ICION 6TH CONFERENCE 2018

Title : Securing Check Point

Bruce Chai

Check Point

06th March 2018 Ambarrukmo, Yogyakarta

ROYAL AMBARRUKMO YOGYAKARTA

Check Point SOFTWARE TECHNOLOGIES LTD

ICION Indonesian CIO Network

Check Point
SOFTWARE TECHNOLOGIES LTD

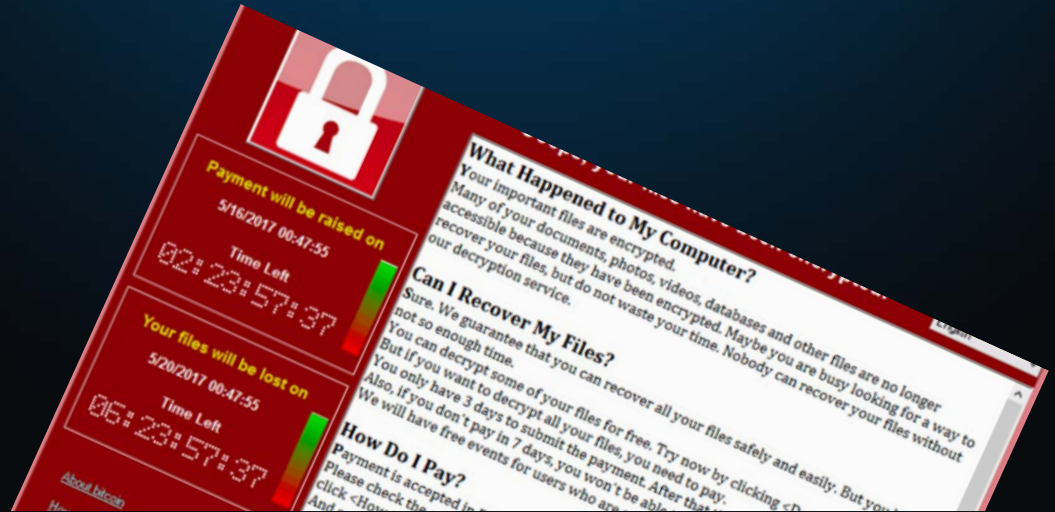
May 12th

2017

Check Point
SOFTWARE TECHNOLOGIES LTD

ZERO

INFECTIONS



CIO

ENABLE GROWTH, ADVANCE THE IT

MAINTAIN SECURITY

ENABLE GROWTH, ADVANCE THE IT

TOOLS

INFRA STRUCTURE

slack

sensu

Office 365

box

CLOUD

Google Cloud Platform

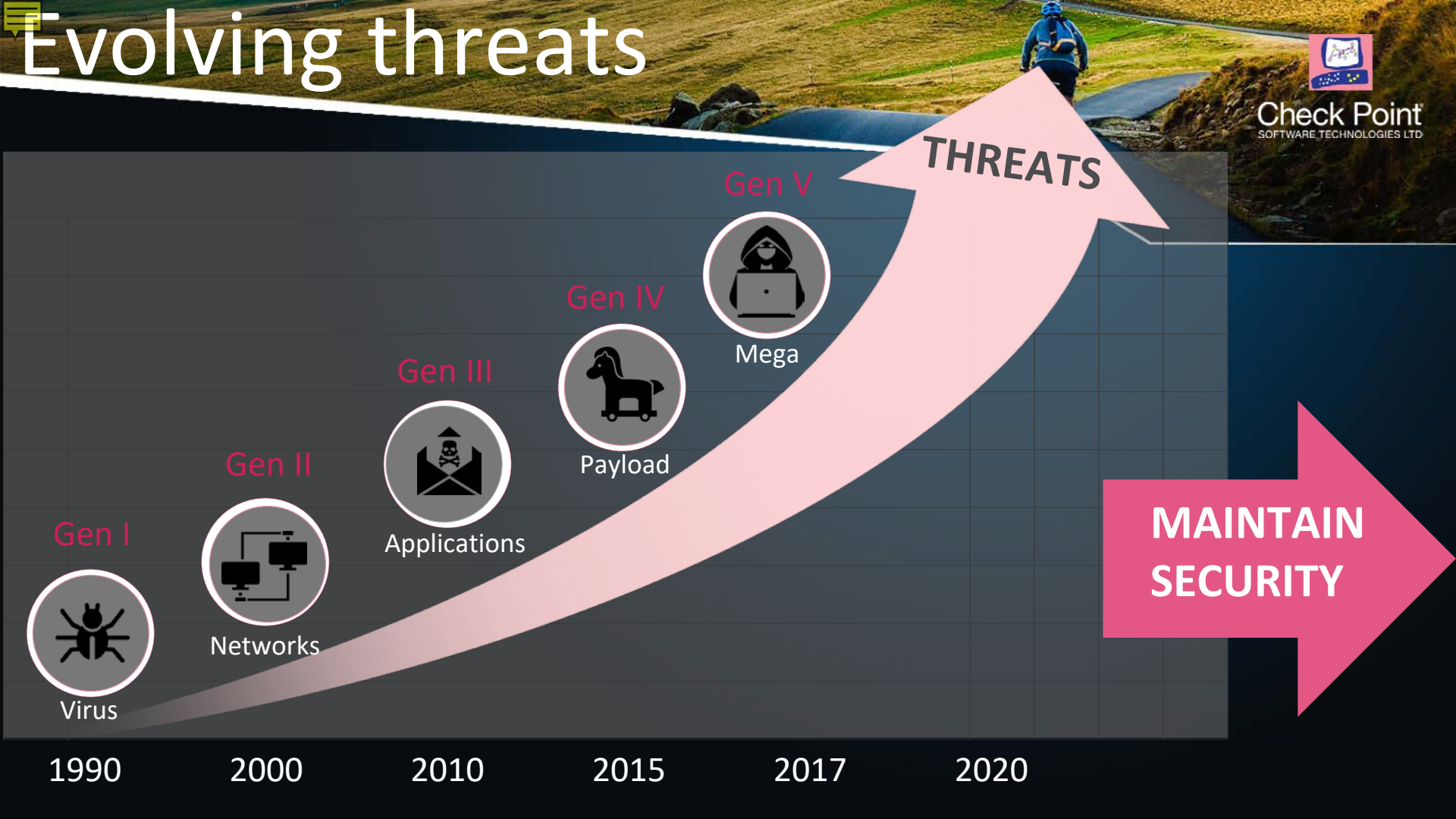
salesforce

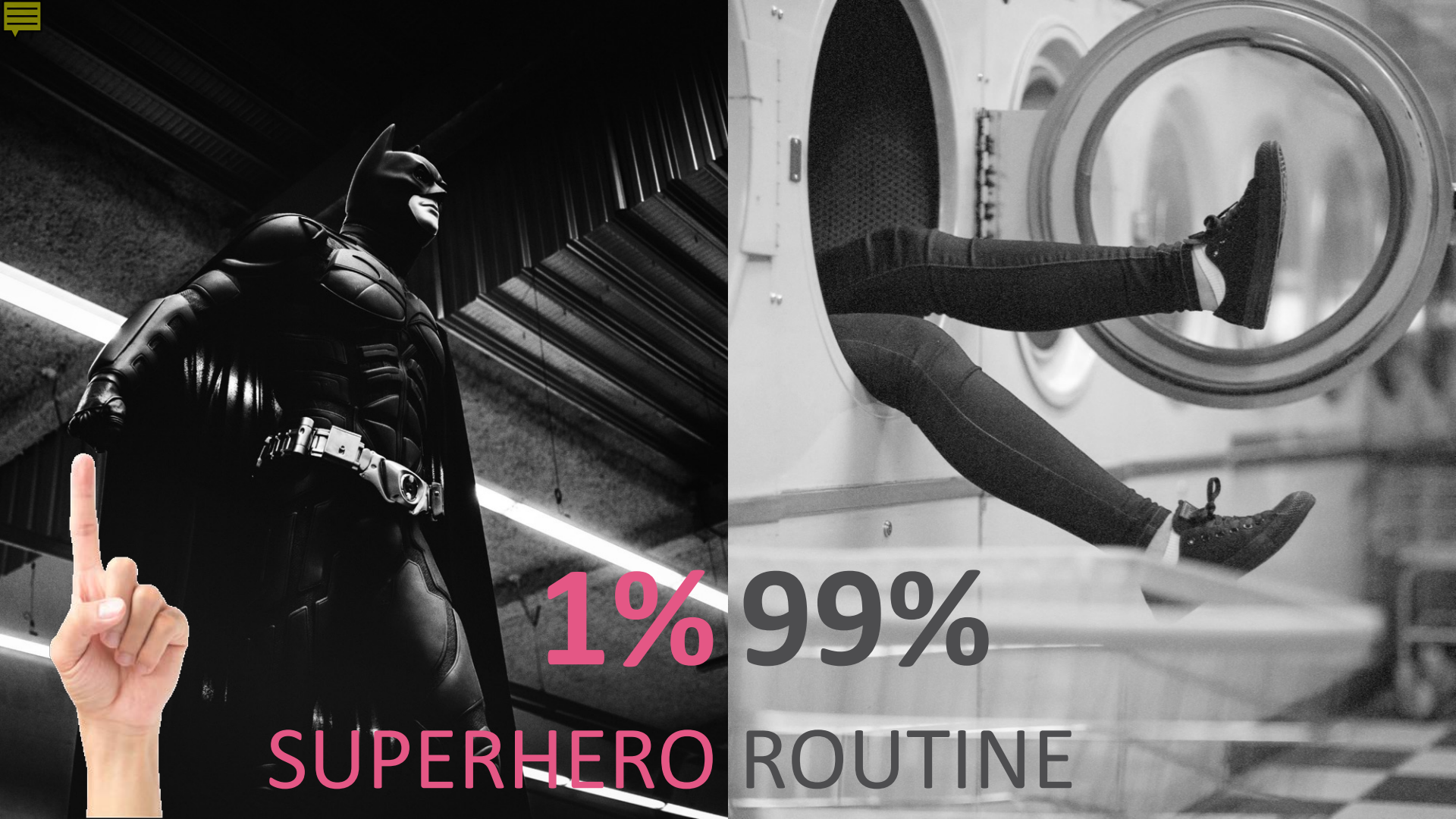
ORACLE CLOUD

amazon web services

Microsoft Azure

Evolving threats

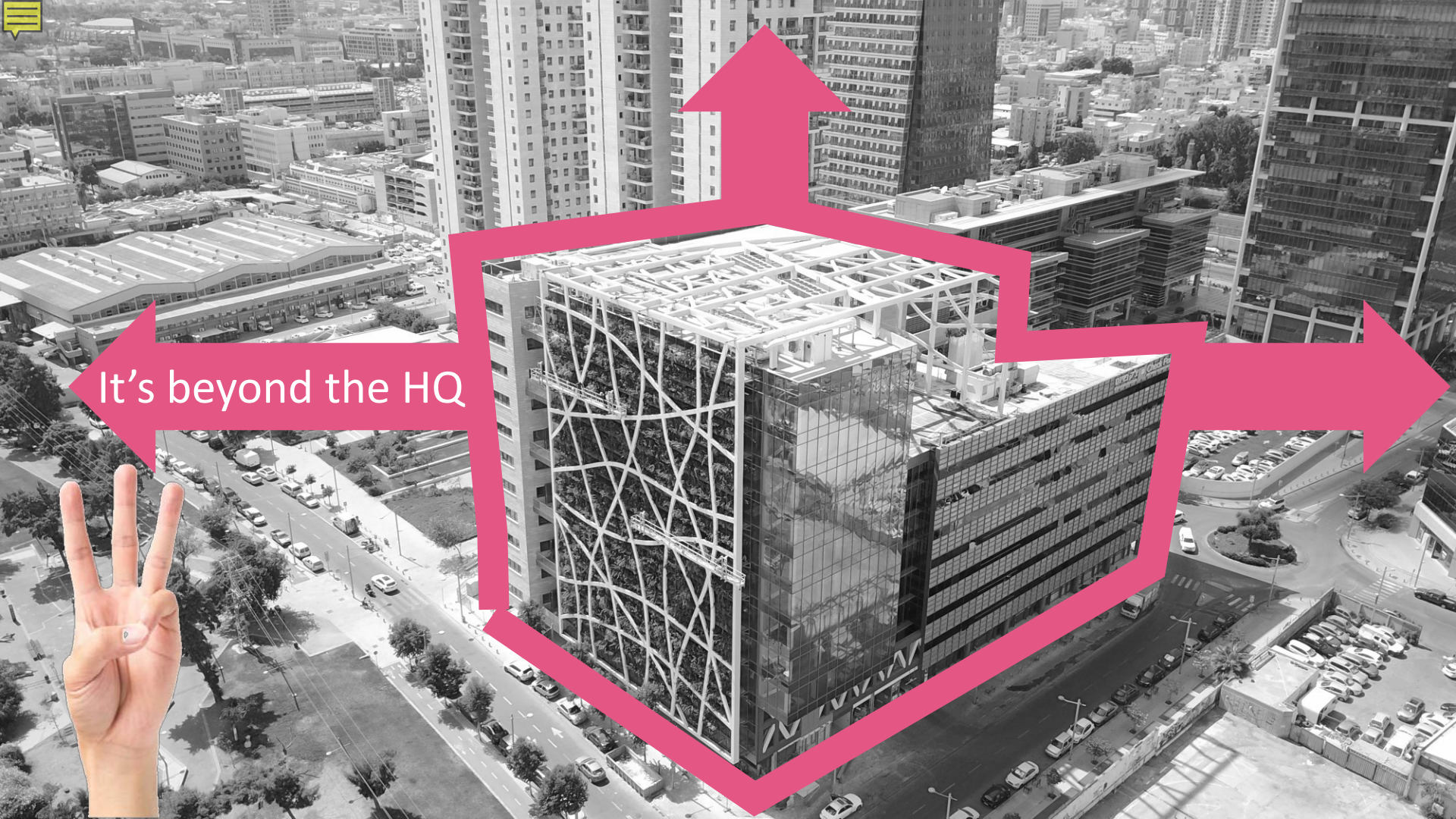



1%
99%
SUPERHERO
ROUTINE

Common culprits

Browsers	Office	Android
35%	23%	23%

©2018 Check Point Software Technologies Ltd.


It’s beyond the HQ


MOBILE
50%
will sacrifice security over usability (BT survey)

Humans…

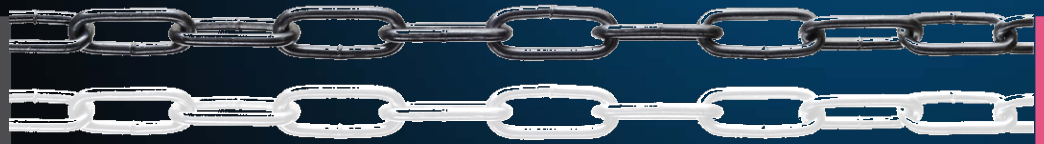
Misjudgment behind
70% of breaches

ENABLE GROWTH
ADVANCE THE IT

MAINTAIN
SECURITY

Technology

ENABLE GROWTH
ADVANCE THE IT



MAINTAIN
SECURITY

Technology

Policy

Check Point
SOFTWARE TECHNOLOGIES LTD

ENABLE GROWTH
ADVANCE THE IT

MAINTAIN
SECURITY

Technology

Policy

People

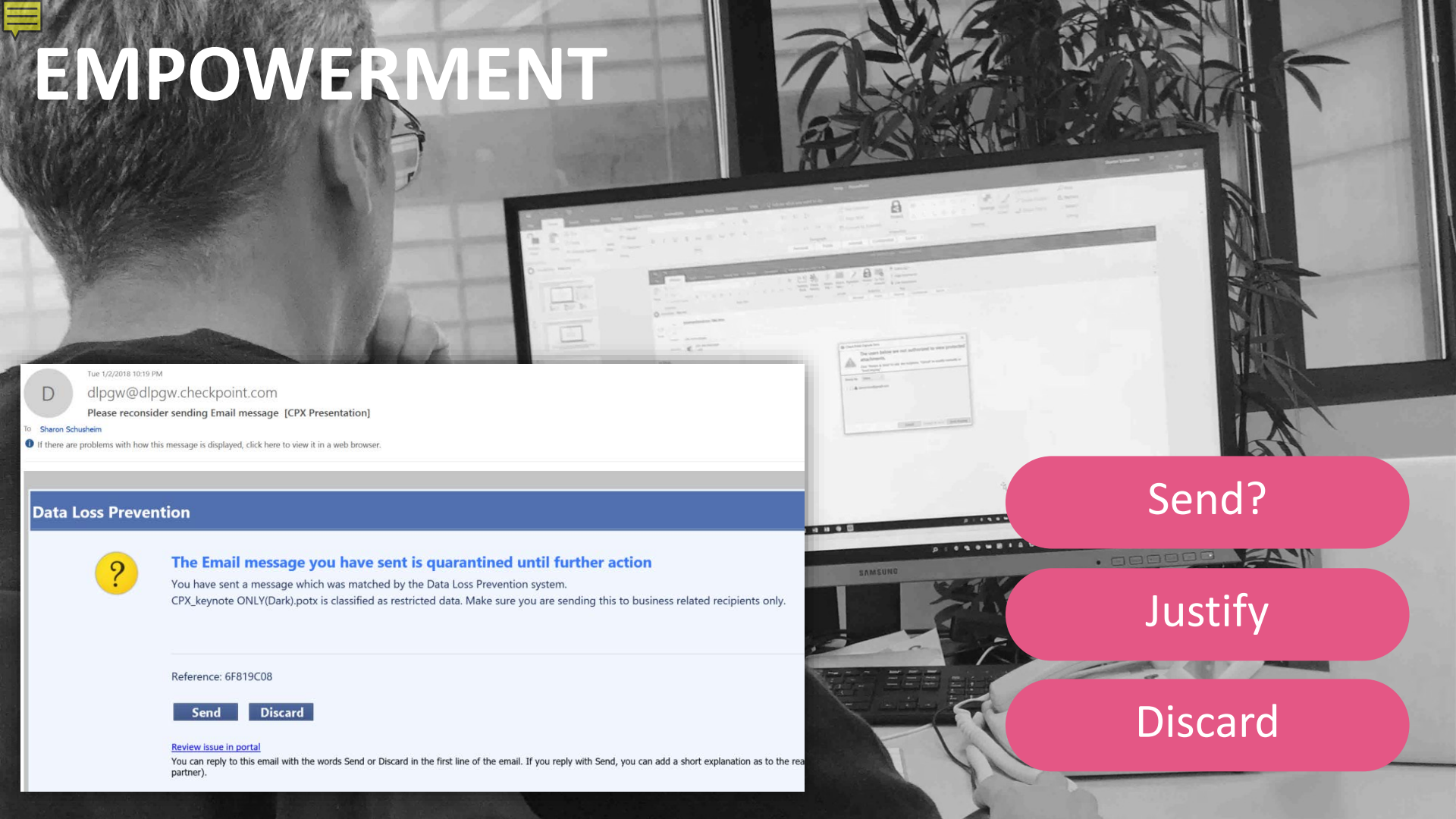
PEOPLE
POLICY
TECHNOLOGY

People WILL make mistakes

On boarding → Follow on training → They tend to forget → Empower-ment + Safety net

"Are you sure?"

EMPOWERMENT

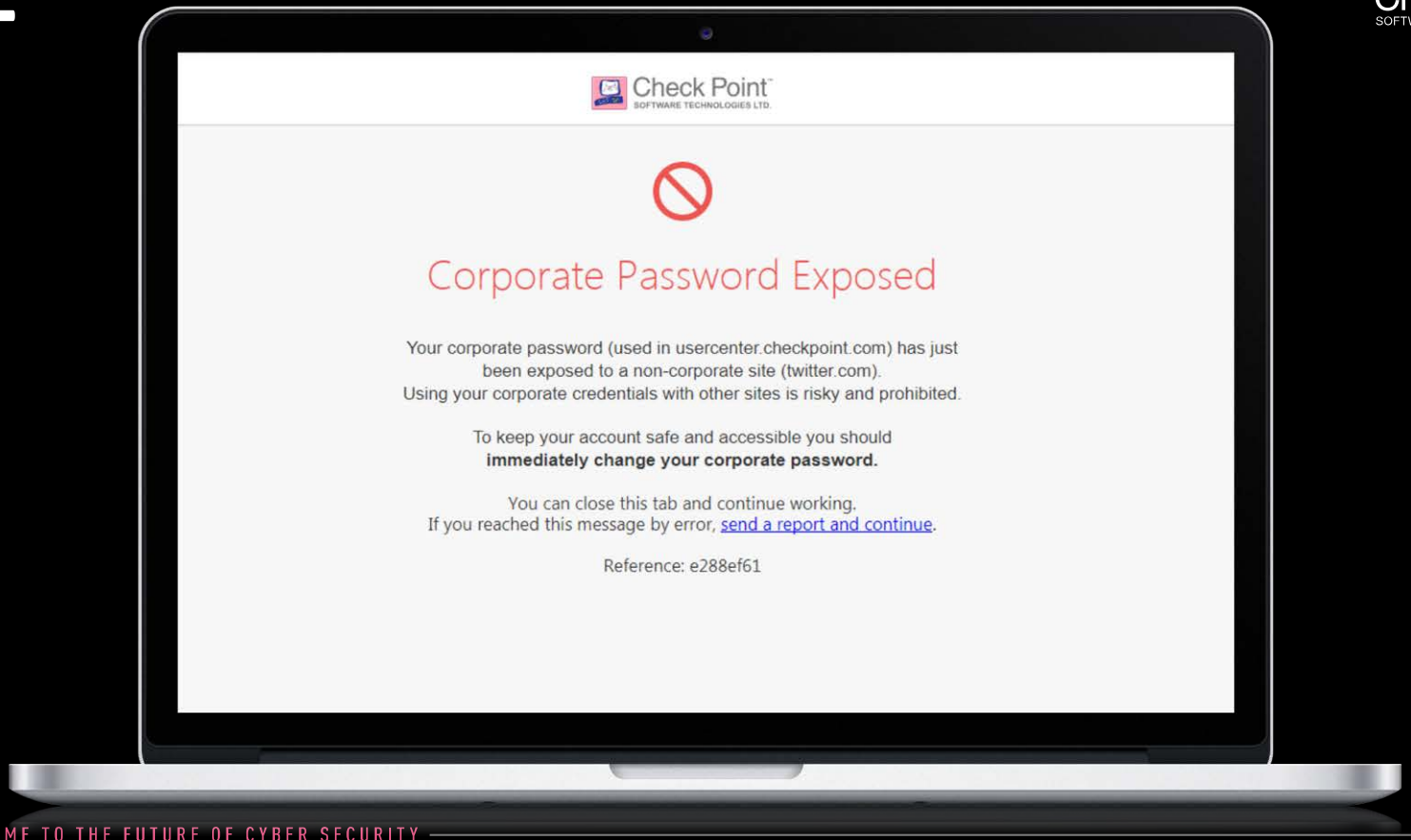


SAFETY NET

©2018 Check Point Software Technologies Ltd.

SAFETY NET

Zero Phishing



©2018 Check Point Software Technologies Ltd.

PEOPLE

POLICY

TECHNOLOGY

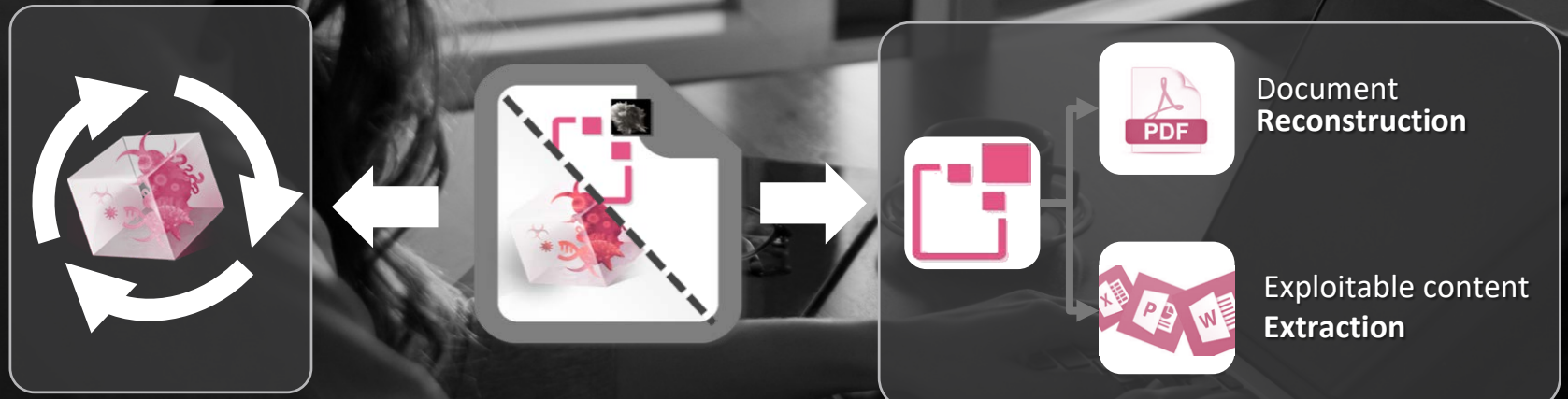
THE GLUE BETWEEN PEOPLE AND TECHNOLOGY

TECHNOLOGY

POLICY

PEOPLE

ADAPTIVE POLICY



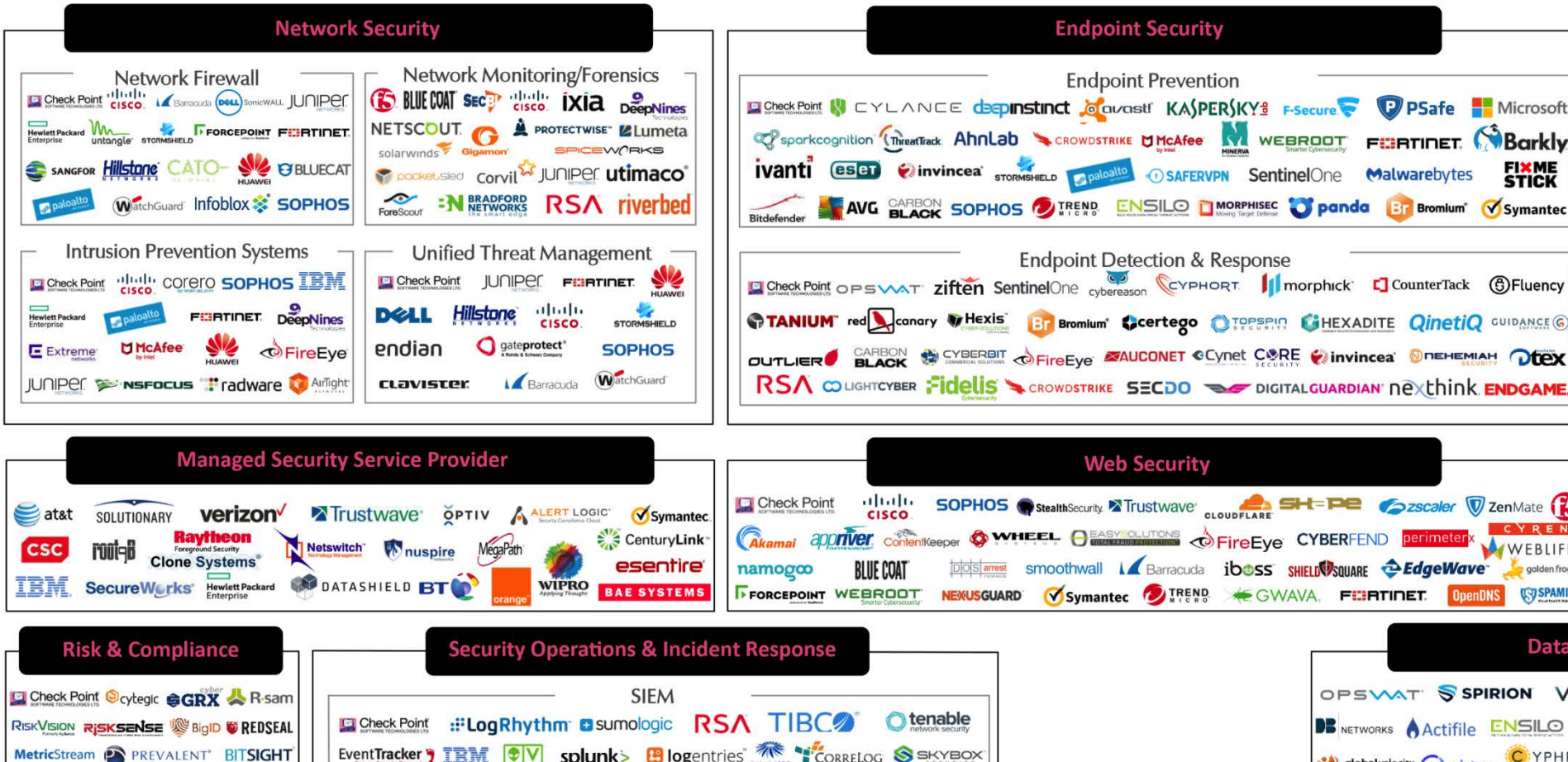
THREAT
EMULATION

ORIGINAL
DOCUMENT

THREAT
EXTRACTION

ICION
Indonesian CIO Network

PEOPLE
POLICY
TECHNOLOGY


Network Security
Network Firewall
Check Point
Cisco
Barracuda
Dell SonicWALL
Juniper
Hewlett Packard Enterprise
Untangle
Stormshield
Forcepoint
Fortinet
Sangfor
Hillstone
CATO
Huawei
BlueCat
paloalto
WatchGuard
Infoblox
Sophos
Network Monitoring/Forensics
Blue Coat
SecPod
Cisco
ixia
DeepNines
NetScout
Protectwise
Lumeta
solarwinds
Gigamon
SpiceWorks
packetsled
Corvil
Juniper
utimaco
ForeScout
Bradford Networks
RSA
riverbed
Intrusion Prevention Systems
Check Point
Cisco
corero
Sophos
IBM
Hewlett Packard Enterprise
paloalto
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
deepinstinct
avast!
Kaspersky
F-Secure
PSafe
Microsoft
sparkcognition
ThreatTrack
AhnLab
CrowdStrike
McAfee
Minerva
Webroot
Fortinet
Barkly
ivanti
eset
invincea
Stormshield
paloalto
SAFERVPN
SentinelOne
Malwarebytes
FIXME STICK
Bitdefender
AVG
Carbon Black
Sophos
Trend Micro
Ensilo
Morphisec
panda
Bromium
Symantec
Endpoint Detection & Response
Check Point
OPSWAT
ziften
SentinelOne
cybereason
Cyphort
morphick
CounterTack
Fluency
Tanium
red canary
Hexis
Bromium
certego
Topspin Security
Hexadite
QinetiQ
Guidance
Outlier
Carbon Black
Cyberbit
FireEye
Auconet
Cynet
Core Security
invincea
Nehemiah Security
tex
RSA
LightCyber
Fidelis Cybersecurity
CrowdStrike
SECDO
Digital Guardian
nexthink
ENDGAME
Managed Security Service Provider
at&t
Solutionary
verizon
Trustwave
OPTIV
Alert Logic
Symantec
CSC
root9B
Raytheon Foreground Security
Clone Systems
Netswitch
nuspire
MegaPath
CenturyLink
esentire
IBM
SecureWorks
Hewlett Packard Enterprise
DATASHIELD
BT
orange
WIPO
BAE SYSTEMS
Web Security
Check Point
Cisco
Sophos
Stealthsecurity
Trustwave
Cloudflare
SHAPE
zscaler
ZenMate
Akamai
appriver
ContentKeeper
WHEEL
EASY SOLUTIONS
FireEye
CYBERFEND
perimeterx
CYREN
WEBLIFE
namogoo
Blue Coat
bpsarrest
smoothwall
Barracuda
iboss
SHIELD SQUARE
EdgeWave
golden fro
Forcepoint
Webroot
NexusGuard
Symantec
Trend Micro
GWAVA
Fortinet
OpenDNS
SPAMI
Risk & Compliance
Check Point
cytegic
cyber GRX
R-sam
RiskVision
RISKSENSE
BigID
REDSEAL
MetricStream
PREVALENT
BITSIGHT
Security Operations & Incident Response
SIEM
Check Point
LogRhythm
sumologic
RSA
TIBCO
tenable network security
EventTracker
IBM
splunk>
logentries
CORRELOG
SKYBOX
Data
OPSWAT
SPIRION
DB NETWORKS
Actifile
ENSILO

Choosing the right technology

PREVENTION

Fixing: looking back

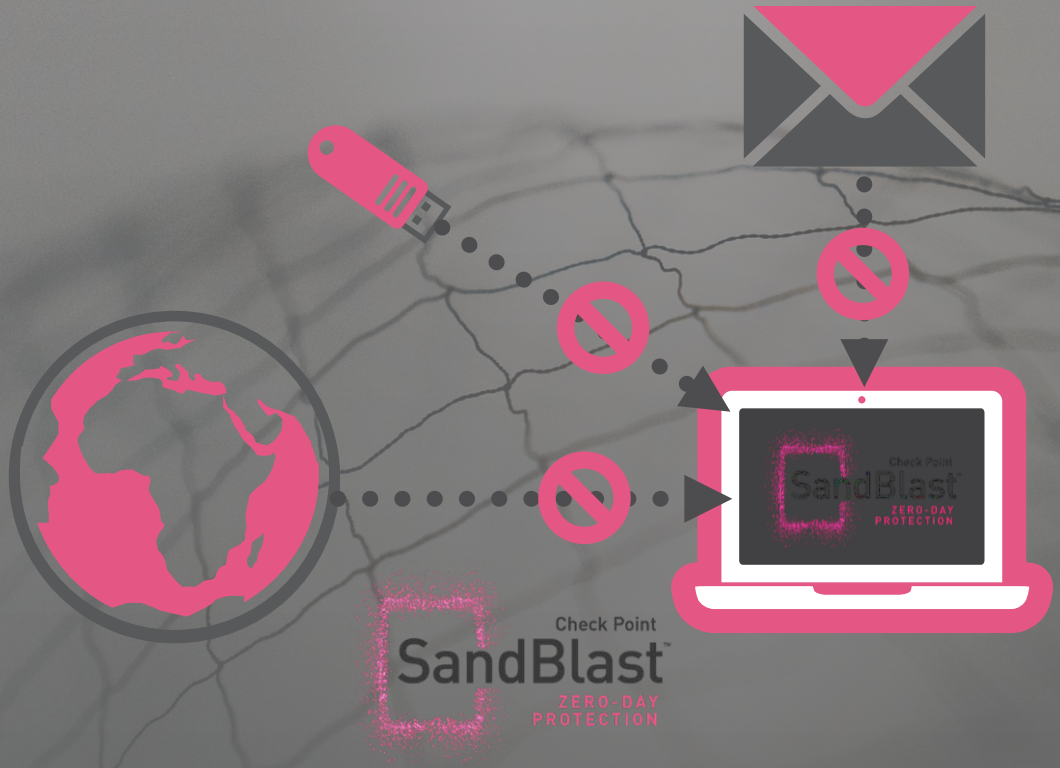
Prevention: looking forward


CONSISTENCY


CONSOLIDATION


EXAMPLES

WannaCry – PREVENTION FIRST

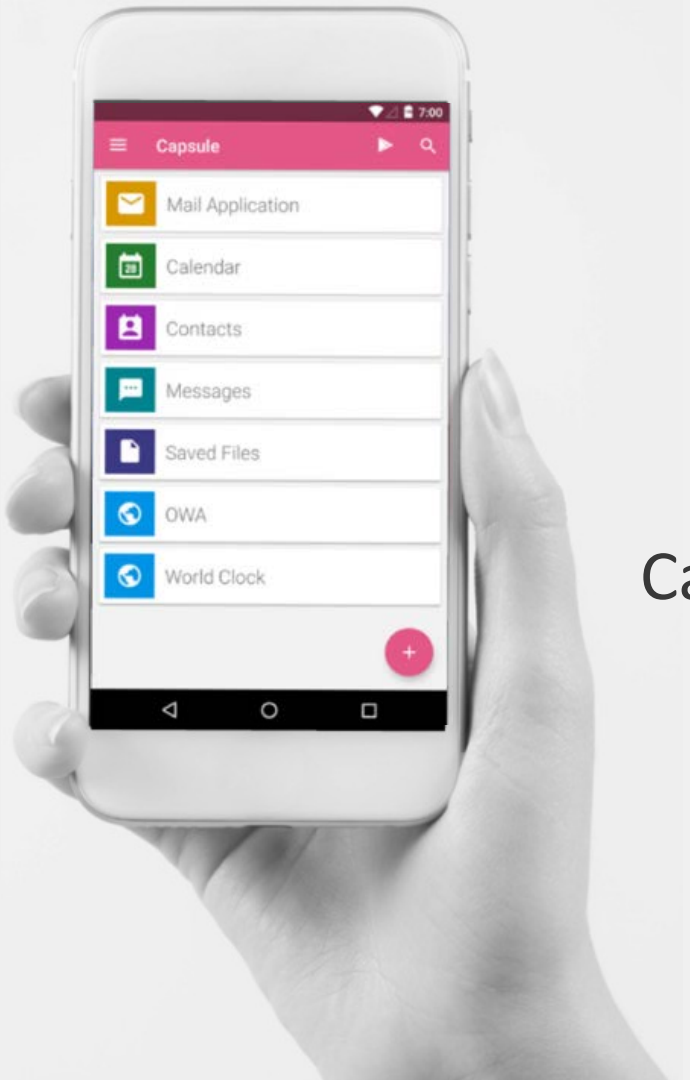


- IPS
- Anti-Virus
- Zero Phishing
- Threat Extraction
- Threat Emulation
- Anti-Bot
- Anti-Ransomware

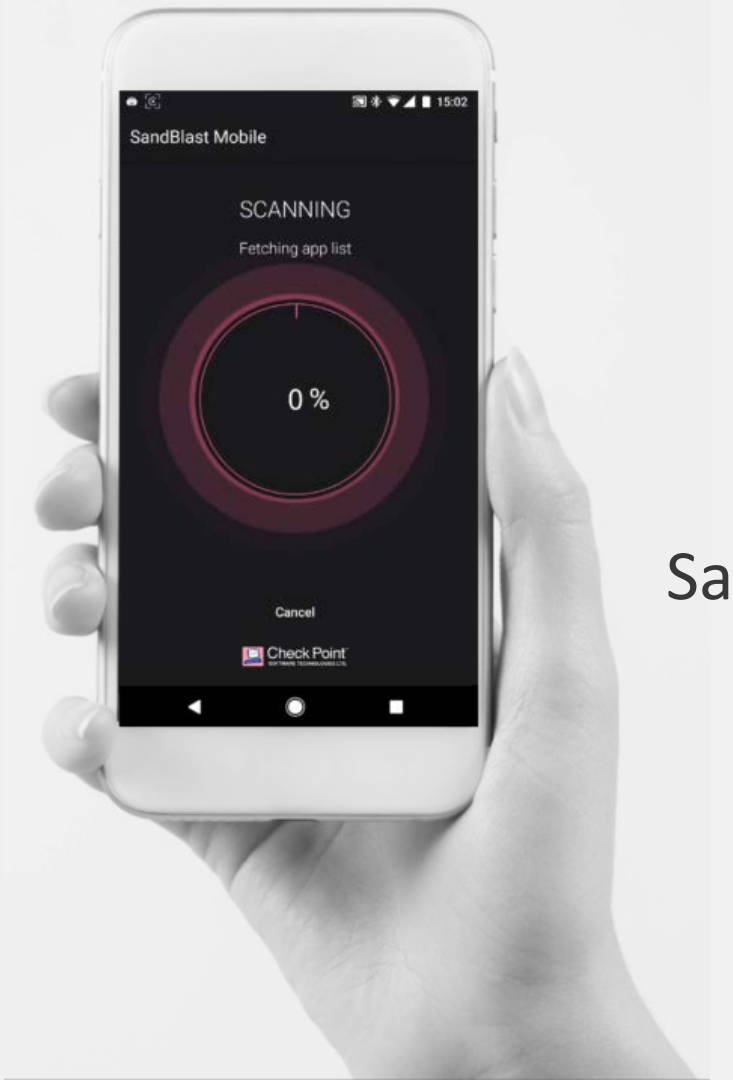
MOBILE – CANNOT IGNORE THEM ANY LONGER

100+

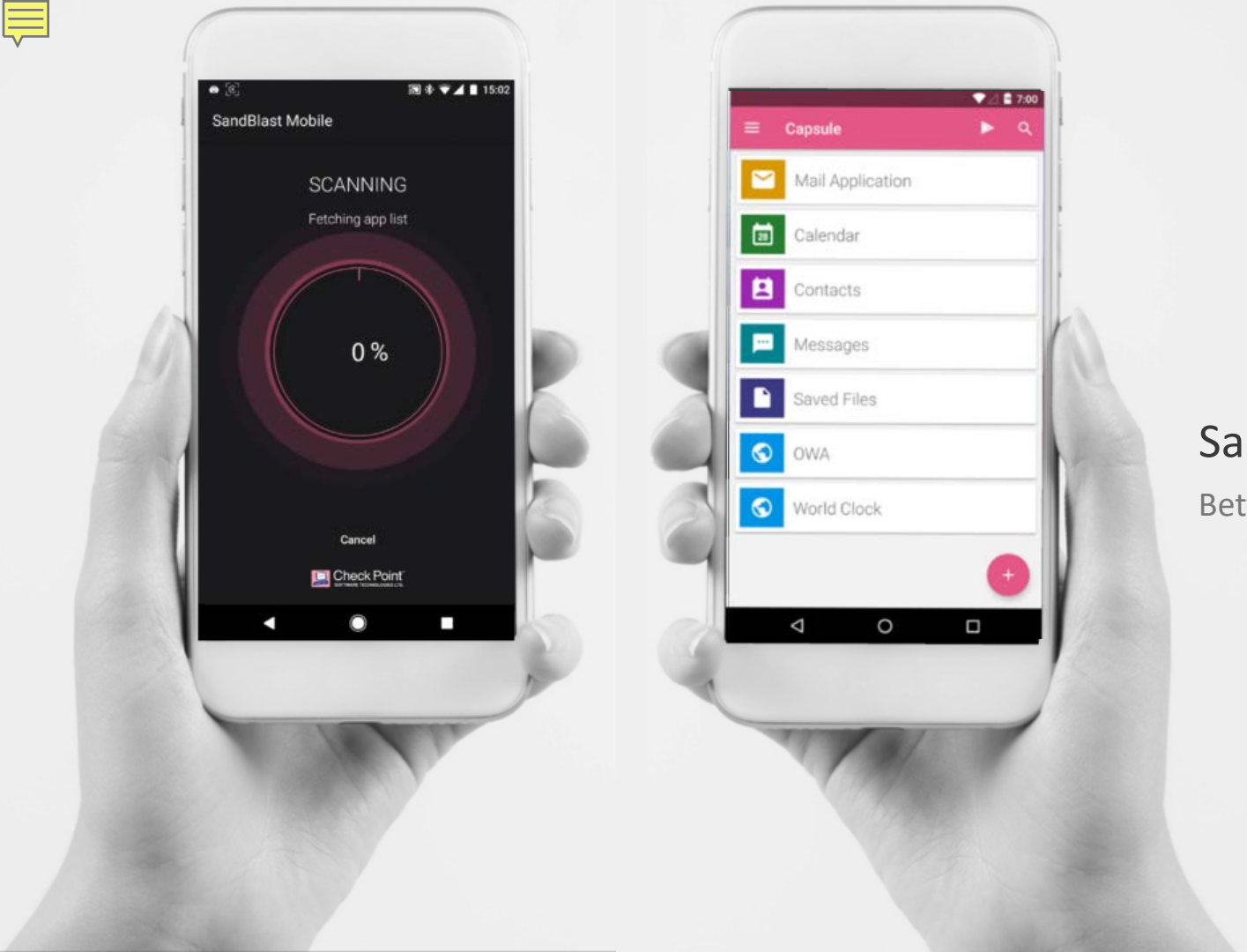
High-risk incidents
in December 2017



Capsule Workspace



SandBlast Mobile

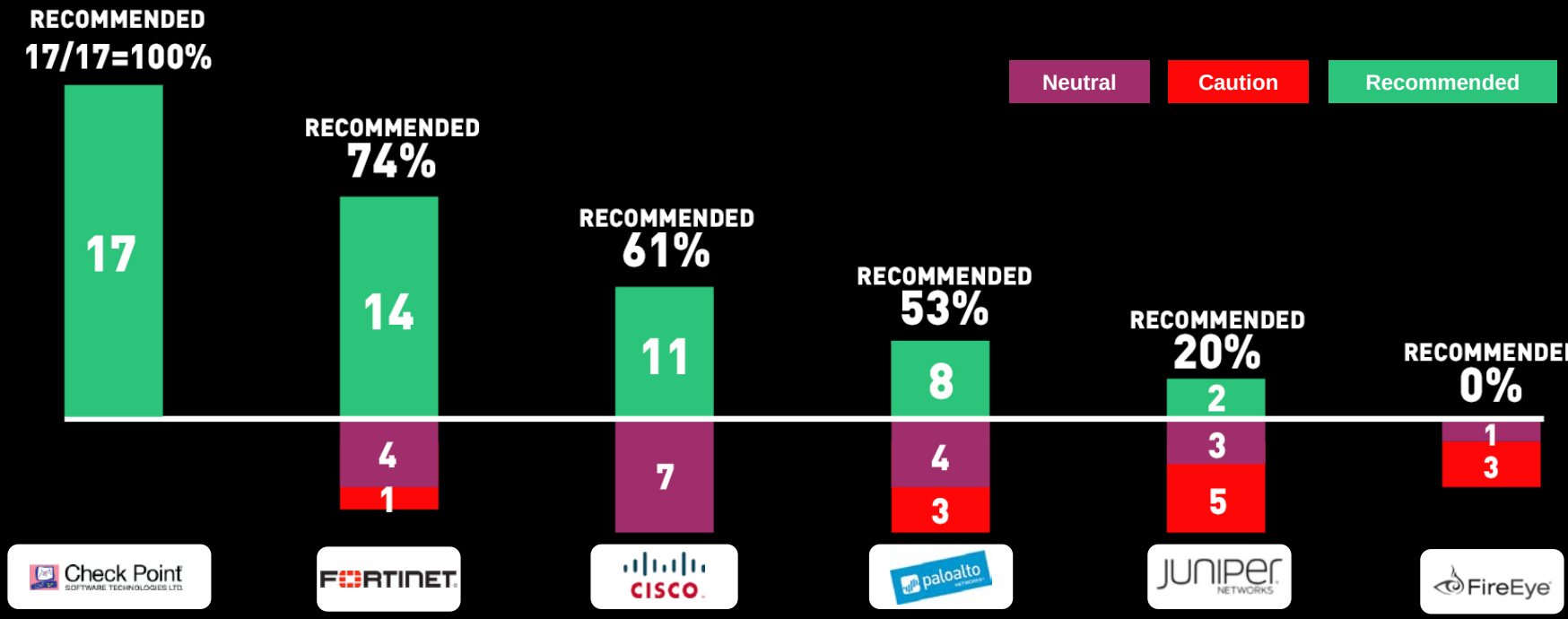


SandBlast & Capsule

Better together

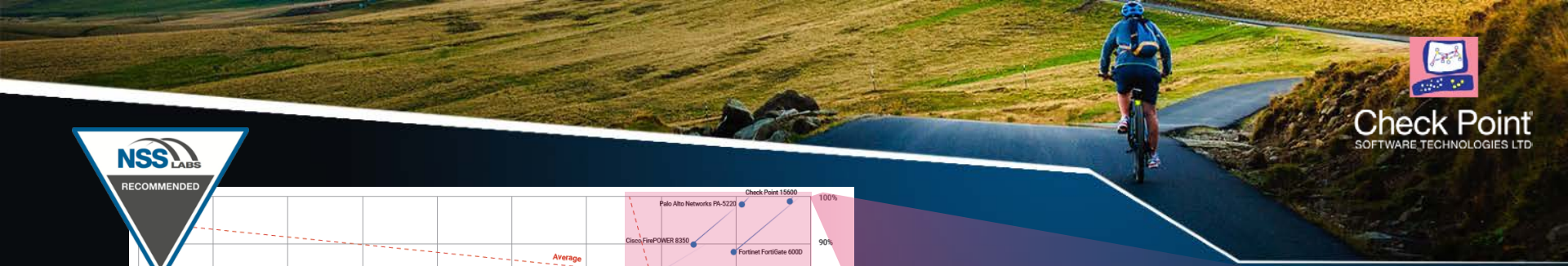
Check Point
SOFTWARE TECHNOLOGIES LTD

CAN THE TECHNOLOGY BE TRUSTED?



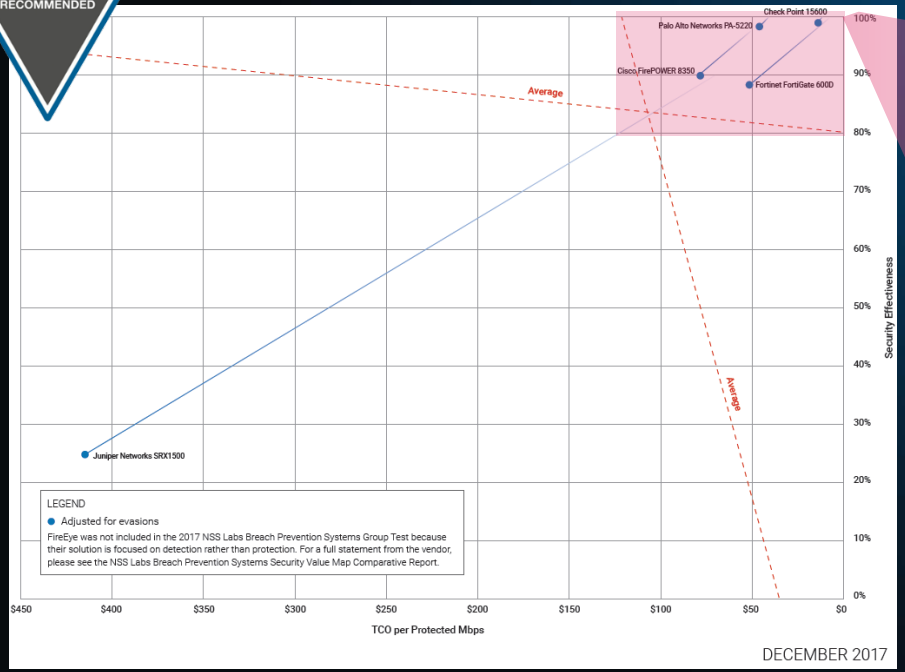
Source: http://tiny.cc/nss_stats NSS Labs Network Security tests (FW/NGFW/IPS/NGIPS/DCIPS/BDS) * PAN NGFW solution have not been recommended since 2013

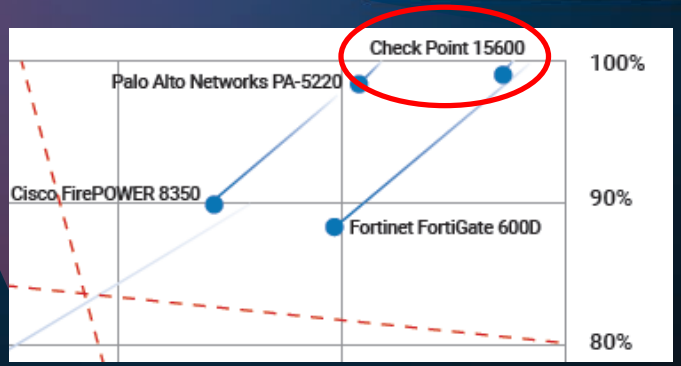
PROVEN 3rd PARTY TRACK RECORD OF SECURITY EXCELLENCE



Check Point
SOFTWARE TECHNOLOGIES LTD

NSS LABS
RECOMMENDED





2017 NSS **Breach Prevention Systems** *Test*

Check Point
SandBlast
ZERO-DAY PROTECTION

Check Point
SOFTWARE TECHNOLOGIES LTD

PEOPLE
POLICY
TECHNOLOGY

ICION
Indonesian CIO Network

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 2rd 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

ICION
Indonesian CIO Network

Kirby Chong, ICION advisory trainer