Check Point
SOFTWARE TECHNOLOGIES LTD.

A multi-layer approach to cyber-security

Niccolò Manfrini

Security Engineer

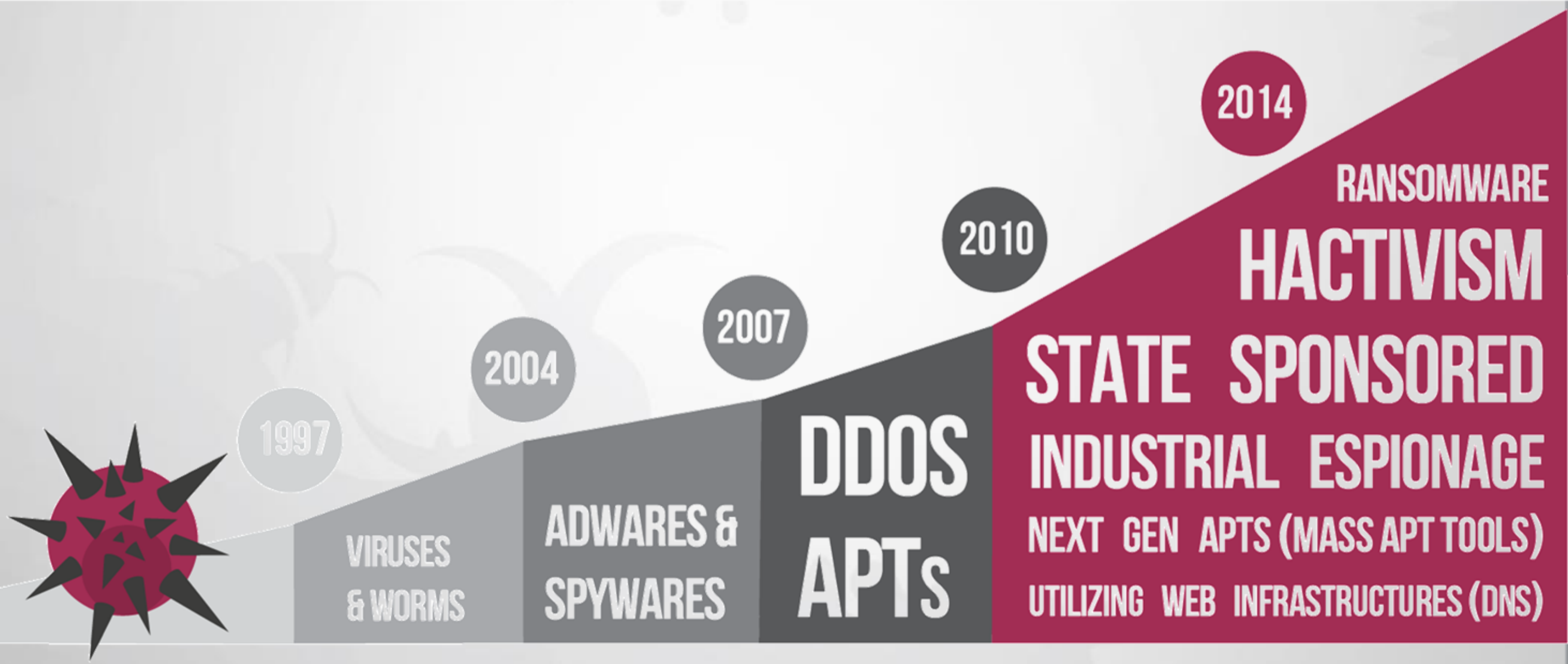
SOFTWARE-DEFINED
PROTECTION

JOIN THE **SECURITY REVOLUTION**

TECHNOLOGY IS EVERYWHERE

The Internet of things **BRINGS WITH IT NEW** challenges

BUT SO ARE THREATS



1997

VIRUSES & WORMS

2004

ADWARES & SPYWARES

2007

DDOS APTs

2010

2014

RANSOMWARE

HACTIVISM

STATE SPONSORED

INDUSTRIAL ESPIONAGE

NEXT GEN APTS (MASS APT TOOLS)

UTILIZING WEB INFRASTRUCTURES (DNS)

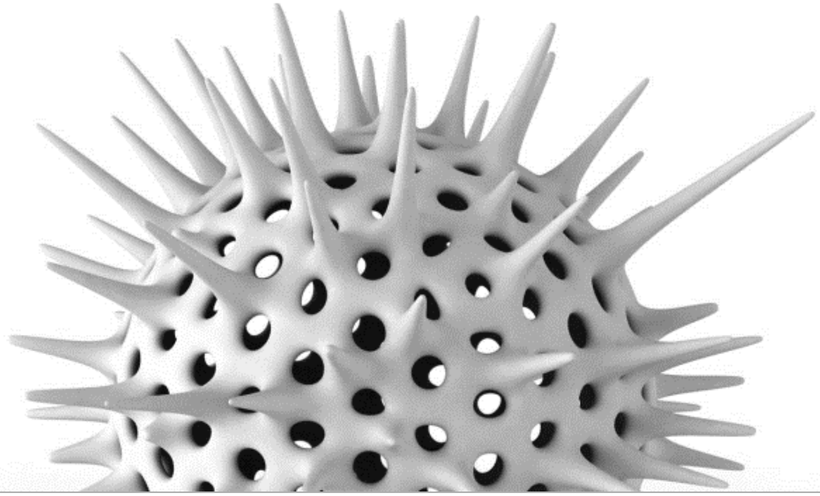
Threat Evolvement…

Traditional threats

Simple and repeatable
Mass-market
Opportunistic

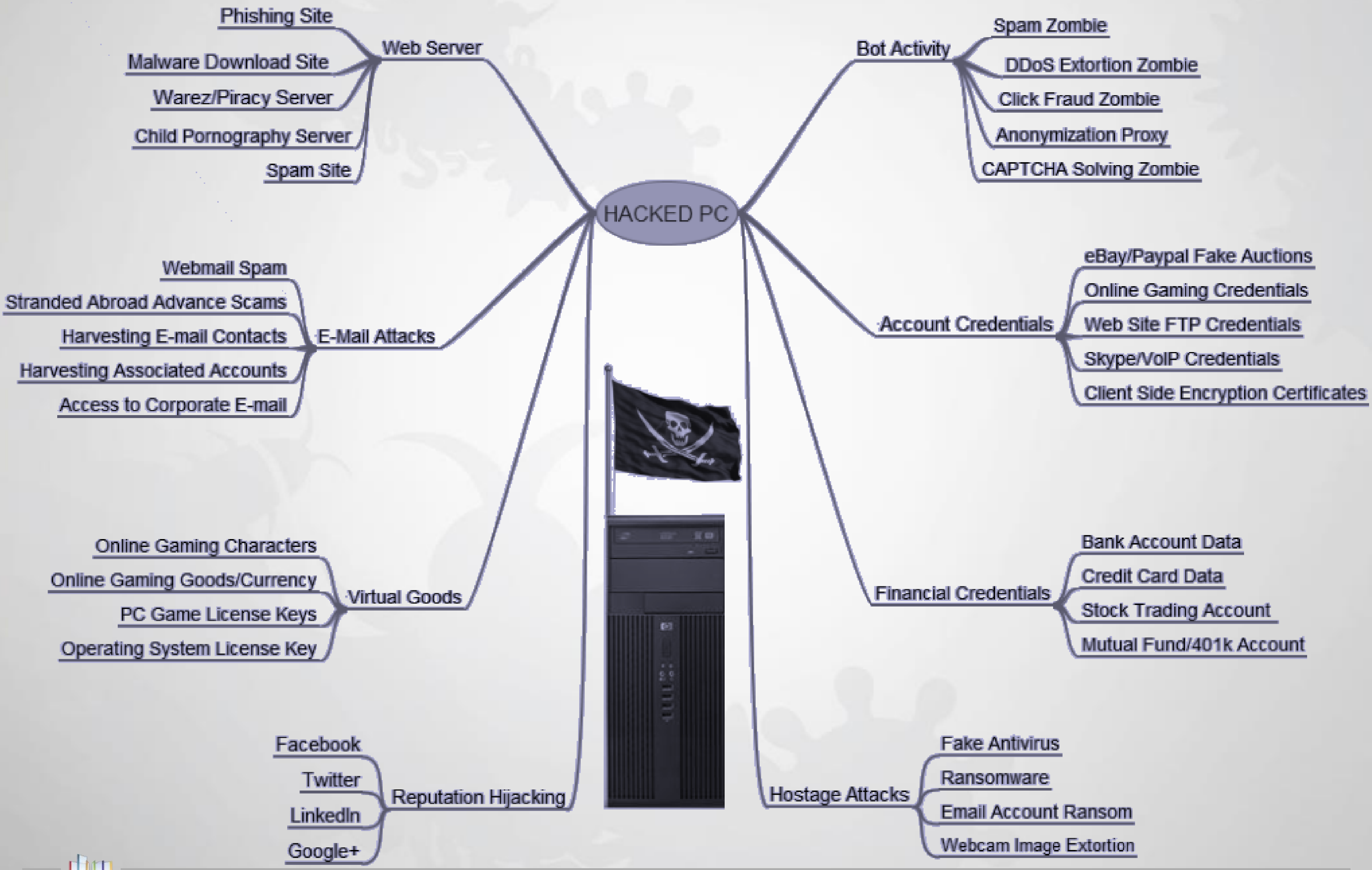
Modern attacks

Sophisticated
Customized
Relentless



Value of a Hacked PC

Check Point SOFTWARE TECHNOLOGIES LTD.

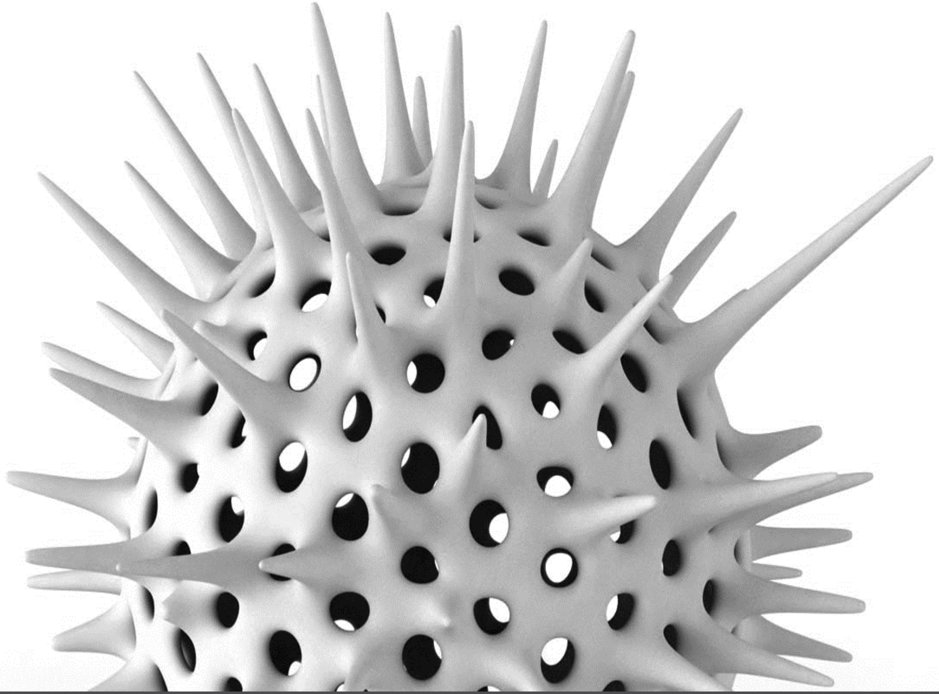


HACKED PC

- Web Server
  - Phishing Site
  - Malware Download Site
  - Warez/Piracy Server
  - Child Pornography Server
  - Spam Site
- E-Mail Attacks
  - Webmail Spam
  - Stranded Abroad Advance Scams
  - Harvesting E-mail Contacts
  - Harvesting Associated Accounts
  - Access to Corporate E-mail
- Virtual Goods
  - Online Gaming Characters
  - Online Gaming Goods/Currency
  - PC Game License Keys
  - Operating System License Key
- Reputation Hijacking
  - Facebook
  - Twitter
  - LinkedIn
  - Google+
- Bot Activity
  - Spam Zombie
  - DDoS Extortion Zombie
  - Click Fraud Zombie
  - Anonymization Proxy
  - CAPTCHA Solving Zombie
- Account Credentials
  - eBay/Paypal Fake Auctions
  - Online Gaming Credentials
  - Web Site FTP Credentials
  - Skype/VoIP Credentials
  - Client Side Encryption Certificates
- Financial Credentials
  - Bank Account Data
  - Credit Card Data
  - Stock Trading Account
  - Mutual Fund/401k Account
- Hostage Attacks
  - Fake Antivirus
  - Ransomware
  - Email Account Ransom
  - Webcam Image Extortion

http://krebsonsecurity.com

Is Your Organization Infected With Malware?

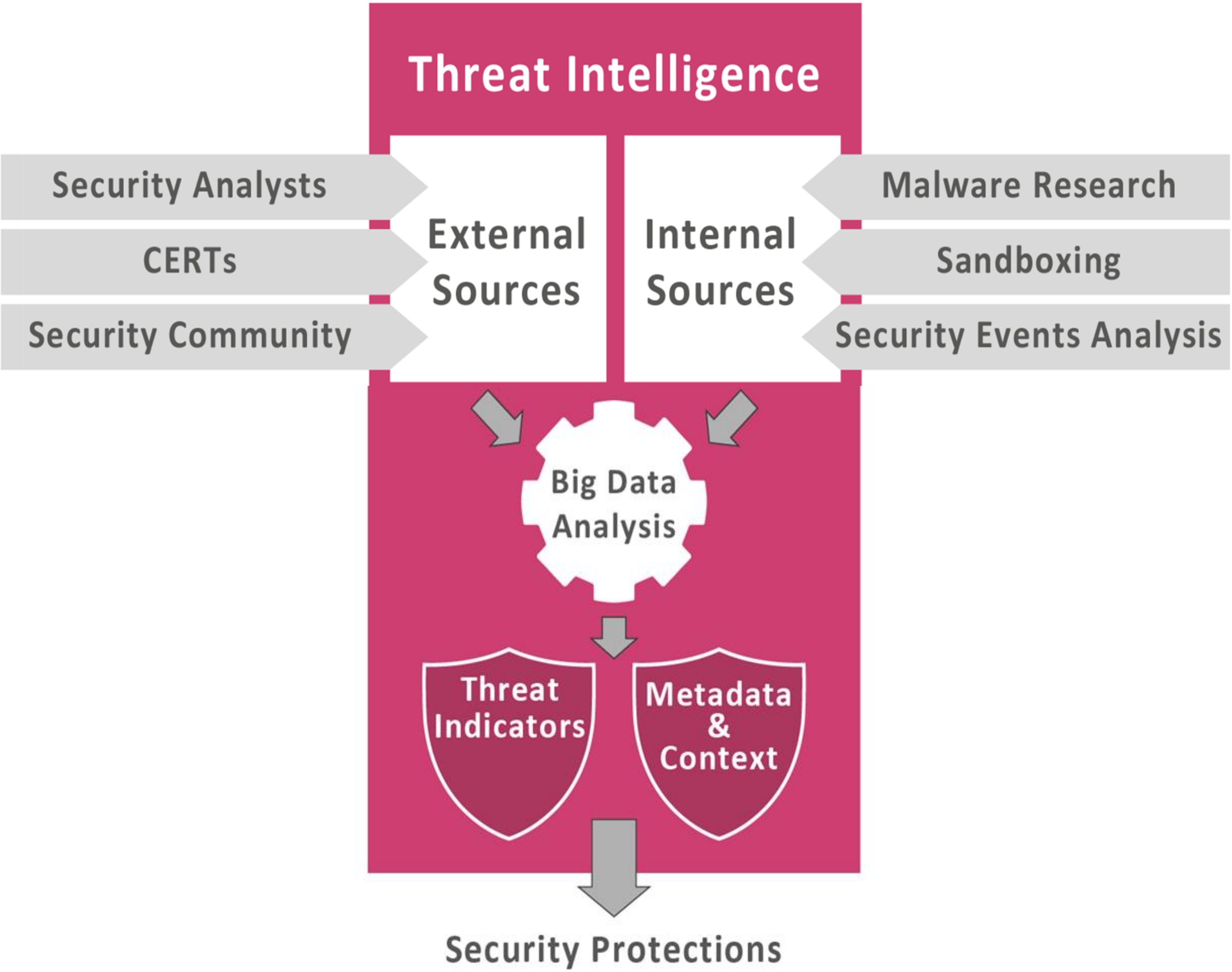


63% of Organizations Are Infected with Bots

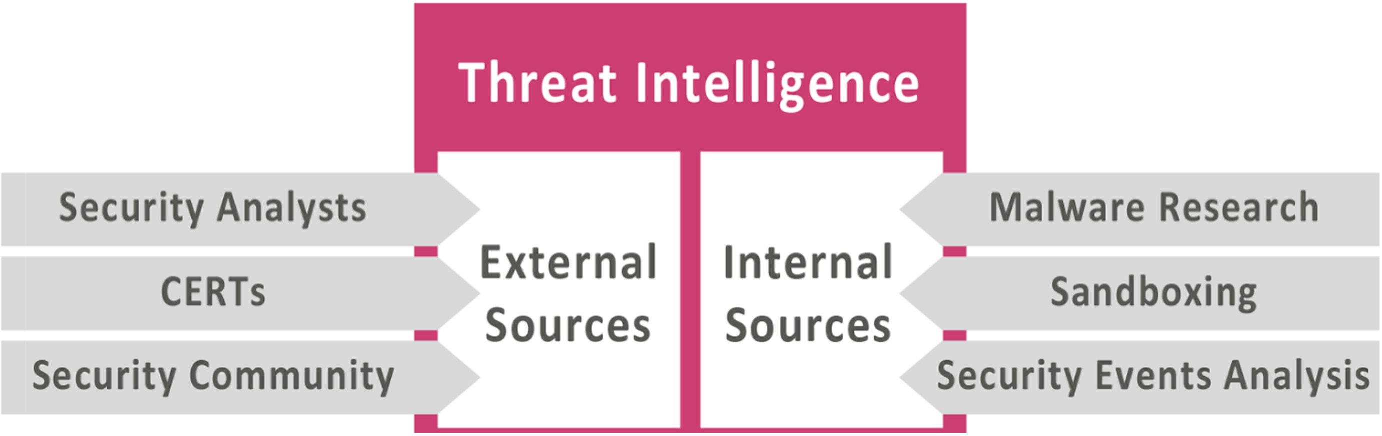
49% of Organizations Have 7+ Bot-infected Hosts

Check Point
Threat Prevention

THREAT INTELLIGENCE



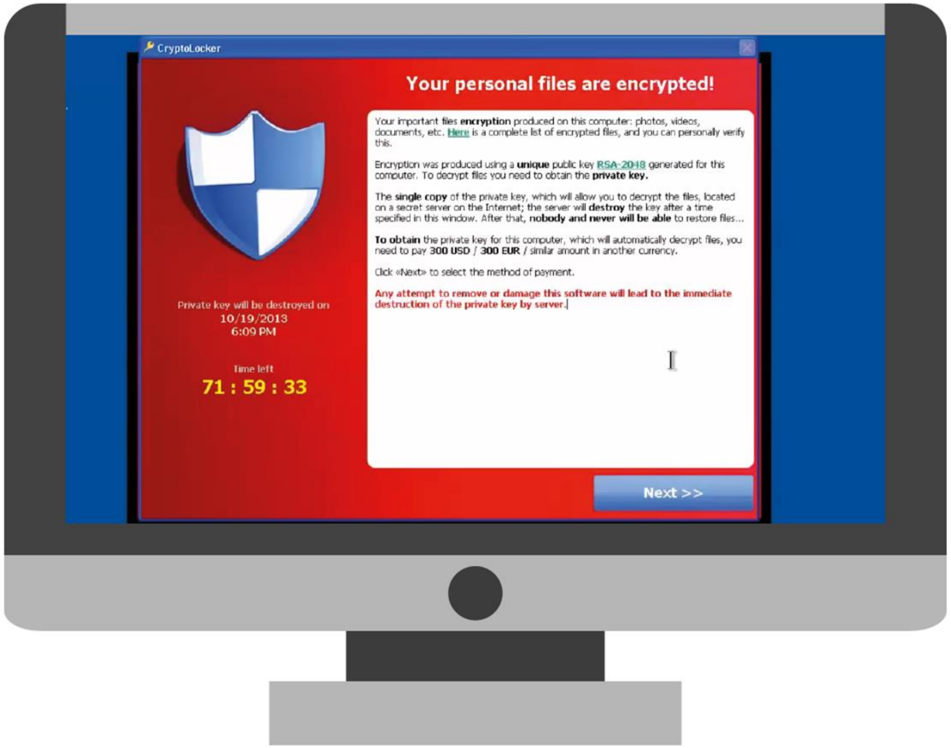
THREAT INTELLIGENCE



CHECK POINT THREATCLOUD™

250M+ addresses
11M+ malware signatures
400K+ updates per day

Threat Intelligence Example: Cryptolocker



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personaly verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/19/2013
6:09 PM

Time left
71 : 59 : 33

Research & Reverse the Domain Generation Algorithm

Feed ThreatCloud with Signatures

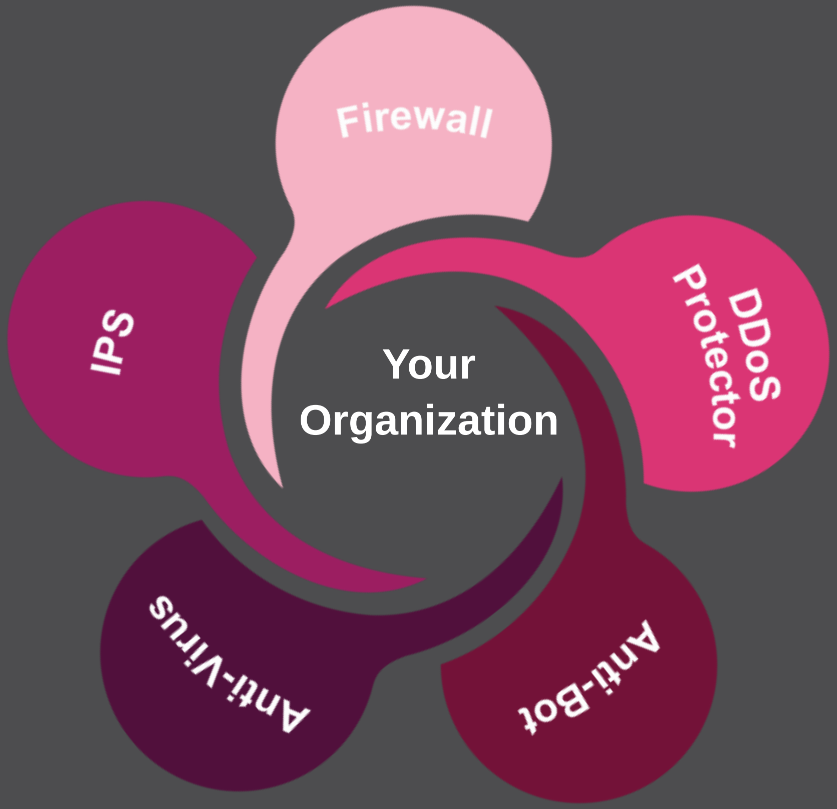
Immediate protections to all Gateways

Prevent threat from Thousands of devices

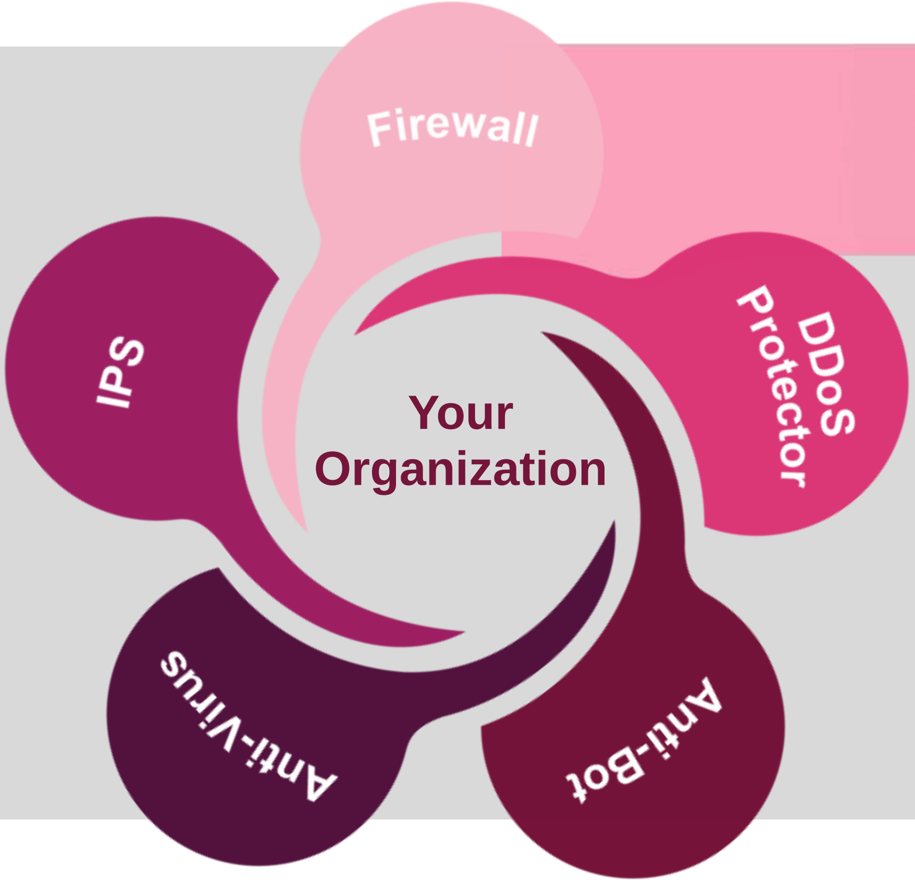
Networks need protection against **ALL**
types of threats

Introducing Check Point

Multi-layered Threat Prevention



Multi-layer Threat Prevention

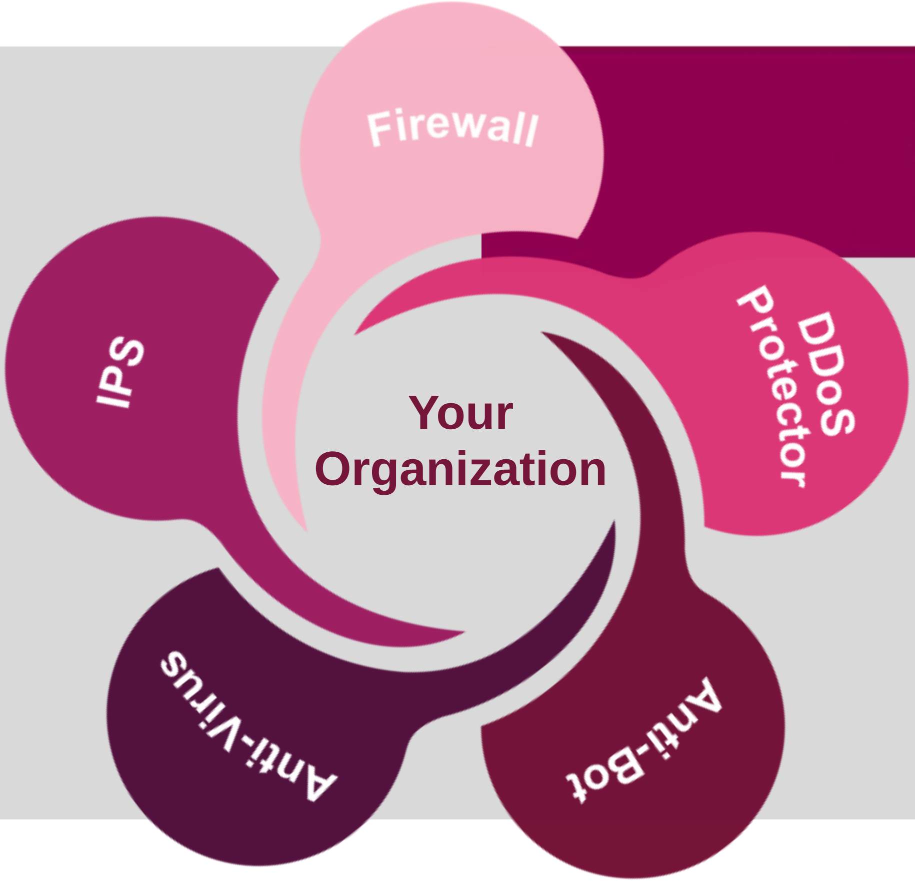


FIREWALL

Secure access to network

Highest Score in Next Generation Firewall

Multi-layer Threat Prevention

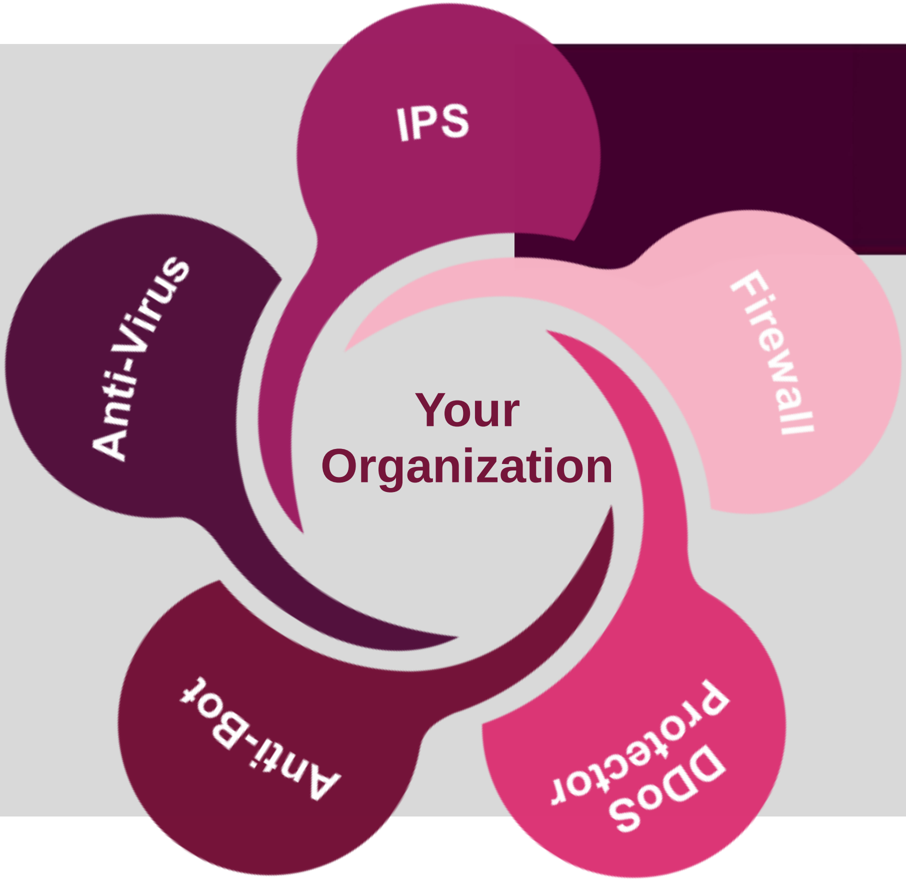


IPS

Stops exploits of known vulnerabilities

NSS Labs
Highest Rating

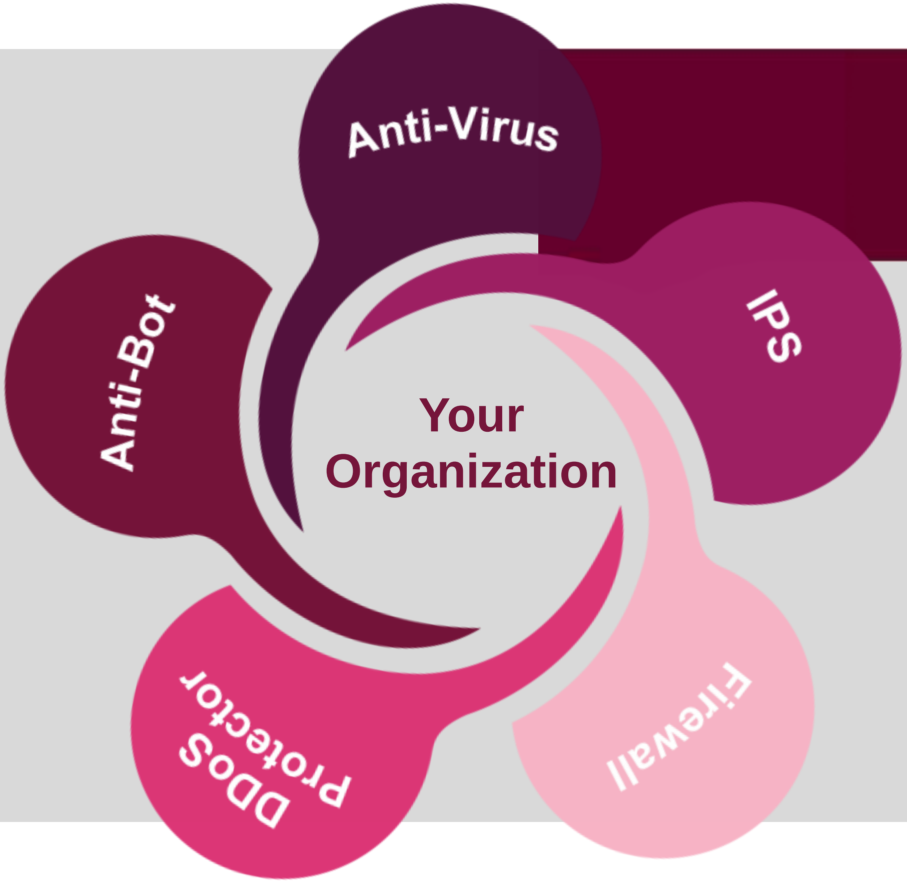
Multi-layer Threat Prevention



Anti-Virus

Over 12+ million malware signatures and 1+ million malware-infected websites

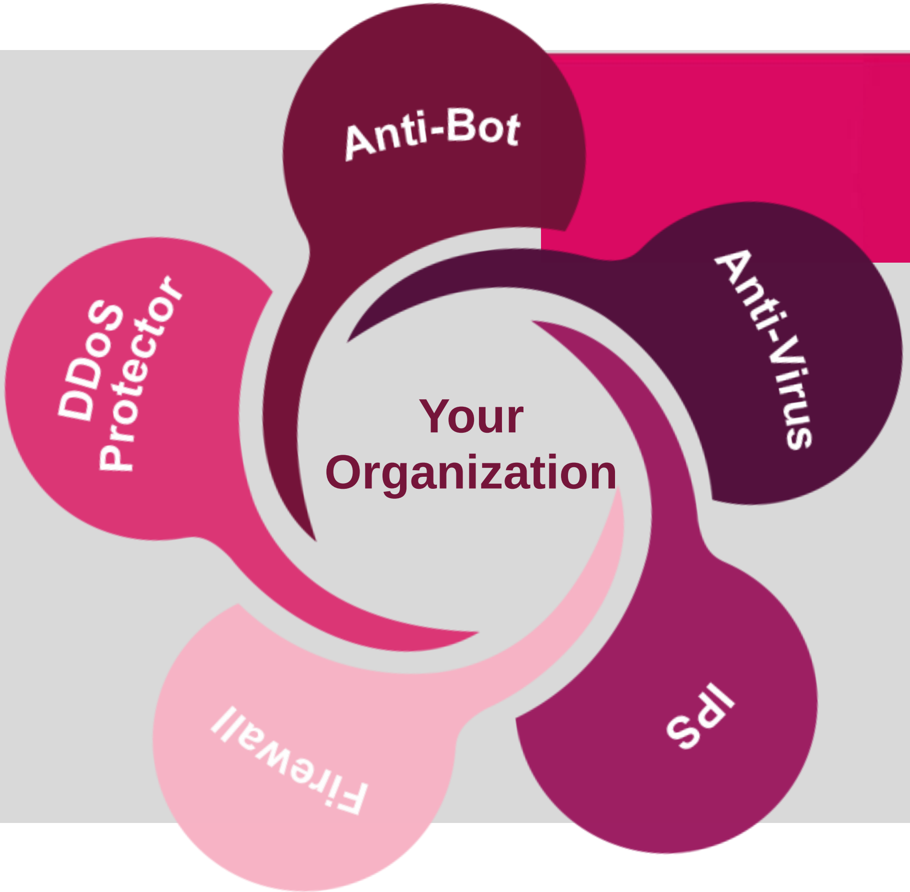
Multi-layer Threat Prevention



Anti-Bot

Detects bot infestations and stops bot damage

Multi-layer Threat Prevention



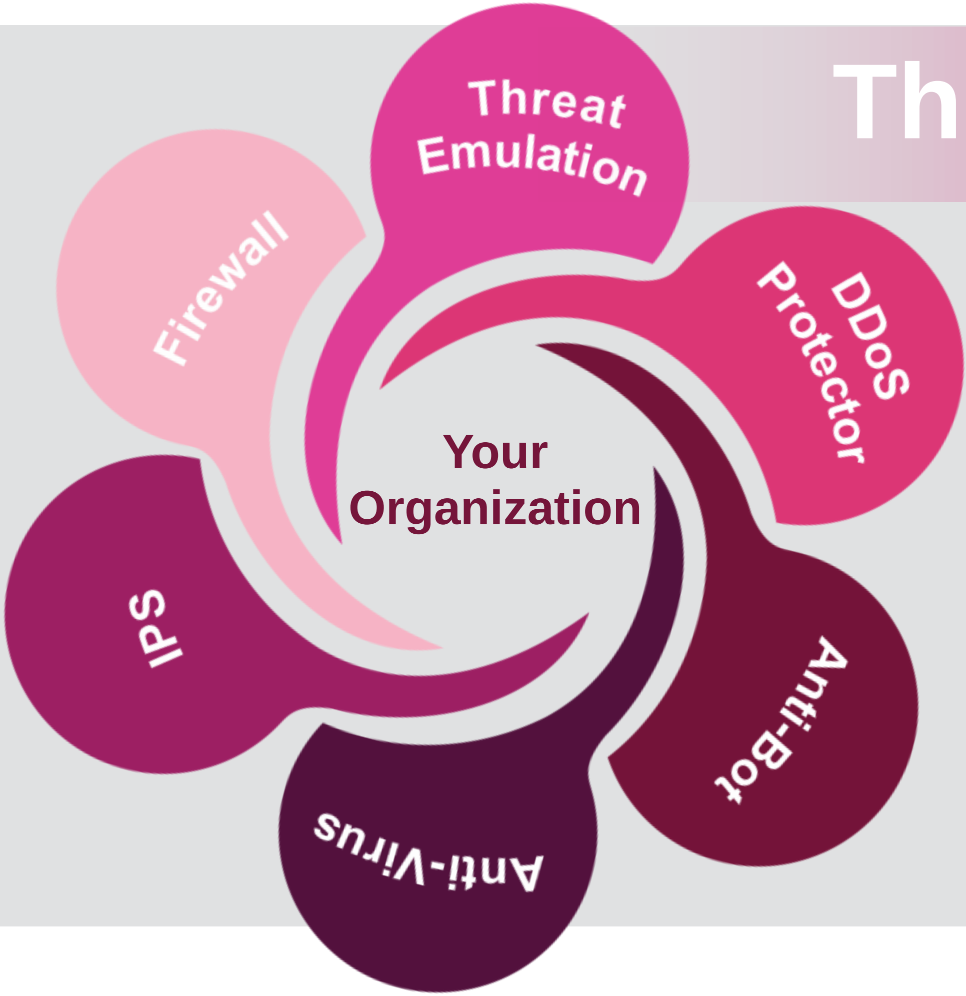
DDoS Protector

Stops attacks within seconds with Network and Application layer protection

New malware?

Zero Day attacks?

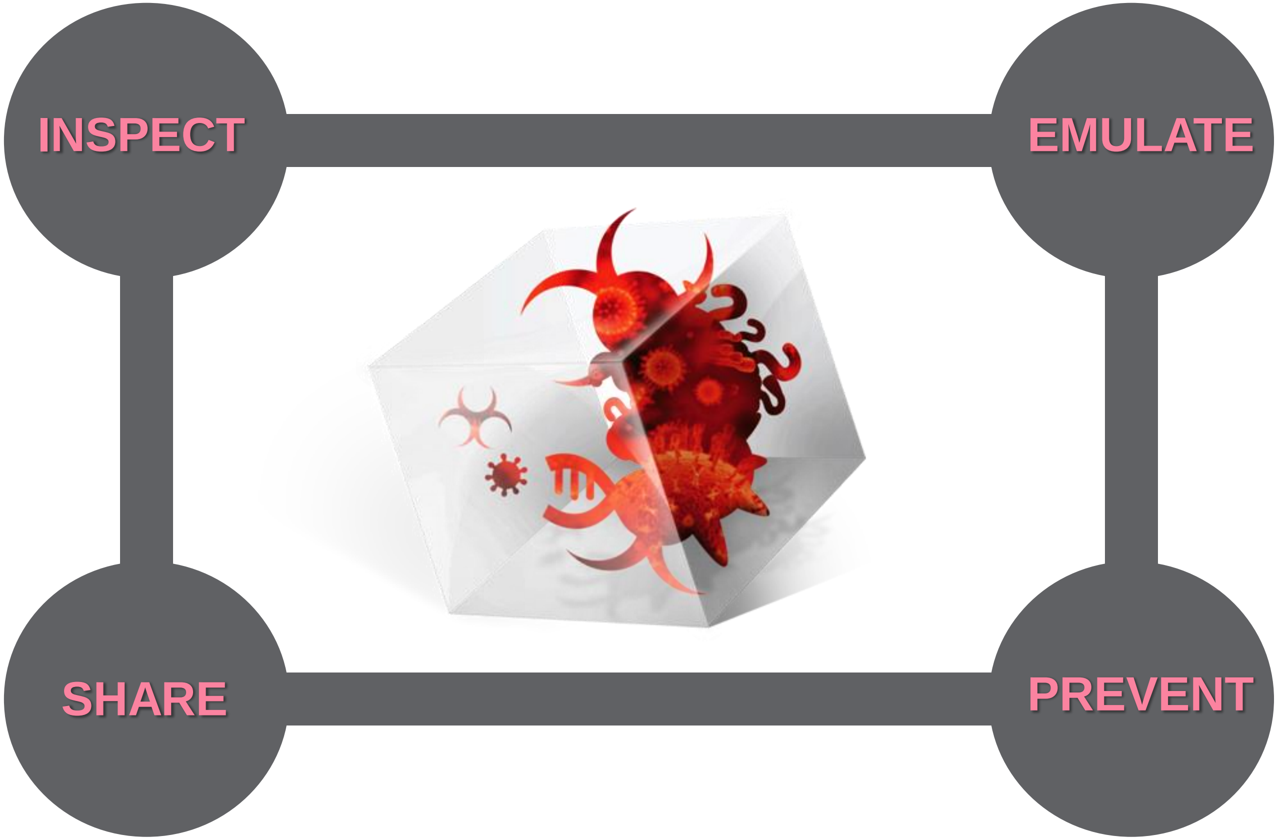
Introducing Threat Emulation



Threat Emulation

Mitigates Unknown Targeted Attacks

Check Point Threat Emulation



Discover and STOP new threats based-on threat behavior

Does you organization control risky applications?

96%

HAVE A LEAST ONE HIGH-RISK APPLICATION

High-Risk Applications Continued to Spread

90% Remote Admin Tools

86% File Storage and Sharing

75% P2P File Sharing

56% Instant Messaging

56% Anonymizers

Check Point
Application Control

Need to Control All Aspects of Web

Websites

www.poker.com

www.hackthissite.org

www.playboy.com

www.fantasyfootball.com

Applications

Not URL-based

Chat

Facebook Chat

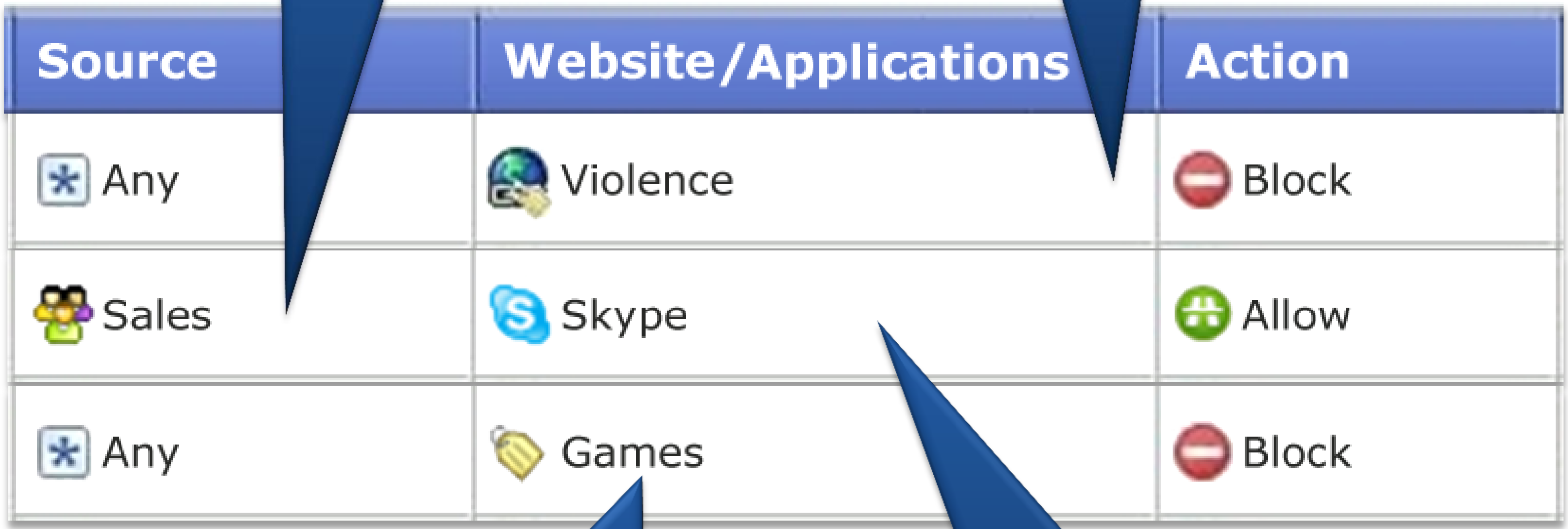
Granularity beyond URLs

Unified Control Needed !

Check Point Unifies URL Filtering and Application Control

User/group granularity

Websites — URL Filtering



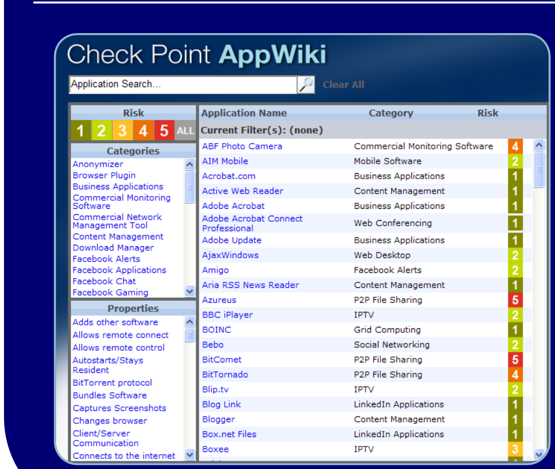
Source	Website/Applications	Action
Any	Violence	Block
Sales	Skype	Allow
Any	Games	Block

Unified categories — URLs and applications

Applications — Application Control

Introducing Check Point AppWiki

Unparalleled Application Control



Categories

- Anonymizer
- Browser Plugin
- Business Applications
- Commercial Monitoring Software
- Commercial Network Management Tool
- Content Management
- Download Manager
- Facebook Alerts
- Facebook Applications
- Facebook Chat
- Facebook Gaming

Properties

- Adds other software
- Allows remote connect
- Allows remote control
- Autostarts/Stays Resident
- BitTorrent protocol
- Bundles Software
- Captures Screenshots
- Changes browser
- Client/Server Communication
- Connects to the internet

Current Filter(s): (none)

Application Name	Category	Risk
ABF Photo Camera	Commercial Monitoring Software	4
AIM Mobile	Mobile Software	2
Acrobat.com	Business Applications	1
Active Web Reader	Content Management	1
Adobe Acrobat	Business Applications	1
Adobe Acrobat Connect Professional	Web Conferencing	1
Adobe Update	Business Applications	1
AjaxWindows	Web Desktop	2
Amigo	Facebook Alerts	2
Aria RSS News Reader	Content Management	1
Azureus	P2P File Sharing	5
BBC iPlayer	IPTV	2
BOINC	Grid Computing	1
Bebo	Social Networking	2
BitComet	P2P File Sharing	5
BitTornado	P2P File Sharing	4
Blip.tv	IPTV	2
Blog Link	LinkedIn Applications	1
Blogger	Content Management	1
Box.net Files	LinkedIn Applications	1
Boxee	IPTV	3

Over **5,600** applications

Over **260,000** social-network widgets

Grouped in over **160** categories

(including Web 2.0, IM, P2P, Voice & Video, File Share)

http://appwiki.checkpoint.com

World's largest

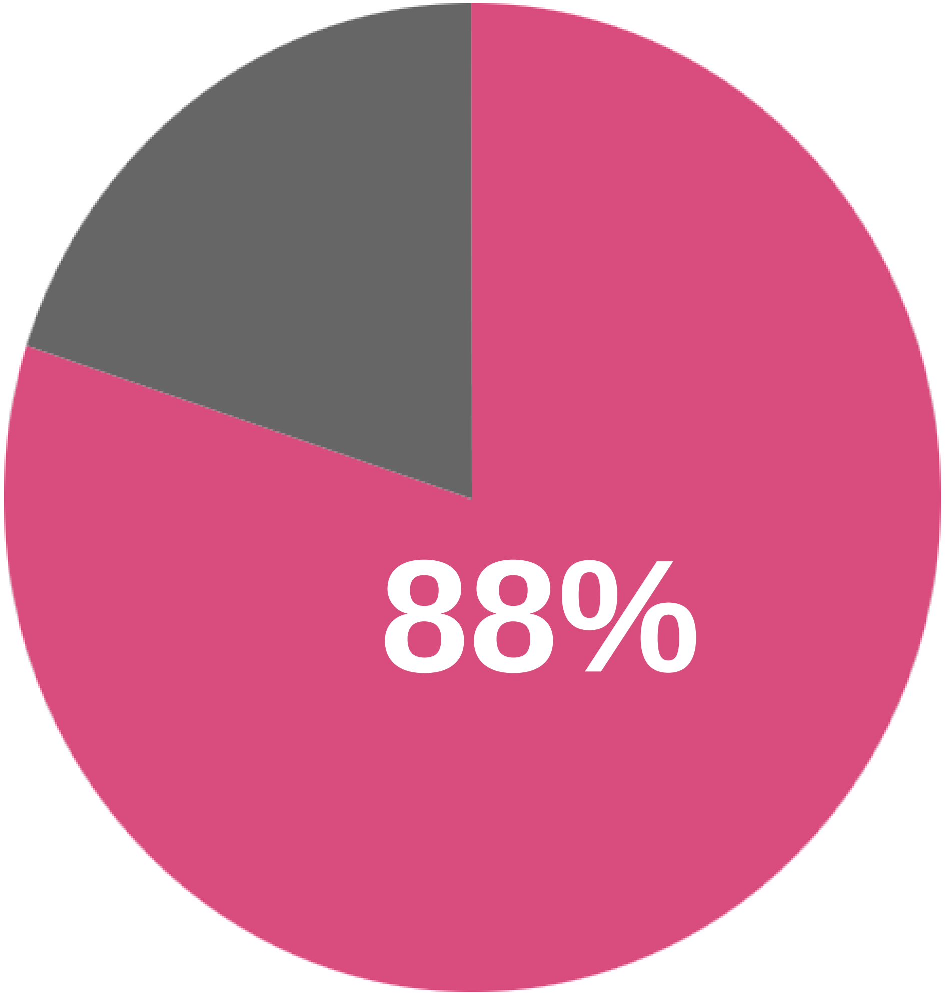
Application Classification Library

Check Point UserCheck

Involve end-users using multiple policy actions

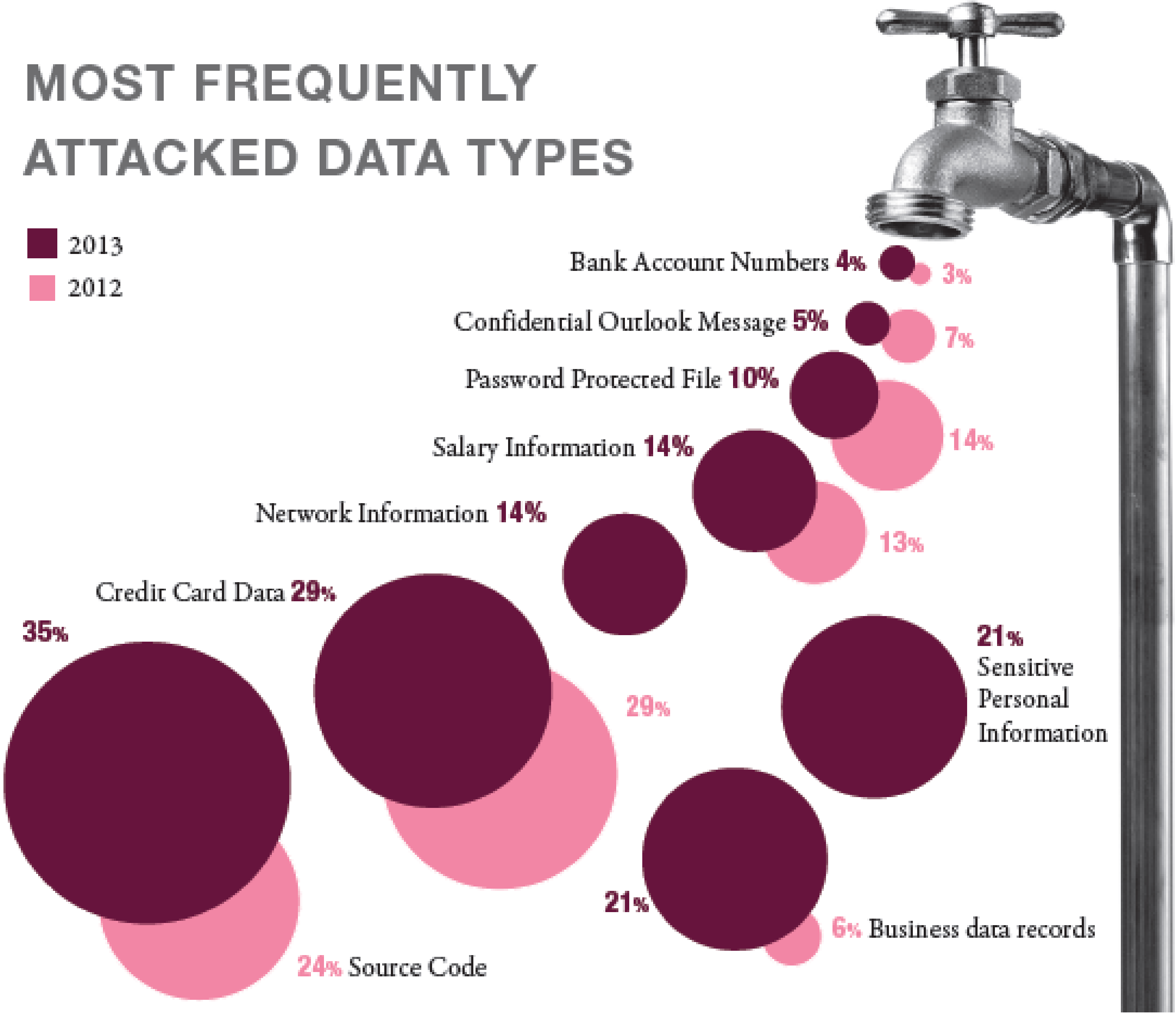
Accept / Drop	Traditional security policies are suitable for clear-cut cases
Inform	Allow but inform the user about the risks
Ask	Learn usage patterns to create better policies
Limit	Use to preserve resources (bandwidth) or control acceptable use

Does your organization need a DLP solution?



of organizations experienced data loss events

Data Loss Events Are Increasing

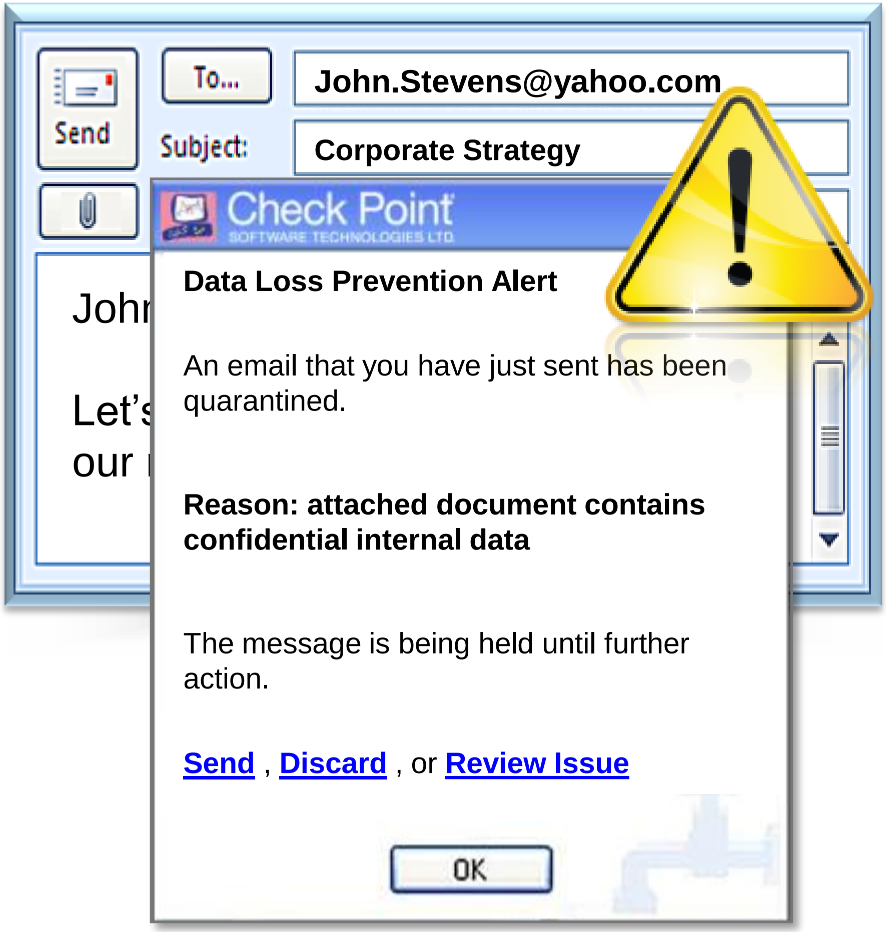


Check Point
Data Loss Prevention

Introducing Check Point Data Loss Prevention

Check Point Combines Technology and Processes to Make DLP Work

NEW!



To... John.Stevens@yahoo.com

Subject: Corporate Strategy

Data Loss Prevention Alert

An email that you have just sent has been quarantined.

Reason: attached document contains confidential internal data

The message is being held until further action.

Send , Discard , or Review Issue

Prevent

Move from detection to prevention

Educate

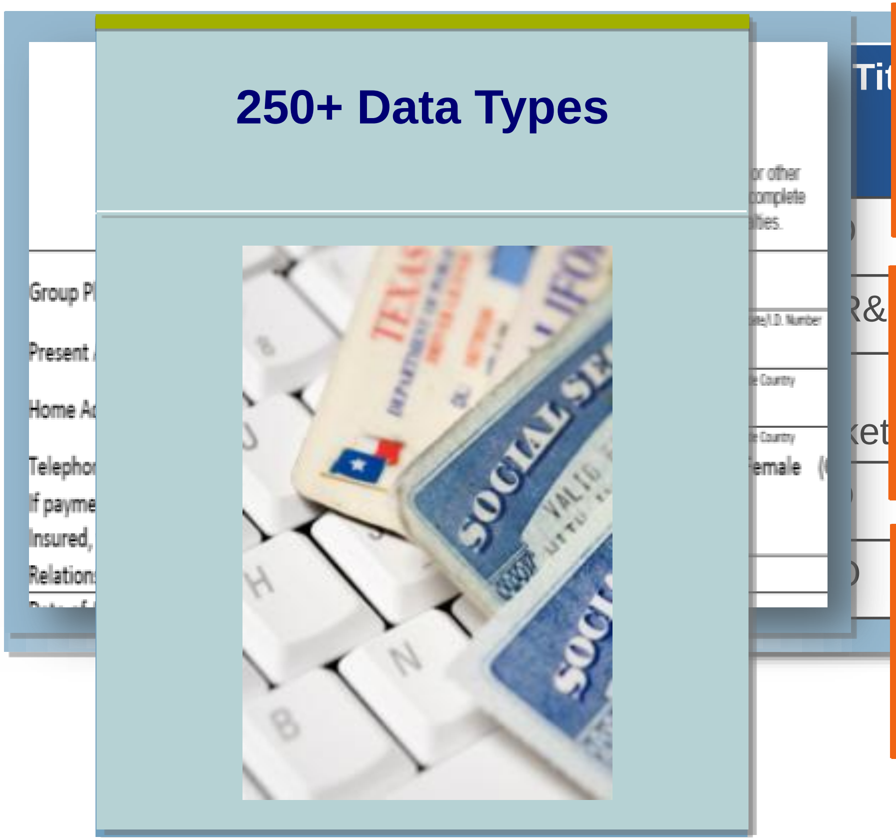
Users on corporate data policies

Enforce

Data loss business processes

New MultiSpect™ Technology

MultiSpect Detection Engine



250+ Data Types

Correlates data from multiple sources using open language

Detects more than 600 file formats

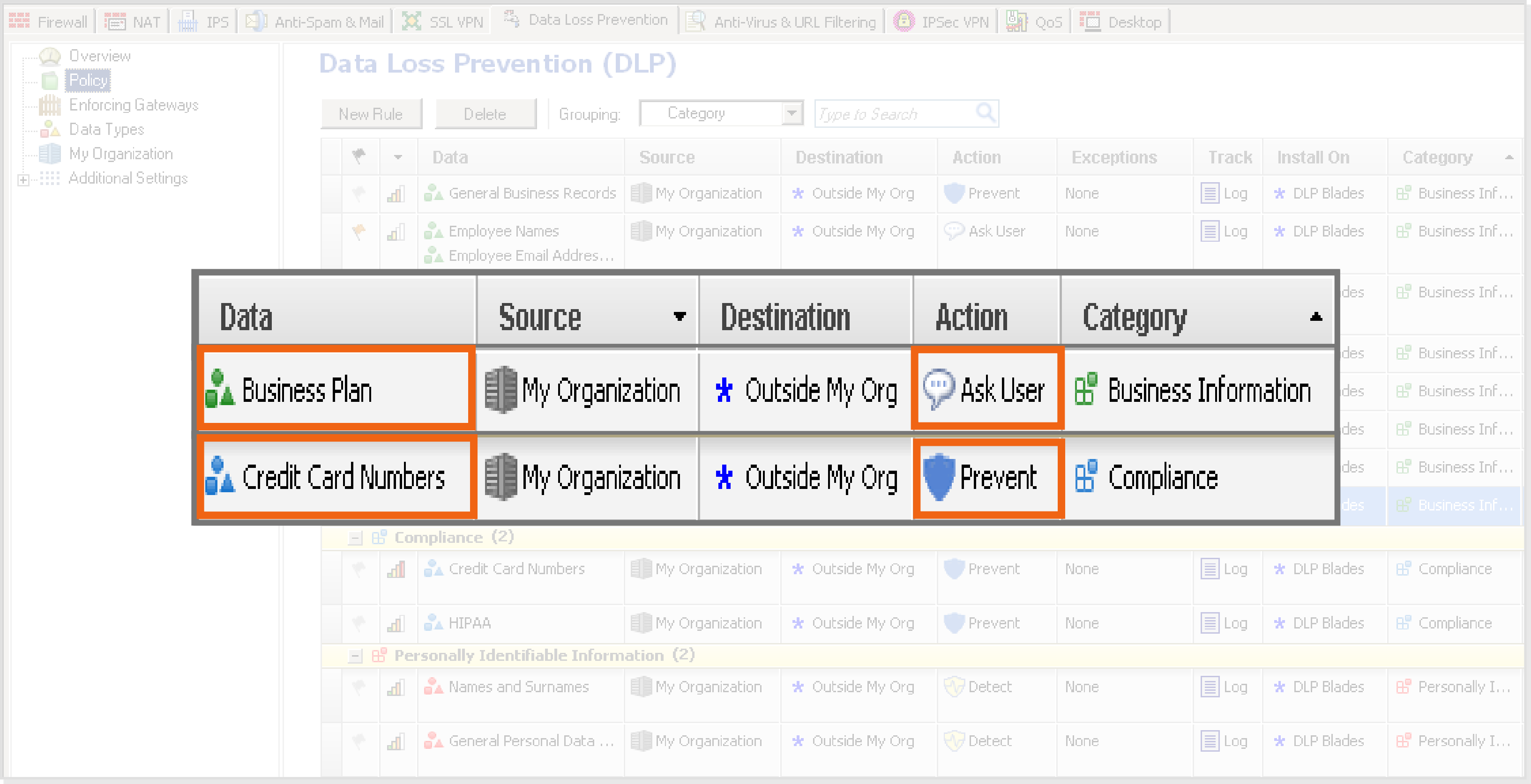
Over 250 pre-defined content data types

Detect and recognize proprietary forms and templates

Simple Rule-based Policy Management

Check Point
SOFTWARE TECHNOLOGIES LTD.

Easily Define Policy to Detect, Prevent or Ask User



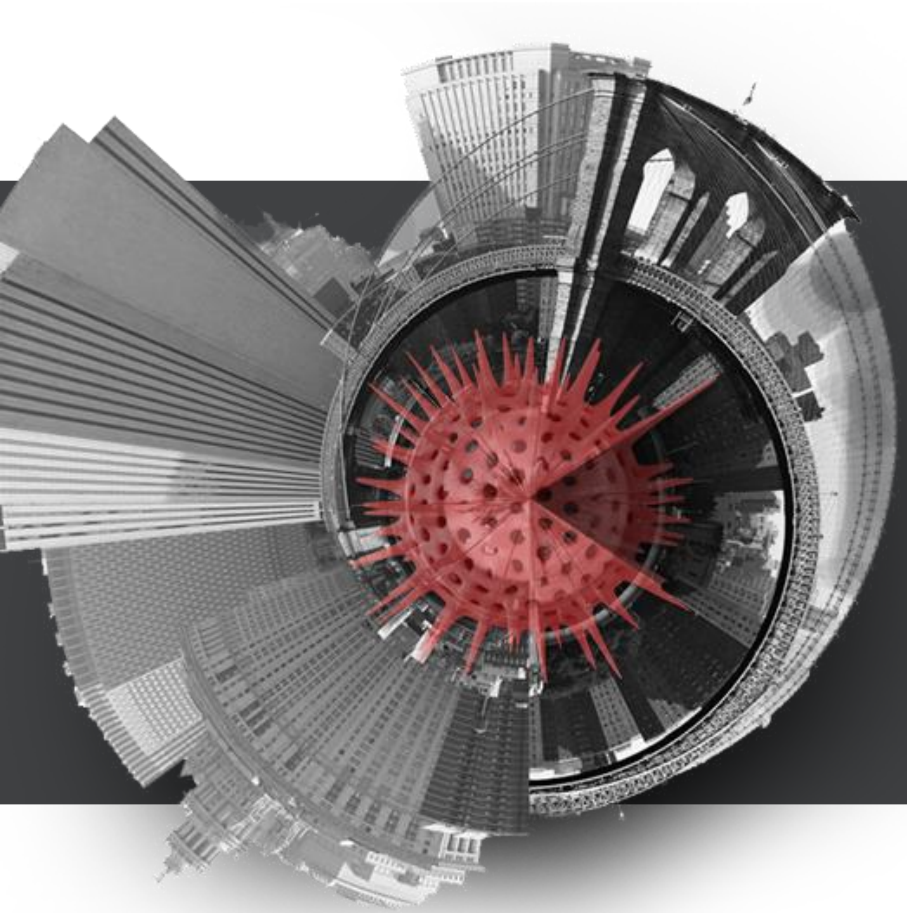
Data Loss Prevention (DLP)

Data	Source	Destination	Action	Exceptions	Track	Install On	Category
General Business Records	My Organization	Outside My Org	Prevent	None	Log	DLP Blades	Business Inf…
Employee Names Employee Email Addres…	My Organization	Outside My Org	Ask User	None	Log	DLP Blades	Business Inf…
						des	Business Inf…
						des	Business Inf…
						des	Business Inf…
						des	Business Inf…
						des	Business Inf…
						des	Business Inf…
Compliance (2)							
Credit Card Numbers	My Organization	Outside My Org	Prevent	None	Log	DLP Blades	Compliance
HIPAA	My Organization	Outside My Org	Prevent	None	Log	DLP Blades	Compliance
Personally Identifiable Information (2)							
Names and Surnames	My Organization	Outside My Org	Detect	None	Log	DLP Blades	Personally I…
General Personal Data …	My Organization	Outside My Org	Detect	None	Log	DLP Blades	Personally I…

Data	Source	Destination	Action	Category
Business Plan	My Organization	Outside My Org	Ask User	Business Information
Credit Card Numbers	My Organization	Outside My Org	Prevent	Compliance

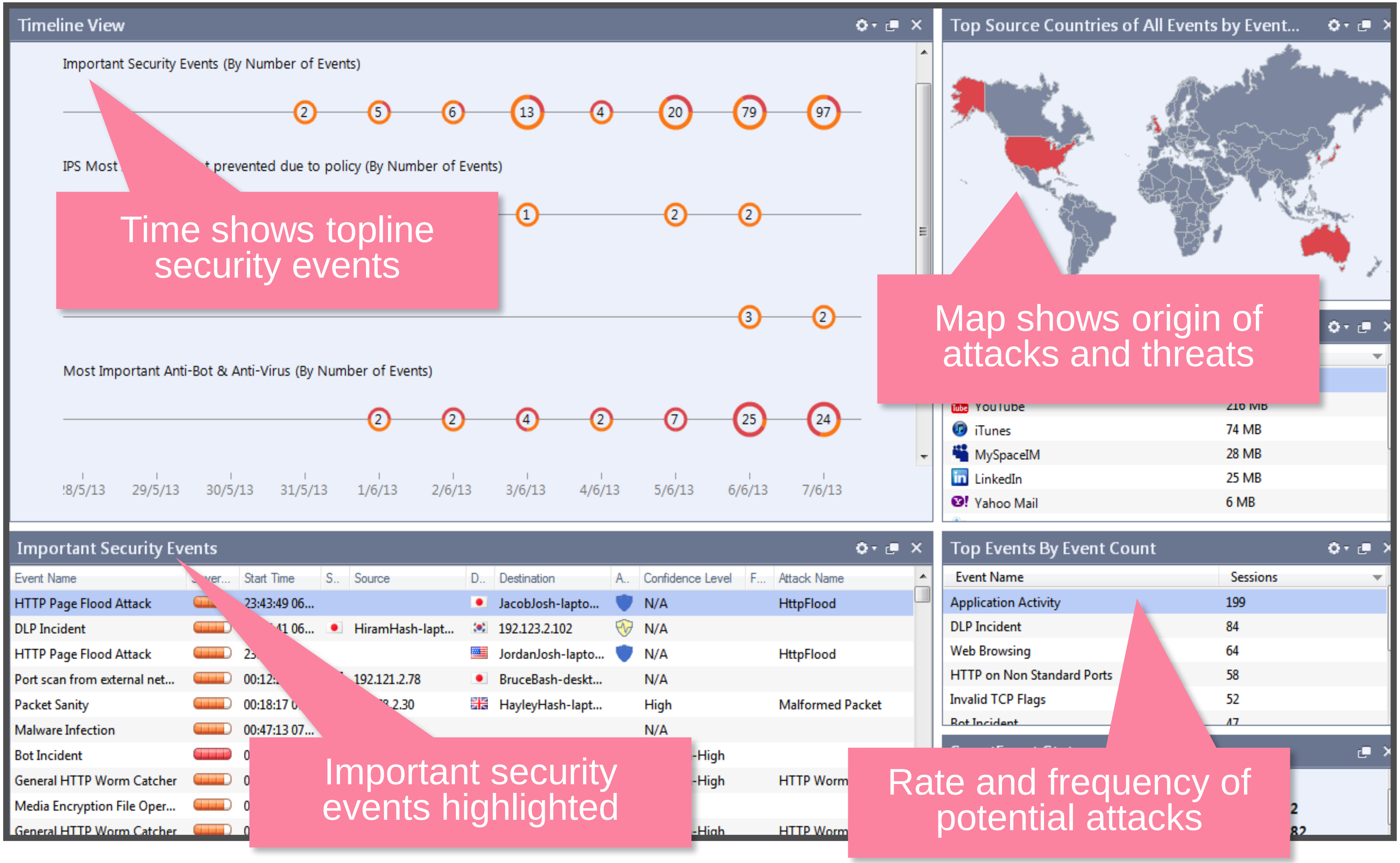
Thousands of security logs…

What about visibility?



The need for 360º visibility

360º Visibility of Network Security



Timeline View
Important Security Events (By Number of Events)
2
5
6
13
4
20
79
97
IPS Most
t prevented due to policy (By Number of Events)
1
2
2
3
2
Most Important Anti-Bot & Anti-Virus (By Number of Events)
2
2
4
2
7
25
24
:8/5/13
29/5/13
30/5/13
31/5/13
1/6/13
2/6/13
3/6/13
4/6/13
5/6/13
6/6/13
7/6/13
Top Source Countries of All Events by Event...

Time shows topline security events

Map shows origin of attacks and threats

YouTube	216 MB
iTunes	74 MB
MySpaceIM	28 MB
LinkedIn	25 MB
Yahoo Mail	6 MB

Important Security Events

Event Name	...ver...	Start Time	S..	Source	D..	Destination	A..	Confidence Level	F...	Attack Name
HTTP Page Flood Attack		23:43:49 06...				JacobJosh-lapto...		N/A		HttpFlood
DLP Incident		...41 06...		HiramHash-lapt...		192.123.2.102		N/A		
HTTP Page Flood Attack		23...				JordanJosh-lapto...		N/A		HttpFlood
Port scan from external net...		00:12...		192.121.2.78		BruceBash-deskt...		N/A		
Packet Sanity		00:18:17 0...		...2.30		HayleyHash-lapt...		High		Malformed Packet
Malware Infection		00:47:13 07...						N/A		
Bot Incident		0...						-High		
General HTTP Worm Catcher		0...						-High		HTTP Worm
Media Encryption File Oper...		0...								
General HTTP Worm Catcher		0...						-High		HTTP Worm

Important security events highlighted

Top Events By Event Count

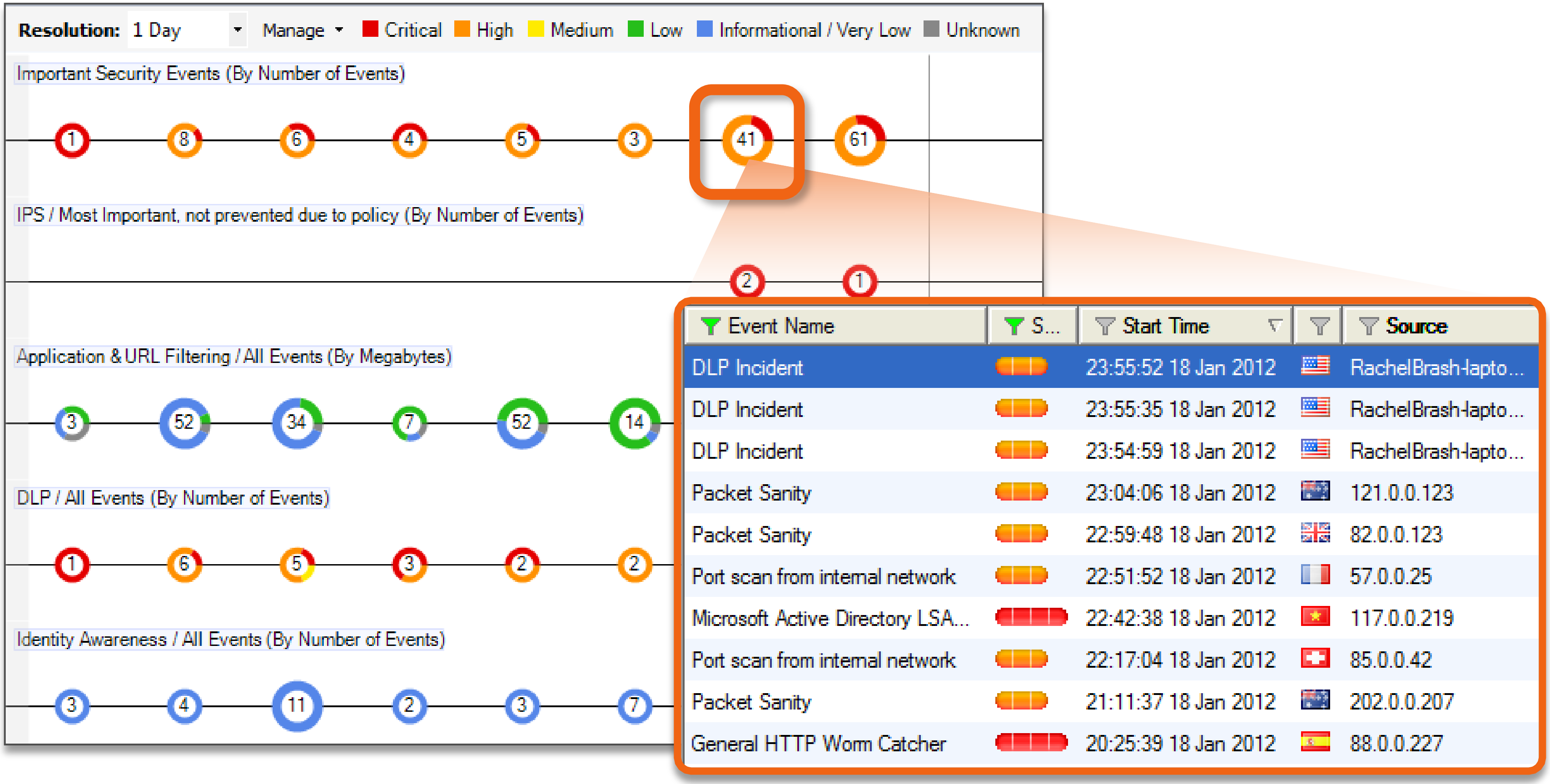
Event Name	Sessions
Application Activity	199
DLP Incident	84
Web Browsing	64
HTTP on Non Standard Ports	58
Invalid TCP Flags	52
Bot Incident	47

Rate and frequency of potential attacks

softwareblades™

Consolidated Visibility: SmartEvent

- Unified event analysis with 360° visibility across Software Blades
- High-level view with drill down to policy



Resolution: 1 Day

Manage
🟥 Critical
🟧 High
🟨 Medium
🟩 Low
🟦 Informational / Very Low
⬛ Unknown
Important Security Events (By Number of Events)
1
8
6
4
5
3
41
61
IPS / Most Important, not prevented due to policy (By Number of Events)
2
1
Application & URL Filtering / All Events (By Megabytes)
3
52
34
7
52
14
DLP / All Events (By Number of Events)
1
6
5
3
2
2
Identity Awareness / All Events (By Number of Events)
3
4
11
2
3
7

Event Name	S...	Start Time		Source
DLP Incident	🟧	23:55:52 18 Jan 2012	🇺🇸	RachelBrash-lapto...
DLP Incident	🟧	23:55:35 18 Jan 2012	🇺🇸	RachelBrash-lapto...
DLP Incident	🟧	23:54:59 18 Jan 2012	🇺🇸	RachelBrash-lapto...
Packet Sanity	🟧	23:04:06 18 Jan 2012	🇦🇺	121.0.0.123
Packet Sanity	🟧	22:59:48 18 Jan 2012	🇬🇧	82.0.0.123
Port scan from internal network	🟧	22:51:52 18 Jan 2012	🇫🇷	57.0.0.25
Microsoft Active Directory LSA...	🟥	22:42:38 18 Jan 2012	🇻🇳	117.0.0.219
Port scan from internal network	🟧	22:17:04 18 Jan 2012	🇨🇭	85.0.0.42
Packet Sanity	🟧	21:11:37 18 Jan 2012	🇦🇺	202.0.0.207
General HTTP Worm Catcher	🟥	20:25:39 18 Jan 2012	🇪🇸	88.0.0.227

Check Point appliances:

A solution for every size organizations

Check Point Appliances and Virtual Editions

Check Point
SOFTWARE TECHNOLOGIES LTD.

Solutions for every size company

600 Appliances
(3 models)

Small Office

2200 Appliance
1100 Appliances
(3 models)

Branch Office

4000 Appliances
(4 models)

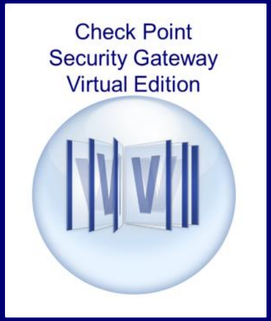
Enterprise

13500 Appliance
12000 Appliances
(3 models)

Data Center

61000 & 41000 Systems
21000 Appliance
(3 models)

Ultra High End



What about mobile devices?

Customers need to have the same security for off-network devices as they do on-premise.

Check Point Cloud Firewall Service

IPS

Application Control

URL Filtering

Anti-Bot

Anti-Virus

DLP

Threat Emulation

Cloud-based security for ALL roaming devices

Check Point: All-In-One WrapUp

Check Point
SOFTWARE TECHNOLOGIES LTD.

Appliances

Small offices

Enterprise

Data Center

Ultra High-End

DDoS Protector

Security Gateway Software Blades

- Firewall
- IpSec VPN
- IPS
- Application Control
- URL Filtering
- Anti Bot
- Antivirus Anti Malware
- Antispam Email Security
- Data Loss Prevention
- Web Security
- Mobile Access
- Threat Emulation
- Identity Awareness

Security Endpoint Software Blades

- Firewall
- Device Control Media Encryption
- VPN
- Anti Malware
- Application Control
- Full Disk Encryption

Mobile Information Protection

- Mobile Enterprise
- IPSec/SSL VPN
- Document Security
- Cloud Connector

Security Management Software Blades

- Multi Domain Management
- Network Policy Management
- Smart Reporter
- Smart Event
- Smart Provisioning
- Smart Workflow
- Logging and Status
- Userdirectory
- Monitoring
- Endpoint Policy Management
- Compliance

Check Point
SOFTWARE TECHNOLOGIES LTD.

THANK YOU

SOFTWARE-DEFINED
PROTECTION

JOIN THE SECURITY REVOLUTION

[Restricted] ONLY for designated groups and individuals