



Check Point®  
SOFTWARE TECHNOLOGIES LTD

# THE POWER OF CONSOLIDATION – CHECK POINT INFINITY

ALSO Event

Sandor Renz | Security Engineer

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

CLOUD • MOBILE • THREAT PREVENTION



# WHAT HAPPENED IN 2017?

## ATTACKS EVERYWHERE

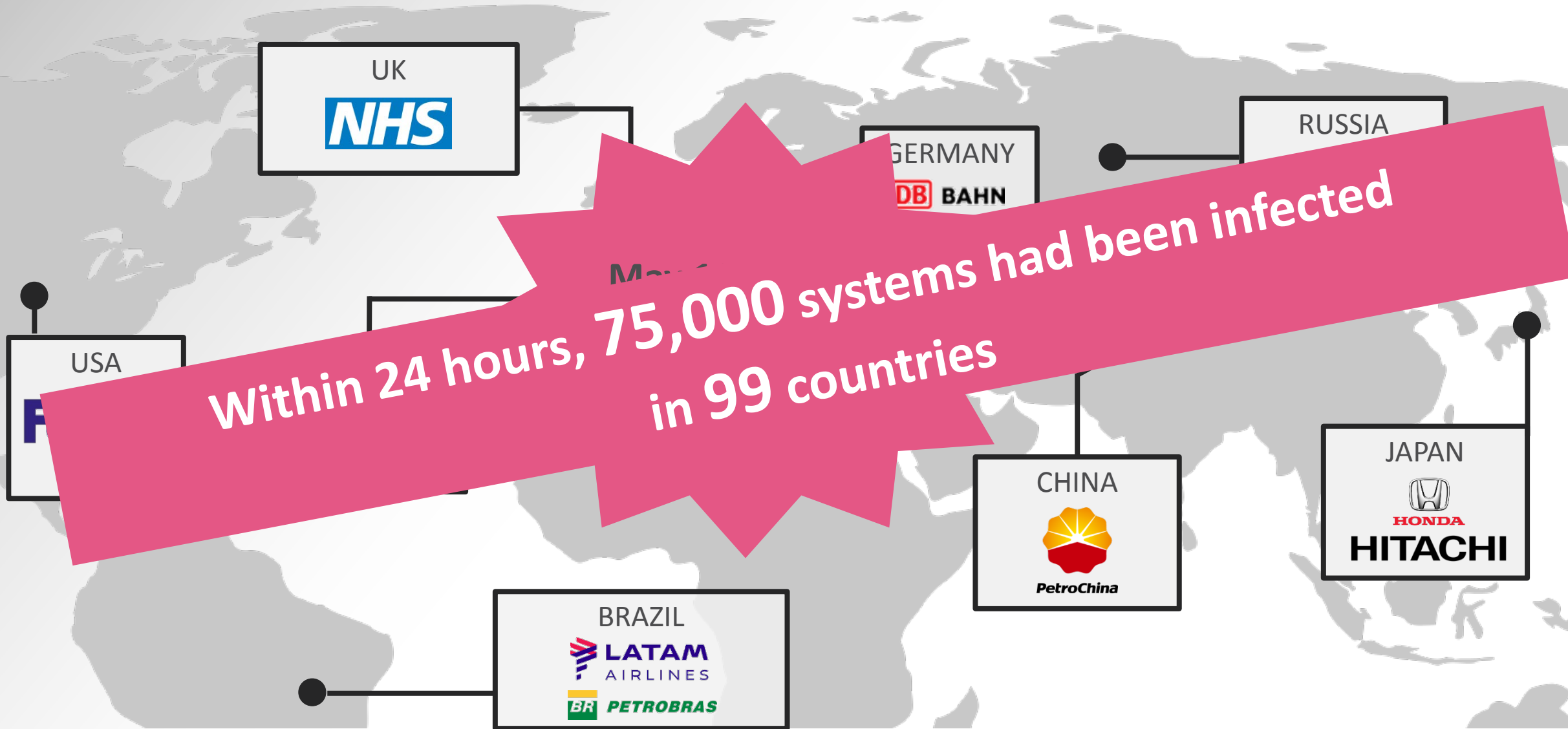
### WANNACRY RANSOMWARE HITS HUNDREDS OF COMPANIES GLOBALLY



### RANSOMWARE ATTACK KEEPS HOTEL GUESTS IN AUSTRIA LOCKED OUT OF ROOMS




# MAY 2017: WANNACRY GLOBAL ATTACKS




# A MONTH LATER: NOTPETYA OUTBREAK



UK  
WPP

DENMARK  
 MAERSK

FRANCE

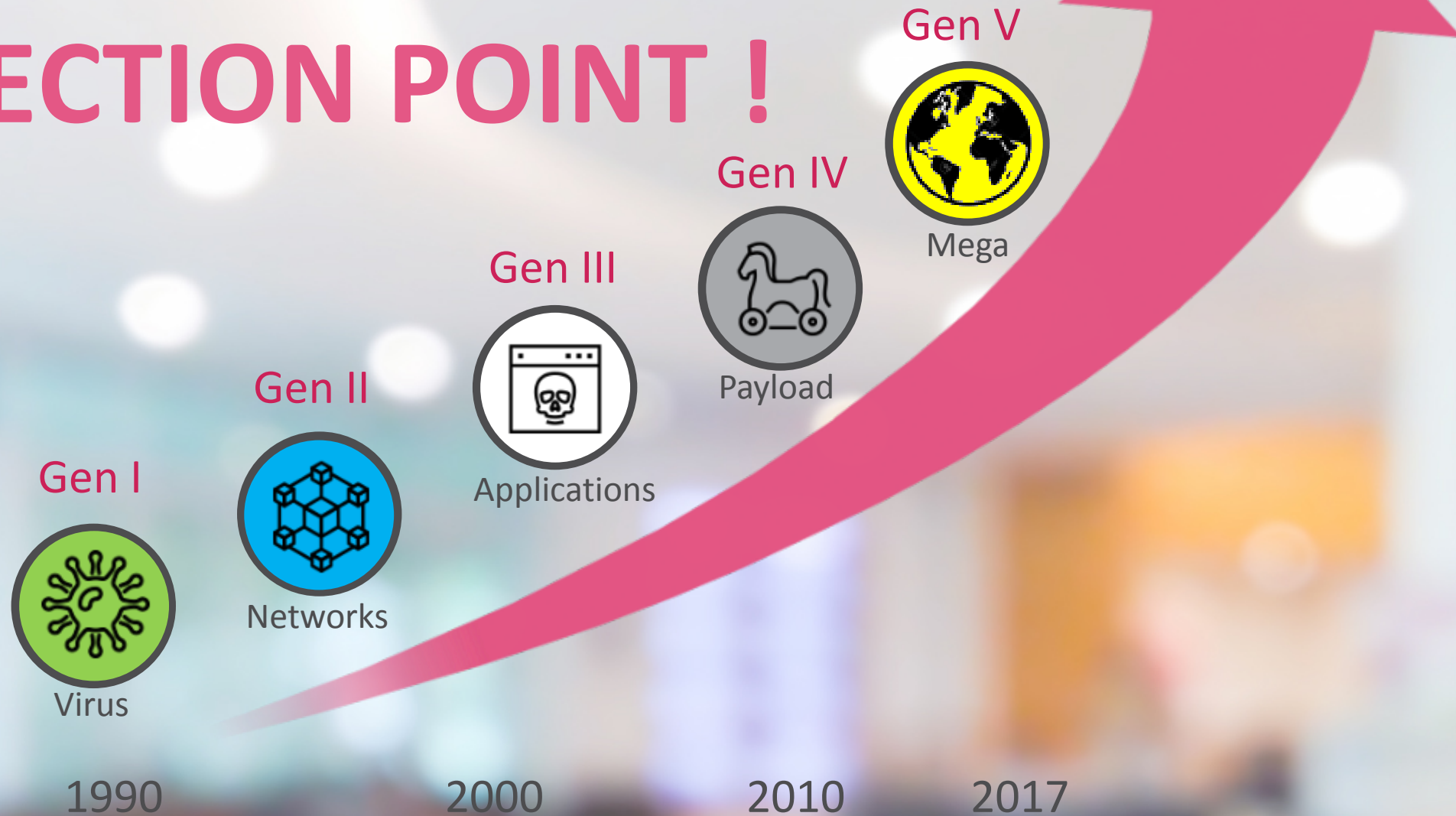
USA  


  
ROSNEFT

International airport  
Chernobyl reactor  
Power grid  
Water supply system  
• Petrol stations

**Major corporations in 65 countries were under attack,  
UKRAINE WAS NEARLY CRIPPLED**

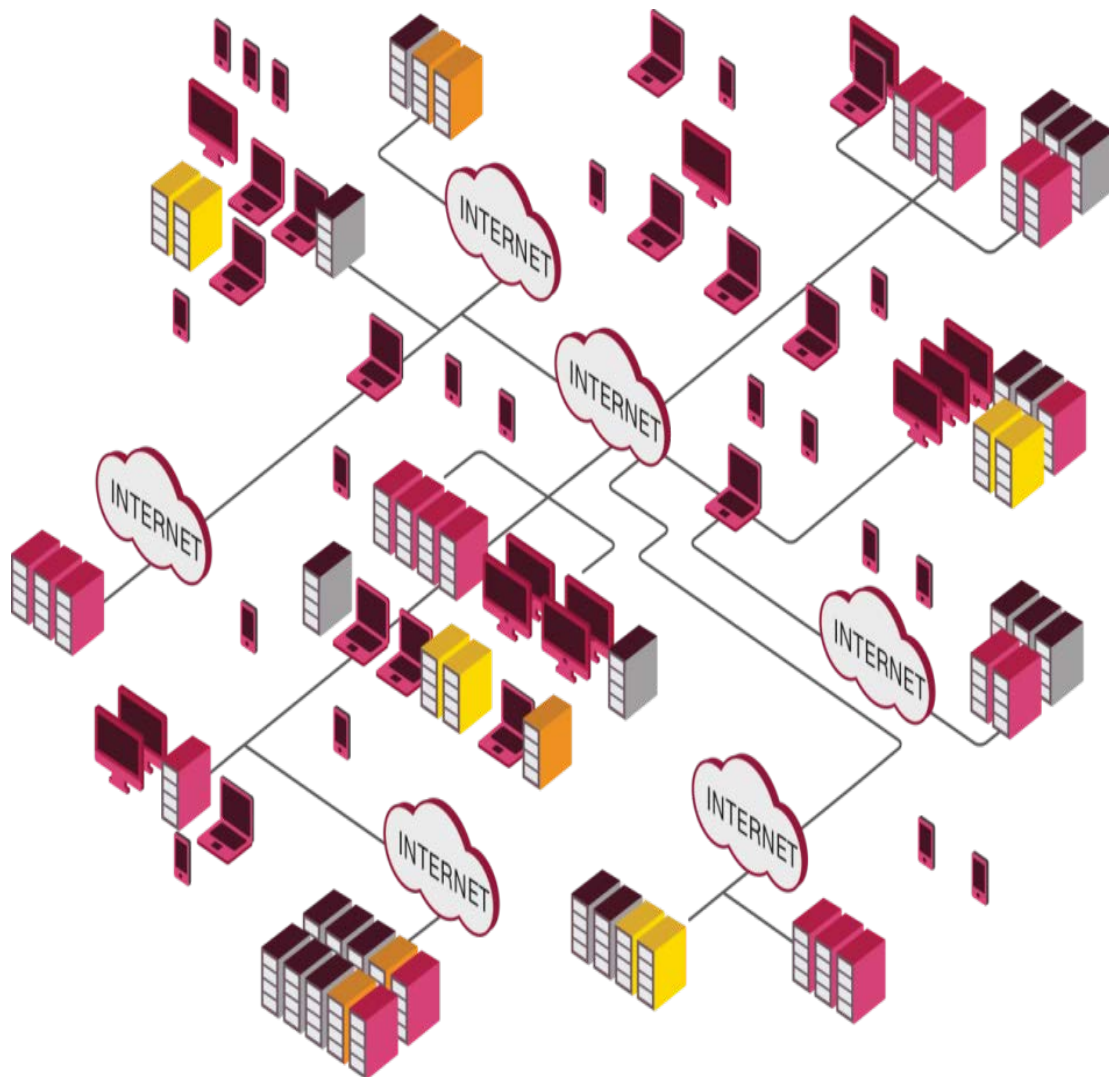
# WE ARE AT AN INFLECTION POINT !





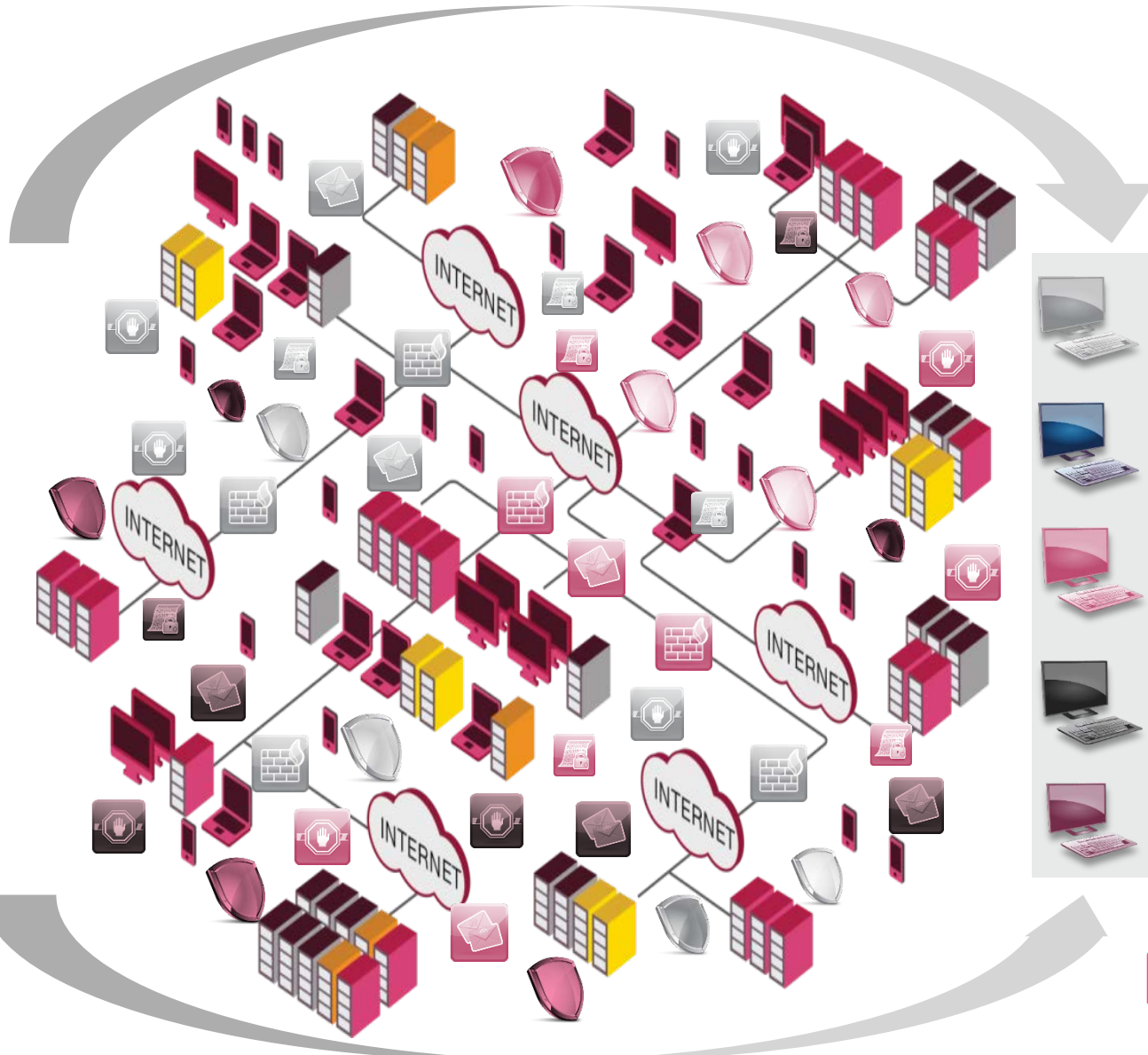


# How to secure such dynamic environments ? With limited resources ? While enabling Business ?



- Virtualization
- Cloud
- Mobility
- Remote branches
- Information sharing
- 3<sup>rd</sup> parties
- Industrial systems
- lot
- Encryption
- Shadow IT
- Compliance
- Segregation
- BYOD
- Scalability
- Operations
- Monitoring
- Availability
- ....

# The “Best of Breed” approach : We know the result...



**Complexity**  
**Added to**  
**Complexity**

**Not manageable & Not secure**



Check Point®  
SOFTWARE TECHNOLOGIES LTD

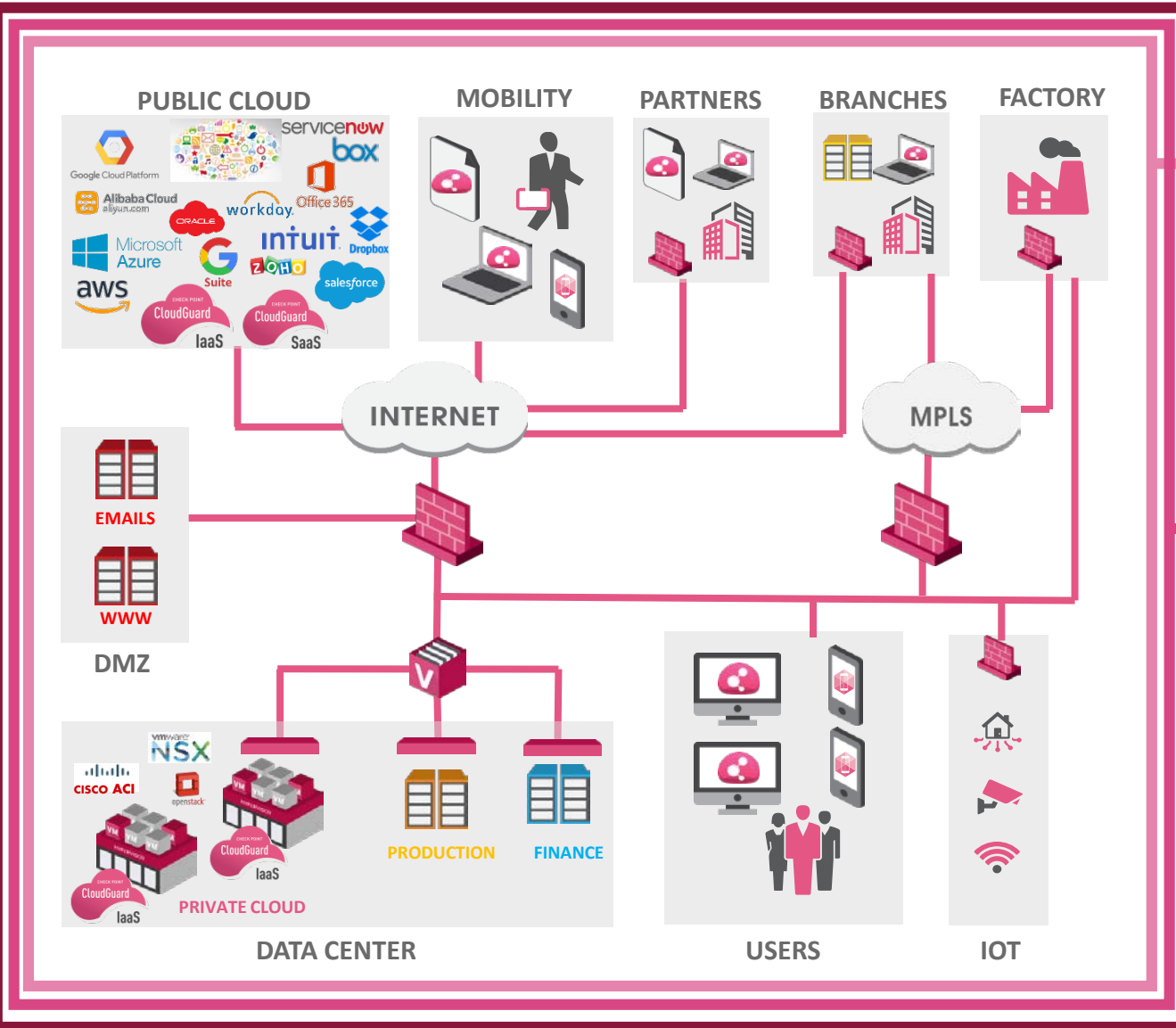


# CHECK POINT INFINITY

THE CYBER SECURITY ARCHITECTURE OF THE FUTURE

THE FIRST **CONSOLIDATED** SECURITY ACROSS **NETWORKS,**  
**CLOUD,** AND **MOBILE,** PROVIDING THE HIGHEST LEVEL  
OF THREAT PREVENTION.





### ONE SECURITY PLATFORM

The bar chart shows the evolution of security appliances: 3200 Appliances (1400 Desktop), 5000 Appliances (4 models), 10000 Appliances (2 models), 23000 Appliances (2 models), and 61000 Ultra High-End. The diagram below it shows **UNIFIED SECURITY ACROSS ALL ENVIRONMENTS** with components like **DATA CENTER**, **CLOUD**, **ENDPOINT**, **NETWORK PERIMETER**, and **MOBILE**, all connected to **SHARED THREAT INTELLIGENCE**.

### BEST SECURITY TECHNOLOGIES

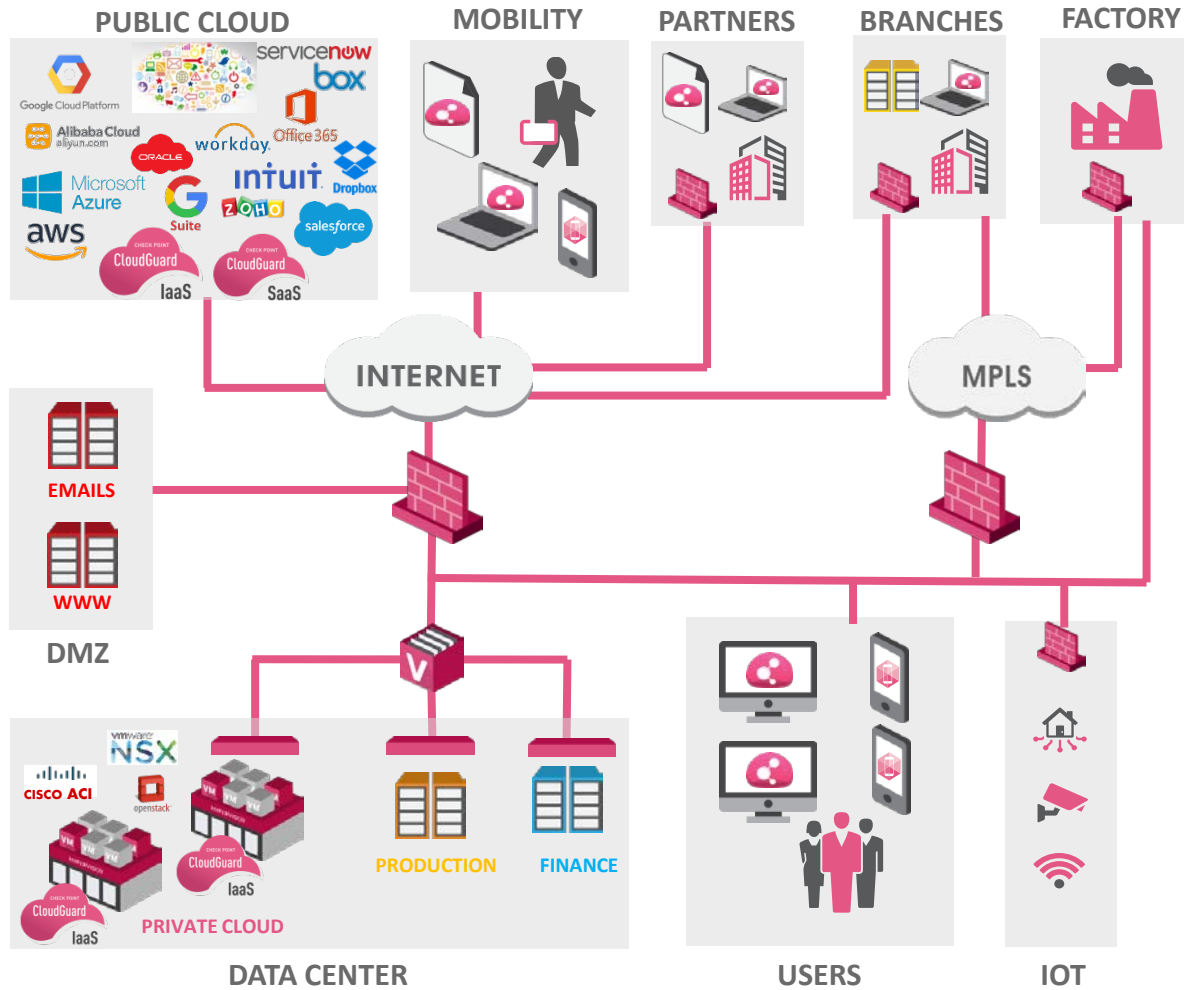
**Web Security, Data Security, Threat Prevention**

Icons representing security technologies: a brick wall, a minus sign, a padlock, a biohazard symbol, a network icon, and logos for **CloudGuard**, **SandBlast** (Check Point Zero-Day Protection), and **THREATCLOUD**.

### CONSOLIDATED MANAGEMENT

**Simplicity, Visibility, Efficiency & Automation**

Icons representing management tools: **R30** management console, a dashboard screenshot, and an **<API>** icon.



**ONE SECURITY PLATFORM**

**LOWER COSTS**  
**HIGHER FLEXIBILITY**

**BEST SECURITY TECHNOLOGIES**

**MORE SECURE**

**CONSOLIDATED MANAGEMENT**

**MORE SIMPLE**



# CHECK POINT INFINITY



Check Point®  
SOFTWARE TECHNOLOGIES LTD



## SECURITY MANAGEMENT





# Check Point Management Architecture

---

“

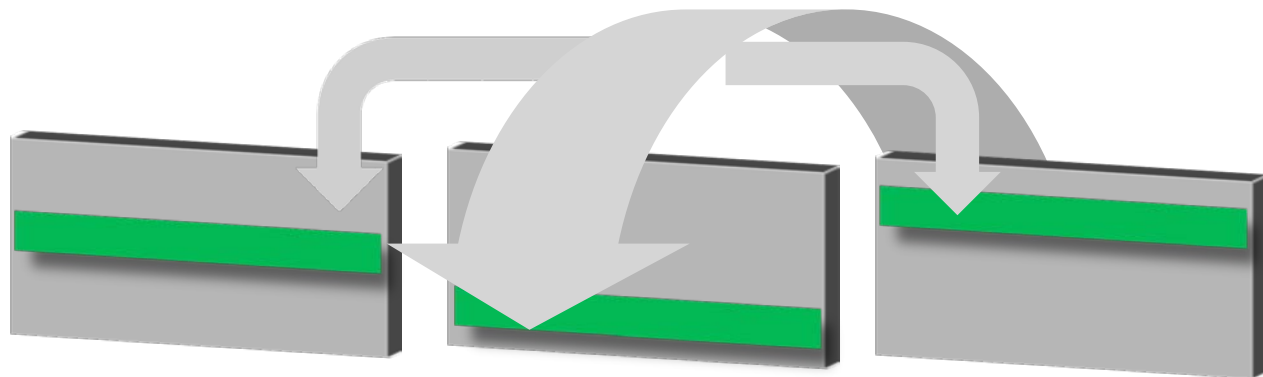
The Check Point management remains the de facto “**gold standard**” against which other consoles are measured.

”

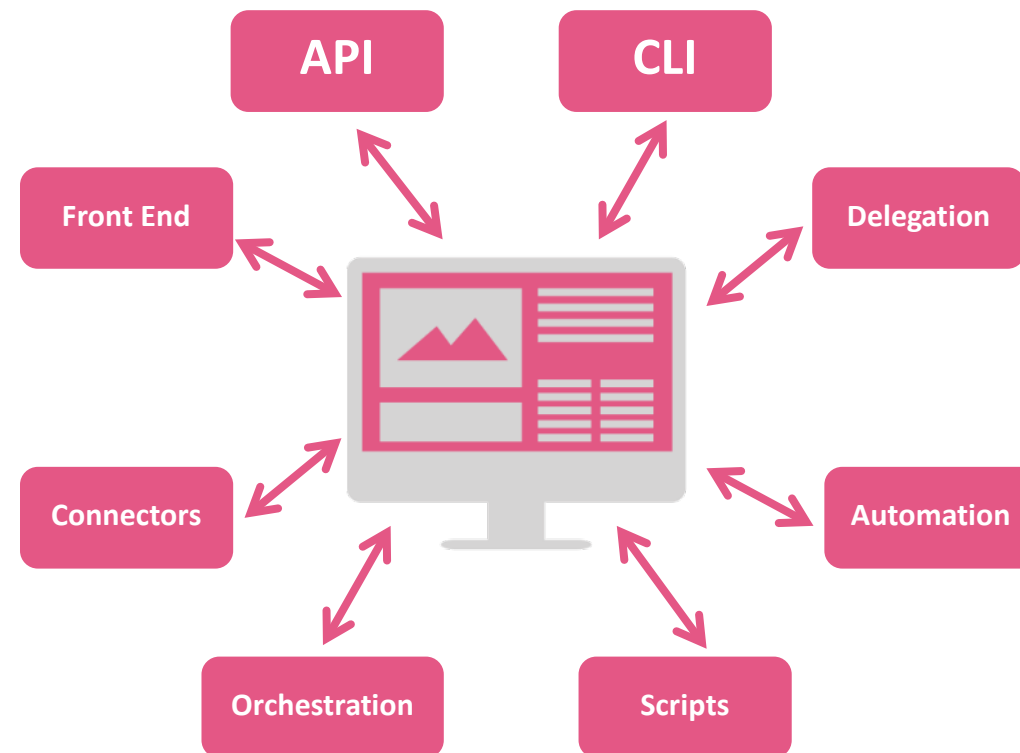




# Unified Policy, Layers and Automation



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



MORE Simple, Clear & Fast = EFFECTIVE

# Visibility : A single view to your security



Check Point  
SOFTWARE TECHNOLOGIES LTD

### Attack Types by Blades

- 4 IPS
- 1 Anti-Bot
- 1 Threat Emulation
- 2 Anti-Virus

### Activity Timeline

### Top Destination Countries

### Top Destinations

Severity	Destination	Blade	Logs
Critical	10.82.92.147	IPS	30
Critical	192.168.55.23	IPS	15
Critical	10.7.210.15	Anti-Bot, Anti-Virus	18
Critical	10.7.98.85	IPS	20
Critical	192.168.72.190	IPS	30
Critical	192.168.72.103	Anti-Bot	7
Critical	10.82.92.109	Anti-Bot	3
Critical	192.168.11.156	IPS	5
Critical	10.226.111.81	Anti-Virus	4
Critical	192.168.11.153	IPS	5

### Top Attacks

Severity	Protection Name	Blade	Logs
Critical	Malicious Binary.balmblj	Anti-Virus	4
Critical	Backdoor.Win32.Taidoor.A	Anti-Bot	37
Critical	MIT Kerberos kadmind RPC...	IPS	160
Critical	Microsoft Windows RASMA...	IPS	30
Critical	Exploited doc document	Threat Emulati...	8
High	Microsoft WINS Local Privile...	IPS	15
High	Alt-N Technologies Security...	IPS	20
High	Virus.WIN32.Eicar-Modified...	Anti-Virus	30
<b>Critical</b>	<b>8 Protections</b>	<b>4 Blades</b>	<b>304</b>

Found 8 results (5.7 sec.) Query Syntax

Time	Blade	Interface	Origin	Action	Source	Destination	Service	Rule	Policy...	Description
29 Nov 15, 3:56:30 AM	Firewall	inbound e...	192.0.2.200	Drop	10.10.5.121	192.168.138.4	nbssession	3	Standard	nbssession Traffic Dropped from 10.10.5.121 to 192.168.138
28 Nov 15, 7:36:50 AM	Firewall	inbound e...	192.0.2.200	Drop	10.82.7.5	192.168.138.4	Napster_dir...	3	Standard	Napster_directory_5555 Traffic Dropped from 10.82.7.5 to 1
28 Nov 15, 1:44:00 AM	Firewall	inbound e...	192.0.2.200	Drop	10.10.5.121	192.168.138.4	nbssession	3	Standard	nbssession Traffic Dropped from 10.10.5.121 to 192.168.138
26 Nov 15, 8:15:30 PM	Firewall	inbound e...	192.0.2.200	Drop	10.0.1.100	192.168.138.4	Napster_dir...	3	Standard	Napster_directory_5555 Traffic Dropped from 10.0.1.100 to
26 Nov 15, 10:47:20 AM	Firewall	inbound e...	192.0.2.200	Drop	10.15.2.34	192.168.138.4	TCP/5053	3	Standard	TCP/5053 Traffic Dropped from 10.15.2.34 to 192.168.138.4



# CHECK POINT INFINITY

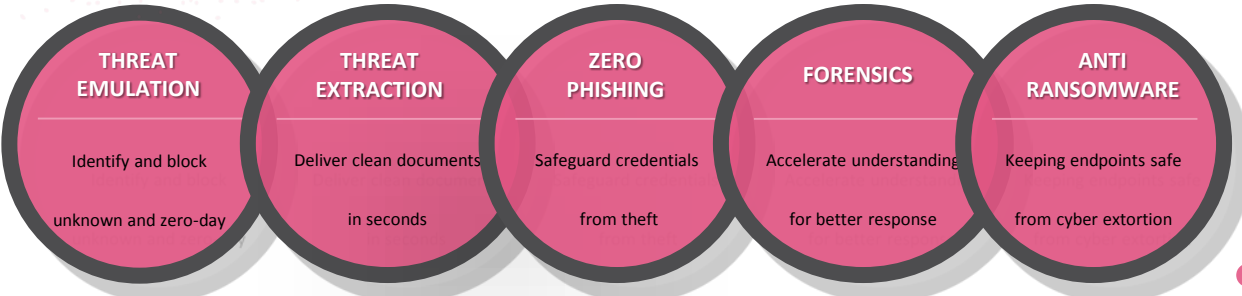


THREAT PREVENTION





# THE FIRST AND ONLY UNIFIED CROSS-PLATFORM THREAT PREVENTION



100% Breach Prevention System Combined Score

100% Protection against Drive-By exploits

100% Protection against Social Exploits

100% Protection against HTTP Malware

100% Protection against Email Malware

100% Protection against Off-Line infections

0.0% False Positives & 99.2% Evasions

CHECK POINT CLOUD



SandBlast Service

HOSTED ON PREMISE



SandBlast TE Appliance



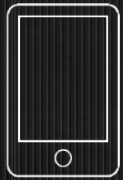




# CHECK POINT INFINITY

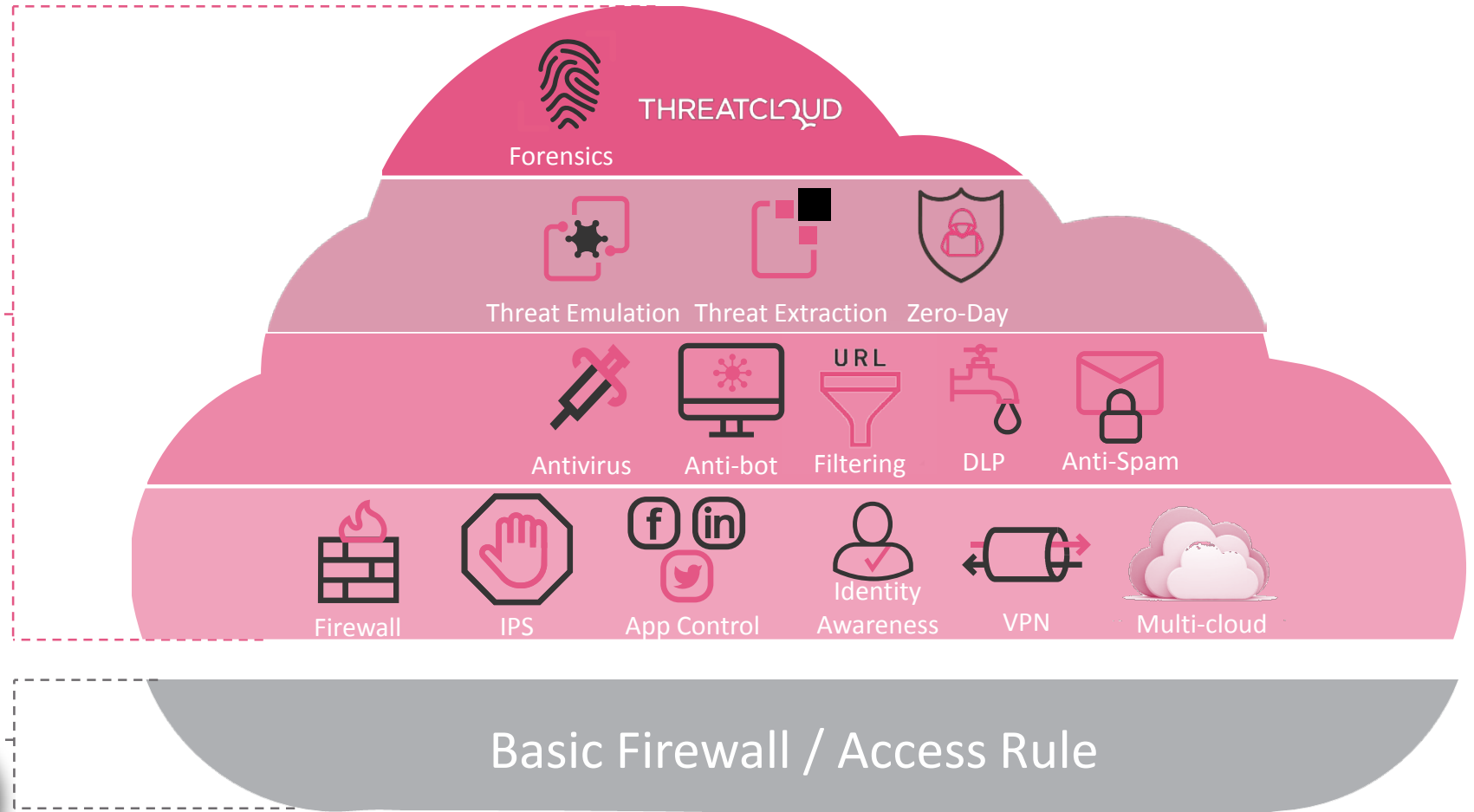


Check Point®  
SOFTWARE TECHNOLOGIES LTD



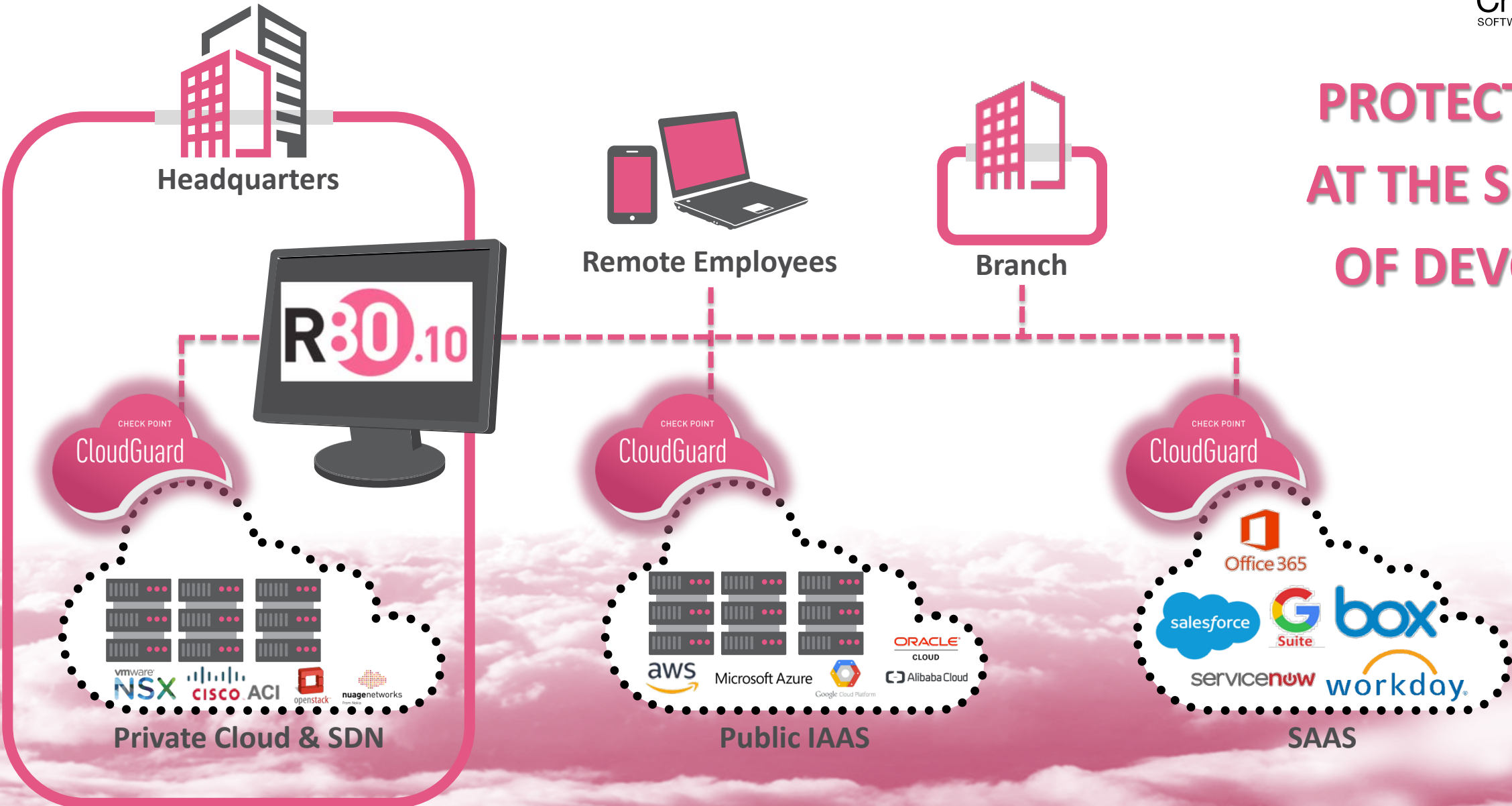
CLOUD SECURITY

# The same UNIFIED security extended for your clouds



# UNIFIED SECURITY FOR ALL CLOUDS

## PROTECTION AT THE SPEED OF DEVOPS







# CHECK POINT INFINITY



Check Point®  
SOFTWARE TECHNOLOGIES LTD



MOBILE SECURITY

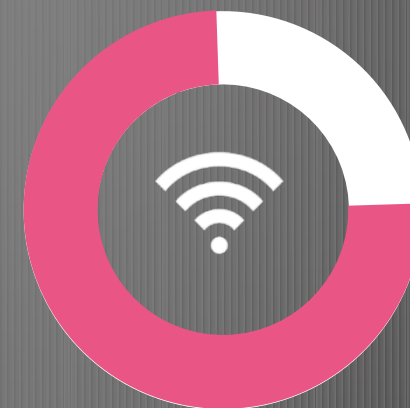
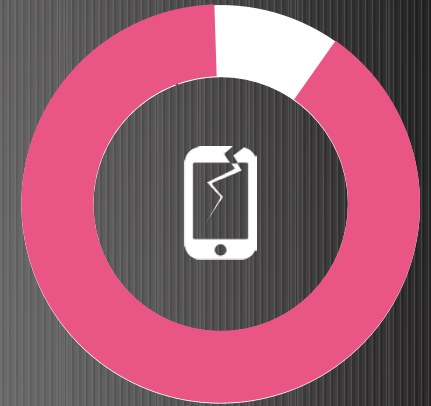




# MOBILE – THE WEAKEST LINK IN OUR ENTERPRISES



74%  
with jailbroken or  
rooted devices



89%  
Experienced a  
man-in-the-middle  
attack over Wi-Fi

Source: Check Point Mobile Threat Prevention | N=850 Check Point customers, each protecting more than 500 devices

**DEMO**


























**Mobility**

---



# Demo content

- How to prevent access to phishing sites
  - Browser
  - Messenger

 FRANCE 24	 Eigene Dateien	 Corporate Intranet	 Capsule	 Protect
 YouTube	 Uhr	 ÖBB	 Rechner	 Galerie
 LinkedIn	 Play Store	 Kalender	 Maps	 HANDY Parken
 Mein A1	 Einstellungen	 BAWAG PSK	 E-Mail	 Expenses
 Telefon	 Nachrichten	 WhatsApp	 Chrome	 Kamera







## Demo content

- Conditional access
  - A compromised devices will be blocked to access corporate resources

SIM gesperrt

20:05

85 %



FaceTime



Podcasts



Rechner



Watch



Dateien



Extras



Home



Health



Videos



Wallet



iBooks



Aktien



Erinnerungen



iTunes Store



Uhr



Notizen



Musik



YouTube



Road Bike



BikeBrain



GPS Cycle



Warten ...



GPX Tracker



CFD





## MOBILE



- App Protection
- Network Protection
- Device Protection
- Blocks SMiSing Attacks



- Remote Access
- Secure Container Business apps
- Protect docs everywhere



# CHECK POINT INFINITY



Threat Intelligence  
**THREATCLOUD**



## CLOUD

### Infrastructure

- Advanced Threat Prevention
- Adaptive Security
- Automation and Orchestration
- Cross Cloud Dynamic Policies
- Multi-Cloud



- Microsoft Azure
- Azure Stack
- VMware NSX
- aws
- openstack

### Applications

- Zero-Day Threat Protection
- Sensitive Data Protection
- End-to-end SaaS Security
- Identity Protection



- Office 365
- salesforce
- Google Apps
- Dropbox
- servicenow



Hybrid Cloud



## ENDPOINT



- Threat Emulation & Extraction
- Anti - Ransomware
- Zero - Phishing
- Forensics & Quarantine

### Complete Protection

- Firewall, VPN & Compliance Check
- Disk & Media Encryption
- Anti-Malware
- Anti-Bot
- Secure Documents



MGMT



R30

Smart Event



Monitoring



Compliance

Multi Layered Security

Advanced Threat Prevention

App Control

Data Protection

## HEADQUARTERS



LAN

Access Control

Advanced Threat Prevention

Segmentation

## BRANCH / ICS



SCADA ICS

LAN

WELCOME TO THE FUTURE OF CYBER SECURITY

©2018 Check Point Software Technologies Ltd.





Check Point®  
SOFTWARE TECHNOLOGIES LTD

# THANK YOU

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

CLOUD • MOBILE • THREAT PREVENTION