

Modern Threat Prevention

Olli Mikkonen
Security Engineer

[Confidential] For designated groups and individuals



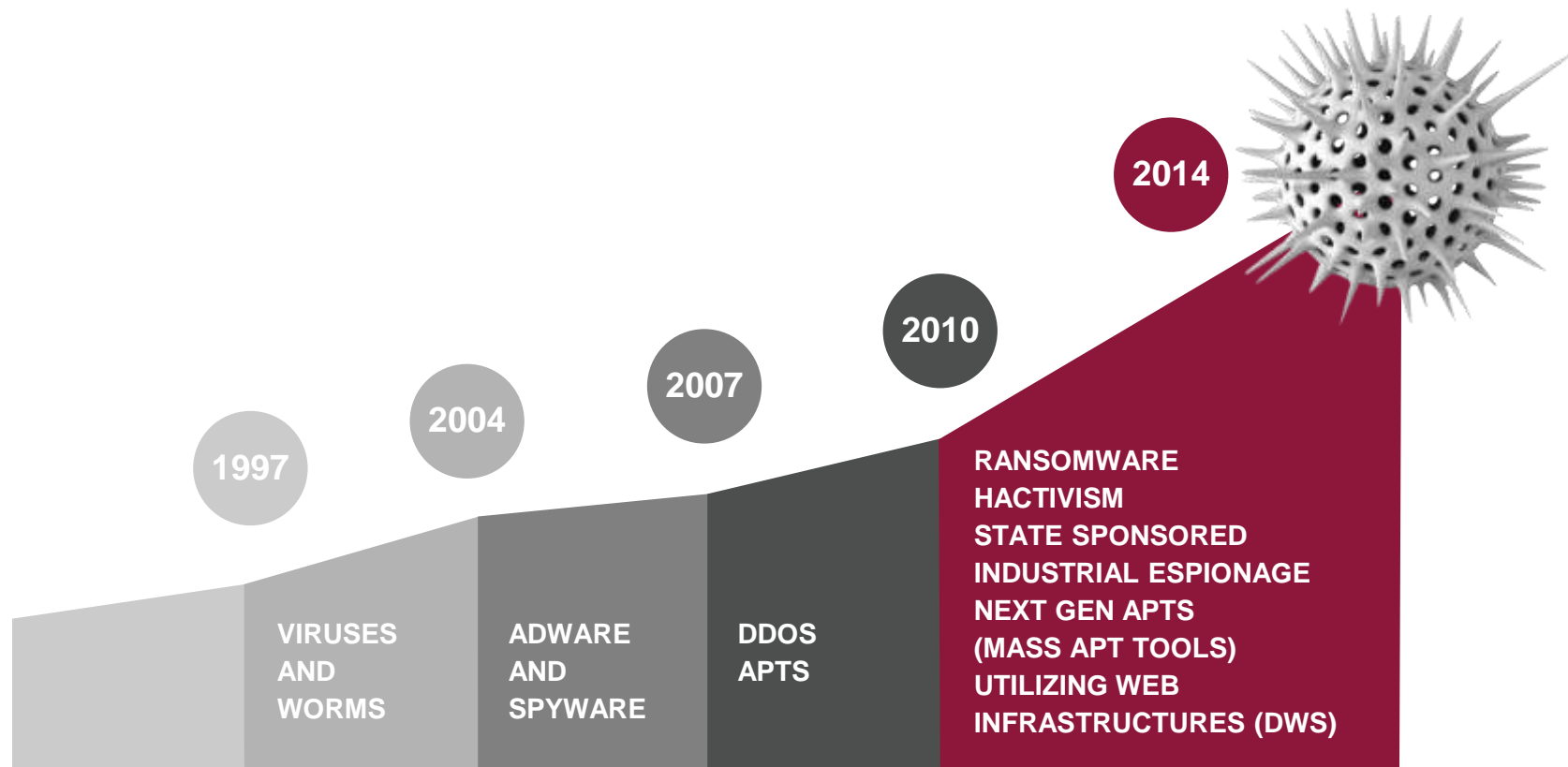
TECHNOLOGY IS **EVERYWHERE**



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

AN EVER-CHANGING THREAT LANDSCAPE

Every year **THREATS** are becoming more sophisticated
and **MORE FREQUENT**



THREATS BECOME A **COMMODITY**

ZERO-DAY EXPLOITS PRICE LIST

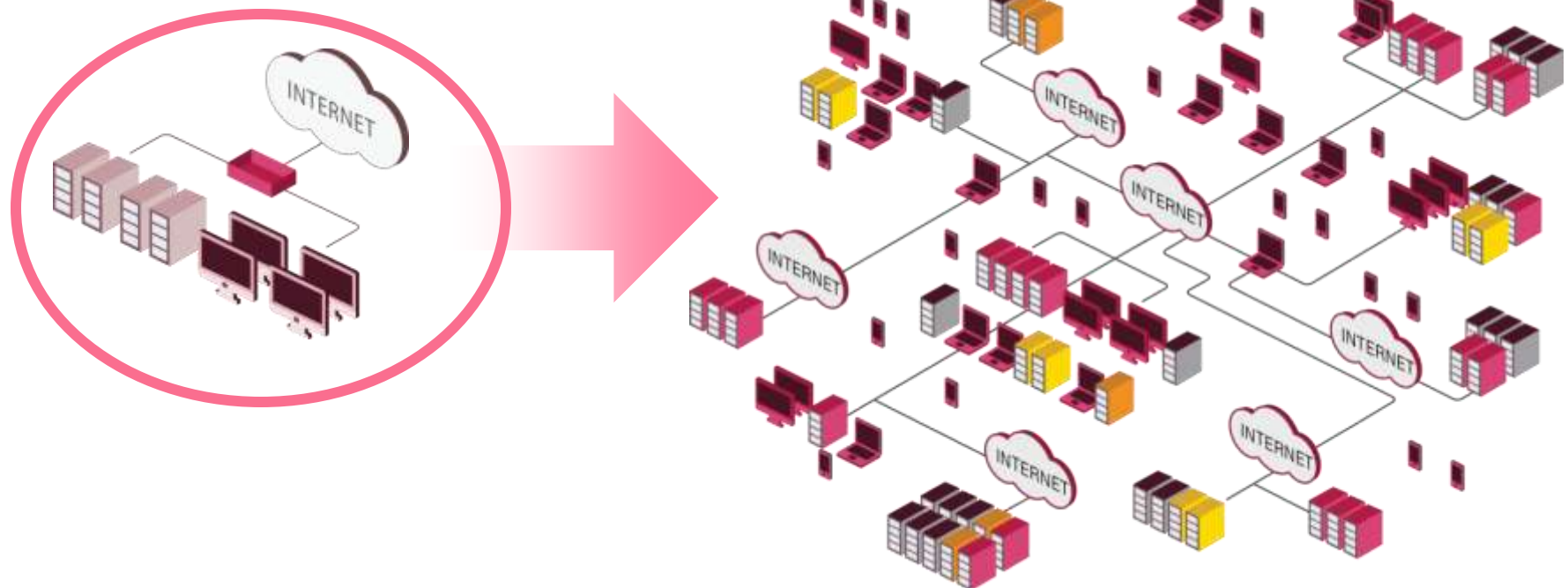
ADOBE READER	\$5,000
MAC OSX	\$20,000
ANDROID.....	\$30,000
FLASH OR JAVA.....	\$40,000
MICROSOFT WORD	\$50,000
WINDOWS.....	\$60,000
FIREFOX OR SAFARI	\$60,000
CHROME OR INTERNET EXPLORER.....	\$80,000
IOS.....	\$100,000



*Source: <http://www.forbes.com>

EVOLVING AND **COMPLEX** IT ENVIRONMENTS

IT environments have **EVOLVED** with new **EMERGING** technologies



WE NEED SECURITY
that is

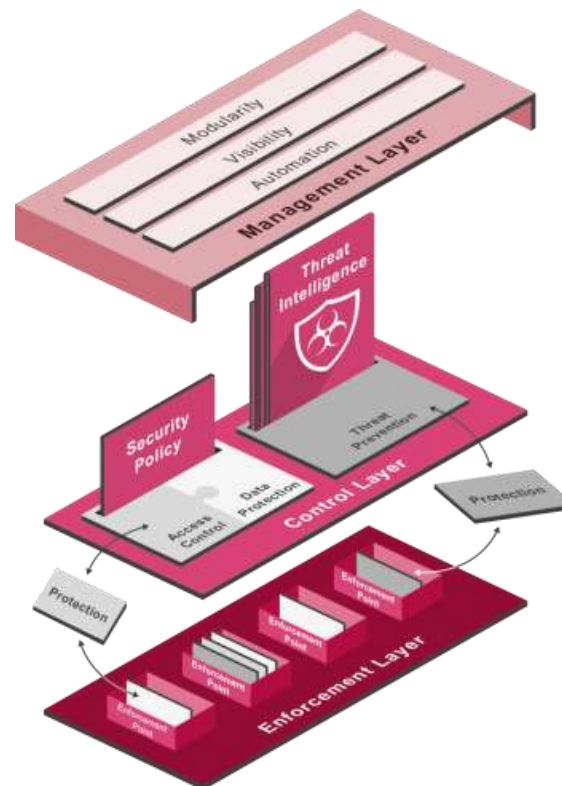
MODULAR
AGILE
SECURE!!!



Introducing

SOFTWARE –DEFINED PROTECTION

Today **SECURITY** for Tomorrow's **THREATS**



SOFTWARE – DEFINED PROTECTION

MANAGEMENT LAYER

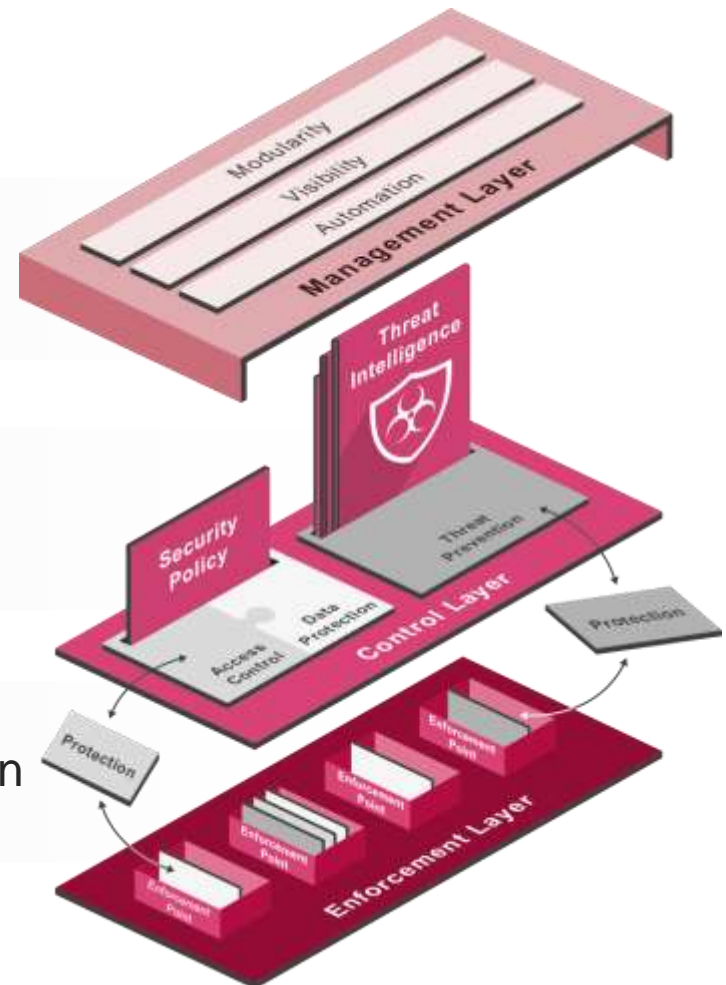
Integrates security with business process

CONTROL LAYER

Delivers real-time protections to the enforcement points

ENFORCEMENT LAYER

Inspects traffic and enforces protection in well-defined segments



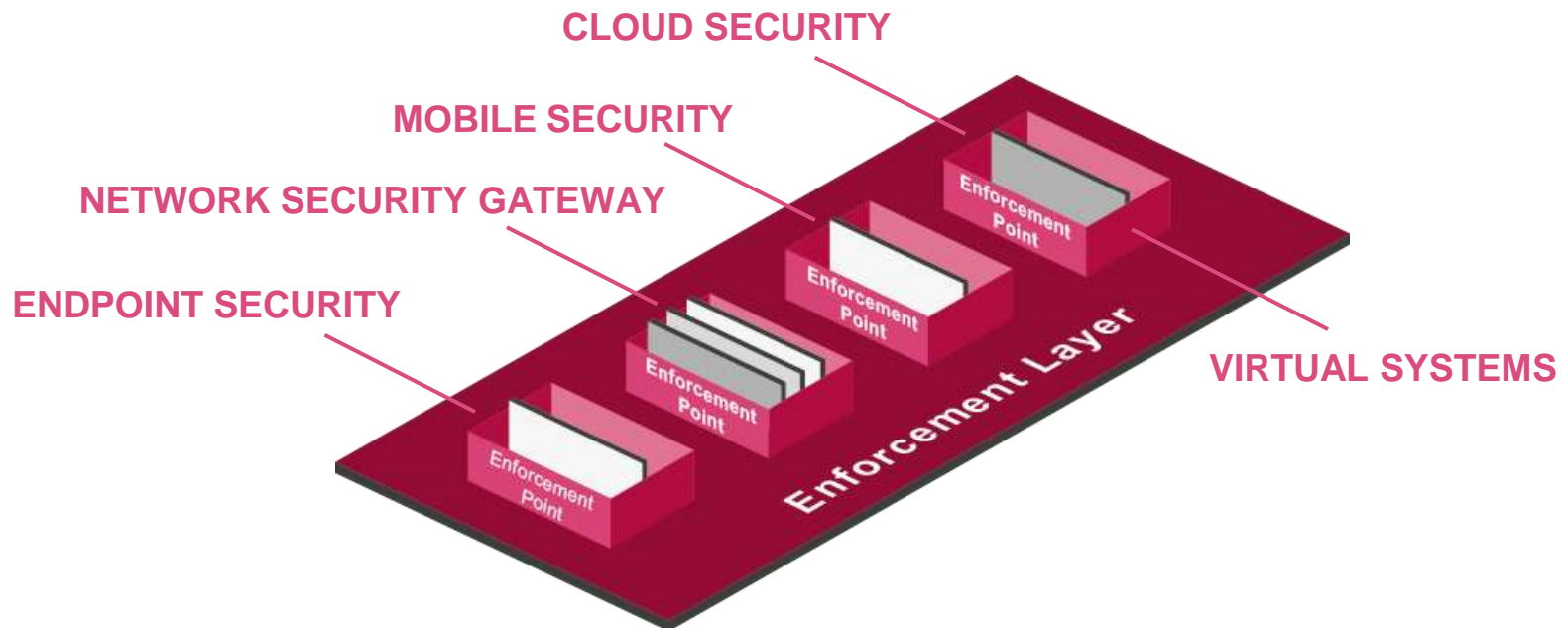
ENFORCEMENT LAYER

RELIABLE and **FAST** to deal with demanding
IT networks and hosts.

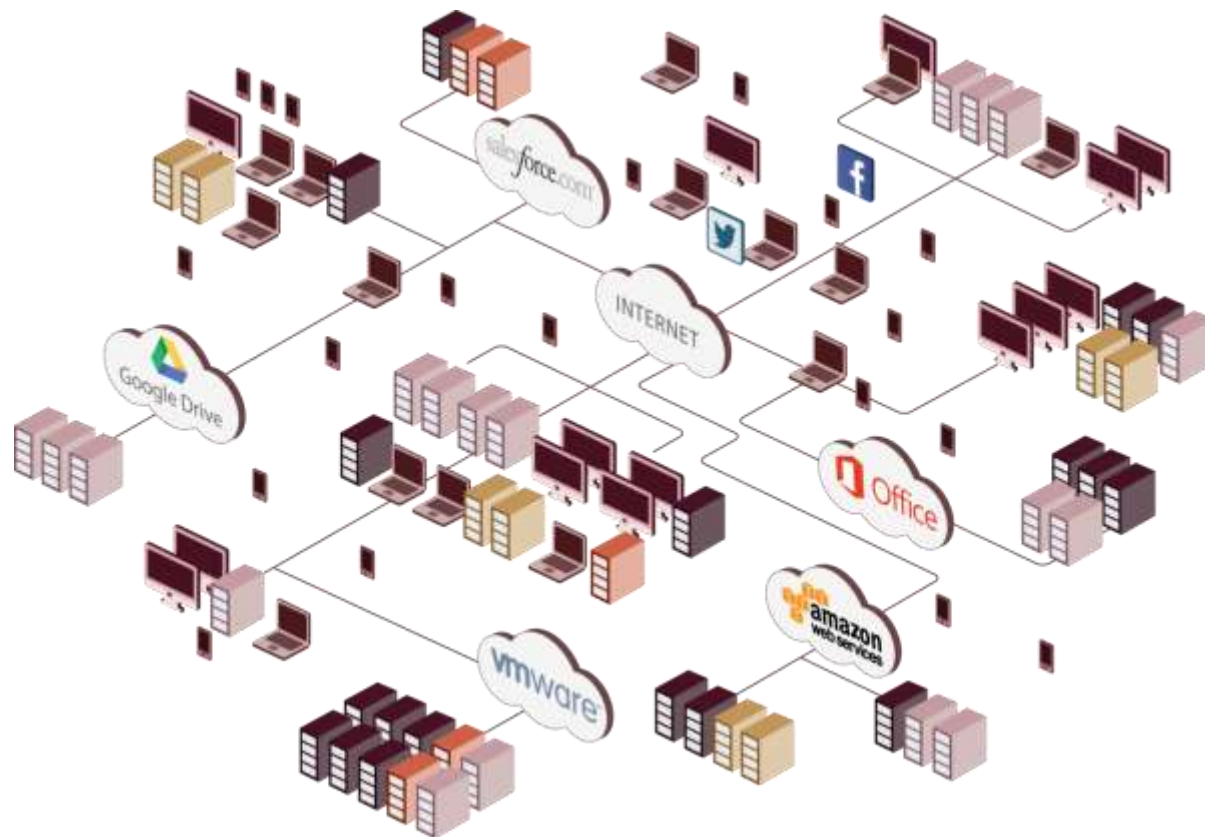


ENFORCEMENT LAYER

Enforcement points **MEDIATE** interactions between users and systems
and **EXECUTE** protections



HOW TO PROTECT BOUNDLESS ENVIRONMENTS?



SEGMENTATION IS THE NEW PERIMETER

In today's **NETWORKS**, there is no single perimeter.
Smartphones, clouds, and cloud move **DATA** and networks
across boundless computing environments.



SEGMENTATION **METHODOLOGY**

STEP 1

ATOMIC SEGMENTS

Elements that share the same policy and protection characteristics

STEP 2

SEGMENT GROUPING

Grouping of atomic segments to allow modular protection

STEP 3

CONSOLIDATION

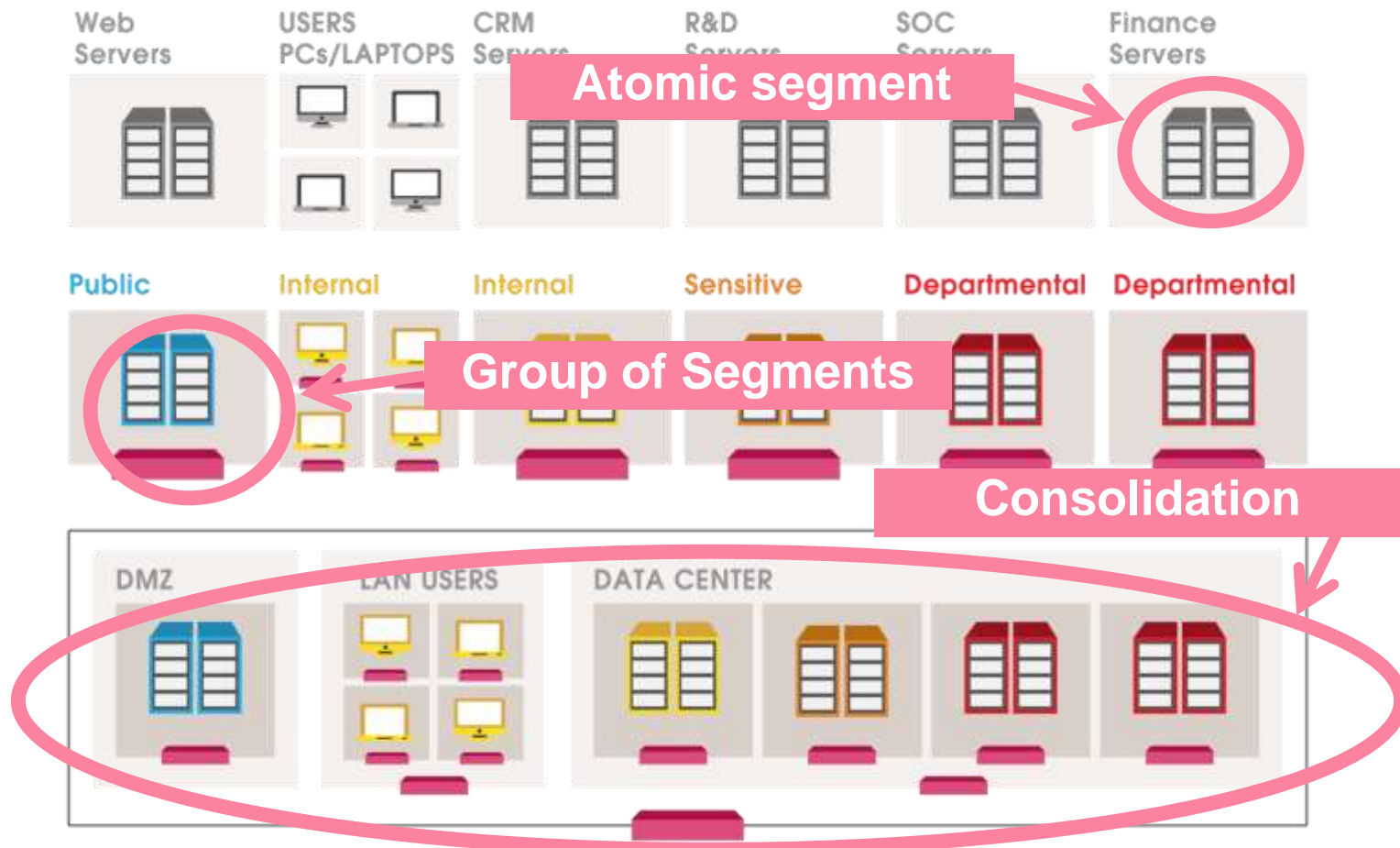
Protect interactions and data flow between segments

STEP 4

TRUSTED CHANNELS

Of physical and virtual components, as network security gateways or as host-based software

SEGMENTING YOUR NETWORK



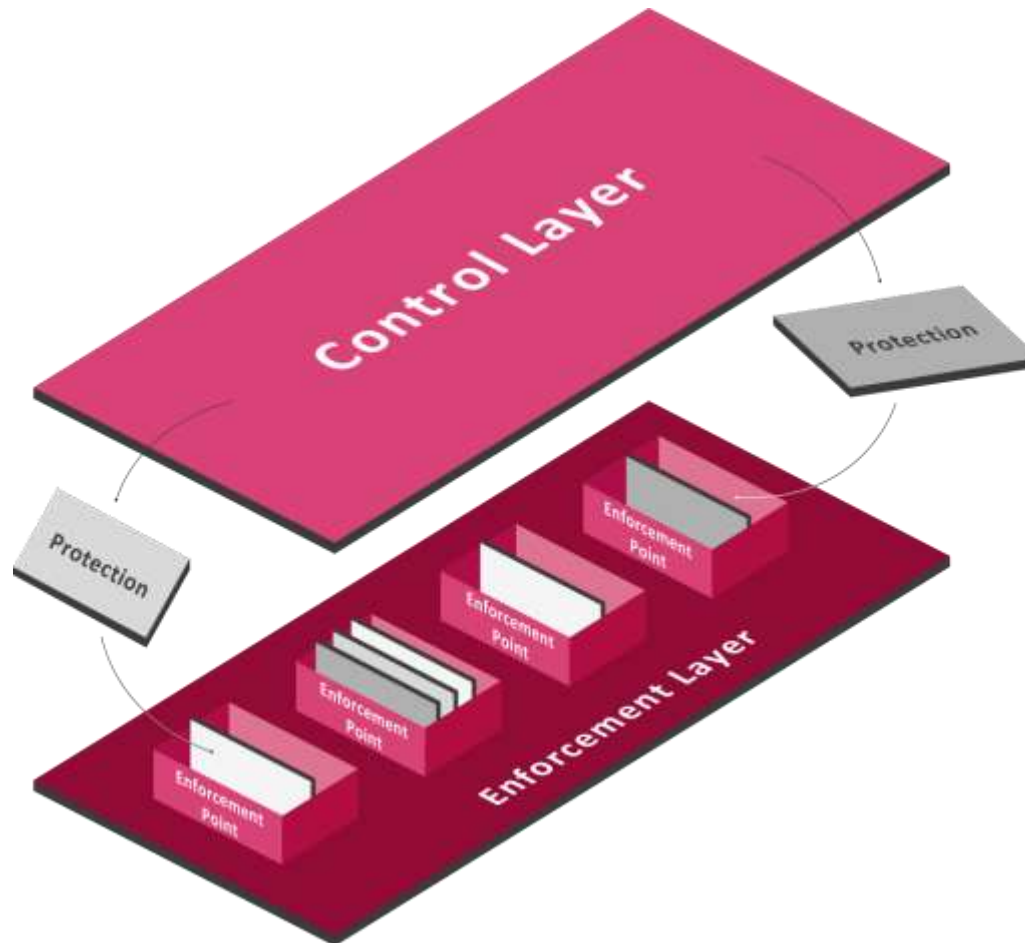
CONTROL LAYER

Generates **SOFTWARE-DEFINED** protections and deploys them at the appropriate **ENFORCEMENT** points.



CONTROL LAYER

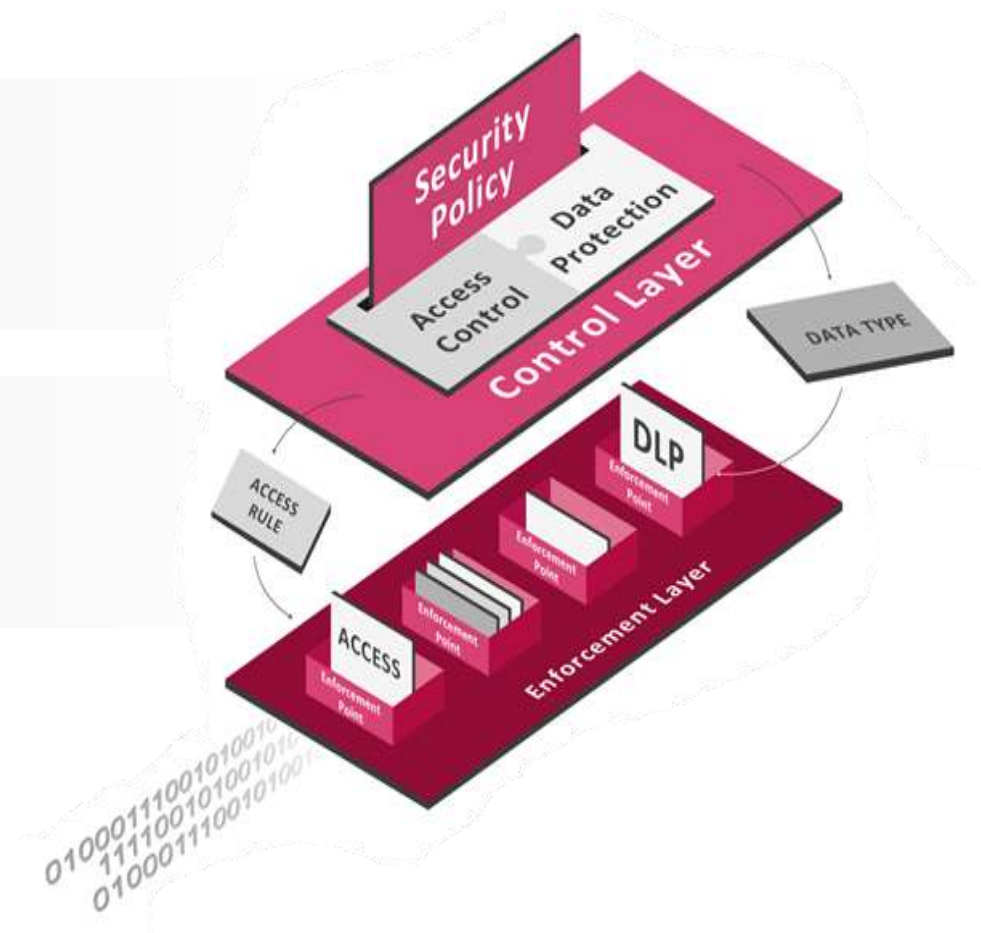
Generate PROTECTIONS



ACCESS CONTROL AND DATA PROTECTION

Control interactions
between users, assets,
data and applications

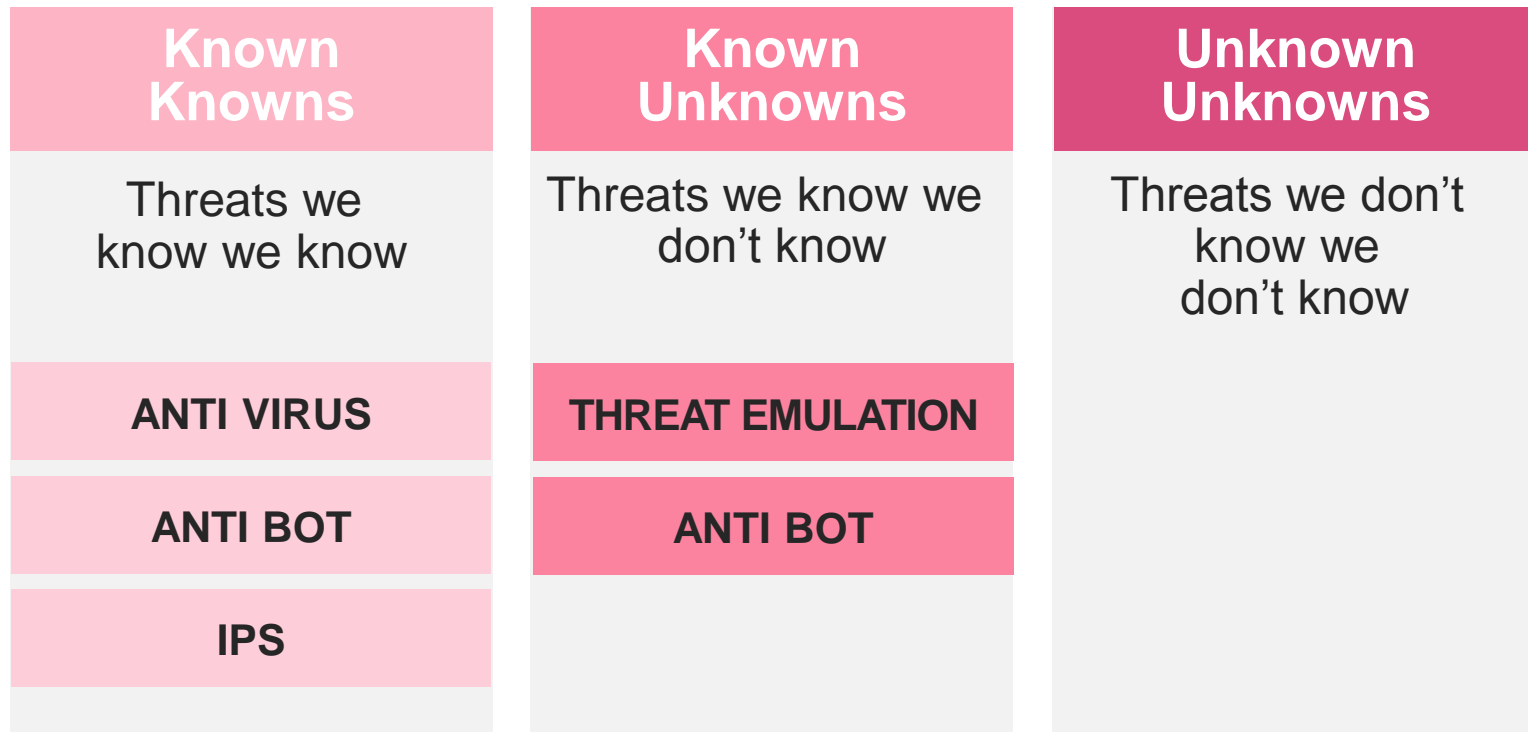
Protect data in
motion and at rest



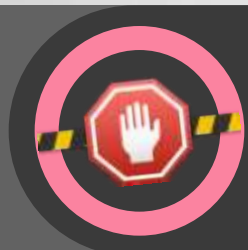


WHAT ABOUT PROTECTING AGAINST THE BAD GUYS?

THE THREATS WE NEED TO PREVENT

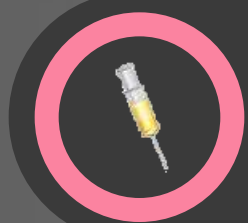


Check Point Multi-Layered Threat Prevention



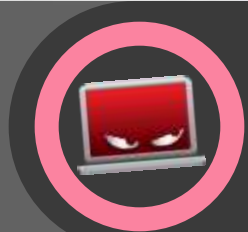
IPS

Stops exploits of known vulnerabilities



Antivirus

Block download of malware infested files



Anti-Bot

Detect and prevent bot damage



IPS Software Blade Summary

■ Security – Sophisticated and Accurate

- Industry leading threat coverage
- Multi-Method Detection Engine
- NSS Recommended in IPS Group Tests



■ Integrated Turn-Key Appliances

- Multiple models covering performance spectrum
- Integrated hardware and software bypass
- Flexibility with integrated, turn-key appliances



■ Management – Operational Efficiency

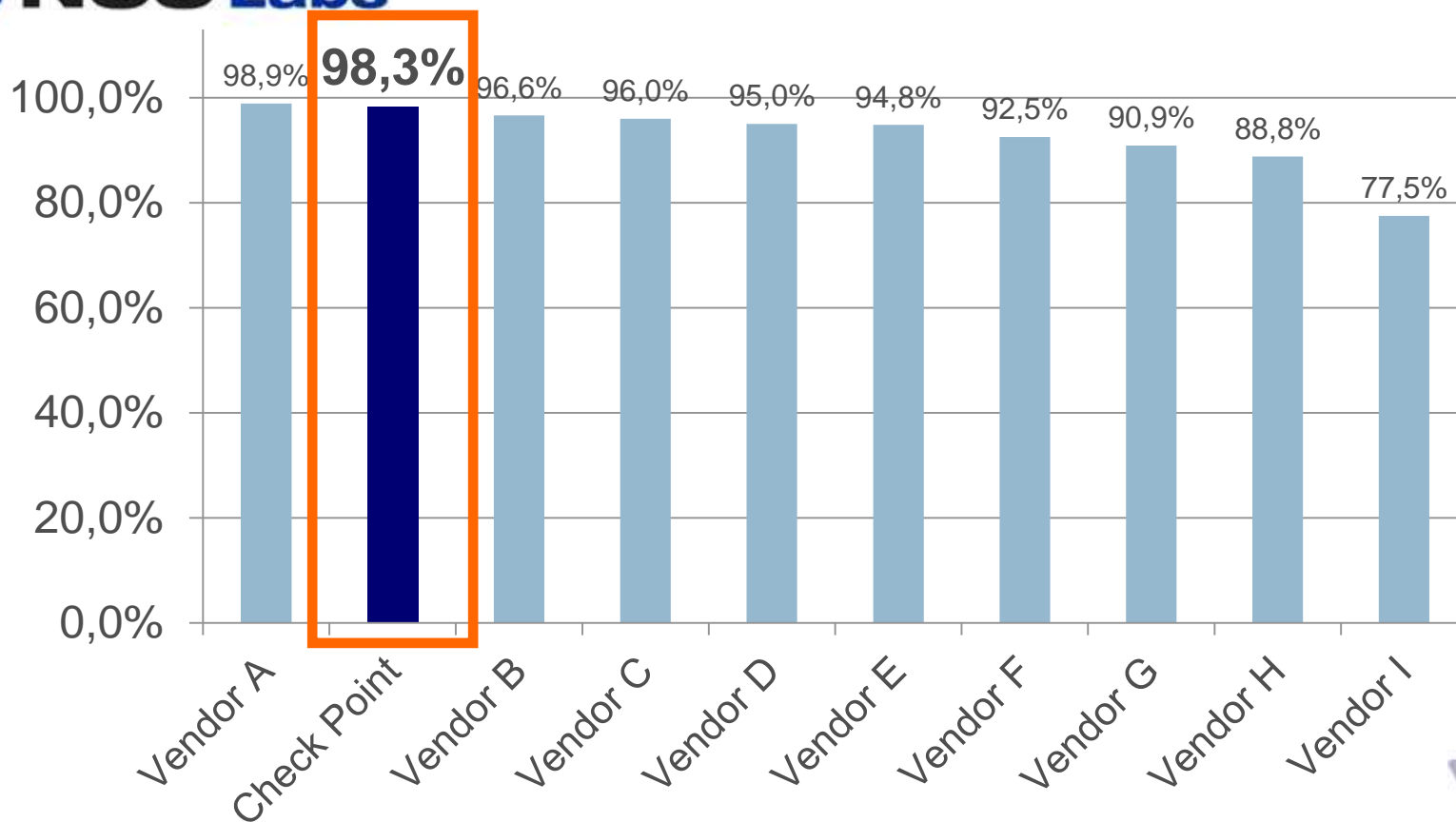
- Unified management of Check Point IPS products
- Easy deployment, configuration and management of IPS policy, features
- Efficient and effective policy and IPS operations management

Increase Security

NSS IPS Group Test Results (2012)



Overall Achievable Block Rate (Tuned*)



*NSS Labs tested only tuned configurations in 2012



Resistance to Evasion Attacks

Missing a type of evasion means a hacker can use an entire class of exploits to circumvent the IPS, rendering it virtually useless

Check Point IPS Software Blade
delivered 100% resistance to evasion

IP Packet
Fragmentation

TCP Stream
Segmentation

RPC
Fragmentation

SMB & NetBIOS
Evasions

URL
Obfuscation

HTML
Obfuscation

Payload
Encoding

FTP
Evasion

IP Frag + TCP
Segmentation

IP Frag + MSRPC
Fragmentation

IP Frag + SMB
Evasions

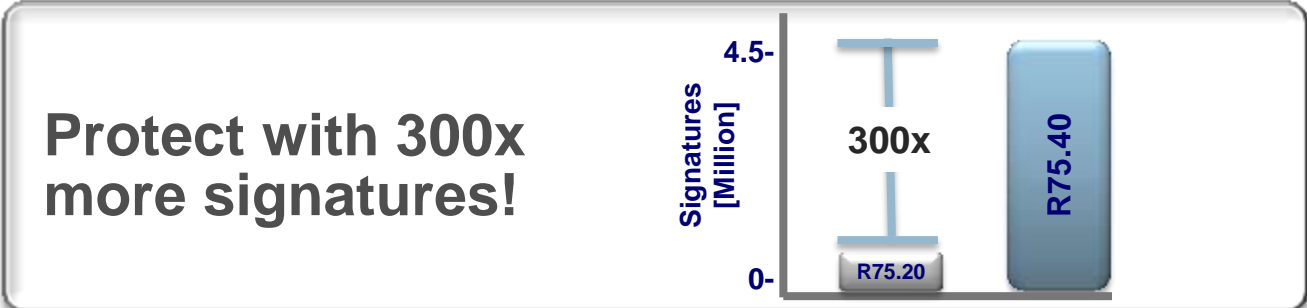
TCP Seg +
NetBIOS
Evasions



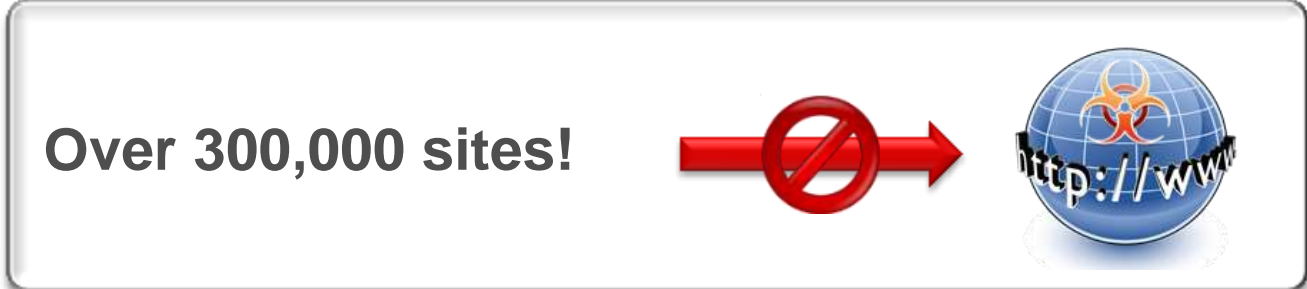


Extended Protection using ThreatCloud™

Stop Incoming Malware Attacks



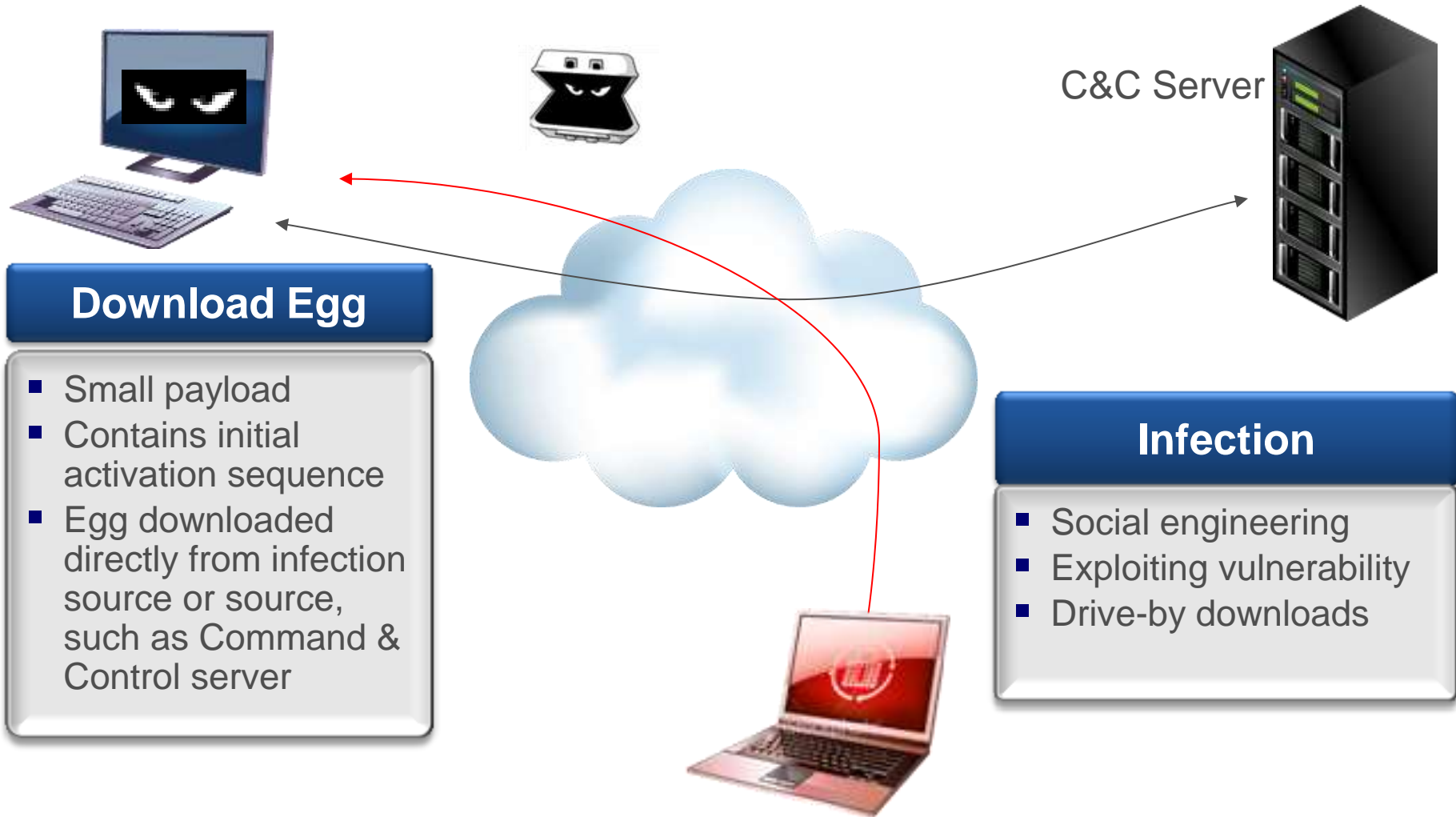
Prevent Access to Malicious Sites



Constantly updated



Botnet Operation: The Infection



Download Egg

- Small payload
- Contains initial activation sequence
- Egg downloaded directly from infection source or source, such as Command & Control server

Infection

- Social engineering
- Exploiting vulnerability
- Drive-by downloads

Botnet Operation: Self -Defense



Self Defense

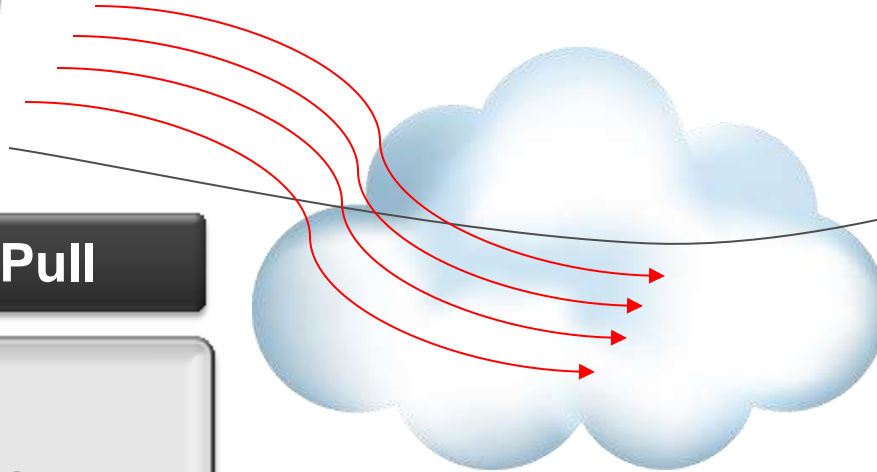
- Stop Anti-Virus service
- Change “hosts” file
- Disable Windows Automatic Updates
- Reset system restore points



Command
& Control
Server



Botnet Operation: The Damages



Command
& Control
Server



Payload Pull

- Spam
- Denial of Service
- Identity Theft
- Propagation
- Click fraud



Anti-Bot

DISCOVER and STOP Bot Attacks

**Discover
Bot infections**

**Multi-tier
discovery**

Command and
Control
IP/URL/DNS



Communication
patterns



Attack
signs and types



**Prevent
Bot damage**

**Stop traffic to
remote operators**



**Investigate
Bot infections**

**Extensive
forensics tools**



ThreatSpect™ Engine

Maximum security with
multi-gig performance

1

Reputation

- Detect Command & Control sites and drop zones
- Over 250 millions addresses in ThreatCloud™
- Real time updates

2

Network
Signatures

- Over 2000 bots' family unique communication patterns
- Dozen of behavioral patterns

3

Suspicious
Email Activity

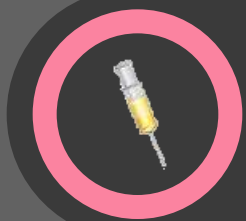
- Over 2 million outbreaks

Check Point Multi-Layered Threat Prevention



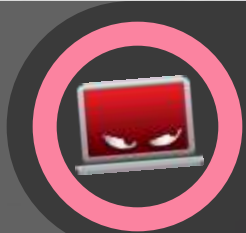
IPS

Stops exploits of known vulnerabilities



Antivirus

Block download of malware infested files



Anti-Bot

Detect and prevent bot damage





TARGETED ATTACKS BEGIN WITH ZERO-DAY EXPLOITS

Duqu Worm Causing Collateral Damage in a Silent Cyber-War

Worm exploiting zero-day vulnerabilities in a Word document

SECURITY
dark READING

Exploiting Zero-day vulnerabilities

2012 Top Vulnerable Applications

 Adobe Reader 30 critical exploits	 Java 17 critical exploits	 Office Microsoft Office 16 critical exploits
 Adobe Flash 57 critical exploits	 FireFox 91 critical exploits	 Internet Explorer 14 critical exploits

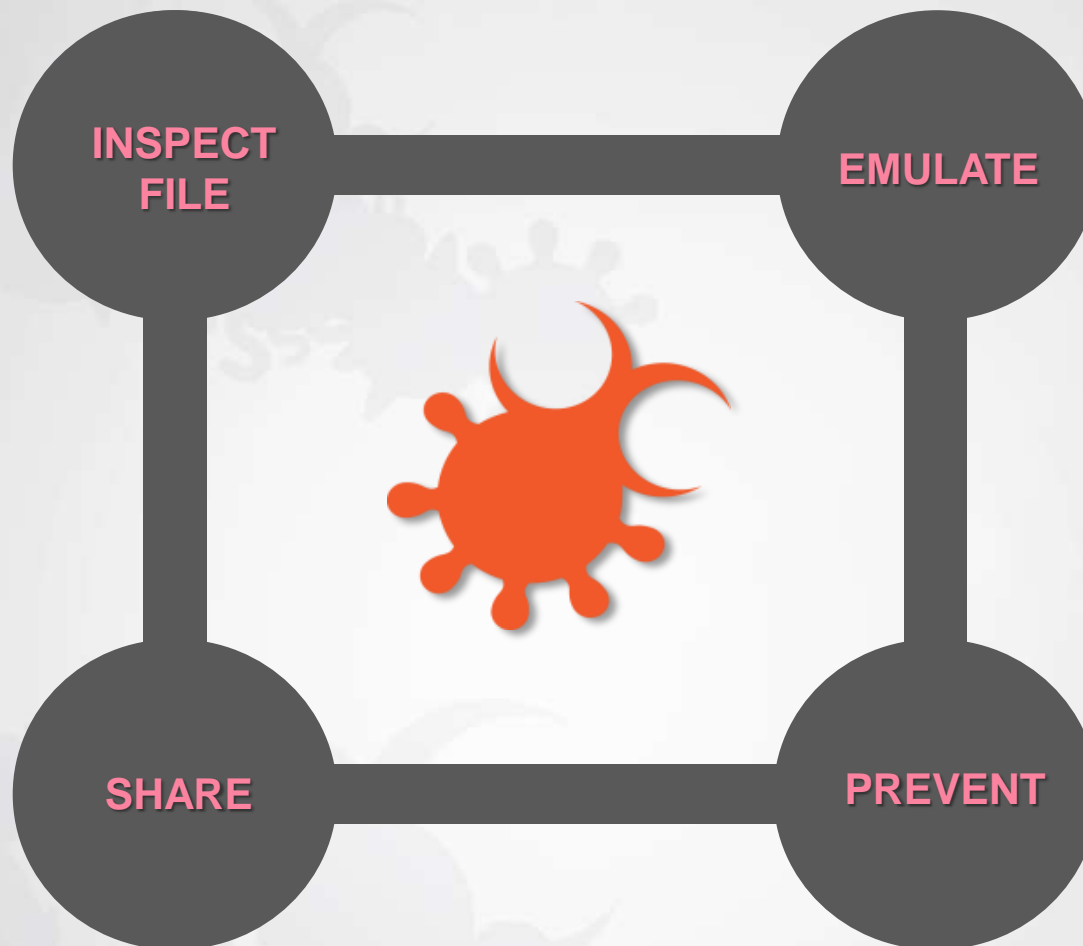
New vulnerabilities



Countless new variants

“nearly 200,000 new malware samples appear around the world each day”

- net-security.org, June 2013



Stop undiscovered attacks with
Check Point Threat Emulation

Requires no
infrastructure
change or
adding devices

Identify files
in email
attachments
and downloads
over the web

Send file to
virtual sandbox

INSPECT



Exe files, PDF and
Office documents

Emulating
Multi OS
environments
WIN 7, 8, XP & user
customized

Open file
and monitor
abnormal
behavior

EMULATE



Monitored
behavior:

- file system
- system registry
- network connections
- system processes

PREVENT



Security Gateway



Unique

Inline
stopping of
malicious
files on any
gateway



SHARE

Immediate
update of all
gateways

CHECK POINT
THREATCLUD™



Joseph H. Nyee

12345 Street Name Ave, New Orange, WA 11111

555-555-5555 (Home)

555-555-5555 (Cell)

xxxxxx@resumewriters.com

Flexible, results-oriented and meticulous Professional interested in continuing work as a Maintenance Technician/ Electrician

QUALIFICATIONS

Experienced, Knowledgeable, Versatile, Adaptable and Dependable

PROFESSIONAL EXPERIENCE

NORTHWEST ELECTRICAL CORP., New Orange, WA 1999 – 2005

Maintenance Electrician

- Used laptop and desktop workstations to troubleshoot problem sources on PLC and CNC program controlled equipment in the machining, production and assembly areas of the plants. Filed reports and looked up parts.
- Assisted other trades in pinpointing mechanical, hydraulic and pneumatic problems.
- Corrected/Repaired equipment.
- Worked on construction projects as needed and continually performed PM tasks.

WONKOR CORP., Pamoma, OR 1994 – 1999

Master Electrician

- Broadened knowledge base since there were only two skilled trades—Mechanical and Electrical.
- Sharpened troubleshooting efficiency skills to match high volume production schedule.
- Provided production machining and assembly line support. Machine center contained G.E. Fanuc-controlled Toyoda and Chiron mills, Okuma lathes and digital servo drives; assembly lines had Allen Bradley PLC 5 controllers, Miller/Hobart wire-feed and stud welders, large spot welders, and various small presses.

GENERAL DYNAMICS, Lima, OH 1984 – 1993

Journeyman Maintenance Electrician

- Began inside maintenance career.
- Repaired and maintained welders, presses, machining centers, hoists, cranes, shape cutting oxy fuel and plasma arc units, and coordinated axis drive systems.
- Worked on Allen Bradley PLC, PLC 2 and PLC 3 controllers, Gould Modicon PLCs and Allen Bradley 7300, 8200 and 9000-series CNC machine controllers.

I.B.E.W./Local 683, Columbus, OH 1979 – Present

Journeyman Inside Wireman

- Worked on industrial and commercial construction projects. Tasks included print reading, job layout, conduit bending, wire pulling, heavy machine and switchgear moving and installation, industrial power distribution and motor control center installation. Trained and supervised apprentices.

EDUCATION

OHIO INSTITUTE OF TECHNOLOGY/DEVRY, Columbus, OH 1975

Diploma, Electronic Technician

SPRINGFIELD LOCAL 669 JOINT APPRENTICE TRAINING COUNCIL, Springfield, OH 1980

Journeyman Inside Wireman

Certifications, Off job site training on Allen Bradley PLC 2-3-5 R.S.LOGIX, troubleshooting, repair and programming, G.E.FANUC 15M CNC controllers and digital servo drives, Toyoda Machining Center spindle maintenance.

A STANDARD CV?



Malware Report



Emulated On: Microsoft Windows XP 32 bit, Service Pack 3, Office 2003 (11.5604.5606), Office 2007 (12.0.4518.1014), Adobe Acrobat Reader 9.0

1



Joseph_Nyee.pdf

Malicious Activity Detected

Type  pdf

MD5 3173d2a0a607eccf21707a3dc5de30da

SHA1 b18de396e6392e9e241e816e662e8f5abdb68a99



Emulation Screenshot



9 Affected Files

3 Files Created | 8 Files Modified | 1 File Deleted

C:\Documents and Settings\All Users\Application Data\google\googleservice.dll
C:\Documents and Settings\All Users\Start Menu\Programs\Startup\googleservice.exe
C:\Documents and Settings\admin\Application Data\google\googleservice.dll
C:\Documents and Settings\admin\Local Settings\Temp\AdobeARM.dll

[more](#)



4 Affected Processes

4 Processes Created | 1 Process Terminated | 0 Processes Crashed

C:\Documents and Settings\All Users\Start Menu\Programs\Startup\googleservice.exe
C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Program Files\Internet Explorer\iexplore.exe



31 Affected Registry Keys

31 Entries Set | 0 Entries Deleted

HKCU\Software\Microsoft\Direct3D\MostRecentApplication\Name
HKCU\Software\Microsoft\Internet Explorer\Main\Window_Placement
HKCU\Software\Microsoft\Internet Explorer\Security\P3Sites
HKCU\Software\Microsoft\Internet Explorer\ToolBar\Locked

[more](#)



1 Attempted Network Connections

winssl.dyndns.org



Abnormal file activity

 **9 Affected Files**
3 Files Created | 8 Files Modified | 1 File Deleted

C:\Documents and Settings\All Users\Application Data\google\googleservice...
C:\Documents and Settings\All Users\Start Menu\Programs\Startup\googleservice.exe
C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Program Files\Internet Explorer\iexplore.exe

Tampered system registry

 **31 Affected Registry Keys**
31 Entries Set | 0 Entries Deleted

HKCU\Software\Microsoft\Direct3D\MostRecentApplication\Name
HKCU\Software\Microsoft\Internet Explorer\Main\Window_Placement
HKCU\Software\Microsoft\Internet Explorer\Security\P3Sites
HKCU\Software\Microsoft\Internet Explorer\Toolbar\Locked

“Naive” processes created

 **4 Affected Processes**
4 Processes Created | 1 Process Terminated

C:\Documents and Settings\All Users\Start Menu\Programs\Startup\googleservice.exe
C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Program Files\Internet Explorer\iexplore.exe

Command & Control Sites

 **1 Attempted Network Connections**
winssl.dyndns.org

 **31 Affected Registry Keys**
31 Entries Set | 0 Entries Deleted

HKCU\Software\Microsoft\Direct3D\MostRecentApplication\Name
HKCU\Software\Microsoft\Internet Explorer\Main\Window_Placement
HKCU\Software\Microsoft\Internet Explorer\Security\P3Sites
HKCU\Software\Microsoft\Internet Explorer\Toolbar\Locked

 **1 Attempted Network Connections**
winssl.dyndns.org

File System Activity

System Registry

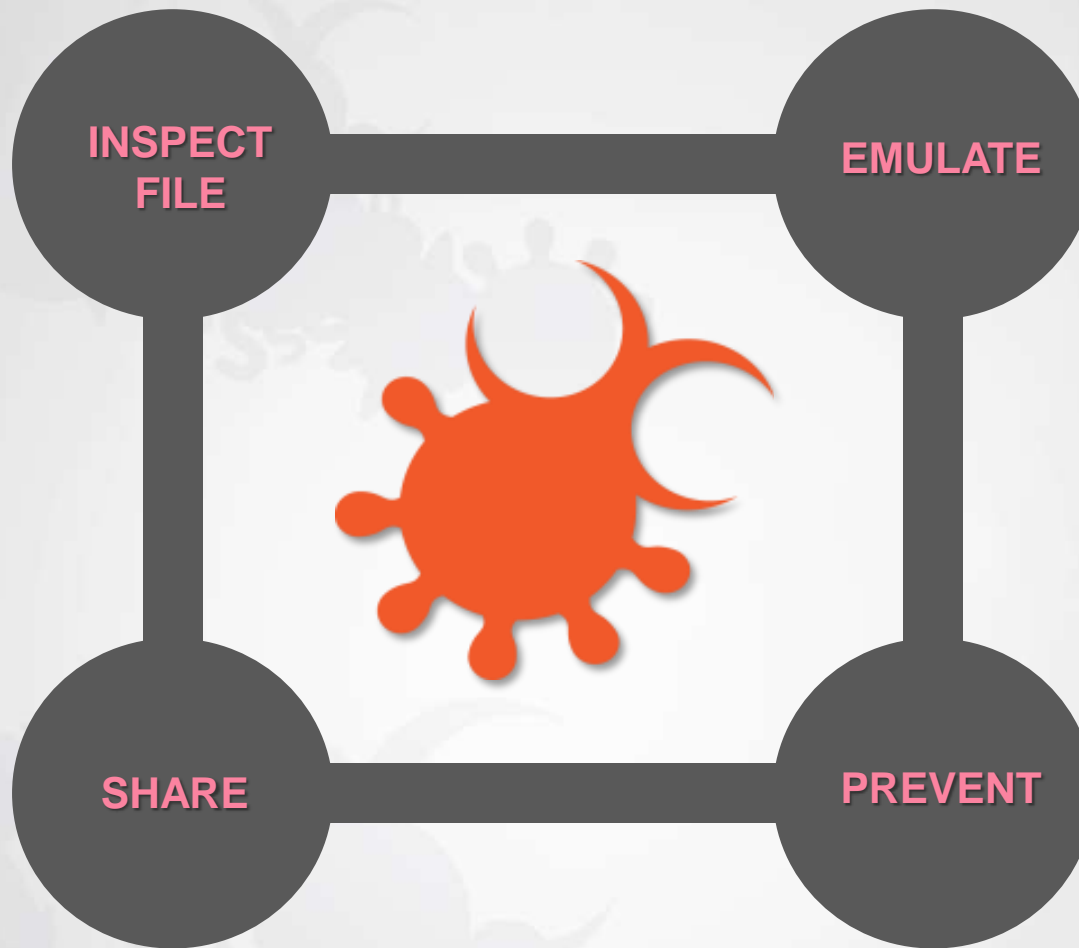
System Processes

Network Connections

Threat Emulation Deployment Options



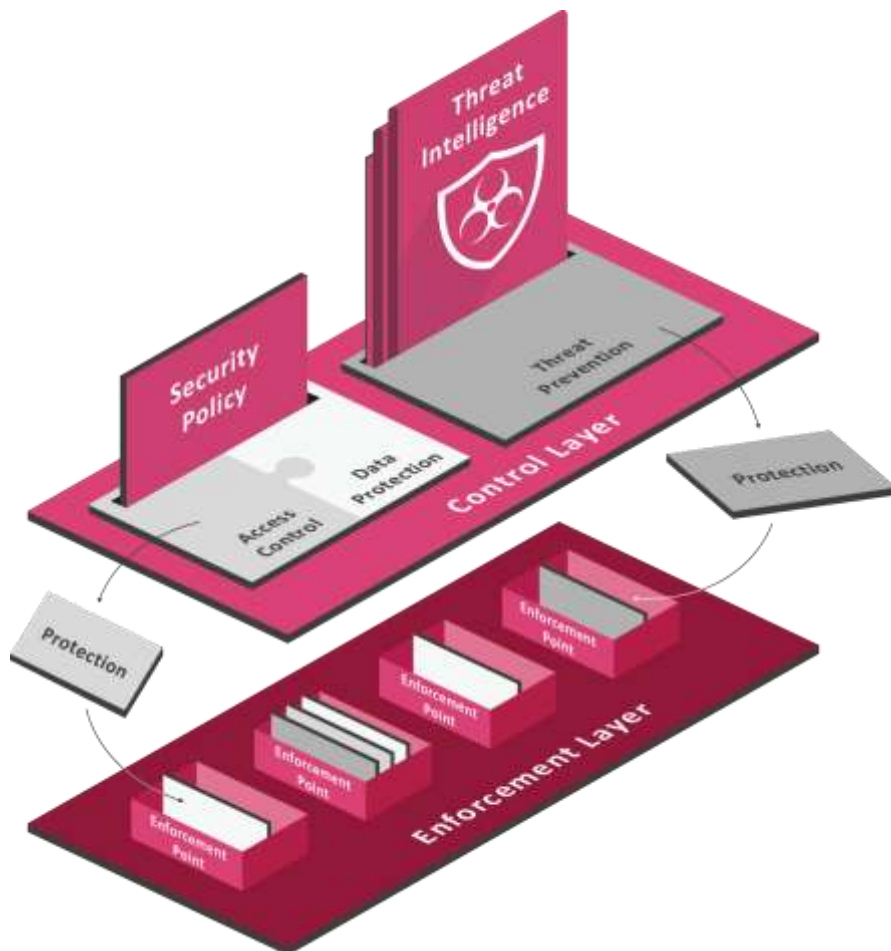
**THE ONLY SOLUTION TO PROVIDE
MULTIPLE DEPLOYMENT OPTIONS**



Stop undiscovered attacks with
ThreatCloud Emulation Service

THREAT PREVENTION

Updated protections in **REAL-TIME**



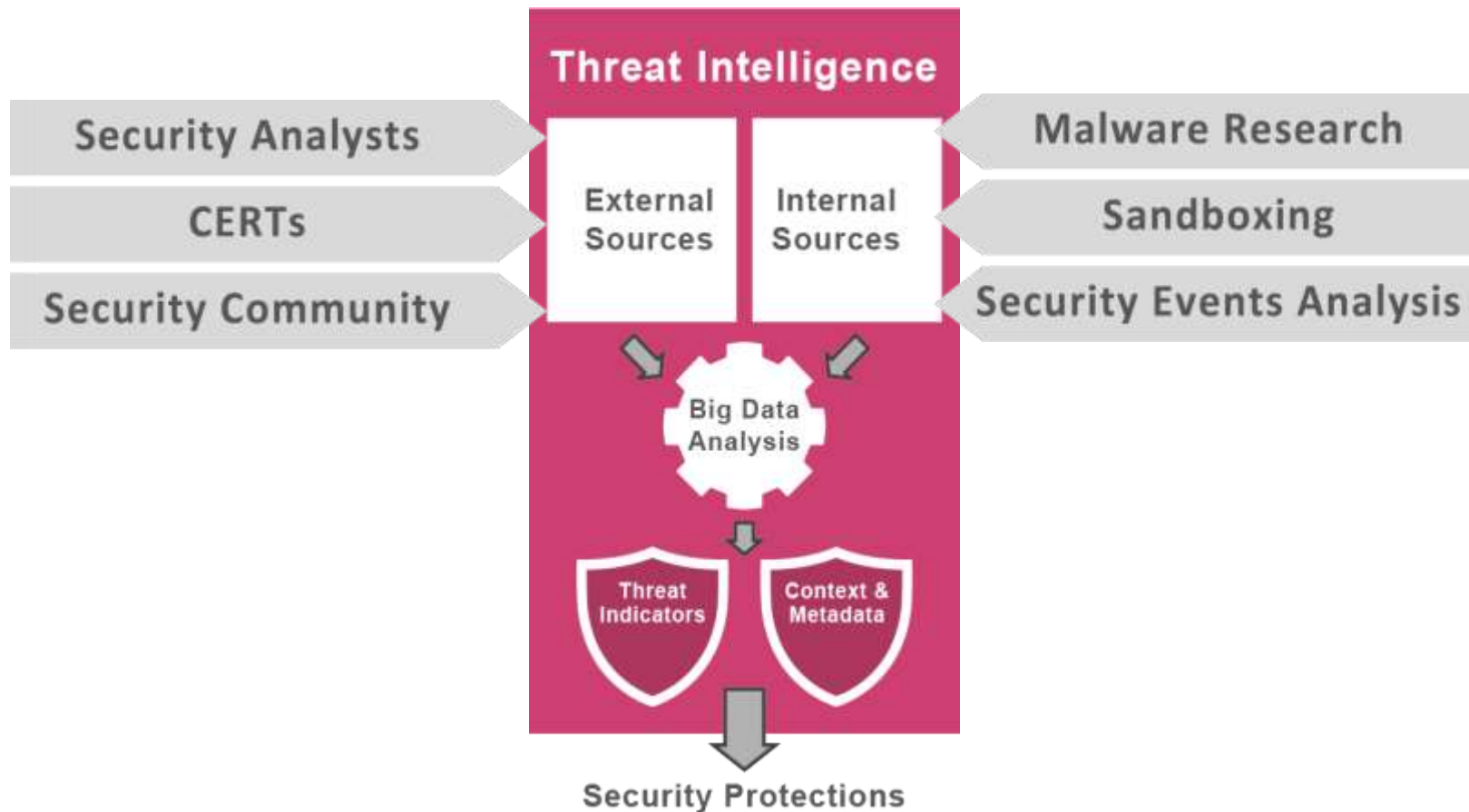
Utilizing the same enforcement points for real time dynamic Threat Prevention protections

EFFCTIVE THREAT PREVENTION IS BASED ON INTELLIGENCE



THREAT INTELLIGENCE

REAL-TIME collaborative and open **INTELLIGENCE** translate into **SECURITY** protections.



ThreatCloud™ First Collaborative Network to Fight Cybercrime

Check Point
ThreatCloud™



Over **250 Million**
Addresses
Analyzed for Bot
Discovery

Over **4.5 Million**
Malware
Signatures

Over **300,000**
Malware-Infested
Sites

Up-to-the-Minute
Security Intelligence



ThreatCloud™ - Dynamically Updated Intelligence

SensorNET



Bot addresses

Malware
Sites



Signatures



Check Point
ThreatCloud™

**Global network of
sensors to identify
emerging threats**

**Collect attack
information from
gateways**

**Industry-best
malware feeds**

Boosting the Collaborative Power of ThreatCloud



Real-time sharing for immediate Protection

ThreatCloud™ Model: High Performance with Extended Protection

Threat Database is kept in the cloud

- Malicious URLs
- Real time signatures
- C&C IP Addresses



Security updates
normalized to the
ThreatCloud

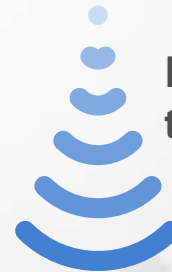


Extended Protection

Gateway consults
the cloud



Download updates to
the gateway



- Binary Signatures
- Heuristic Engine
- Traffic Anomaly Check



High Performance

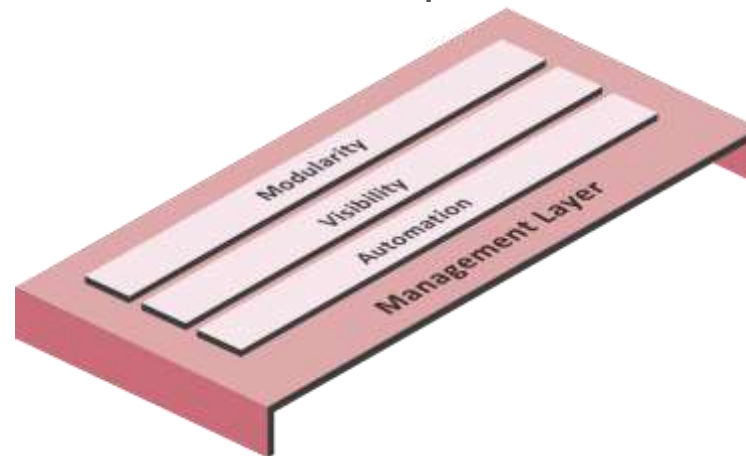
MANAGEMENT LAYER

The **MANAGEMENT** Layer **ORCHESTRATES** the infrastructure and brings the highest degree of **AGILITY** to the entire architecture.



MANAGEMENT LAYER

BRINGS the SDP architecture to **LIFE** by integrating security with business processes



MODULARITY

Support segmentation and segregation of management duties

AUTOMATION

Automates security policy administration and synchronizes it with other systems

VISIBILITY

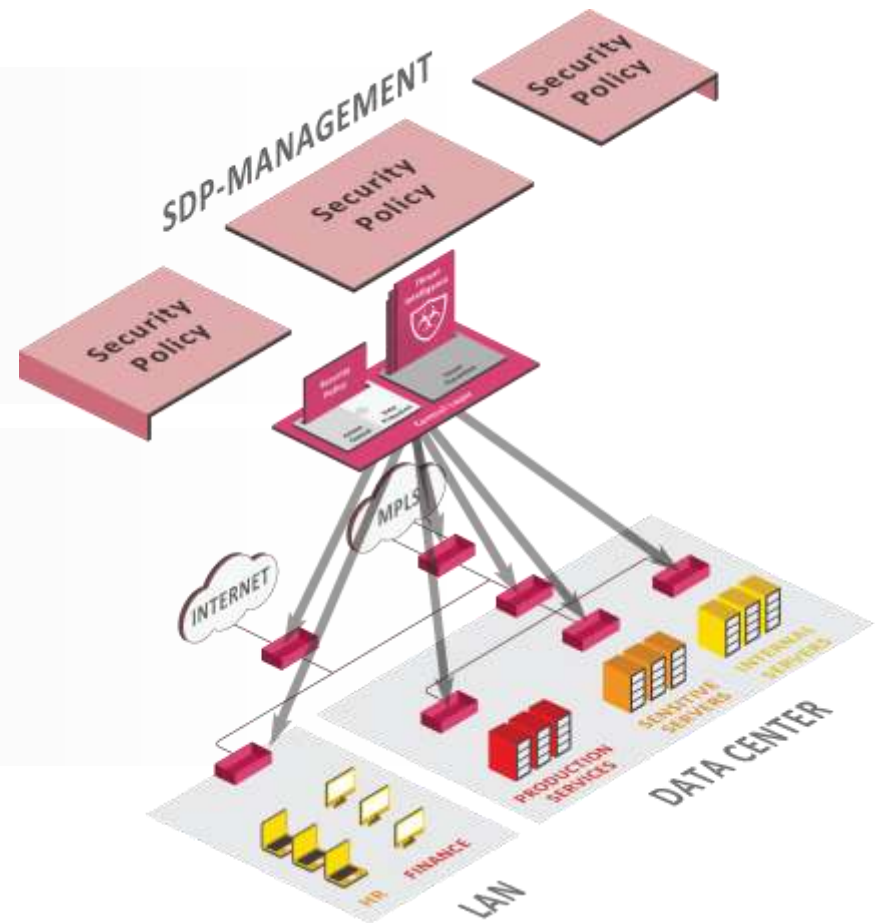
360 degree situational awareness

MODULARITY

ENDLESS FLEXIBILITY with **LAYERS** of **POLICIES**

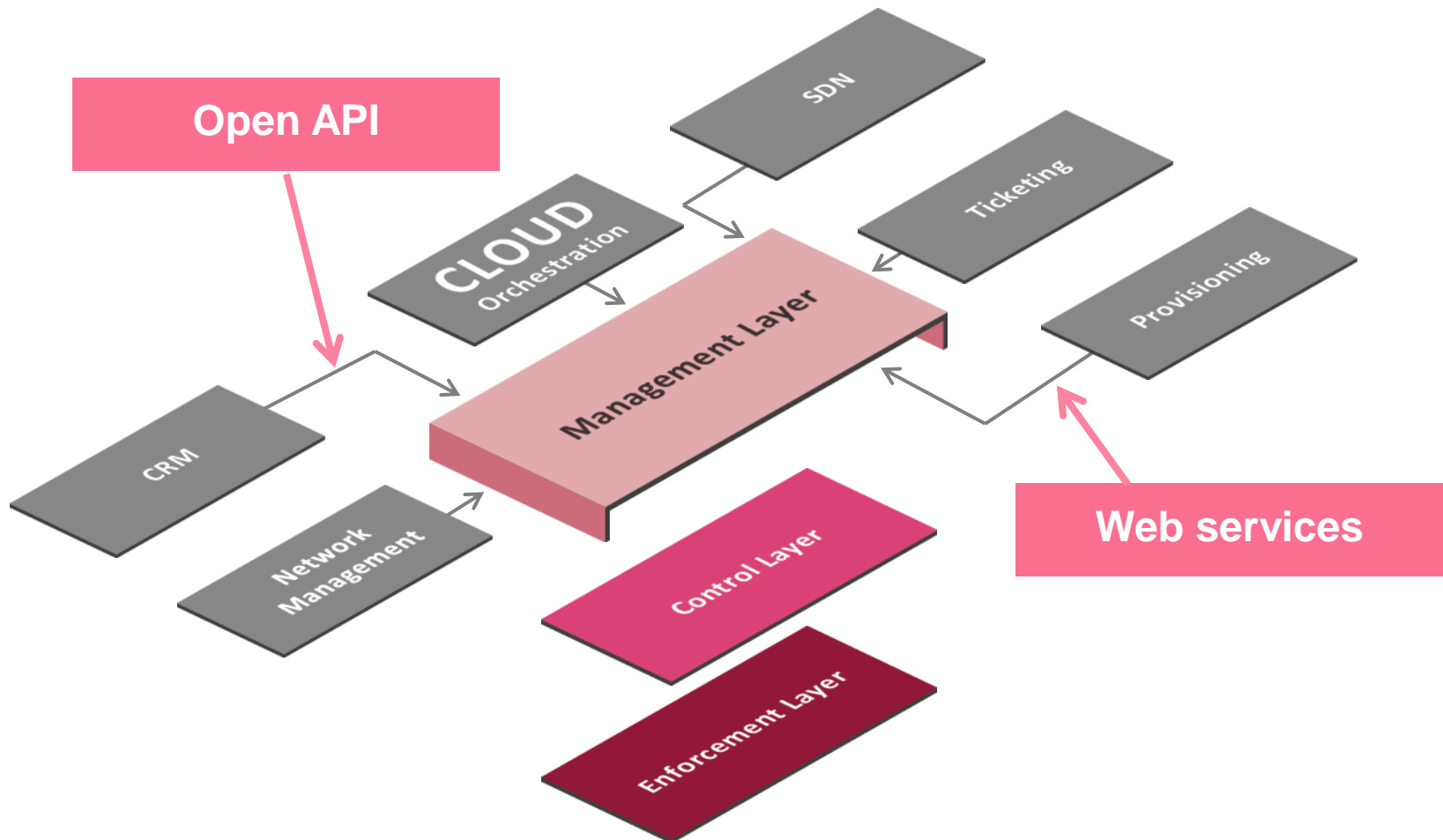
Management modularity provides the flexibility to manage each segment and control

Segregation of duties
Layers of policy



AUTOMATION

OPEN INTERFACES support business process changes



SDP AND SDN WORKING IN SYNERGY

SDN

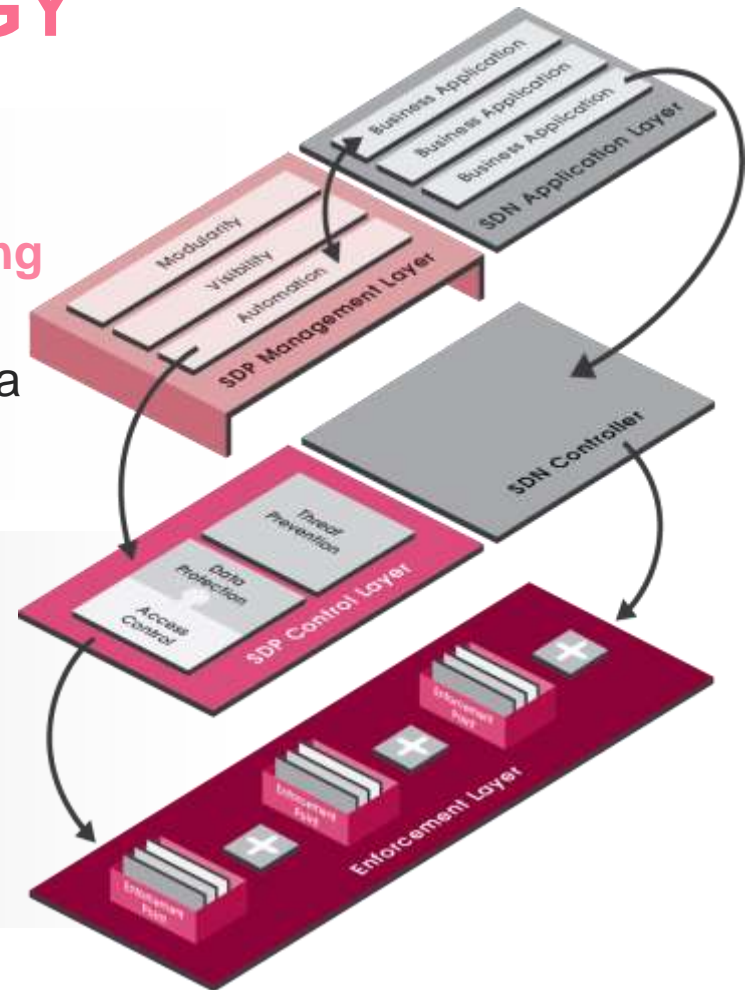
An emerging network architecture, decoupling network control and data planes.

Data flows between network nodes controlled via a programmable network SDN controller.

SDP

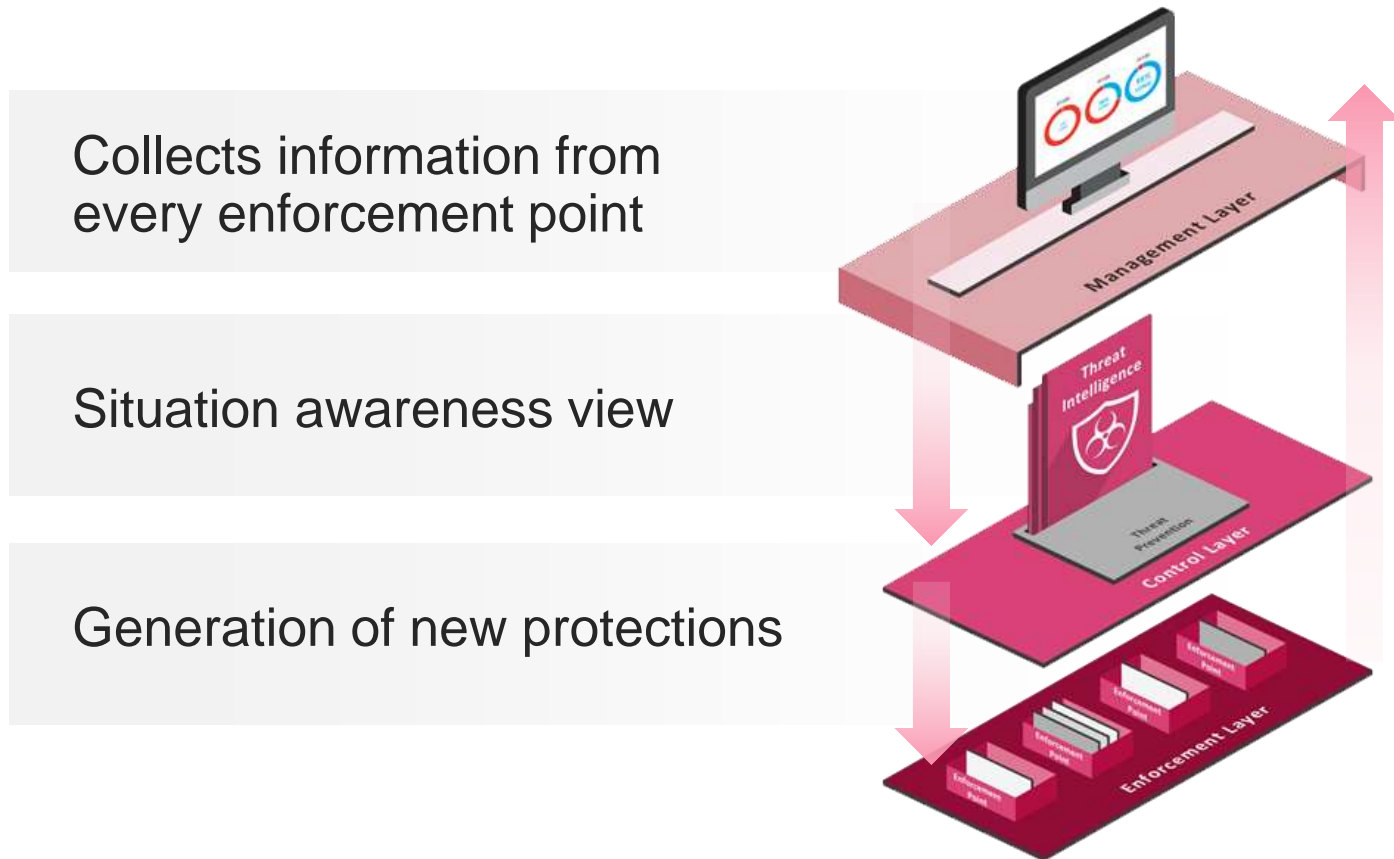
An overlay architecture enforcing security traffic flows within an SDN network

Data flows are programmed to pass through SDP enforcement points



VISIBILITY

SITUATION AWARENESS & INCIDENT RESPONSE



Management Challenges

Too Much Log Data

A Multitude of Devices

**No Time to View
Events**



Management Challenge

Finding the Relevant
Events

Knowing What Poses
the Real Threat



Management Challenge

**Getting Actionable
Information**

**Leveraging Information
to Stop Attacks Across
the Enterprise**



Check Point SmartEvent



Check Point translates
security information
into **action**

Identify critical security events from the clutter
with visual timelines

Correlate events across all security systems

Stop attacks straight from the event screen

Monitor *Only* what is Important!

The screenshot shows a network security monitoring dashboard with several key components and callouts:

- Overview Tab:** The main navigation bar includes Overview, Events, Timelines, Reports, and Policy. The Overview tab is active, showing a timeline of events with colored circles representing event counts.
- Callout 1:** "See all recent critical events" points to the Overview tab.
- Callout 2:** "Get attack source and see through the mass to get top event sources, destinations and attacks" points to the main dashboard area.
- Callout 3:** "Easily monitor top events" points to the "Recent Critical Events" table.
- Recent Critical Events Table:**

Start Time	Severity	Event Name	Source
11:32:54 17...	High	Internet Explorer SetSlice Meth...	NA 10.10.0.24
11:31:33 17...	High	Microsoft Windows SMB Pack...	NA 10.10.0.24
11:31:19 17...	High	Non Compliant DNS	NA 10.10.0.24
11:30:34 17...	High	FTP Bounce	NA 10.10.0.24
11:18:03 17...	High	FTP Bounce	NA 10.10.0.24
11:18:02 17...	High	Microsoft Active Directory LDA...	NA 10.10.0.24
11:18:02 17...	High	Symantec Veritas Backup Exe...	NA 10.10.0.24
11:17:52 17...	High	Non Compliant DNS	NA 10.10.0.24
11:16:18 17...	High	Office Files	NA 10.10.0.24
11:15:37 17...	High	Microsoft Visual Studio WMI O...	NA 10.10.0.24
11:15:37 17...	High	MIT Kerberos kadmind RPC Li...	NA 10.10.0.24
- Top Destinations Table:**

IP Address	Events
NA 10.20.0.4	6334
NA 10.20.0.5	3027
NA 10.20.0.6	2747
209.64.204.28	37
51.82.38.17	31
185.191.51.123	30
217.26.29.127	25
198.35.123.50	22
188.196.1.83	20
106.7.122.89	20
- Top Events Figure:** A pie chart showing the distribution of event types: Ping of Death (21%), Packet Sanity (21%), IP Fragments (18%), IGMP (12%), Teardrop (5%), and Other (23%).
- Status:** Shows "Eventia Components" with "Status: OK" and "Object Sync: OK".
- Events received in the:** Shows "Last Minute: 0" and "Last Hour: 537".

Best Integration

Monitor all events for IPS, DLP, endpoint and more



Timelines View

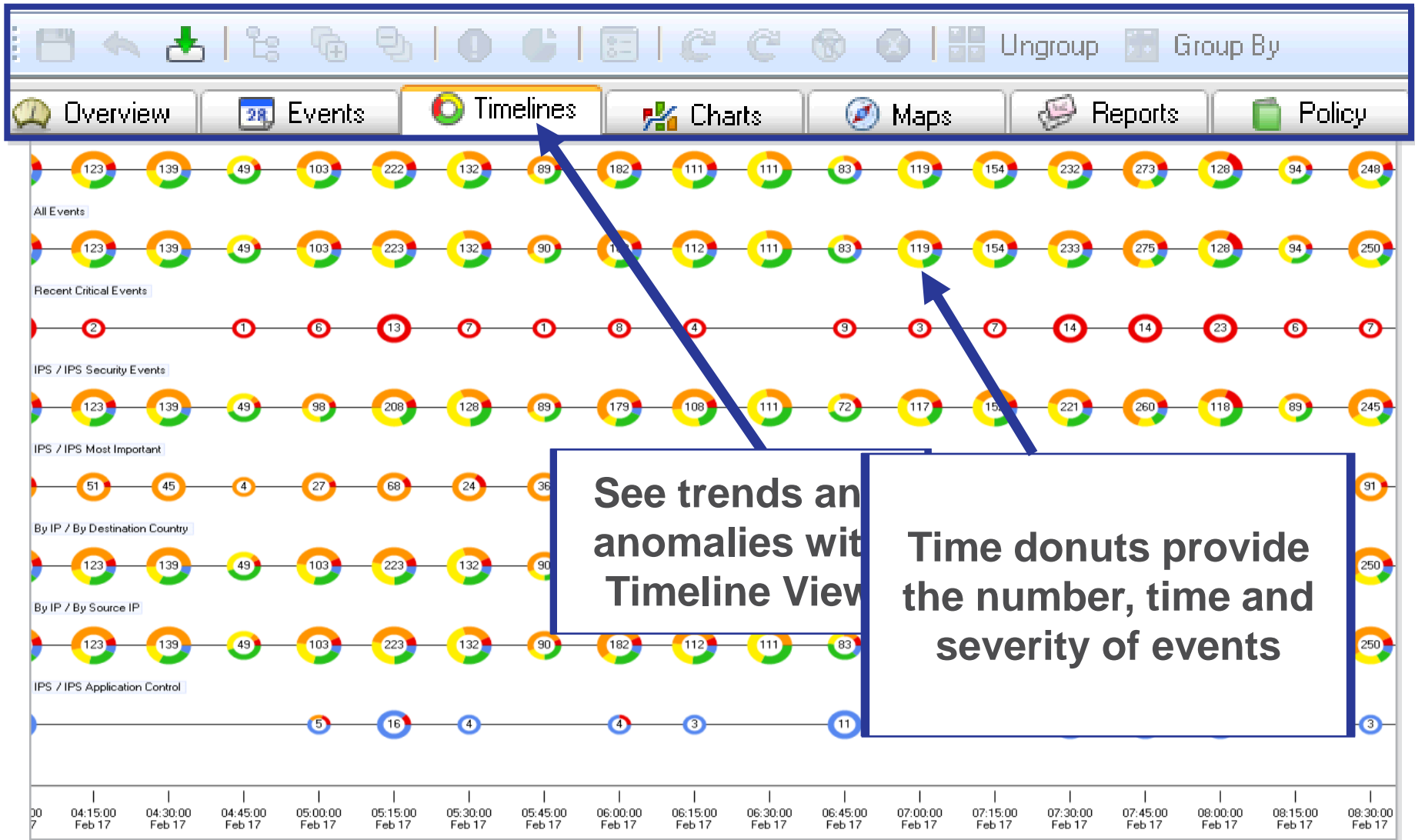


Chart View

Configure how to split the charts

Configure how to split the charts

Bar charts show how events differ over time

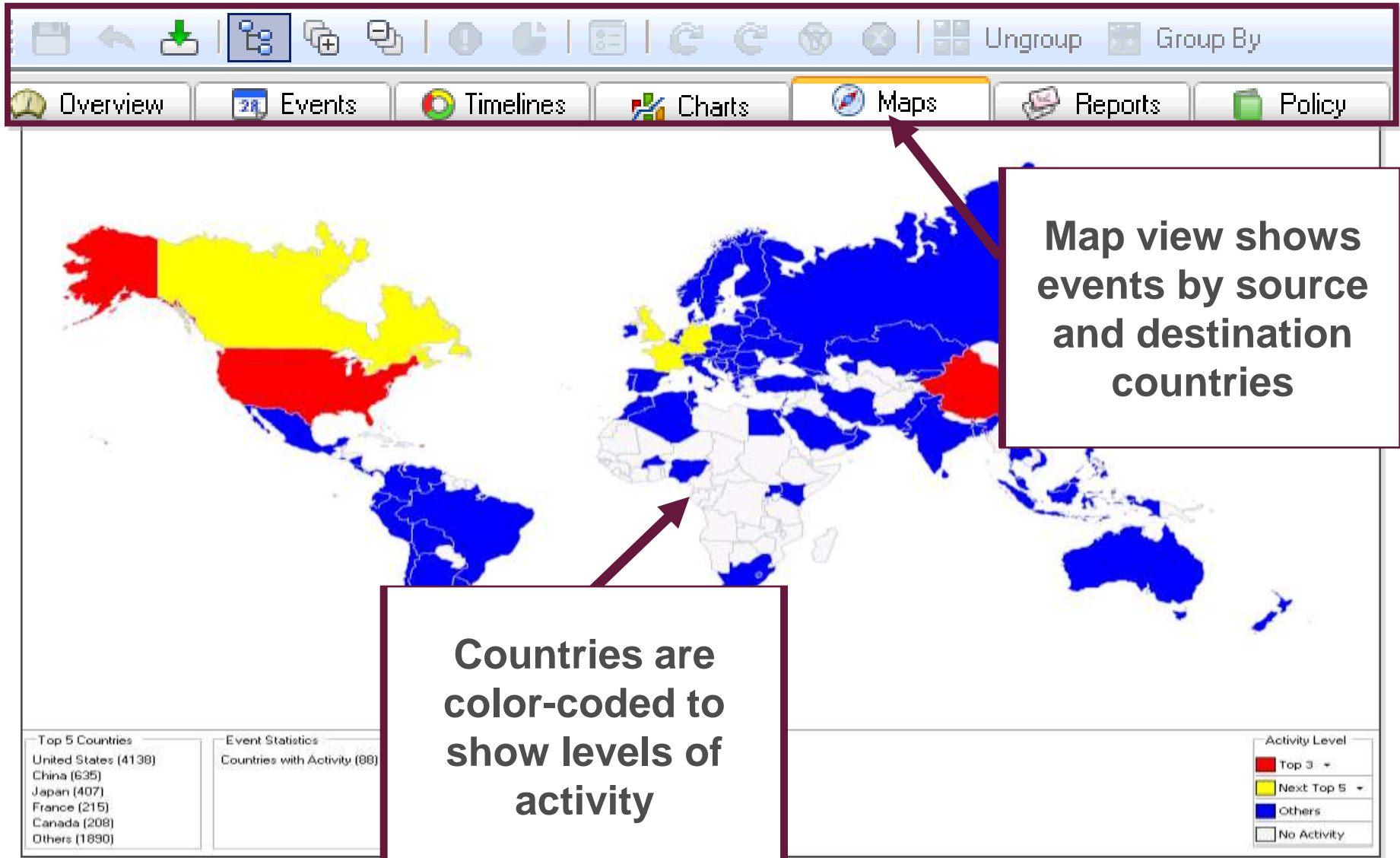
Investigate security issues using pie or bar charts

Pie charts show percentage of events with specific properties

Severity	Percentage
Critical	6%
Low	20%
Medium	29%

Events	Count
Informational	758
Low	2974

Map View



Map View

The screenshot displays the 'Map View' interface in Check Point. On the left is a navigation tree with categories: Custom, Predefined, By Direction, By IP, Endpoint Events, and Ticketing. Under 'Predefined', 'IPS' is expanded, and 'IPS Most Important' is selected. The main area shows a world map titled 'IPS Most Important by Source Country for the Last 2 Weeks'. The map uses color coding: red for the top 3 countries (USA, Australia, and a country in Europe), yellow for the next top 5 (China, India, etc.), and blue for others. A text box with an arrow points to the 'IPS Most Important' item in the tree, containing the text 'Run any query on the map'. The interface also shows a 'Server Time' of 3/24/2010 12:38 AM and a legend for 'Activity Level'.

Server Time: 3/24/2010 12:38 AM

Countries: | Maps: World Map

IPS Most Important by Source Country for the Last 2 Weeks

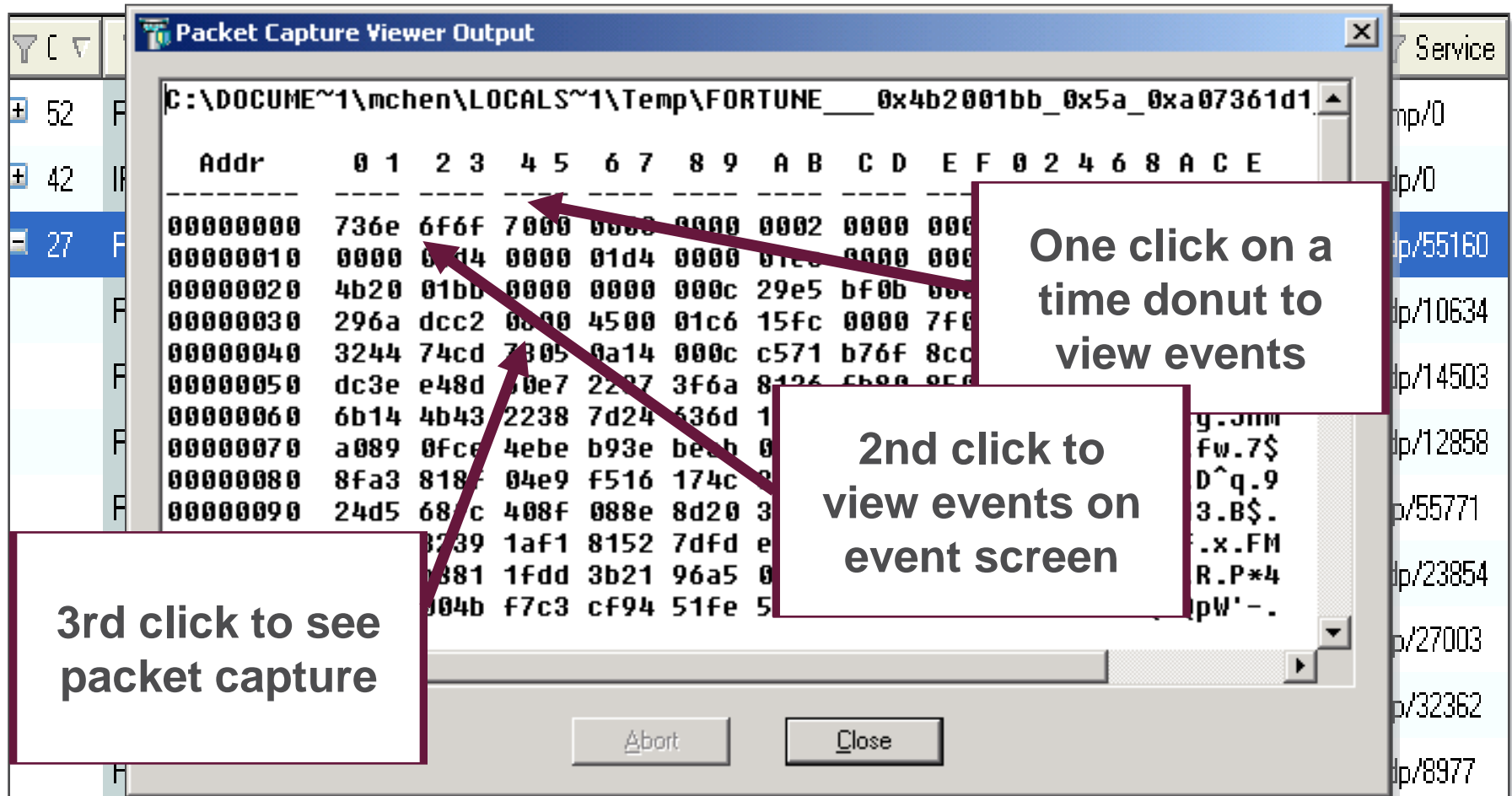
Run any query on the map

Statistics
Events with Activity (12)

Activity Level
Top 3
Next Top 5
Others
No Activity

Easy Drill-Down

From business view to forensics in 3 clicks



Packet Capture Viewer Output

C:\DOCUME~1\mchen\LOCALS~1\Temp\FORTUNE__0x4b2001bb_0x5a_0xa07361d1

Addr	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	2	4	6	8	A	C	E
00000000	736e	6f6f	7000	0000	0000	0000	0002	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
00000010	0000	0044	0000	01d4	0000	01e0	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
00000020	4b20	01b0	0000	0000	0000	000c	29e5	bf0b	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
00000030	296a	dcc2	0000	4500	01c6	15fc	0000	7f00	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
00000040	3244	74cd	7305	0a14	000c	c571	b76f	8cc0	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
00000050	dc3e	e48d	00e7	2237	3f6a	8126	cb00	0500	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
00000060	6b14	4b43	2238	7d24	636d	1000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
00000070	a089	0fce	4ebe	b93e	be3b	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
00000080	8fa3	818f	04e9	f516	174c	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
00000090	24d5	687c	408f	088e	8d20	3000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000

One click on a time donut to view events

2nd click to view events on event screen

3rd click to see packet capture

Abort Close

Better Remediation

Add protections on the fly

The screenshot displays the 'Protection Details' window for a specific threat. The window title is 'Protection Details - Microsoft Windows RASMAN Service Memory Corruption (MS06-025)'. It features several tabs: 'General', 'Network Exceptions', and 'Description'. The 'General' tab is active, showing the following details:

- Type:** Signature
- Severity:** Critical
- Confidence Level:** Medium-high
- Performance Impact:** Low
- Protection Type:** Servers, Clients

Below these details is a table with columns: Profile, Action, Override, Track, Exceptions, and a final empty column. The table contains three rows:

Profile	Action	Override	Track	Exceptions	
Default_Protection	Detect	Yes	Log	None	
Recommended_Protection	Detect	Yes	Log	None	
Standard_Protection	Prevent			None	

The 'Standard_Protection' row is highlighted in blue and enclosed in a red rectangular box. A red arrow points from a callout box to this row. The callout box contains the text: 'Proactive protection is now enabled!'.

At the bottom of the window, there are buttons for 'Edit...', 'Change Action...', 'Follow Up...', and 'View Logs'. At the very bottom, there are 'OK', 'Cancel', and 'Help' buttons.

Setting Automatic Response for Event Definition

The screenshot shows the SmartView Configuration interface. The left pane displays a tree view of event policies, with 'High connection rate to internal host on service' selected under 'Denial Of Service'. The main pane shows the configuration for this event, including detection criteria (at least 500 connections over 60 periods) and a severity of 'Medium'. The 'Automatic Reactions' field is highlighted with a blue box. A callout box with a blue border and white background points to this field, containing the text: **Block source according to configured time**. The 'Automatic Reactions' dialog is open, showing a list of reactions with 'Block Source example' checked. Below the dialog, a table shows the configuration for the selected reaction.

Severity	Reactions	Origin Type
High	<Default>	User
High	<Default>	User

Configuring Automatic Responses

The screenshot displays the 'Automatic Reactions' configuration window. On the left, a tree view shows the navigation structure, with 'Automatic Reactions' highlighted under the 'Objects' category. The main area contains a table of existing reactions:

Name	Type	Comment
<input checked="" type="checkbox"/> Block Source example	Block Source	Example for Block Source automatic reaction.
<input checked="" type="checkbox"/> Block Event Activity example	Block Event Activity	Example for Block Event Activity automatic reaction.
<input checked="" type="checkbox"/> Mail example	Mail	Example for Mail automatic reaction.
<input checked="" type="checkbox"/> External Script example	External Script	Example for External Script automatic reaction.
<input checked="" type="checkbox"/> Snmp Trap example	SNMP Trap	Example for Snmp Trap automatic reaction.

An 'Add Automatic Reaction' dialog box is open, showing the configuration for a new reaction:

- Name: Block Source
- Comment: Block Source for the next hour.
- Blocking Timeout: For **Next Hour** (selected)
- Alternative: For [] minutes

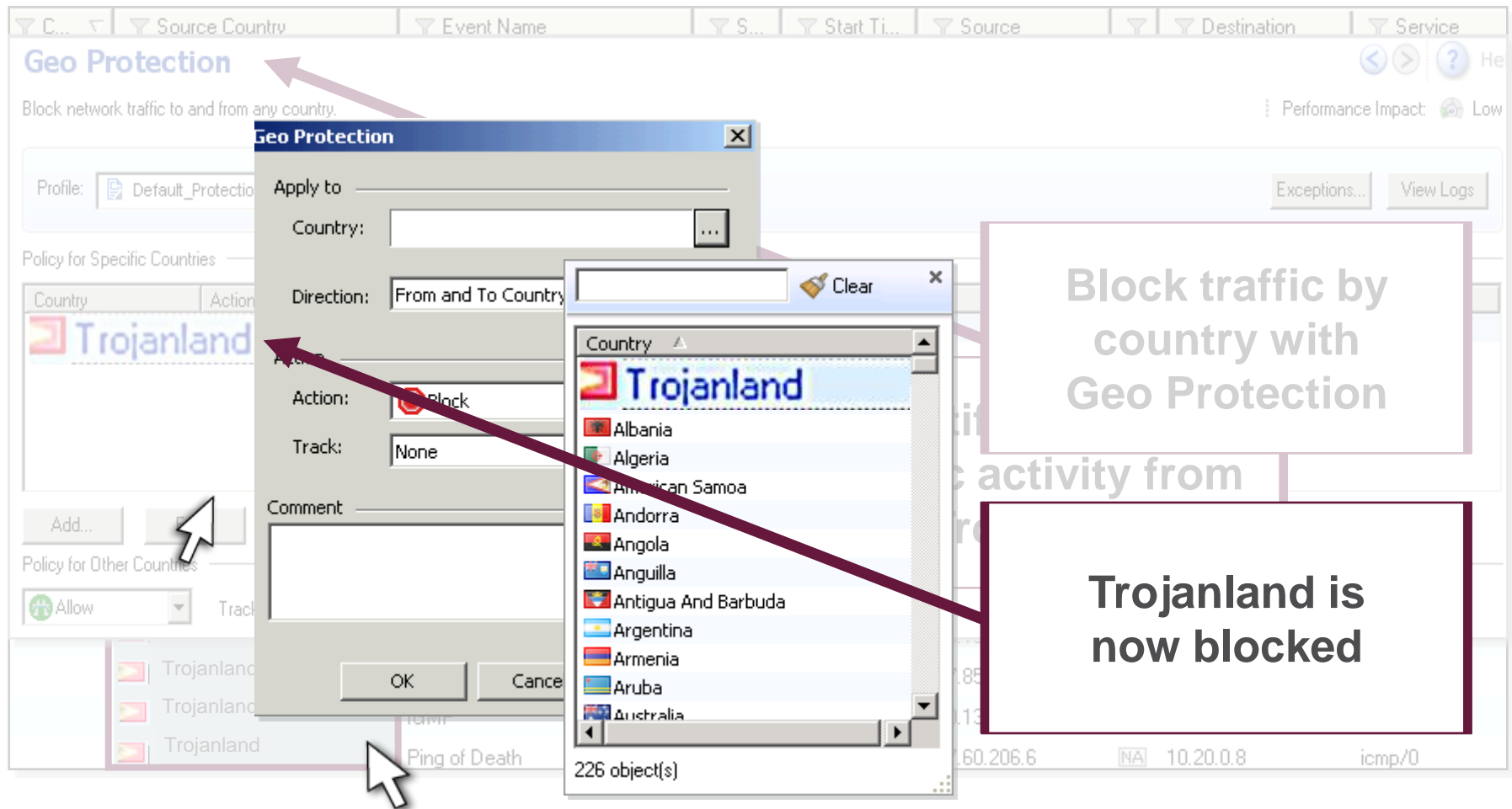
A callout box with a blue border and arrow points to the 'Next Hour' dropdown, containing the text: **Generate response for a configurable time**

At the bottom of the dialog, there is a note: "Note: Upon 'Save' the changes will be saved in the Server immediately." and buttons for 'Save', 'Cancel', and 'Help'.



Better Remediation—Geo Protection

The entire rogue nation is blocked!



The screenshot displays the Check Point Geo Protection configuration interface. A modal dialog box titled "Geo Protection" is open, showing the configuration for blocking traffic from a specific country. The "Country" field is set to "Trojanland", and the "Direction" is set to "From and To Country". The "Action" is set to "Block". A list of countries is shown, with "Trojanland" selected. A callout box points to the "Geo Protection" title, and another callout box points to the "Trojanland" entry in the country list. A third callout box points to the "Block" action. A fourth callout box points to the "Trojanland" entry in the country list, stating "Trojanland is now blocked".

Block traffic by country with Geo Protection

Trojanland is now blocked

SUMMARY



SOFTWARE – DEFINED **PROTECTION**

**MODULAR AND DYNAMIC SECURITY
ARCHITECTURE**

**FAST AND RELIABLE ENFORCEMENT WITH
REAL-TIME INTELLIGENCE**

**TODAY'S SECURITY ARCHITECTURE FOR
TOMORROW'S THREATS**

CHECK POINT SOFTWARE – DEFINED PROTECTION

MANAGEMENT LAYER

Check Point Next Generation Security Management



CONTROL LAYER

Next Generation Firewall, Threat Prevention, ThreatCloud™



ENFORCEMENT LAYER

Network, Host, Mobile, Cloud



GO TO WWW.checkpoint.com/sdp
TO DOWNLOAD THE WHITE PAPER



THANK YOU!