

ICION 6TH CONFERENCE 2018

Title : Securing Check Point

Bruce Chai

Check Point

06th March 2018 Ambarrukmo, Yogyakarta



Check Point[®]
SOFTWARE TECHNOLOGIES LTD





Check Point
SOFTWARE TECHNOLOGIES LTD

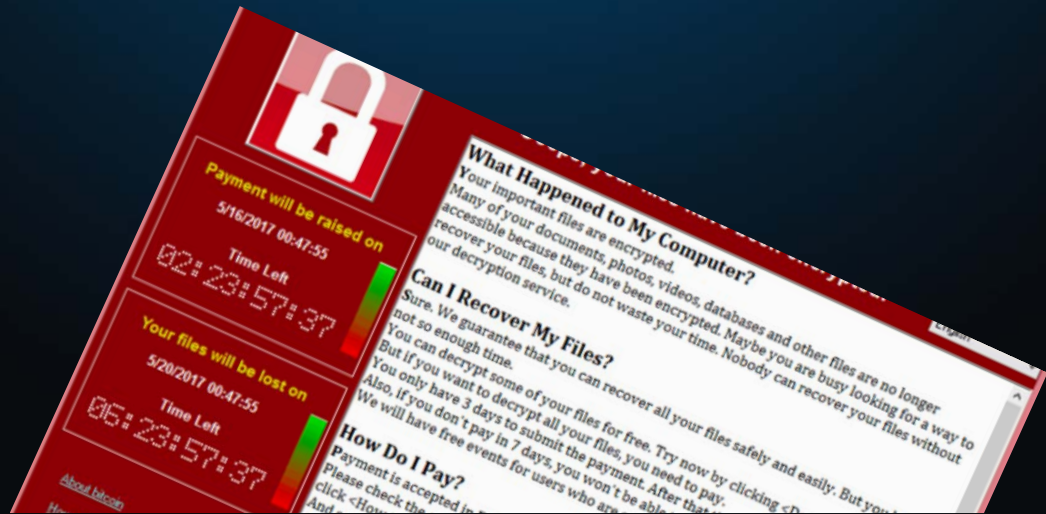
May 12th

2017



Check Point
SOFTWARE TECHNOLOGIES LTD

ZERO INFECTIONS





Check Point
SOFTWARE TECHNOLOGIES LTD

CIO

ENABLE GROWTH,
ADVANCE THE IT

MAINTAIN
SECURITY





Check Point
SOFTWARE TECHNOLOGIES LTD

TOOLS



ENABLE GROWTH,
ADVANCE THE IT

INFRA STRUCTURE



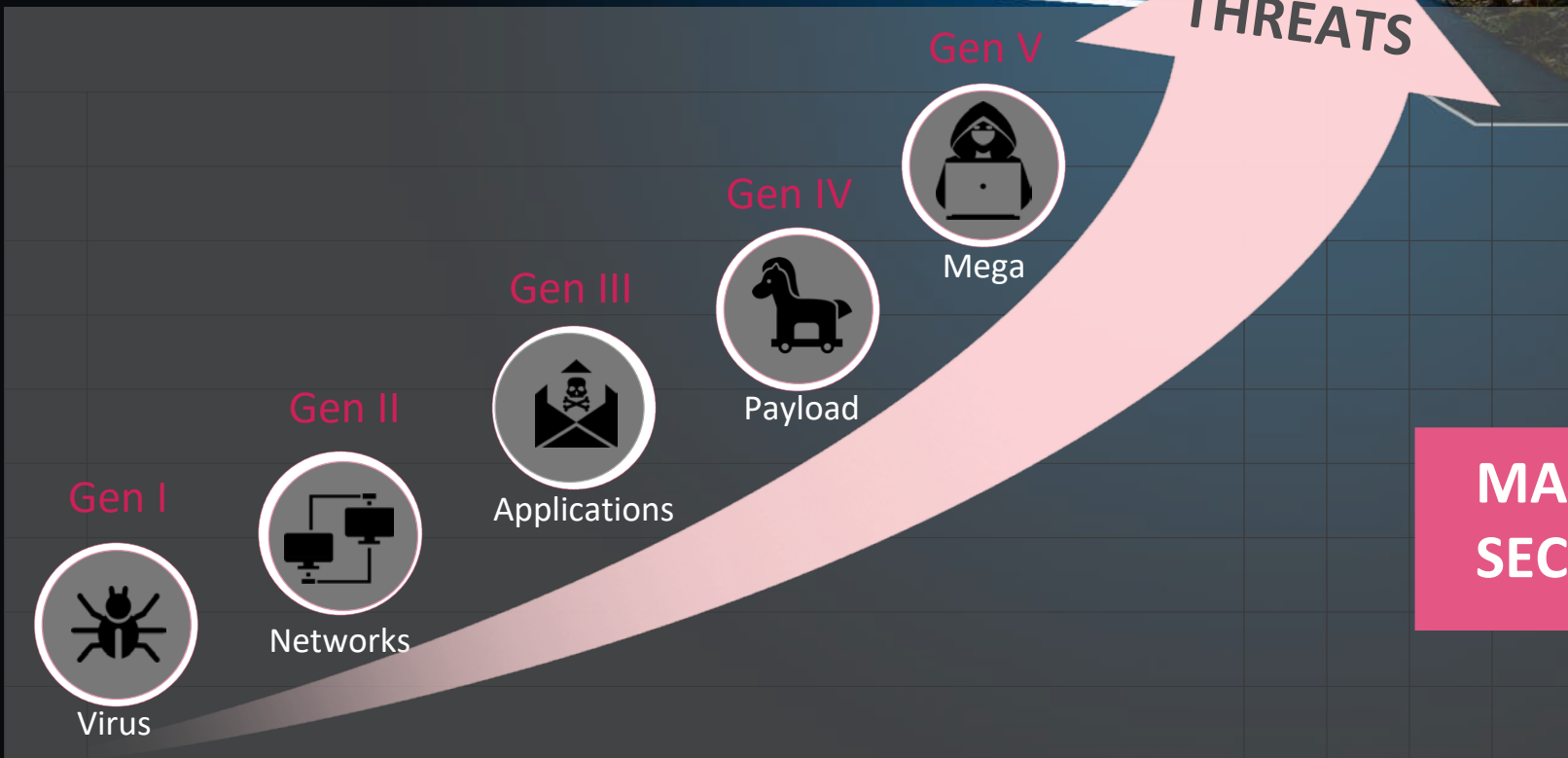
CLOUD



Evolving threats



Check Point
SOFTWARE TECHNOLOGIES LTD



1990 2000 2010 2015 2017 2020



1%

SUPERHERO



99%

ROUTINE



Common culprits



Check Point
SOFTWARE TECHNOLOGIES LTD



Browsers

35%



Office

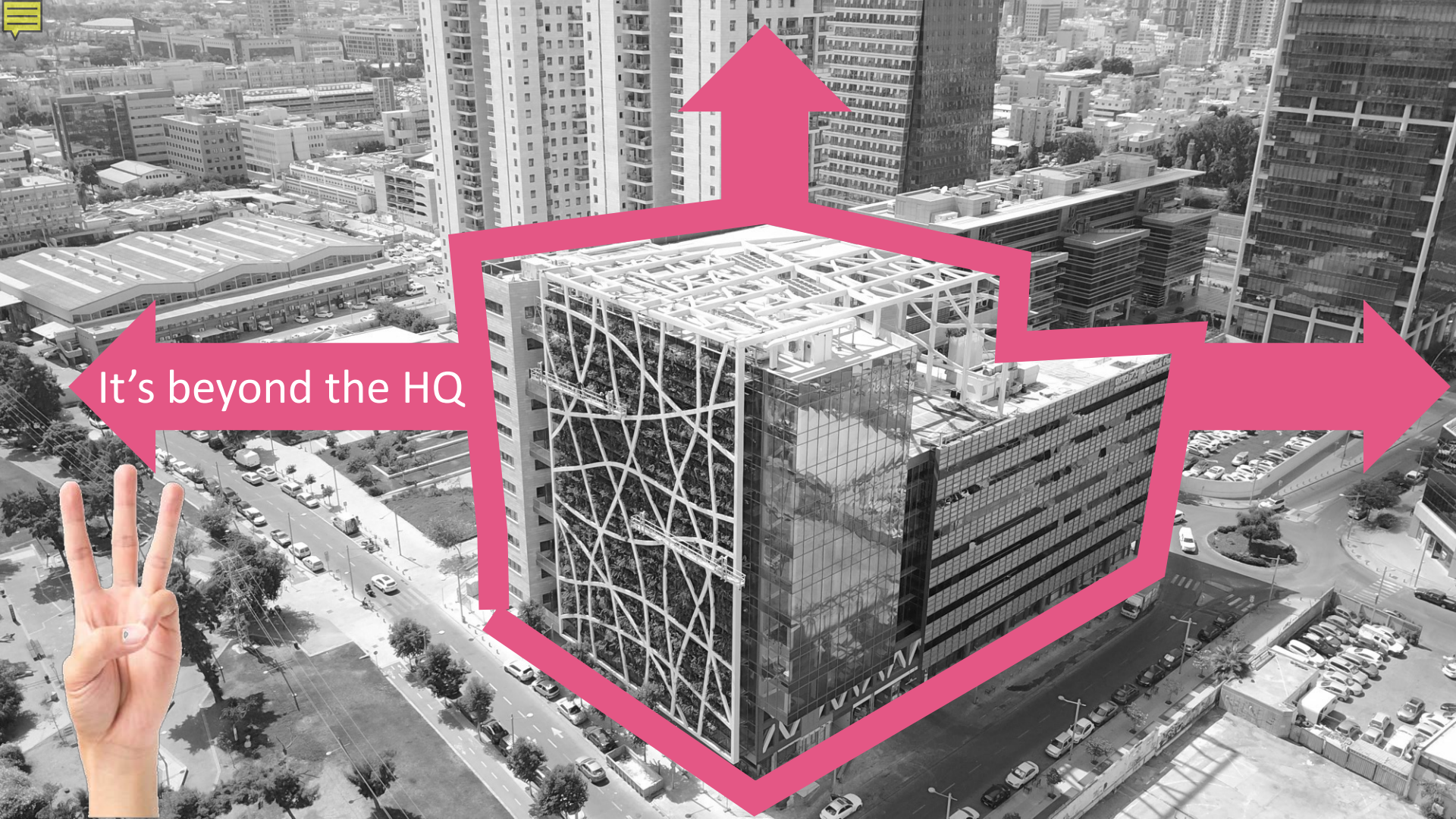
23%



Android

23%





It's beyond the HQ





MOBILE



50%
will sacrifice
security over
usability
(BT survey)



Humans...



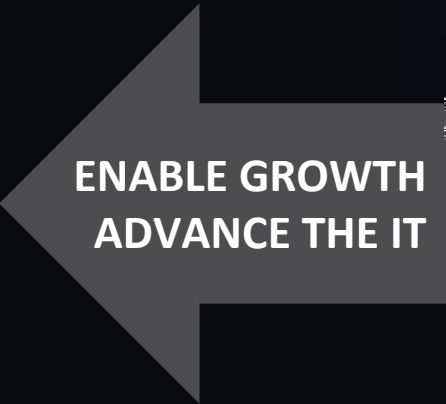
מגוון
משמעות
תורה

Misjudgment behind
70% of breaches





Check Point
SOFTWARE TECHNOLOGIES LTD



**ENABLE GROWTH
ADVANCE THE IT**

Technology



**MAINTAIN
SECURITY**



Check Point
SOFTWARE TECHNOLOGIES LTD



**ENABLE GROWTH
ADVANCE THE IT**

**MAINTAIN
SECURITY**

Technology

Policy



Check Point
SOFTWARE TECHNOLOGIES LTD



ENABLE GROWTH
ADVANCE THE IT

MAINTAIN
SECURITY

Technology

Policy

People



Check Point
SOFTWARE TECHNOLOGIES LTD

PEOPLE

POLICY

TECHNOLOGY



Check Point
SOFTWARE TECHNOLOGIES LTD

People WILL make mistakes

On
boarding



Follow on
training



They tend
to forget



Empower-
ment



Safety
net

“Are you
sure?”

EMPOWERMENT



Tue 1/2/2018 10:19 PM

dlpgw@dlpgw.checkpoint.com

Please reconsider sending Email message [CPX Presentation]

To Sharon Schusheim

If there are problems with how this message is displayed, click here to view it in a web browser.

Data Loss Prevention



The Email message you have sent is quarantined until further action

You have sent a message which was matched by the Data Loss Prevention system. CPX_keynote ONLY(Dark).potx is classified as restricted data. Make sure you are sending this to business related recipients only.

Reference: 6F819C08

Send

Discard

[Review issue in portal](#)

You can reply to this email with the words Send or Discard in the first line of the email. If you reply with Send, you can add a short explanation as to the reason (partner).

Send?

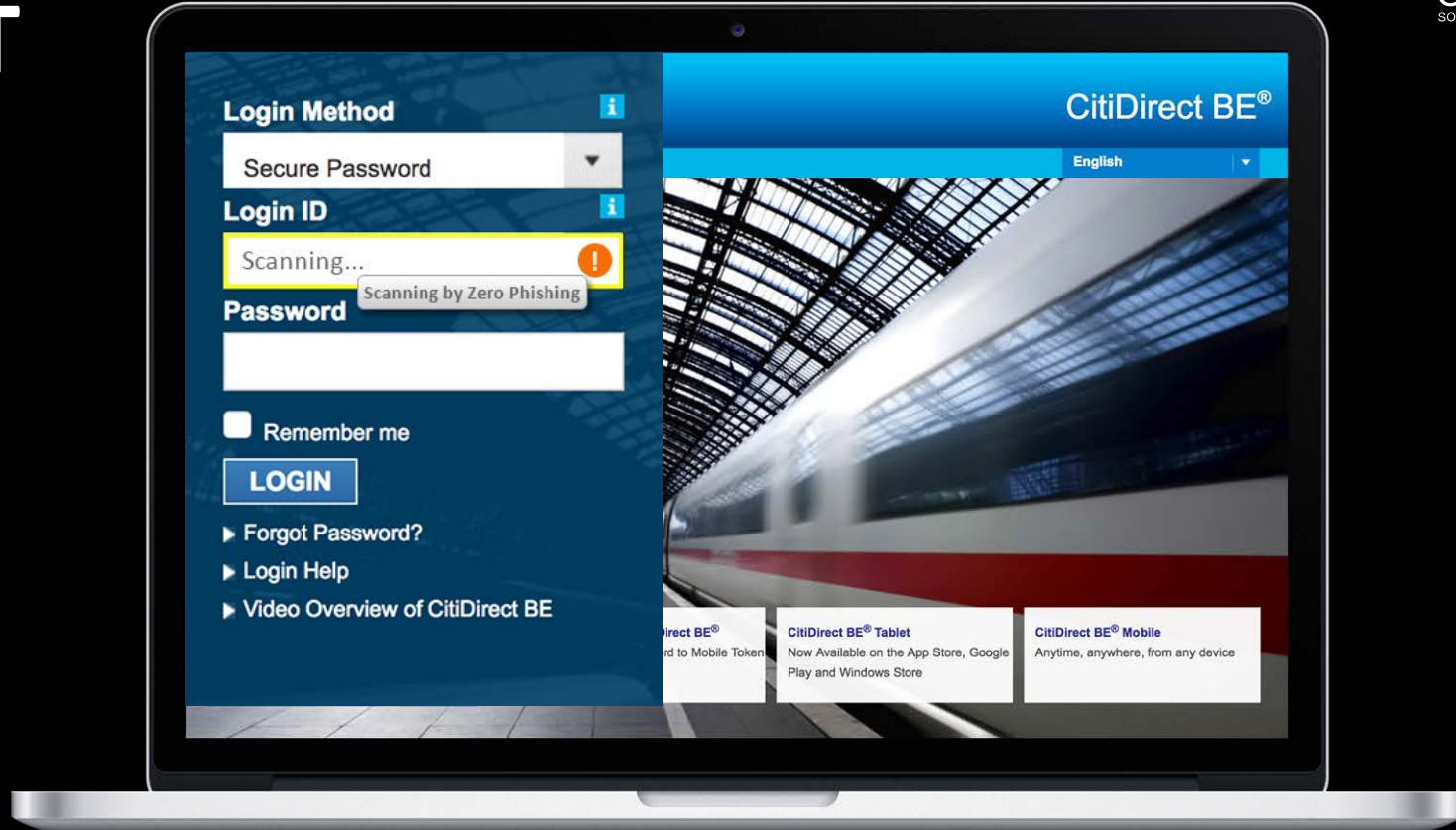
Justify

Discard

SAFETY NET

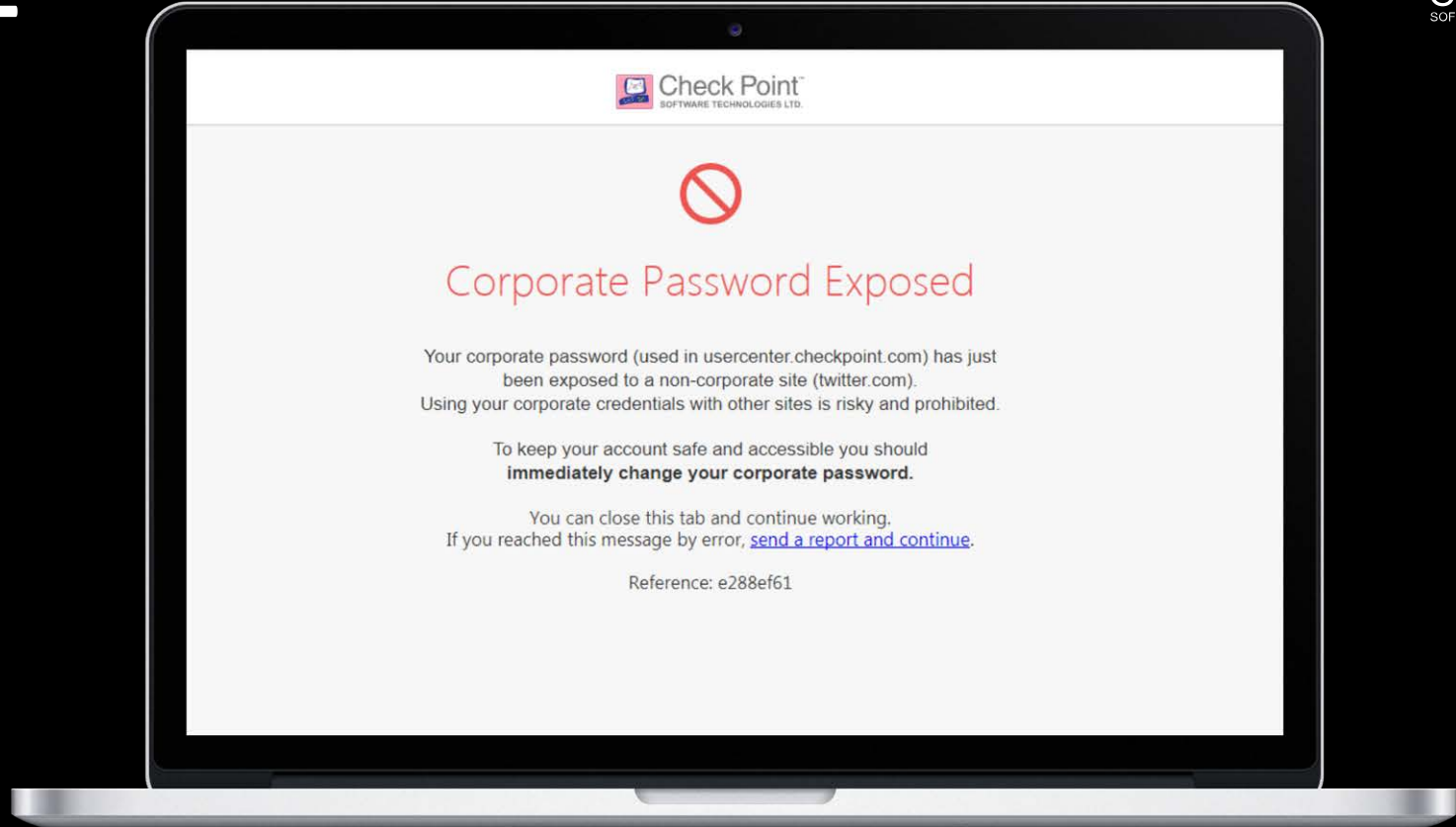


Check Point
SOFTWARE TECHNOLOGIES LTD



WELCOME TO THE FUTURE OF CYBER SECURITY

©2018 Check Point Software Technologies Ltd.



Corporate Password Exposed

Your corporate password (used in usercenter.checkpoint.com) has just been exposed to a non-corporate site (twitter.com). Using your corporate credentials with other sites is risky and prohibited.

To keep your account safe and accessible you should **immediately change your corporate password.**

You can close this tab and continue working. If you reached this message by error, [send a report and continue.](#)

Reference: e288ef61



Check Point
SOFTWARE TECHNOLOGIES LTD

PEOPLE

POLICY

TECHNOLOGY



Check Point
SOFTWARE TECHNOLOGIES LTD

THE GLUE BETWEEN PEOPLE AND TECHNOLOGY

TECHNOLOGY

POLICY

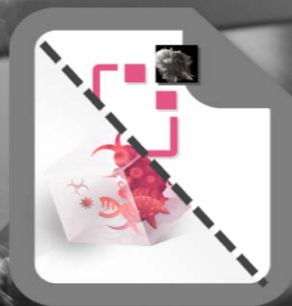
PEOPLE



ADAPTIVE POLICY



THREAT
EMULATION



ORIGINAL
DOCUMENT



THREAT
EXTRACTION



Check Point
SOFTWARE TECHNOLOGIES LTD

PEOPLE POLICY TECHNOLOGY



Network Security

Network Firewall

Check Point, Cisco, Barracuda, Dell, SonicWall, Juniper, Palo Alto, WatchGuard, Infoblox, Sophos, SANGFOR, Hillstone, CATO, Huawei, BlueCat, Fortinet, Forcepoint, Stormshield, Untangle, Stormshield, Forcepoint, Fortinet, SANGFOR, Hillstone, CATO, Huawei, BlueCat, Palo Alto, WatchGuard, Infoblox, Sophos.

Network Monitoring/Forensics

Blue Coat, Sec, Ixia, DeepNines, Netscout, Solarwinds, Giganon, Protectwise, Lumeta, Spiceworks, Utimaco, Corvil, Juniper, Riverbed, RSA, Riverbed, ForeScout, Bradford Networks, RSA, Riverbed.

Intrusion Prevention Systems

Check Point, Cisco, Coreero, Sophos, IBM, Palo Alto, Fortinet, DeepNines, Extreme Networks, McAfee, Huawei, FireEye, Juniper, NSFOCUS, Radware, AirTight.

Unified Threat Management

Check Point, Juniper, Fortinet, Huawei, Dell, Hillstone, Cisco, Stormshield, Endian, Gateprotect, Sophos, Clavister, Barracuda, WatchGuard.

Endpoint Security

Endpoint Prevention

Check Point, Cylance, Deep Instinct, Avast, Kaspersky, F-Secure, P-Safe, Microsoft, SparkCognition, ThreatTrack, AhnLab, CrowdStrike, McAfee, Webroot, Fortinet, Barkly, Ivanti, Eset, Invincea, Stormshield, Palo Alto, Safervpn, SentinelOne, Malwarebytes, Fixme Stick, Bitdefender, AVG, Carbon Black, Sophos, Trend Micro, Emsisoft, Morphisec, Panda, Bromium, Symantec.

Endpoint Detection & Response

Check Point, Opswat, Ziften, SentinelOne, Cybereason, CypHort, Morphick, CounterTack, Fluency, Tanium, Red Canary, Hexis, Bromium, Certego, Topspin, Hexadite, Qinetiq, Guidance, Outlier, Carbon Black, Cyberbit, FireEye, Augonnet, Cynet, Core Security, Invincea, Nemehia, Dtex, RSA, LightCyber, Fidelis, CrowdStrike, Secdo, Digital Guardian, Nextthink, Endgame.

Managed Security Service Provider

AT&T, Solutionary, Verizon, Trustwave, Optiv, Alert Logic, Symantec, CSC, FortiQ, Raytheon, Clone Systems, Netswitch, Nuspire, MegaPath, CenturyLink, Esentire, IBM, SecureWorks, Hewlett Packard Enterprise, Datashield, BT, Orange, Wipro, BAE Systems.

Web Security

Check Point, Cisco, Sophos, Stealth Security, Trustwave, Cloudflare, SHPE, Zscaler, ZenMate, Akamai, Appriver, ContentKeeper, Wheel, Easy Solutions, FireEye, Cyberfend, PerimeterX, Cyren, Namogoo, Blue Coat, Totals, Arrest, Smoothwall, Barracuda, Iboss, ShieldSquare, EdgeWave, Golden Frog, Forcepoint, Webroot, Nexus Guard, Symantec, Trend Micro, Gwava, Fortinet, OpenDNS, Spamhaus.

Risk & Compliance

Check Point, Cyteleg, GRX, R-sam, RiskVision, RiskSense, BigID, RedSeal, MetricStream, Prevalent, Bitsight.

Security Operations & Incident Response

SIEM

Check Point, LogRhythm, Sumologic, RSA, Tibco, Tenable, EventTracker, IBM, Solunk, Logentries, Correlog, Skybox.

Data

Opswat, Spion, Veeva, Networks, Actifile, Emsisoft, YP.

Choosing the **right** technology



PREVENTION

Fixing: looking back

Prevention: looking forward





CONSISTENCY

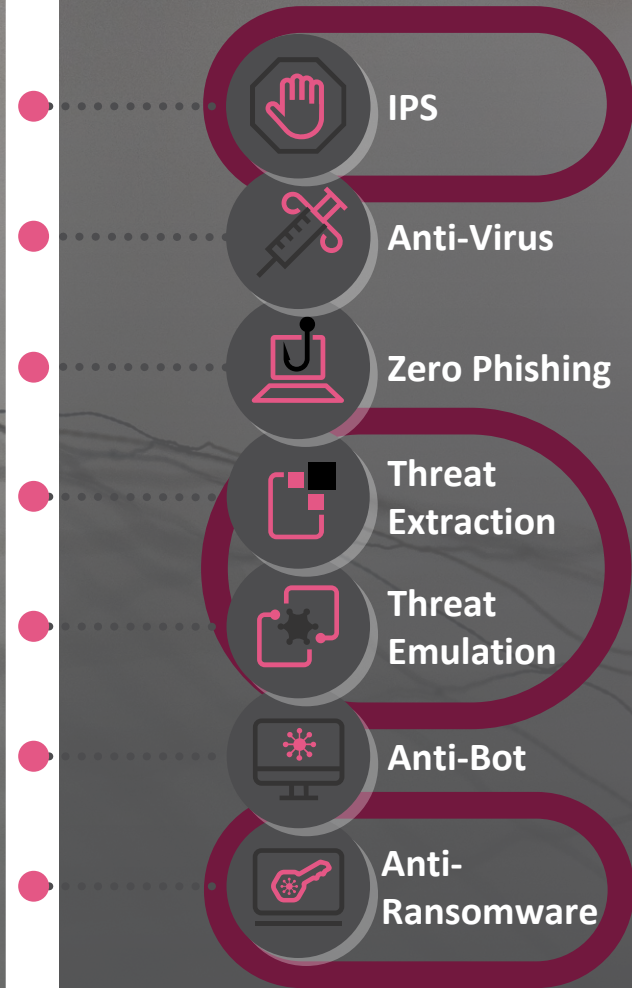
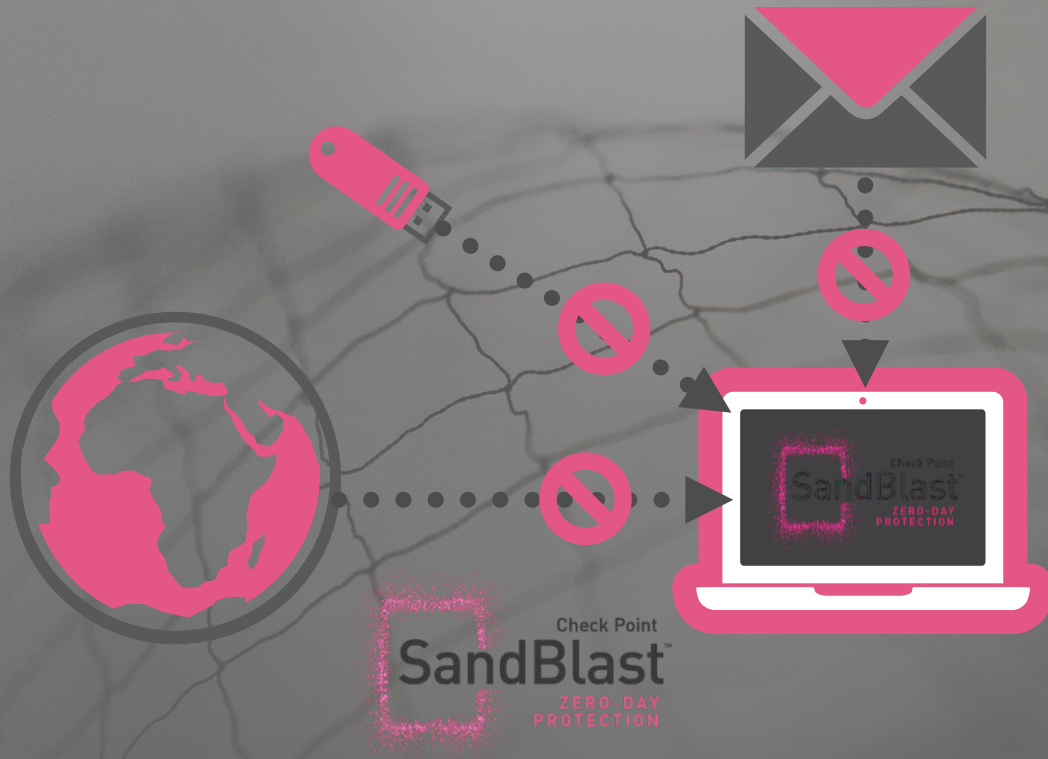


CONSOLIDATION



EXAMPLES

WannaCry – PREVENTION FIRST





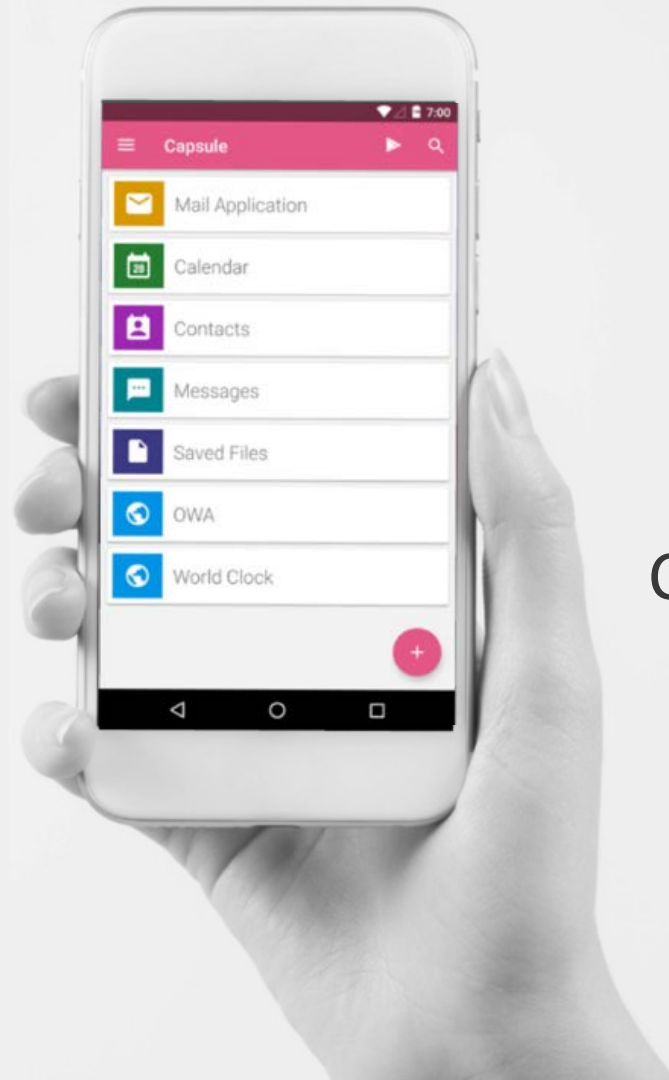
Check Point
SOFTWARE TECHNOLOGIES LTD

**MOBILE – CANNOT IGNORE
THEM ANY LONGER**

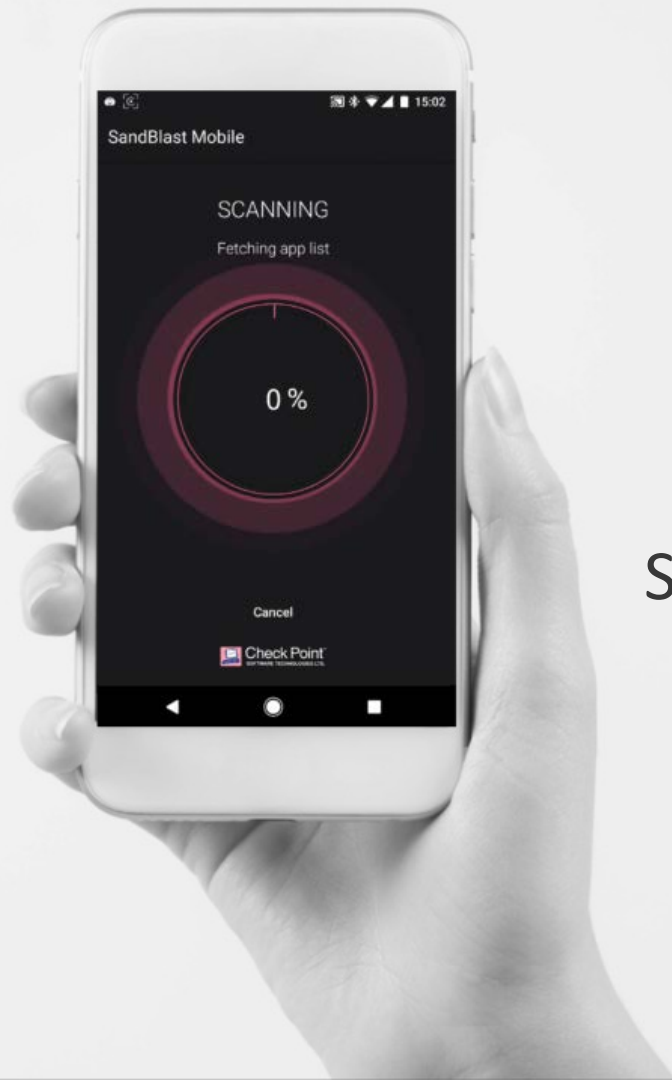


100+

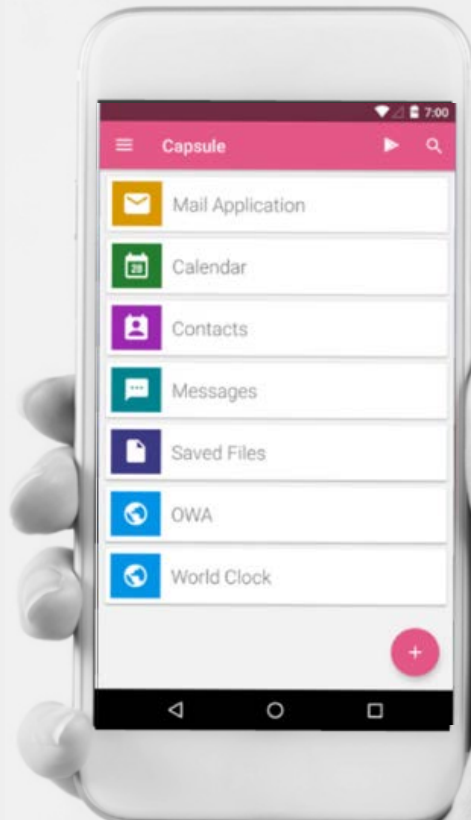
High-risk incidents
in December 2017



Capsule Workspace



SandBlast Mobile



SandBlast & Capsule
Better together



Check Point
SOFTWARE TECHNOLOGIES LTD

CAN THE TECHNOLOGY BE TRUSTED?





Check Point
SOFTWARE TECHNOLOGIES LTD

RECOMMENDED
17/17=100%

RECOMMENDED
74%

RECOMMENDED
61%

RECOMMENDED
53%

RECOMMENDED
20%

RECOMMENDED
0%

Neutral

Caution

Recommended

17

14

11

8

2

0

4

1

7

4

3

3

5

1

3



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

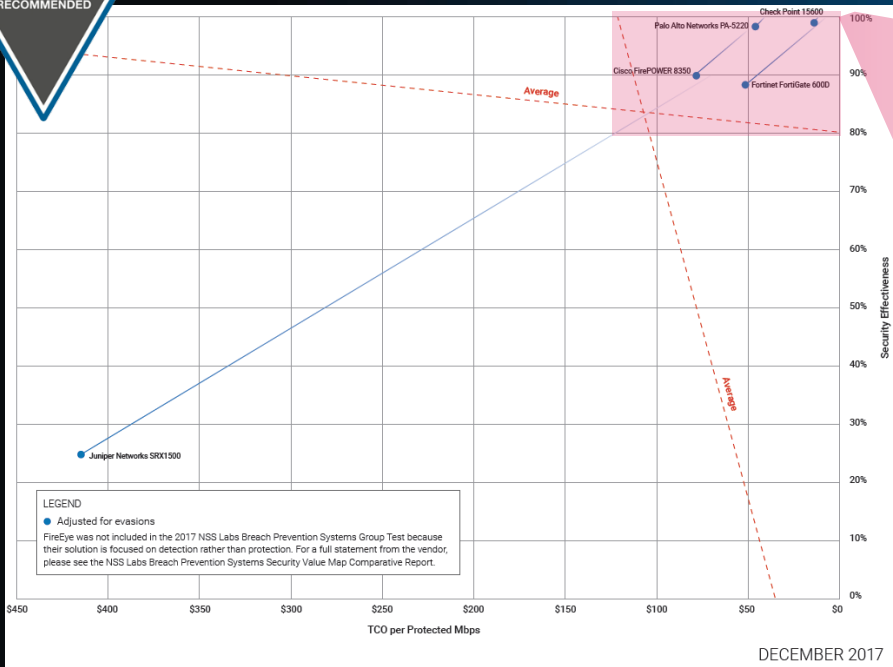
PROVEN 3rd PARTY TRACK RECORD OF SECURITY EXCELLENCE



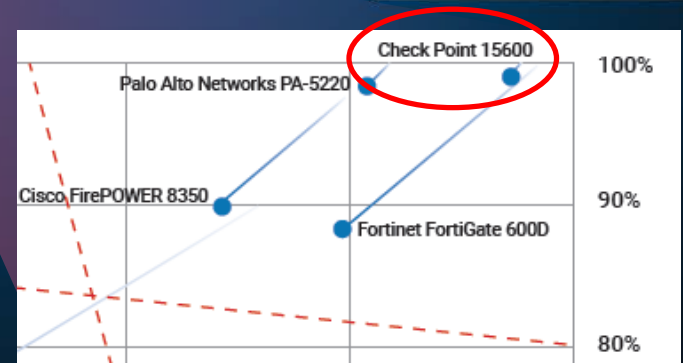
Check Point
SOFTWARE TECHNOLOGIES LTD



RECOMMENDED



LEGEND
 ● Adjusted for evasions
 FireEye was not included in the 2017 NSS Labs Breach Prevention Systems Group Test because their solution is focused on detection rather than protection. For a full statement from the vendor, please see the NSS Labs Breach Prevention Systems Security Value Map Comparative Report.



2017 NSS Breach Prevention Systems Test



Check Point
SOFTWARE TECHNOLOGIES LTD

PEOPLE POLICY TECHNOLOGY



Small text: 100% Free Event Registration

SHAPING AND SECURING THE DIGITAL ECONOMY IN INDONESIA

INDONESIAN CIO NETWORK 6TH CONFERENCE 05TH, 06TH AND 07TH OF MARCH 2018

Yogyakarta www.icion-leadership.com Key Media Partner: **KOMI^{Te}.id** Key Supporting Organization: **ABD**

Auddy +62 878 7724 6011 iclon@advancedtechpac.com **KOMI^{Te}.id** ICT NEWS PORTAL & MAGAZINE **ABD** ASSOCIATION OF BUSINESS DIGITAL



Check Point[®]
SOFTWARE TECHNOLOGIES LTD

THANK YOU



Please contact me directly with any questions or comments

bchai@checkpoint.com

+65 9001 6841



May 2018 ,Three Days SOC AND SIEM CLASS

- Three Days from 2nd 3rd and 4th of May 2018
- Chief Trainer : Kirby Chong
- Suitable for : itsec teams, audit and compliance, IT heads whom wanna understand SOCs etc
- Contact : ping to icion@advancedtechpac.com or to 0818102085





Kirby Chong, ICION advisory trainer

