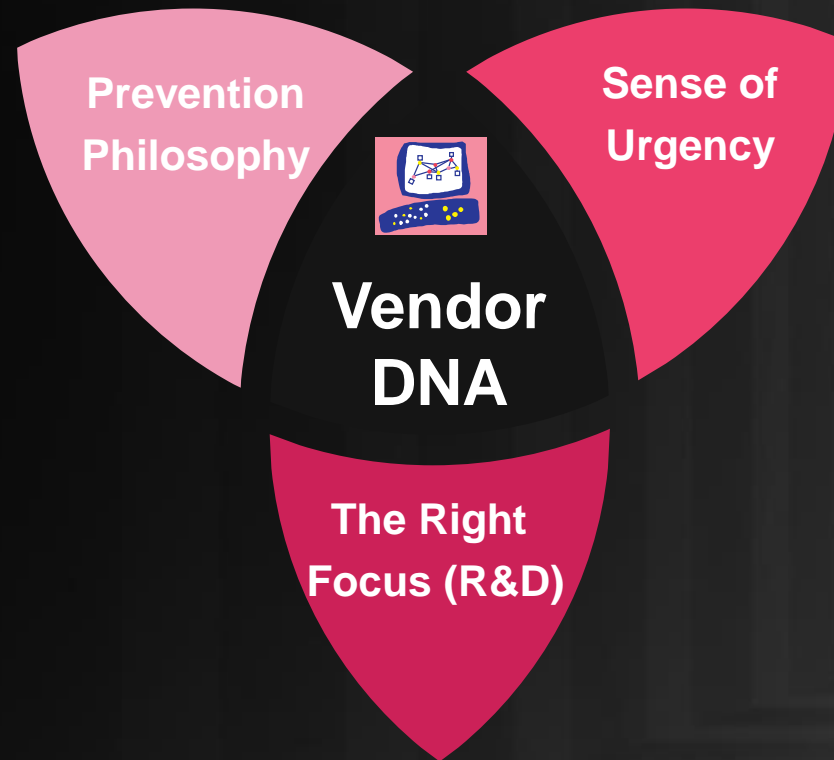


#of software vulnerabilities in 2016

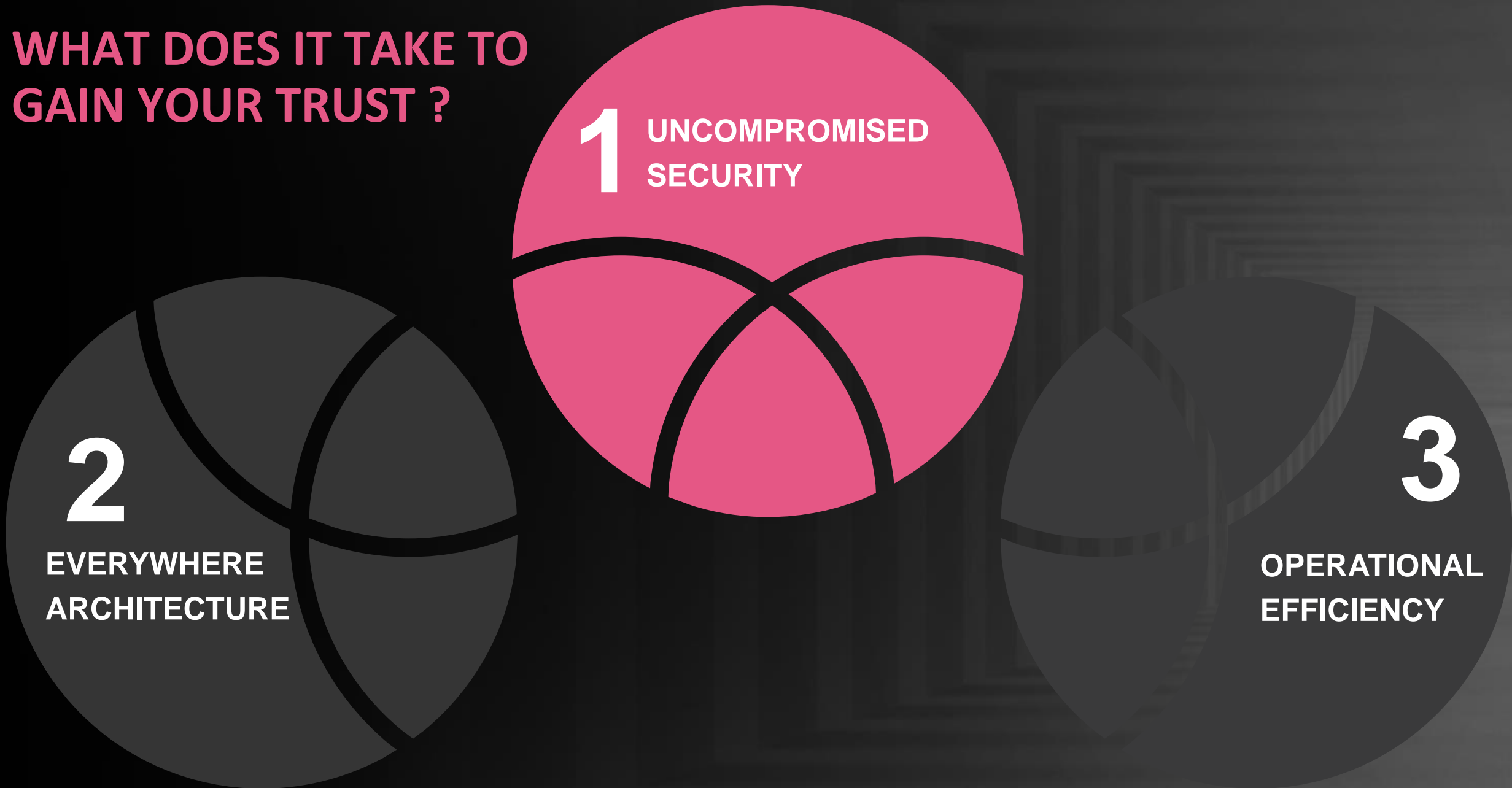
Source: vendors security advisories web pages & <http://goo.gl/5ZsHv6>

# SUMMARY: THE CORE OF VENDOR DNA

## COMMITMENT TO CUSTOMER SUCCESS

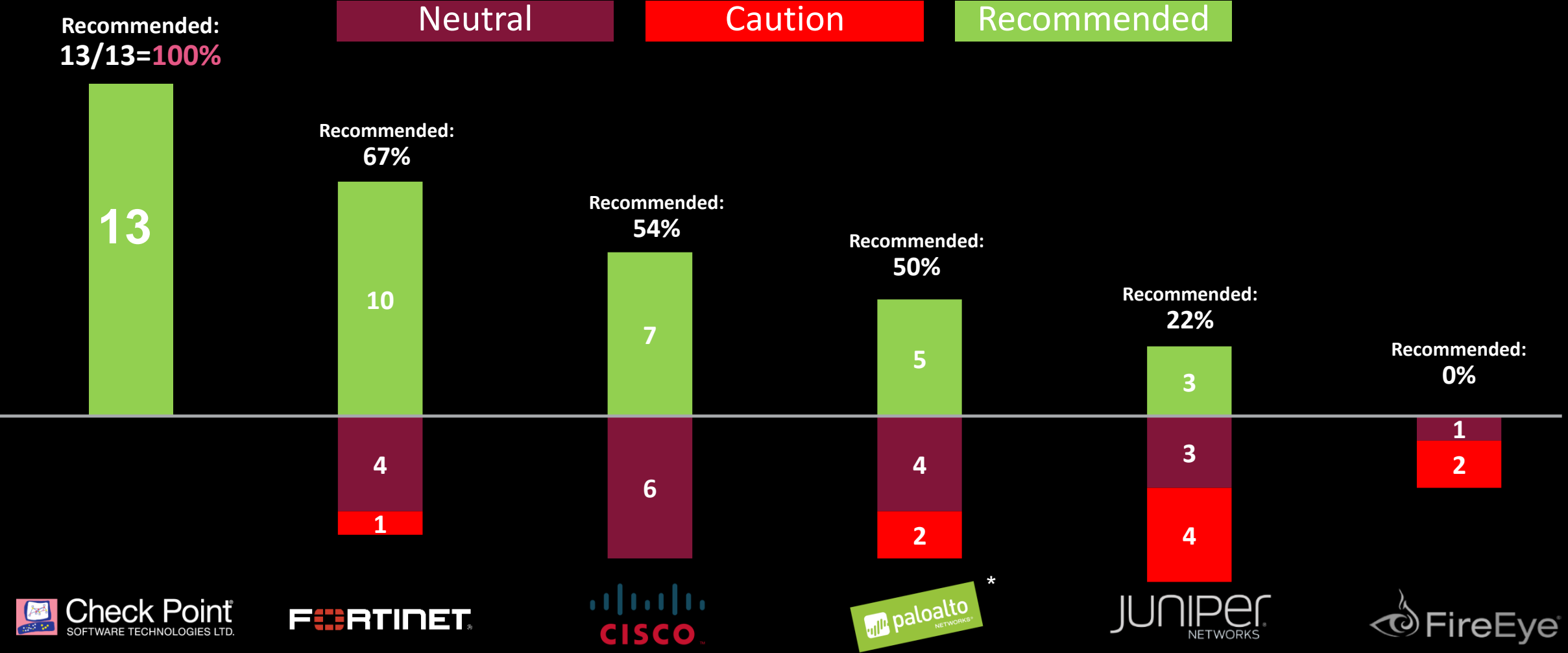


# WHAT DOES IT TAKE TO GAIN YOUR TRUST ?



# UNCOMPROMISED SECURITY STARTS WITH 3<sup>RD</sup> PARTY

## PROVEN TRACK RECORD OF SECURITY EXCELLENCE



Source: NSS Labs Network Security tests (FW/NGFW/IPS/NGIPS/DCIPS/BDS) \* PAN NGFW solution have not been recommended since 2013

# SECURITY SHORTCUTS RISK AND REWARD



Check Point  
WARE TECHNOLOGIES LTD

Security Services Settings

☐ Disable DPI Engine

☐ Apply IPS Signatures Bidirectionally

☒ Enable IP fragment reassembly in DPI

☐ Extra dev debug info

☐ Disable App-Firewall SMTP CHUNKING modification

☐ Disable <https://10.99.99.70/diag.html>

☐ Disable Gateway AV POPS Auto Deletion

Hidden configuration page

Options

Log Setting

☒ Log at Session Start

☒ Log at Session End

Log Forwarding: None

☒ Disable Server Response Inspection

Schedule: None

QoS Marking: None

☒ Disable Server Response Inspection

```
FortiGate-VM64 # config ips global
FortiGate-VM64 (global) # get
fail-open      : disable
database       : regular
traffic-submit  : disable
anomaly-mode    : continuous
session-limit-mode : heuristic
intelligent-mode : enable
socket-size     : 4 (mb)
engine-count    : 0
algorithm       : engine-pick
skype-client-public-ipaddr:
deep-app-insp-timeout: 86400
deep-app-insp-db-limit: 25000
```

Targets

Servers

default

Configuration

Networks: default

Ports: 80, 1220, 1741, 2301, 2980, 3128,

Oversize Dir Length: 500 (1 or greater)

Client Flow Depth: 300 bytes

(Maximum allowed)

(0 - 255. When Small CH

WatchGuard Fireware XTM Web UI

DASHBOARD

SYSTEM STATUS

NETWORK

FIREWALL

SUBSCRIPTION SERVICES

Application Control

WebBlocker

spamBlocker

Gateway AV

IPS

Quarantine Server

IPS

☒ Enable Intrusion Prevention

Settings Update Server Signatu

Scan Mode

☐ Full Scan ☒ Fast Scan

# HOW TO EXPOSE SECURITY SHORTCUTS IN POC'S

DOWNLOAD THE GUIDE <http://tiny.cc/poc-shortcuts>



Check Point  
SOFTWARE TECHNOLOGIES LTD



## HOW TO EXPOSE SHORTCUTS IN COMPETITIVE POC

When testing different vendors in a PoC, it is important to do an Apples-to-Apples Comparison in order to measure all vendors' capabilities equally. Unfortunately, some security vendors use shortcuts with their security solutions and products (e.g. IPS, AV) in order to gain better performance results in a competitive PoC, which do not reflect their actual functionality and performance in production networks. Shortcuts can improve performance but on the expense of the solution overall security. The list below, will show how to expose if a vendor attempted to shortcuts and how to disable those shortcuts in a PoC

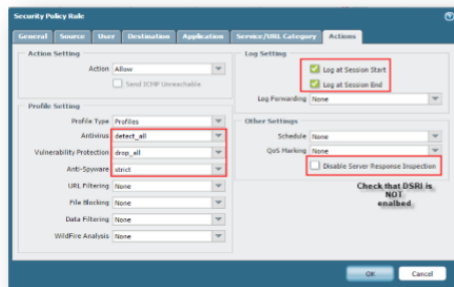
### GENERAL CONFIGURATION (FOR ALL VENDORS)

- **Networking** - Use Layer 3 interfaces and routing instead of bridge mode/virtual wire/span port/port mirror to reflect production network settings
- **Policy Rules** - Create policy rules with NAT & full session logging which reflect production policies and has effect on performance
- **Best Practices** - Configure policy according to each vendor security best practices

### Palo Alto Networks

- **Enable Advanced Security** - set Vulnerability and Anti-spyware security profiles to strict and Antivirus profile to drop (equivalent to CP recommended protection)
- **Logging** - enable logging at the session start and at session end
- **Disable Shortcuts** - disable DSR1 on all policy rules to prevent partial scan of traffic (this feature is activated in PoC to gain better performance results)

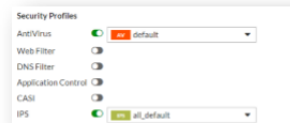
\*Palo Alto Web GUI > Policies > Add/edit rule > Actions



### Fortinet

- **Enable Advanced Security** - set IPS and Anti-Virus security profiles to block malware in all policy rules, and set AV profile to proxy mode vs. quick/flow mode which is often used in POC but has minimum security effect  
\*Fortigate > Policies & Objects > IPv4 Policies > Add/edit rule > Security Profiles
- **Disable Shortcuts** - disable intelligent-mode which scans only part of IPS/AV traffic

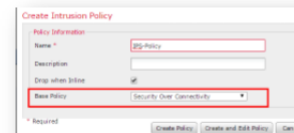
\*Fortigate CLI > 'config ips global' > 'set intelligent-mode disable'



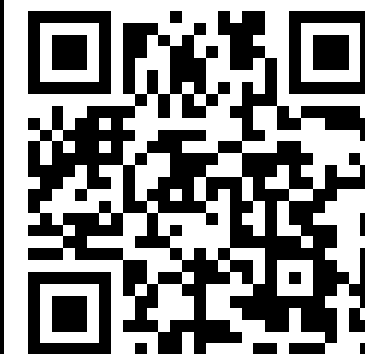
```
FG100D3G13814900 # config ips global
FG100D3G13814900 (global) # set intelligent-mode disable
FG100D3G13814900 (global) # get
fail-open : enable
database : regular
traffic-submit : disable
exempt-mode : continuous
session-limit-mode : heuristic
intelligent-mode : disable
packet-size : 64 (MB)
engine-connat : 0
algorithm : engine-pick
sync-session-ctl : disable
skip-client-public-ipaddr :
deep-app-insp-timeout : 64000
deep-app-insp-dm-limit : 100000
exclude-signatures : industrial
FG100D3G13814900 (global) #
```

### Cisco

- **Enable Advanced Security** - set IPS security profile to security over connectivity
- **Disable Shortcuts** - set the HTTP Client Body Extraction Depth to zero to inspect all HTTP traffic  
\*FireSIGHT > Access Policy > Network Analysis Policy > create new > Choose 'Security over connectivity' > go to 'HTTP Configuration' > change 'HTTP Client Body Extraction Depth' from 4000 to 0



HTTP Client Body Extraction Depth: 0



©2016 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content  
Q2, 2016 | 3



# THE “CHECK-BOX” SYNDROME



# NSS LABS NGFW 2016 TEST EXPLOIT **BLOCK-RATE** BY YEAR



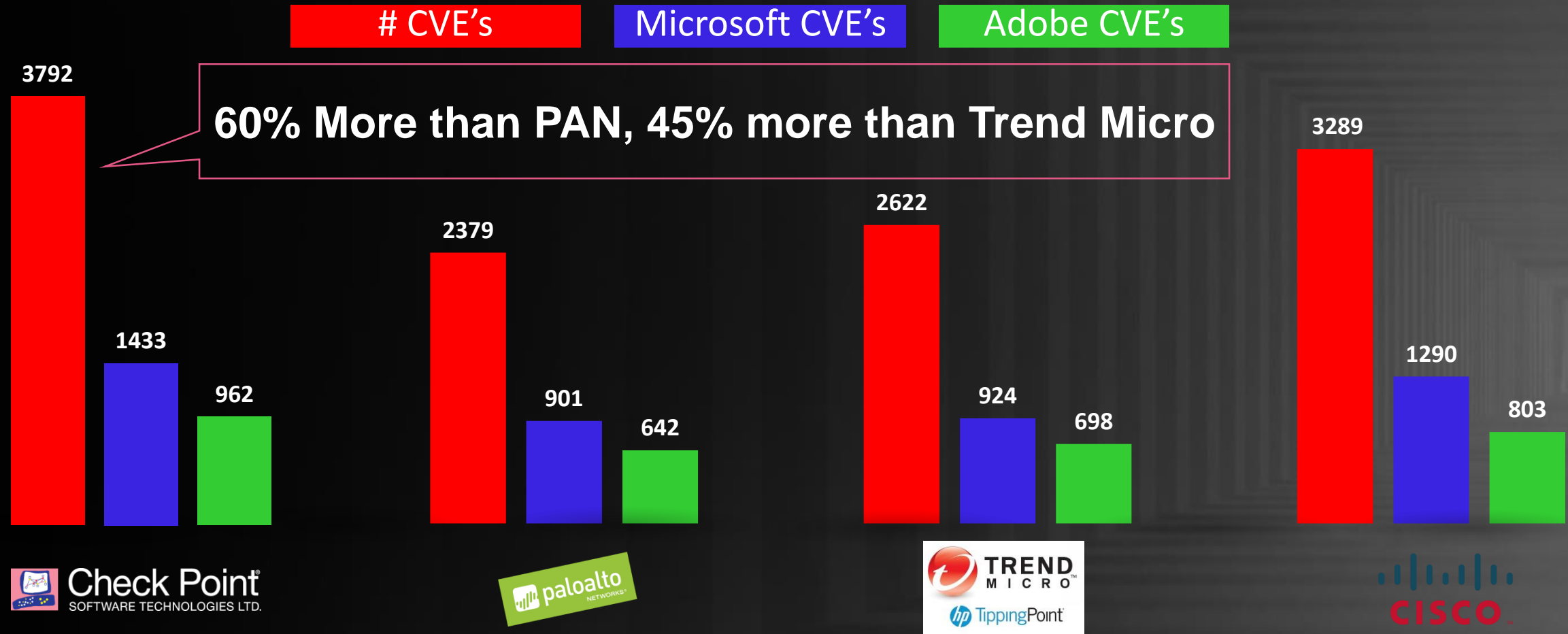
	2012	2013	2014	2015	# of exploits missed (of 1999)
Check Point	100%	100%	100%	100%	3
Cisco FirePower	95.6%	97.5%	83.0%	74.2%	87
Dell SonicWall	98.5%	97.5%	82.5%	83.9%	52
Fortinet	99.5%	100%	94.3%	100%	14
Palo Alto Networks	94.6%	97.5%	83.0%	87.1%	83

Source: [http://www.slideshare.net/zztop\\_2764/fortinet-nss-ngfw-2016-latency-catchrate](http://www.slideshare.net/zztop_2764/fortinet-nss-ngfw-2016-latency-catchrate)

# ITS NOT BY CHANCE: NUMBER OF THREATS (CVE'S) COVERED BY IPS (2010-2016)



Check Point  
SOFTWARE TECHNOLOGIES LTD



Information is current as of Jan 2010 - Oct 2016 | Source: [Check Point Advisories](#) | [Palo Alto ThreatVault](#) | [Fortinet FortiGuard](#) | [Mcafee Threat Intelligence](#) | [Tipping Point Digital Vaccine](#) | [SourceFire Advisories](#)

# WHAT DOES IT TAKE TO GAIN YOUR TRUST ?



Check Point®  
SOFTWARE TECHNOLOGIES LTD

**1** UNCOMPROMISED  
SECURITY

**2**

EVERYWHERE  
ARCHITECTURE

**3**

OPERATIONAL  
EFFICIENCY



# THE CHALLENGE OF SECURING BORDERLESS NETWORKS



Check Point<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD



# THE NEED: BLOCKING ATTACKS IN ANY ENVIRONMENT



Check Point  
SOFTWARE TECHNOLOGIES LTD.

SECURITY  
ACROSS  
ALL  
BUSINESS  
PLATFORMS

CLOUD  
IoT  
SERVER  
MOBILE  
VIRTUALIZATION

Background network diagram with nodes labeled: CAR, HOME, DOOR, SENSOR, MOBILE, CLOUD, WEARABLES, MOBILE.



# CHECK POINT SOFTWARE BASED ARCHITECTURE MEANS EVERYWHERE AGILE SECURITY



Check Point  
SOFTWARE TECHNOLOGIES LTD



vmware®



openstack™

vmware®  
vCloud Air



ANDROID



# WHAT DOES IT TAKE TO GAIN YOUR TRUST ?



Check Point<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD

**1** UNCOMPROMISED  
SECURITY

**2**

EVERYWHERE  
ARCHITECTURE

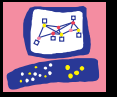
**3**

OPERATIONAL  
EFFICIENCY

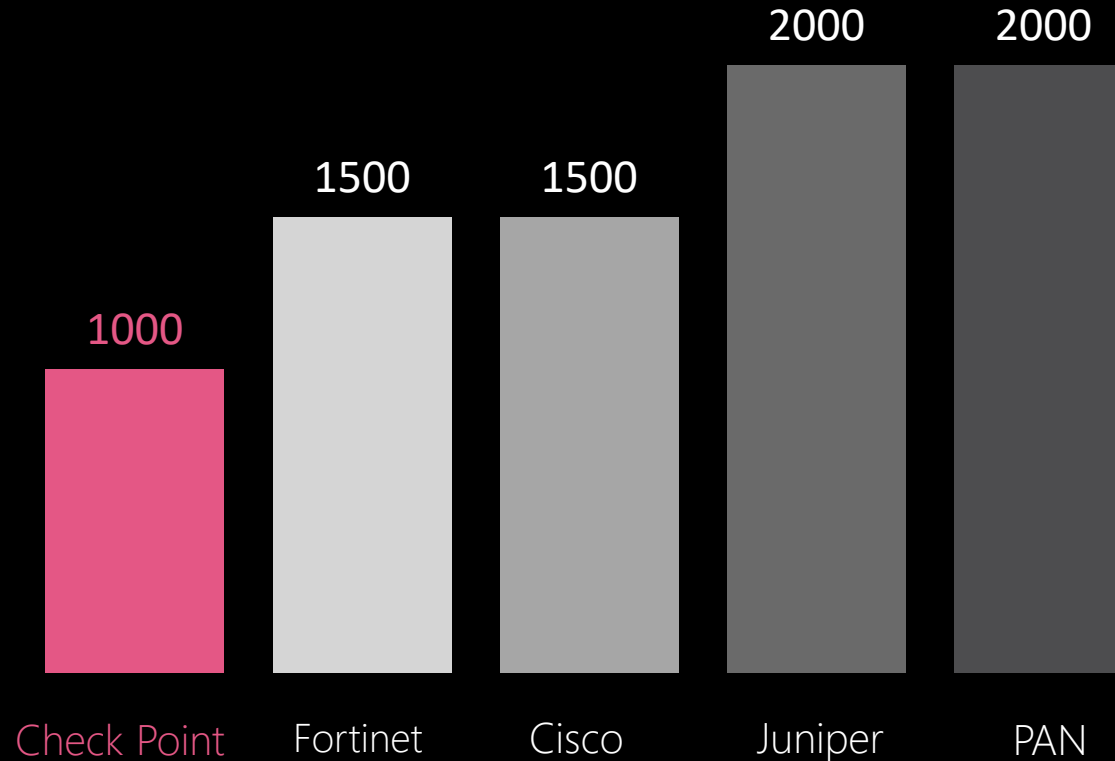


# IMPROVED PRODUCTIVITY

Man hours required for yearly management of 50 gateways per site



Check Point<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD



Source: NSS Labs NGFW Group Test

*“The Check Point management remains the de facto **“GOLD STANDARD”** against which other consoles are measured”*

**Gartner**

# THE WHY - UNMATCHED UNIFIED ACCESS POLICY



Check Point  
SOFTWARE TECHNOLOGIES LTD

Name	Source	Destination	Services & Applications	Data	Action	Install On
Outbound access	production_net	Internet	* Any	* Any	AccessSubLayer	* Policy Targets
Social media for marketing	marketing_role John	Internet	Twitter LinkedIn Instagram	* Any	Accept	SG13800
Developers upload	developer_role	Internet	Dropbox Box	Any Direction Source Code - JAVA	Accept	SG13800 CapsuleCloud
Access Sensitive Servers	* Any	* Any	* Any	* Any	SensitiveServers	* Policy Targets
Mobile Access	Mobile Devices	MailUS	MailServer	* Any	Accept	Mobile
Access to Web Server	* Any	WebServer	https	* Any	Accept	AWS VMWare

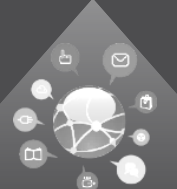
Users



Devices



Applications



Data



Gateways



Mobile



Public Cloud



Private Cloud





Check Point®  
SOFTWARE TECHNOLOGIES LTD

# SUMMARY



# THE DIFFERENCE

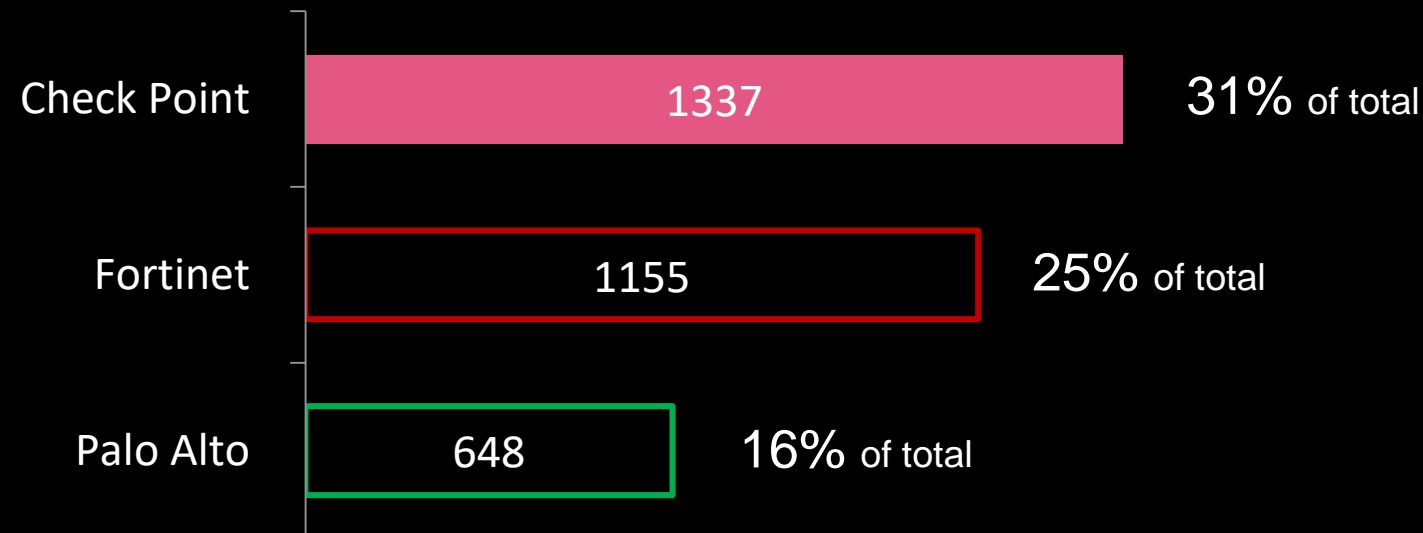
1337

R&D Engineers

31% of Employees

2X more than Palo Alto

“Do they put their  
Headcount where their  
MOUTH is???”



Source: Palo Alto's Form 10-Q for the quarterly period ended October 31, 2016  
Fortinet Q3 2016 Financial Results October 27, 2016

# ...WHY IT MATTERS



Check Point<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD

**1** UNCOMPROMISED  
SECURITY

**2**

EVERYWHERE  
ARCHITECTURE

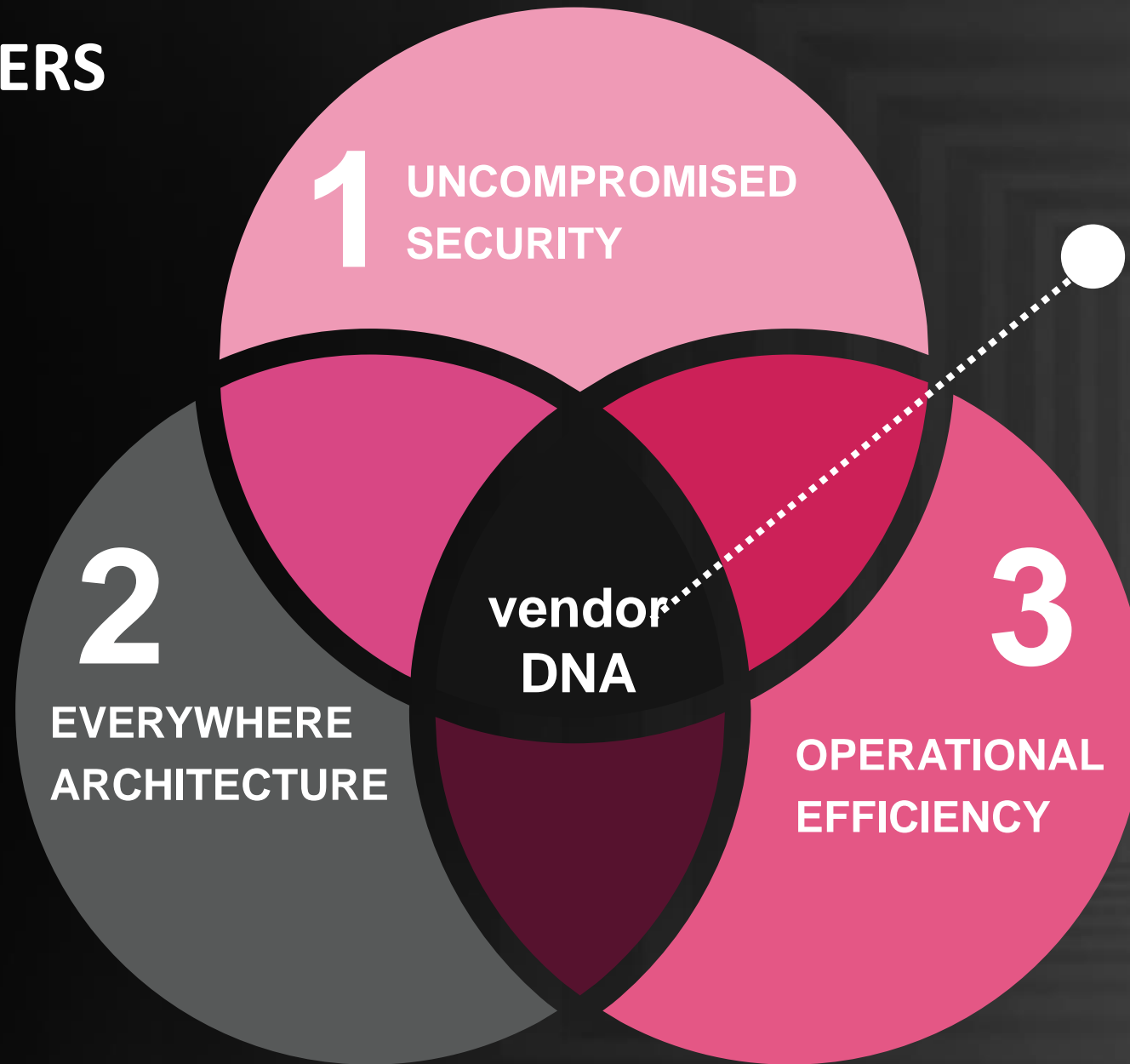
**3**

OPERATIONAL  
EFFICIENCY

# ...WHY IT MATTERS



Check Point<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD



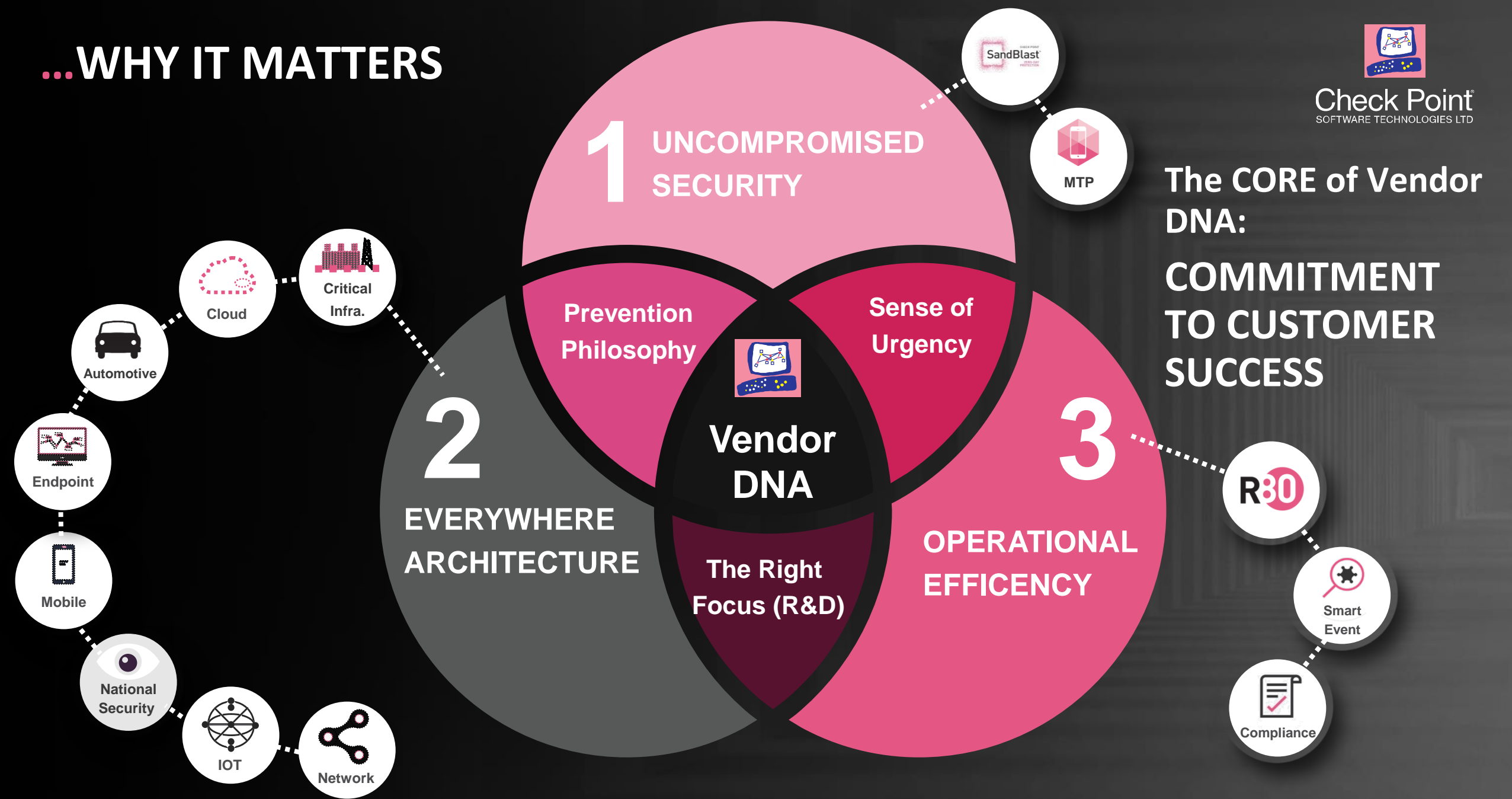
The CORE of Vendor  
DNA:  
**COMMITMENT  
TO CUSTOMER  
SUCCESS**

# ...WHY IT MATTERS



Check Point  
SOFTWARE TECHNOLOGIES LTD

The CORE of Vendor  
DNA:  
**COMMITMENT  
TO CUSTOMER  
SUCCESS**





**Check Point**  
SOFTWARE TECHNOLOGIES LTD

**SKO2017**  
ONE STEP > AHEAD

# THANK YOU

<http://tiny.cc/thedifference>