Check Point
SOFTWARE TECHNOLOGIES LTD.

SECURITY CHANGING DYNAMICS

From Known to Unknown

Parikshit Gangaher | System Engineer

AGENDA

Check Point
SOFTWARE TECHNOLOGIES LTD.

Challenges for Cyber Security

New thinking required in Cyber Security

Why Checkpoint?

Business Needs Are Changing Network

Out Sourcing

IoT

Information Sharing

Cost Effective Options

BYOD

24x7 Access/ Connectivity

If Network are evolving as Business need changes, the Cyber Security have to Evolve and stay ONE STEP AHEAD of ever changing Business Needs

Threats Evolution

Check Point
SOFTWARE TECHNOLOGIES LTD.

- Known Exploits/Malware

Done with Motivation for making there names and for Fame. Hence easy to detect and prevent with conventional solution such as NGFW

- Unknown- Unknown or Zero-Day Exploit/Malware

These attacks can be States sponsored or Competitor sponsored.

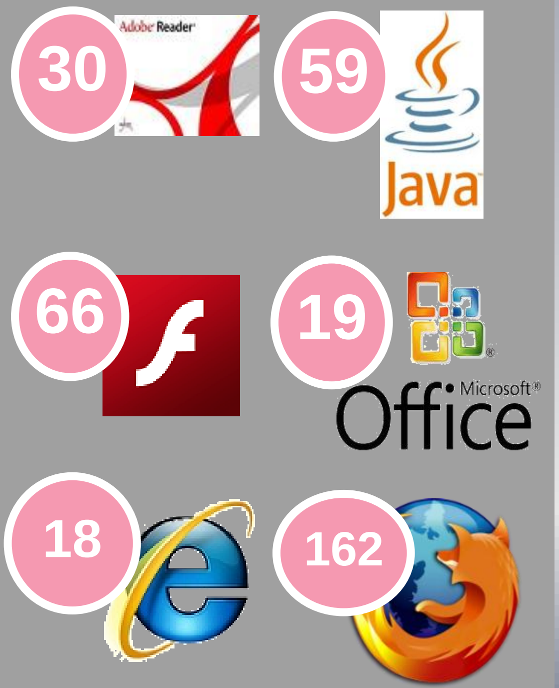
Main motive is to make money and to remain hidden as long as possible

- Known- Unknown Exploits/Malware

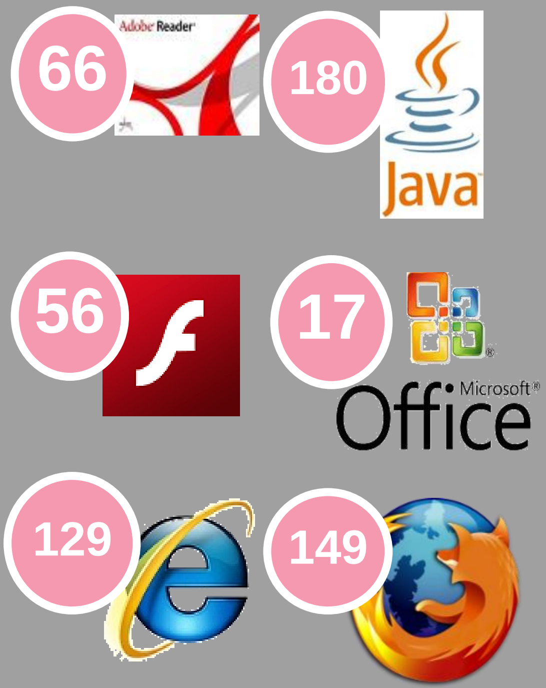
Interestingly 80 to 85% attacks are known attacks modified to avoid detection by conventional Security

There are known knowns

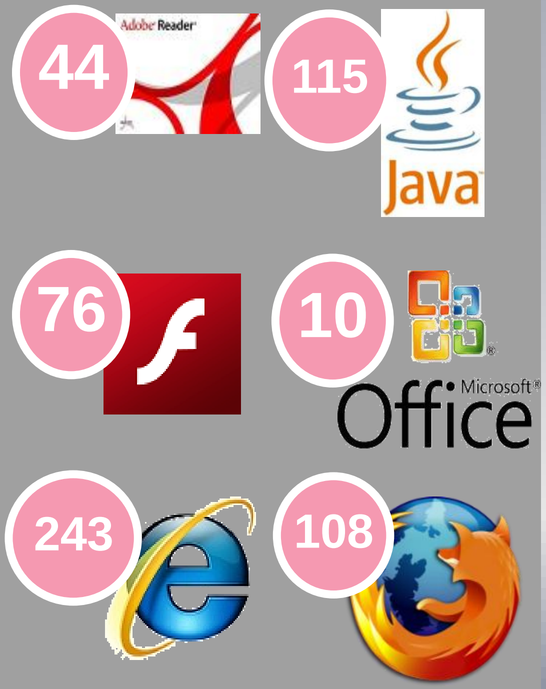
2012
vulnerabilities



2013
vulnerabilities



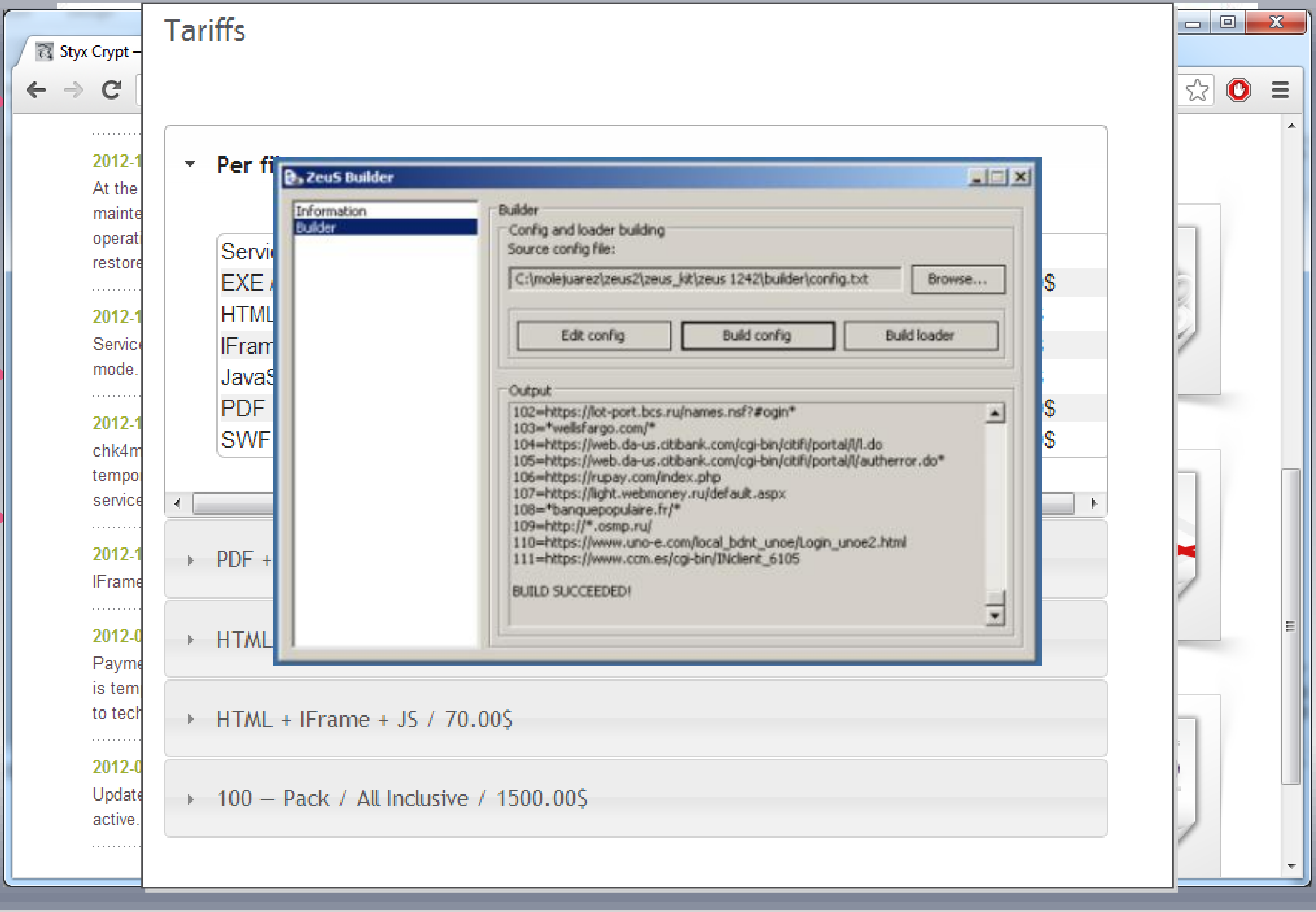
2014
vulnerabilities



[Confidential] For designated groups and individuals

See http://www.cvedetails.com

Known → Unknown Back Again!



Tariffs

HTML + IFrame + JS / 70.00$

100 – Pack / All Inclusive / 1500.00$

Builder

Config and loader building

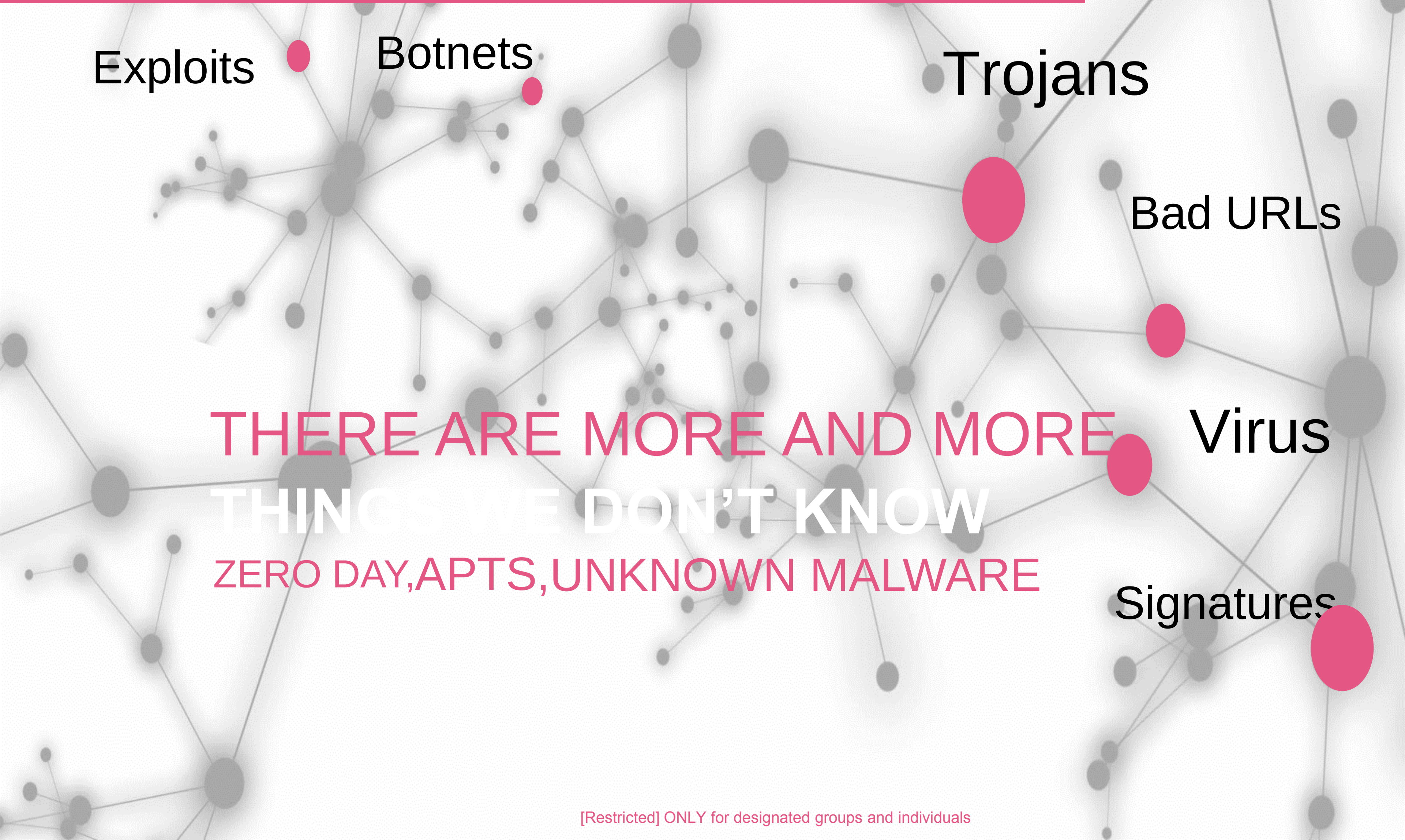
Source config file: C:\molejuarez\zeus2\zeus_kit\zeus 1242\builder\config.txt

Output

```
102=https://lot-port.bcs.ru/names.nsf?#ogin*
103=*wellsfargo.com/*
104=https://web.da-us.citibank.com/cgi-bin/citifi/portal/l/l.do
105=https://web.da-us.citibank.com/cgi-bin/citifi/portal/l/autherror.do*
106=https://rupay.com/index.php
107=https://light.webmoney.ru/default.aspx
108=*banquepopulaire.fr/*
109=http://*.osmp.ru/
110=https://www.uno-e.com/local_bdnt_unoe/Login_unoe2.html
111=https://www.ccm.es/cgi-bin/INclient_6105

BUILD SUCCEEDED!
```

THE GROWTH OF THE UNKNOWN MALWARE



CVEs

Exploits

Botnets

Trojans

Bad URLs

Virus

Signatures

THERE ARE MORE AND MORE THINGS WE DON’T KNOW

ZERO DAY,APTS,UNKNOWN MALWARE

New ways to deal with Know Unknowns?

Without looking at specific patterns

Static Analysis	Evaluating code without running it	👍	Examine all possible execution paths
		👎	Slow and not scalable
Dynamic Analysis (sandbox)	Evaluating code during run-time	👍	Faster and more accurate
		👎	You see what happens in that environment for a short time

Traditional Sandboxes are Slow

INSPECTION TAKES TIME and LET FIRST FILE THROUGH

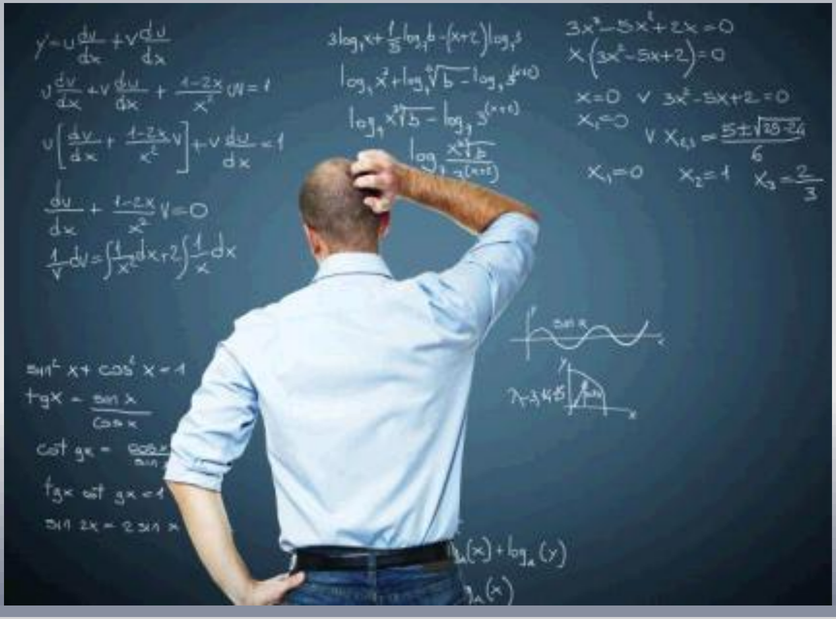
- As a result many sandboxes are deployed in non-blocking mode
- Allows malicious files to reach the user while the sandbox inspects the file in the background

Sandbox detection/evasion

Anti-VM OUT, Anti-Analysis IN

Problem:
Malware drop anti-VM technique and **focus** on Anti-Analysis techniques

Solution:
Subvert the analysis machine with a rootkit before executing the malware



Staying One Step Ahead…

Check Point
SOFTWARE TECHNOLOGIES LTD.

Highest Catch Rate

Evasion-resistant malware detection

CPU-level Detection

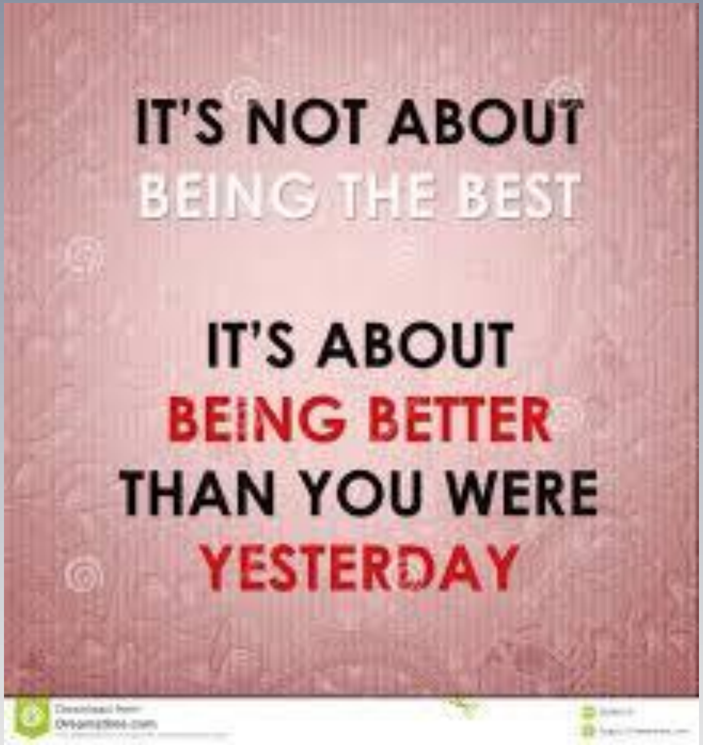
CHECK POINT
SandBlast™
ZERO-DAY PROTECTION

Proactive Prevention

Deployable in blocking mode

Threat Extraction

Real-time Prevention Against Unknown Malware, Zero-Day and Targeted Attacks



IT'S NOT ABOUT
BEING THE BEST

IT'S ABOUT
BEING BETTER
THAN YOU WERE
YESTERDAY

Introducing SandBlast Agent Zero-Day Prevention for Endpoint

Block **UNKNOWN** and **ZERO-DAY ATTACKS** on your endpoints

HIGHEST CATCH RATE

THREAT EMULATION

Evasion resistant sandboxing at CPU- and OS-Level

PROACTIVE PREVENTION

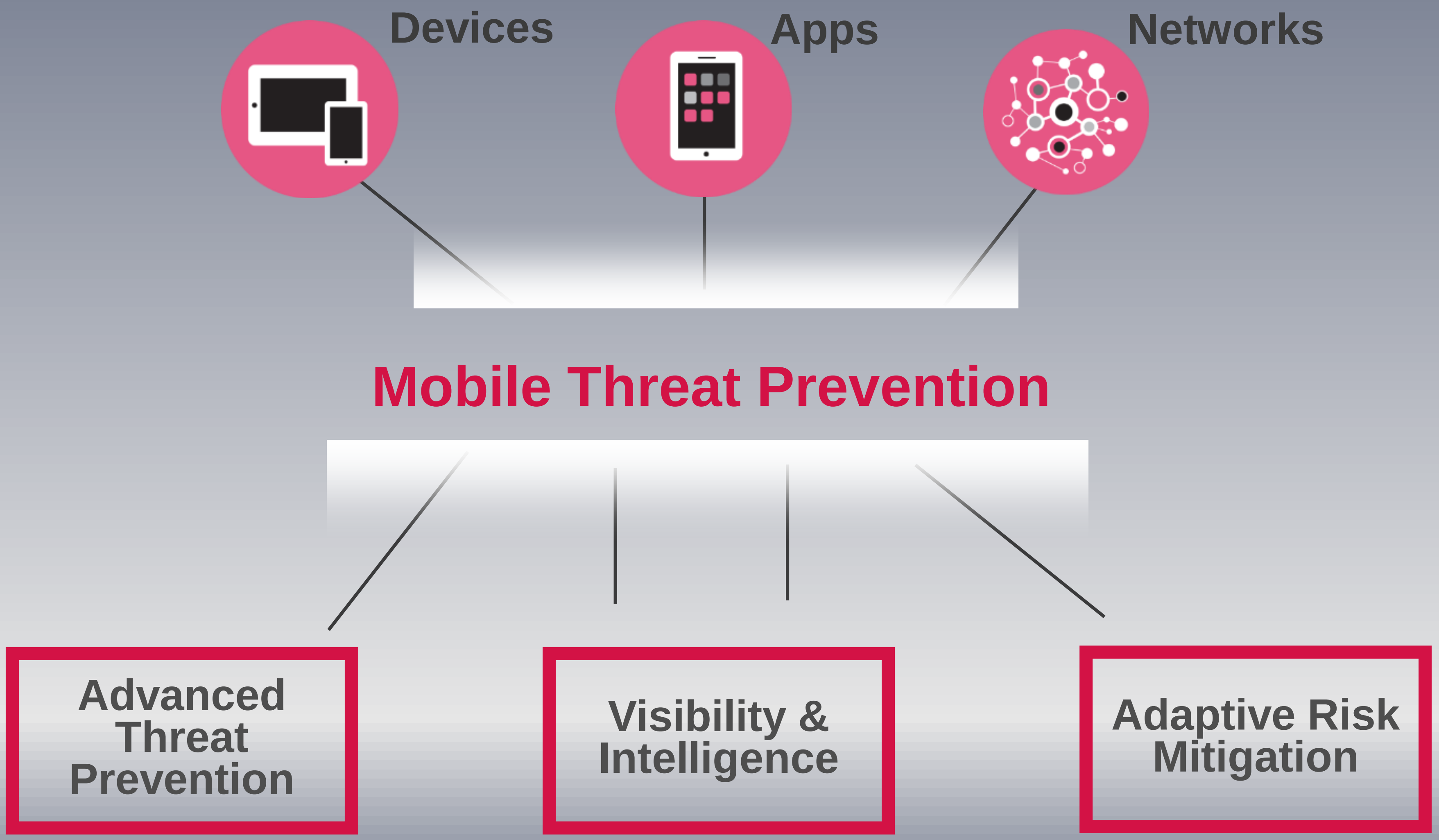
THREAT EXTRACTION

Quick delivery of safe reconstructed content

NON-INTRUSIVE

Processing offloaded from endpoints to the cloud

Checkpoint
Mobile Threat Prevention



Devices

Apps

Networks

Mobile Threat Prevention

Advanced Threat Prevention

Visibility & Intelligence

Adaptive Risk Mitigation

Solving the Mobile Security Gap

ADVANCED THREAT DETECTION AND MITIGATION

Check Point Mobile Threat Prevention

- HIGHEST LEVEL OF SECURITY FOR IOS AND ANDROID
- BEST MOBILE THREAT CATCH RATE
- FULL VISIBILITY
- THREAT ANALYTICS
- REAL-TIME REMEDIATION OF THREATS
- SIMPLE DEPLOYMENT
- TRANSPARENT USER EXPERIENCE

The Power to Prevent Attacks

On the Network and At the Endpoint

CHECK POINT
SandBlast™
ZERO-DAY
PROTECTION

Check Point
SOFTWARE TECHNOLOGIES LTD.

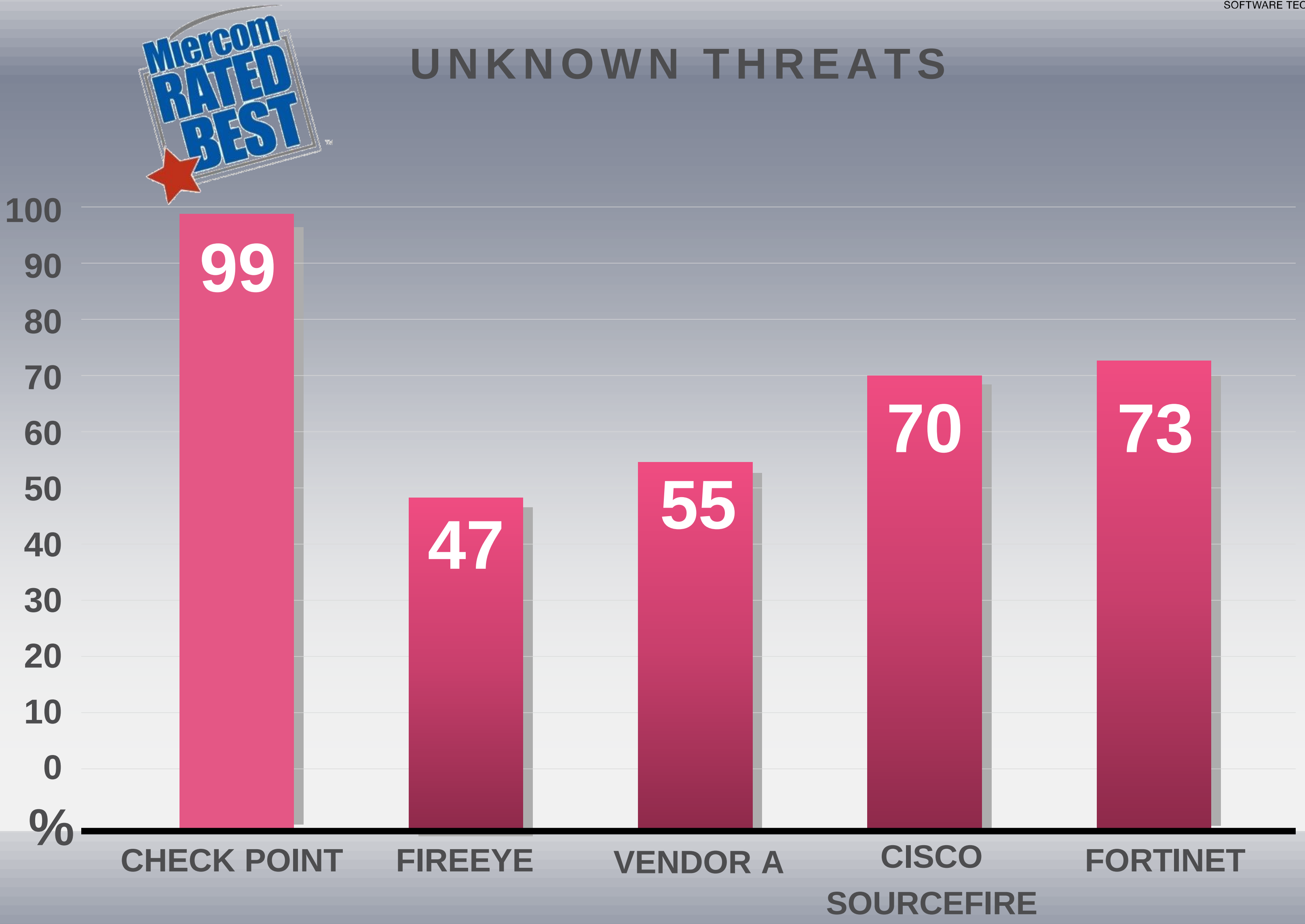
MTP

CHECK POINT
SandBlast™
AGENT

Catches More Malware. Proactive Prevention. Complete Integrated Protection.

The Insight to Understand Them.

Industry’s best catch-rate

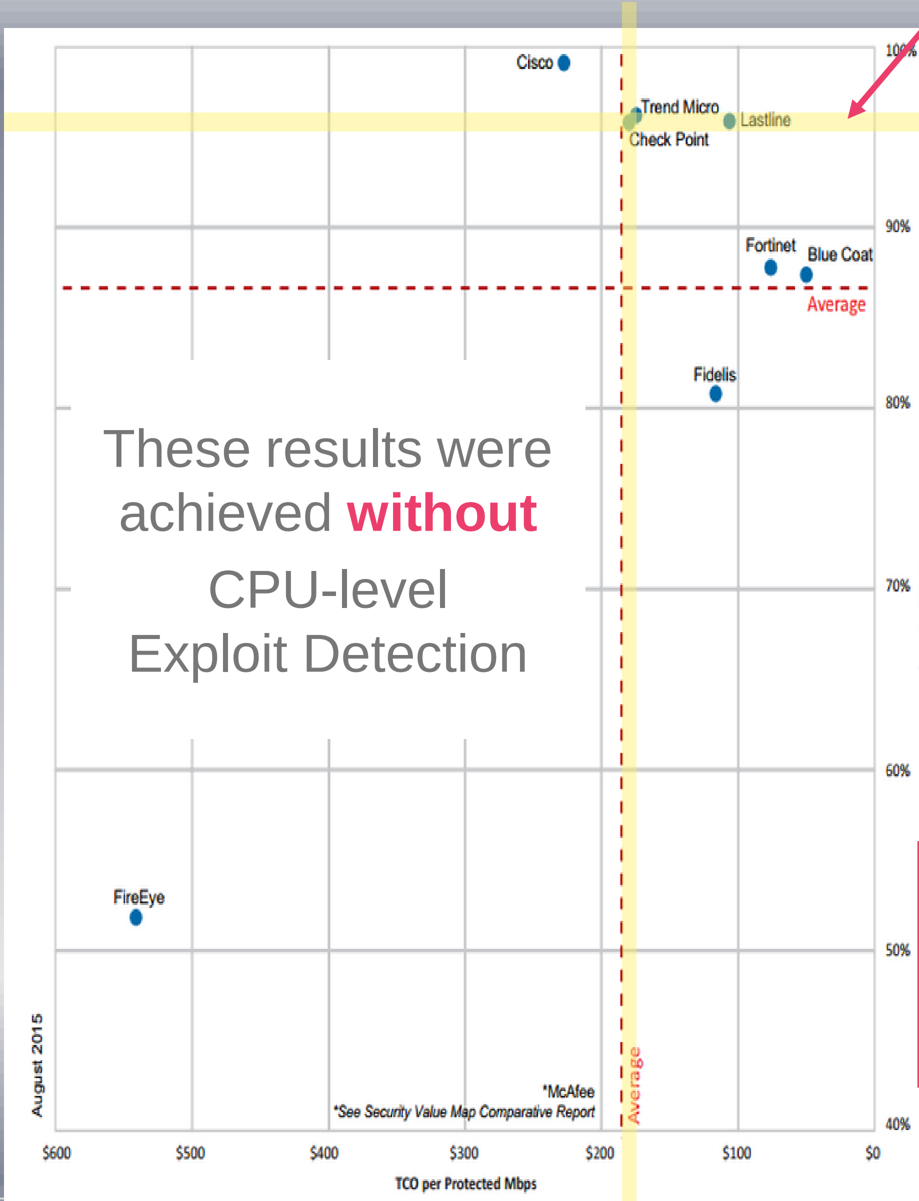


Source: Miercom APT Industry Assessment 2014

NSS Breach Detectio ems

Check Point
SOFTWARE TECHNOLOGIES LTD.

We cannot put a dot here…



These results were achieved **without** CPU-level Exploit Detection

but NSS can

NSS Names Check Point a Top Scoring Recommended Vendor For Sandboxing

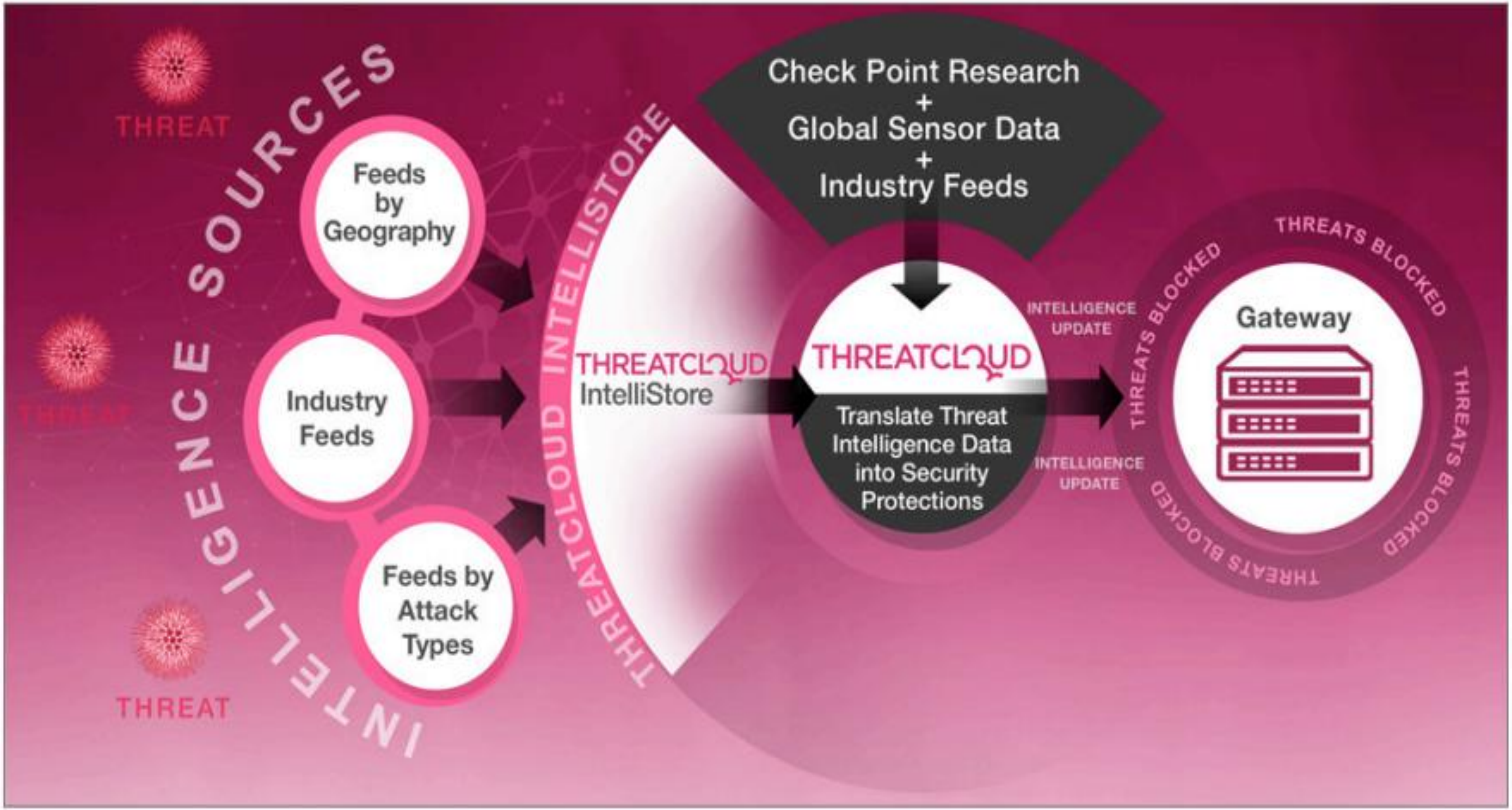
UPDATED RESULTS:

Industry Leading Value at $27 / Mbps

See NSS webcast at:

http://public.brighttalk.com/resource/core/89391/ nss-bds-group-test-update-dec-2015_133131.pdf

System Layers – Private threat Cloud



CHECK POINT SOFTWARE – DEFINED PROTECTION

Check Point
SOFTWARE TECHNOLOGIES LTD.

MANAGEMENT LAYER

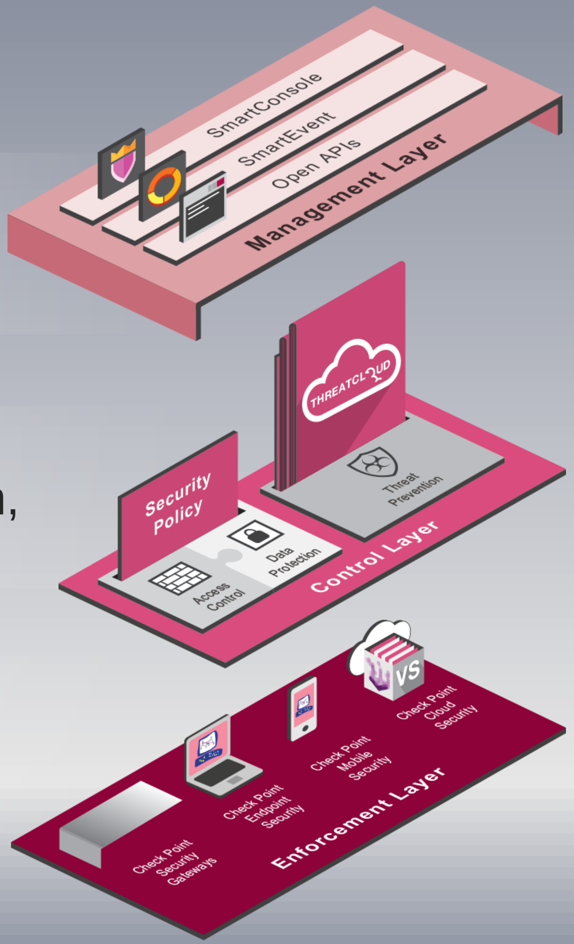
Check Point Next Generation Security Management

CONTROL LAYER

Next Generation Firewall, Threat Prevention, ThreatCloud™

ENFORCEMENT LAYER

Network, Host, Mobile, Cloud



Check Point
SOFTWARE TECHNOLOGIES LTD.

THANK YOU