

차세대보안 구축 청사진

SOFTWARE-DEFINED PROTECTION

\$1.34 Billion (Revenue)

2012 revenue, 영업이익 0.8B, 2006~2012 년 평균 성장률 15.17%

100% (Security)

Pure focus on security

Fortune 500 기업이 모두 Check Point의 고객

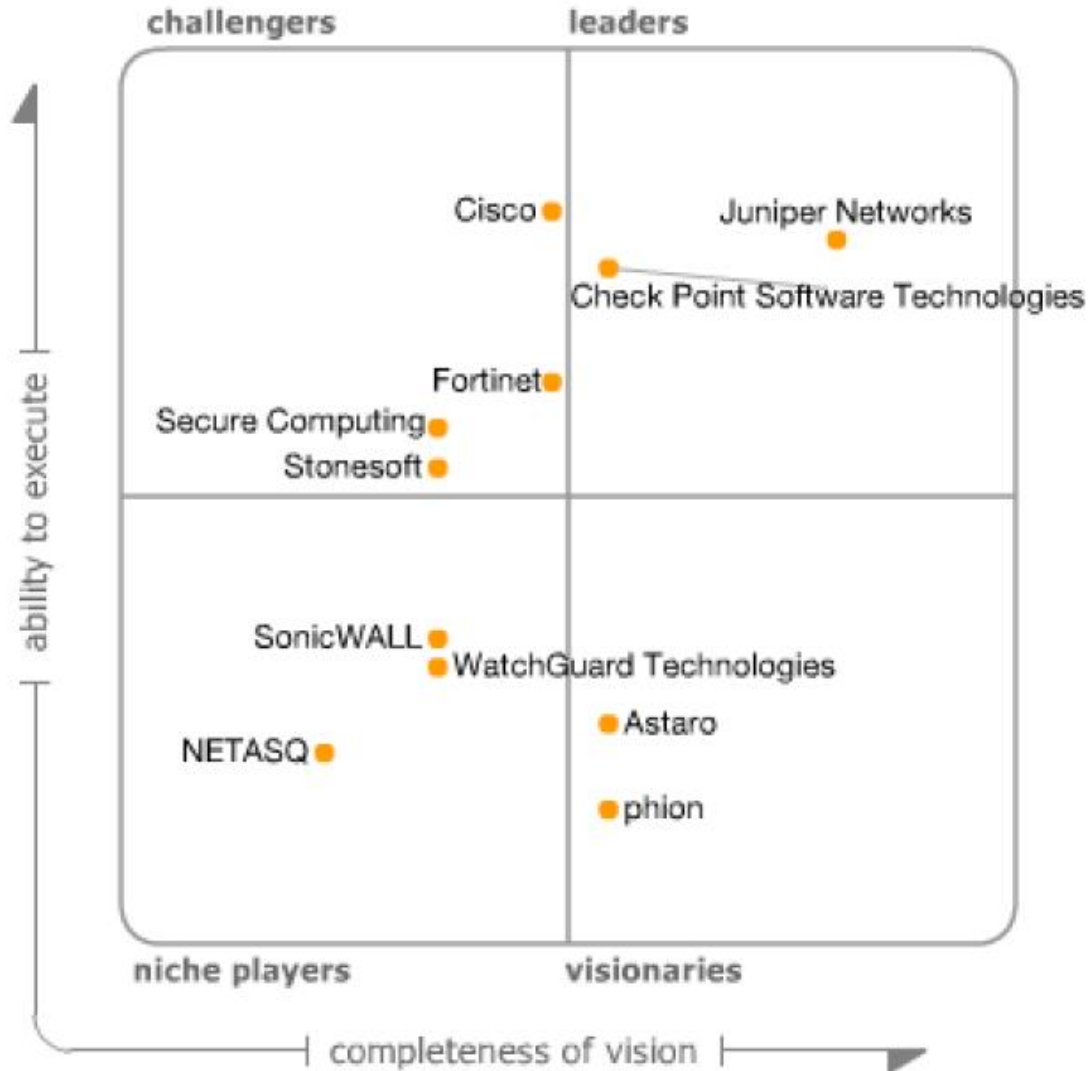
#1 (Threat Coverage)

Top Ranked NGFW by NSS Labs, Gartner, SC Magazine

“Leader” in Gartner Enterprise Firewall for 17th year

가트너 매직 쿼드런트

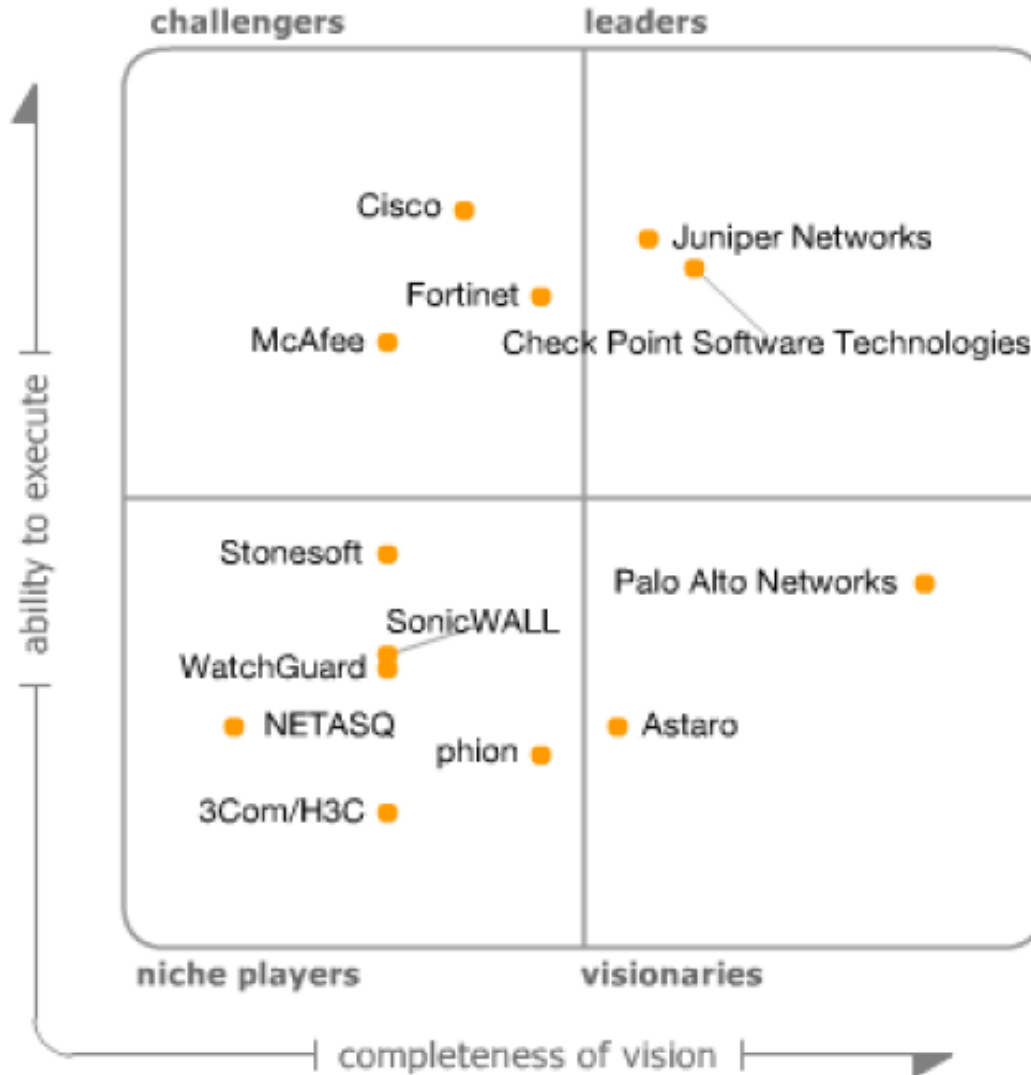
· Magic Quadrant for Enterprise Network Firewalls



As of November 2008

가트너 매직 쿼드런트

· Magic Quadrant for Enterprise Network Firewalls

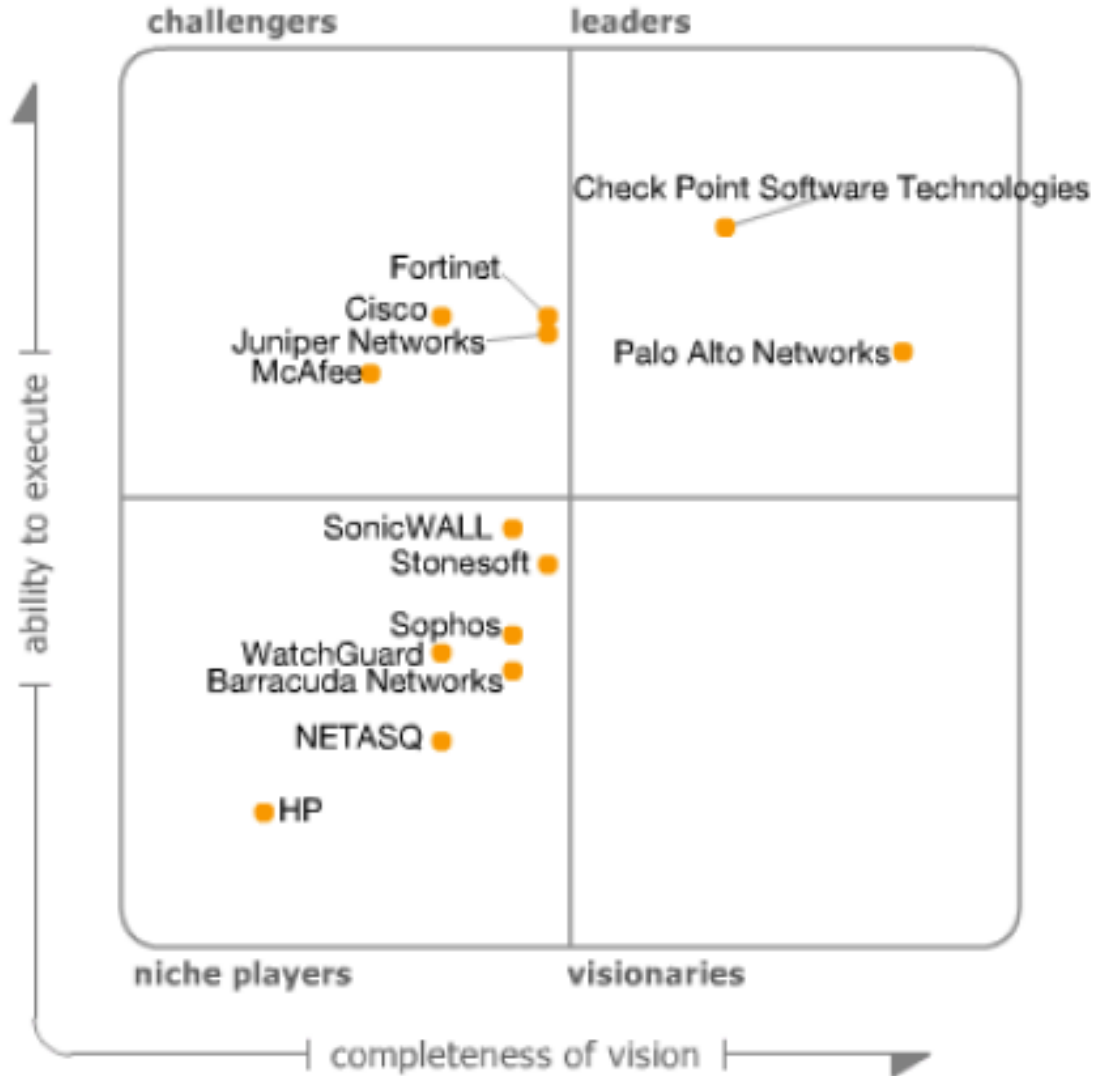


As of March 2010



가트너 매직 쿼드런트

· Magic Quadrant for Enterprise Network Firewalls

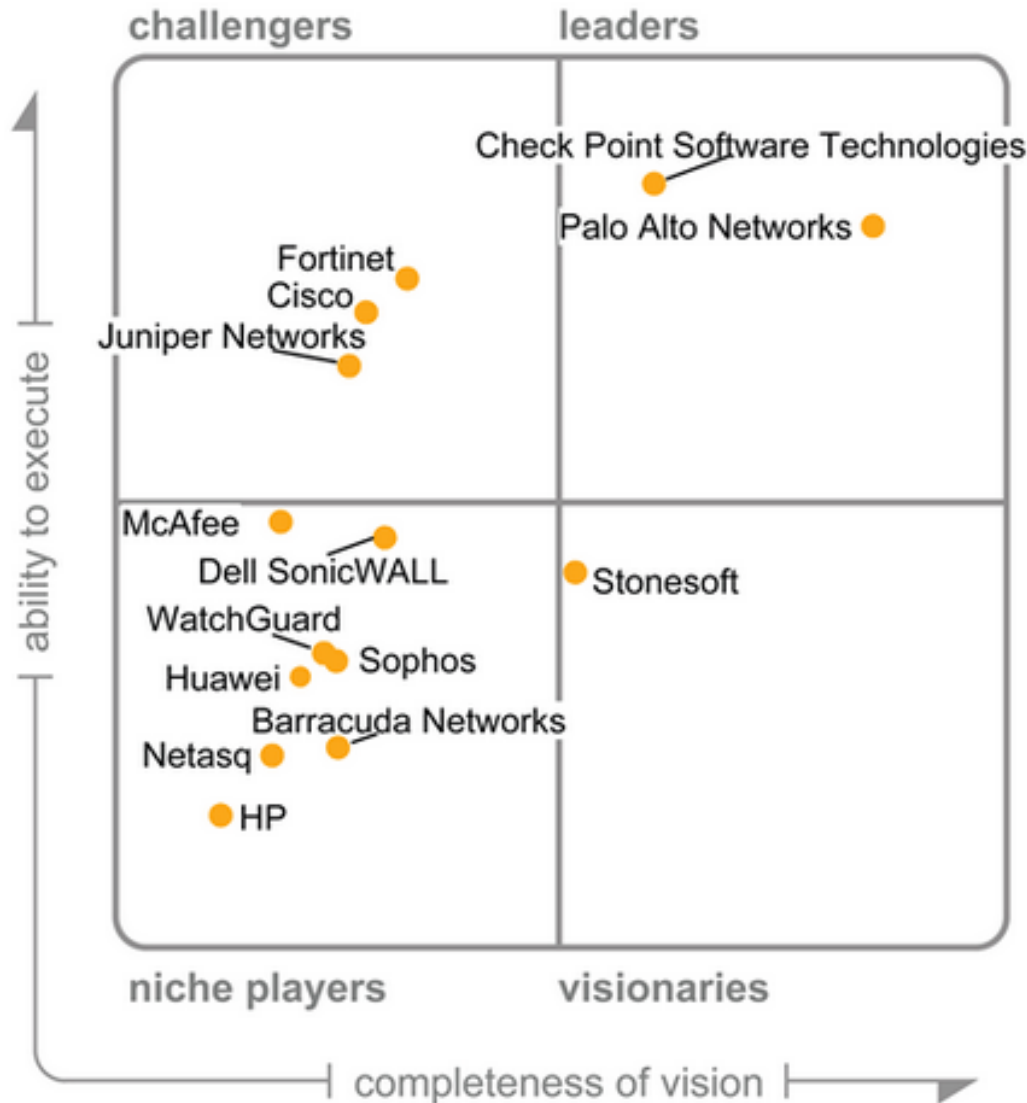


As of December 2011



가트너 매직 쿼드런트

· Magic Quadrant for Enterprise Network Firewalls



As of February 2013

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Who should you trust to secure your business?

Source: Gartner (April 2014)



SOFTWARE-DEFINED PROTECTION

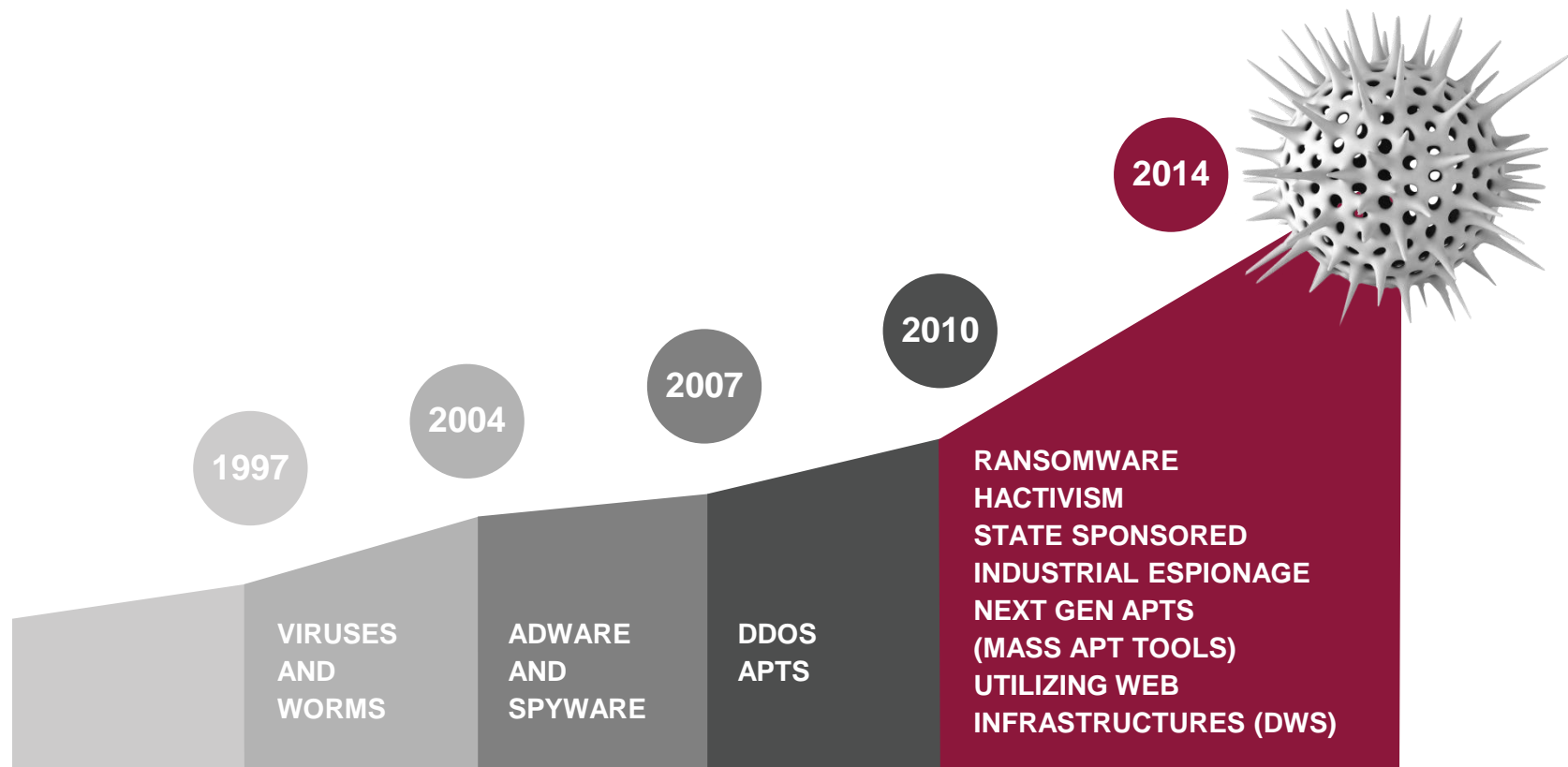
TECHNOLOGY IS **EVERYWHERE**



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

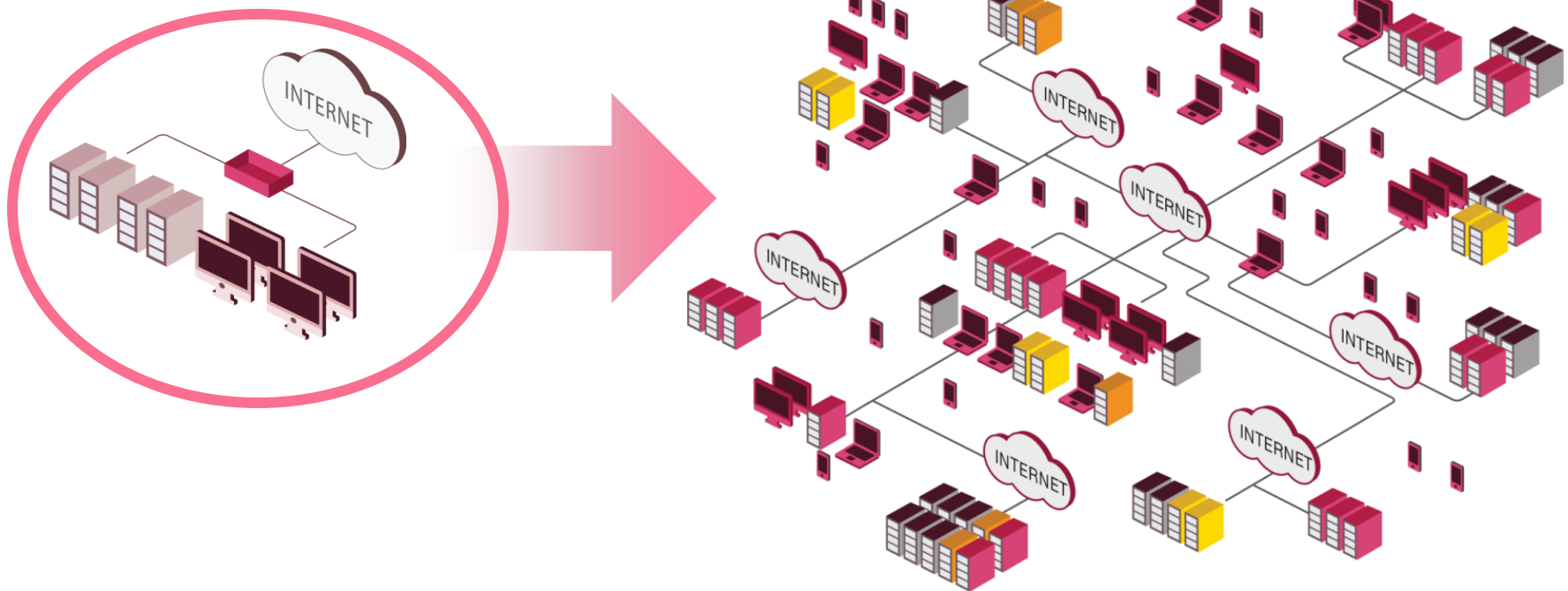
ADOBE READER	\$5,000
MAC OSX	\$20,000
ANDROID.....	\$30,000
FLASH OR JAVA.....	\$40,000
MICROSOFT WORD	\$50,000
WINDOWS.....	\$60,000
FIREFOX OR SAFARI	\$60,000
CHROME OR INTERNET EXPLORER.....	\$80,000
IOS.....	\$100,000



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

EVOLVING AND COMPLEX IT ENVIRONMENTS

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



HOW TO **SECURE** SUCH AN ENVIRONMENT?



- IPS
- VPN
- URLF
- App Control
- Anti-virus
- Anti-Spam
- Firewall
- DDoS
- Mobile Security
- Anti-Bot

HOW TO PROTECT AND MANAGE SUCH ENVIRONMENTS?

WE NEED SECURITY
that is

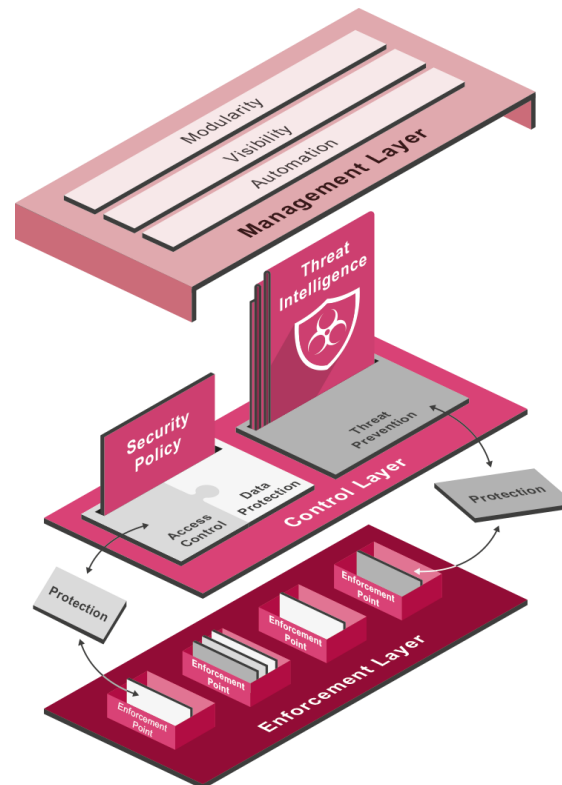
MODULAR
AGILE
SECURE!!!



Introducing

SOFTWARE –DEFINED PROTECTION

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



SOFTWARE – DEFINED PROTECTION

MANAGEMENT LAYER

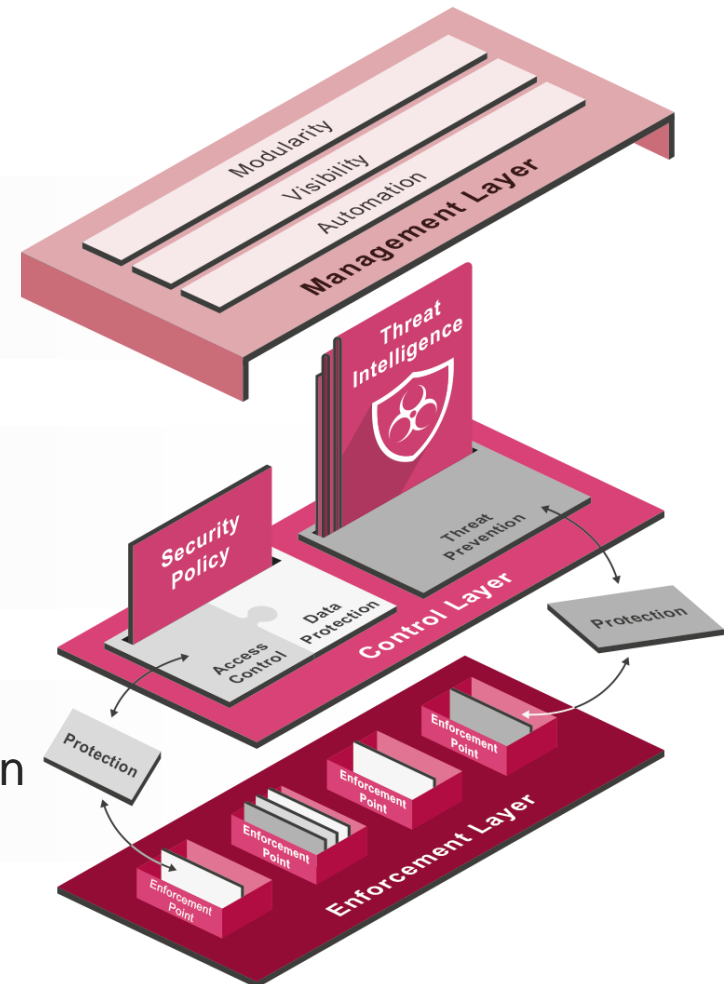
Integrates security with business process

CONTROL LAYER

Delivers real-time protections to the enforcement points

ENFORCEMENT LAYER

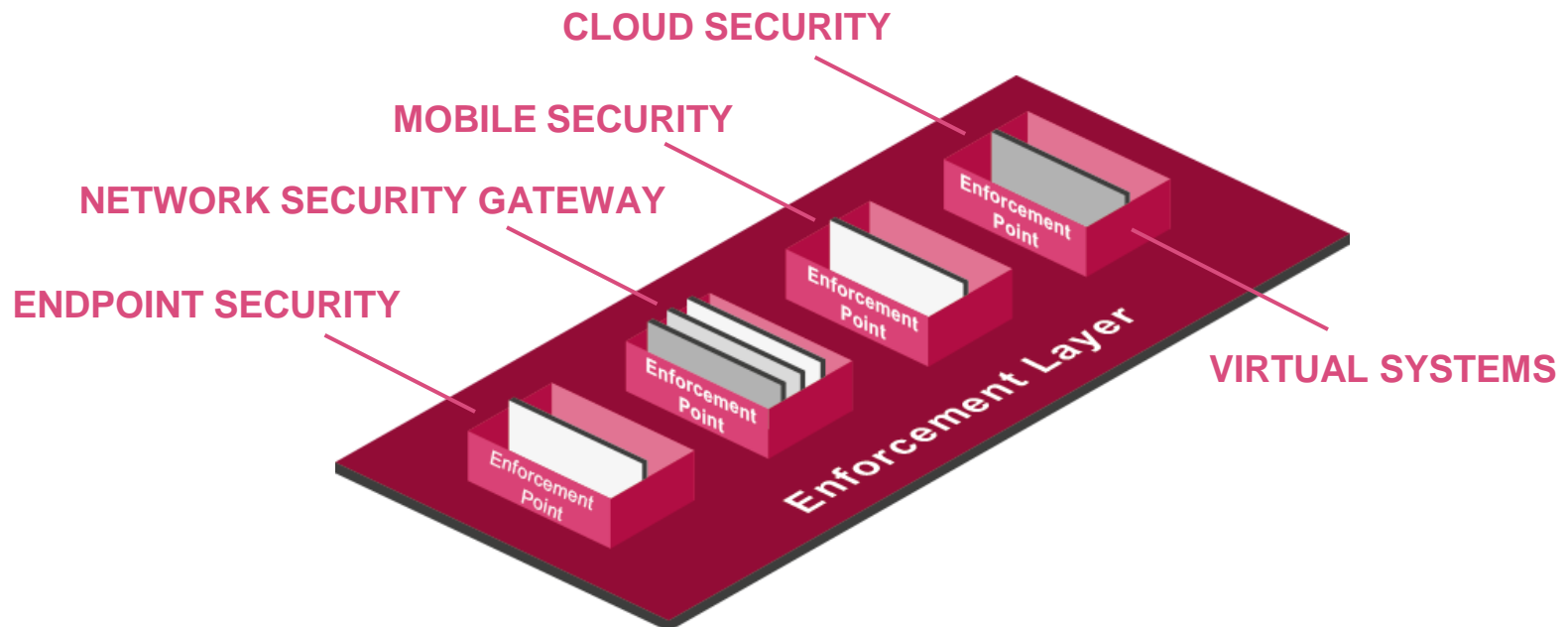
Inspects traffic and enforces protection in well-defined segments



ENFORCEMENT LAYER

ENFORCEMENT LAYER

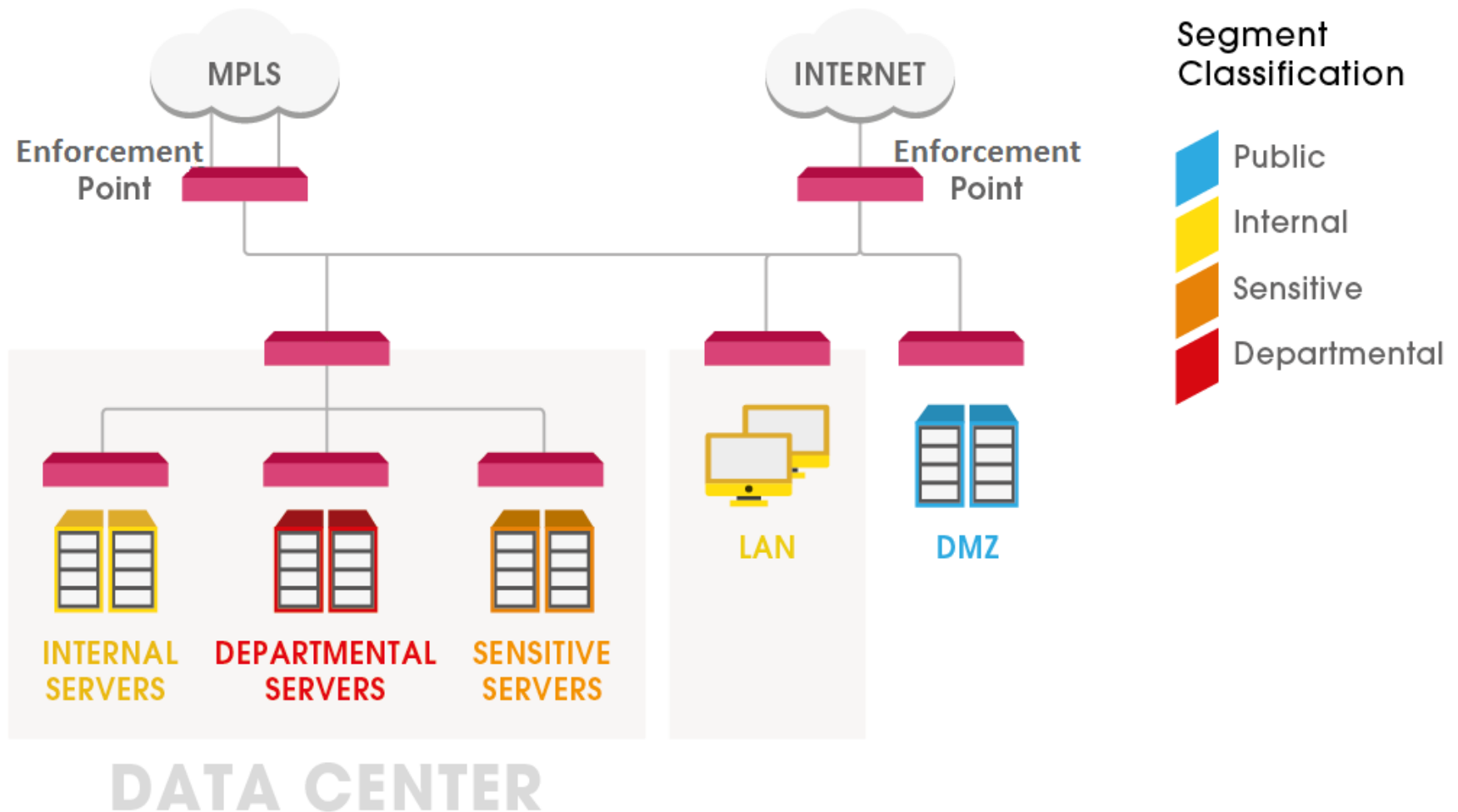
Enforcement points **MEDIATE** interactions between users and systems
and **EXECUTE** protections



SEGMENTATION IS THE NEW PERIMETER



SEGMENTATION IS THE NEW PERIMETER



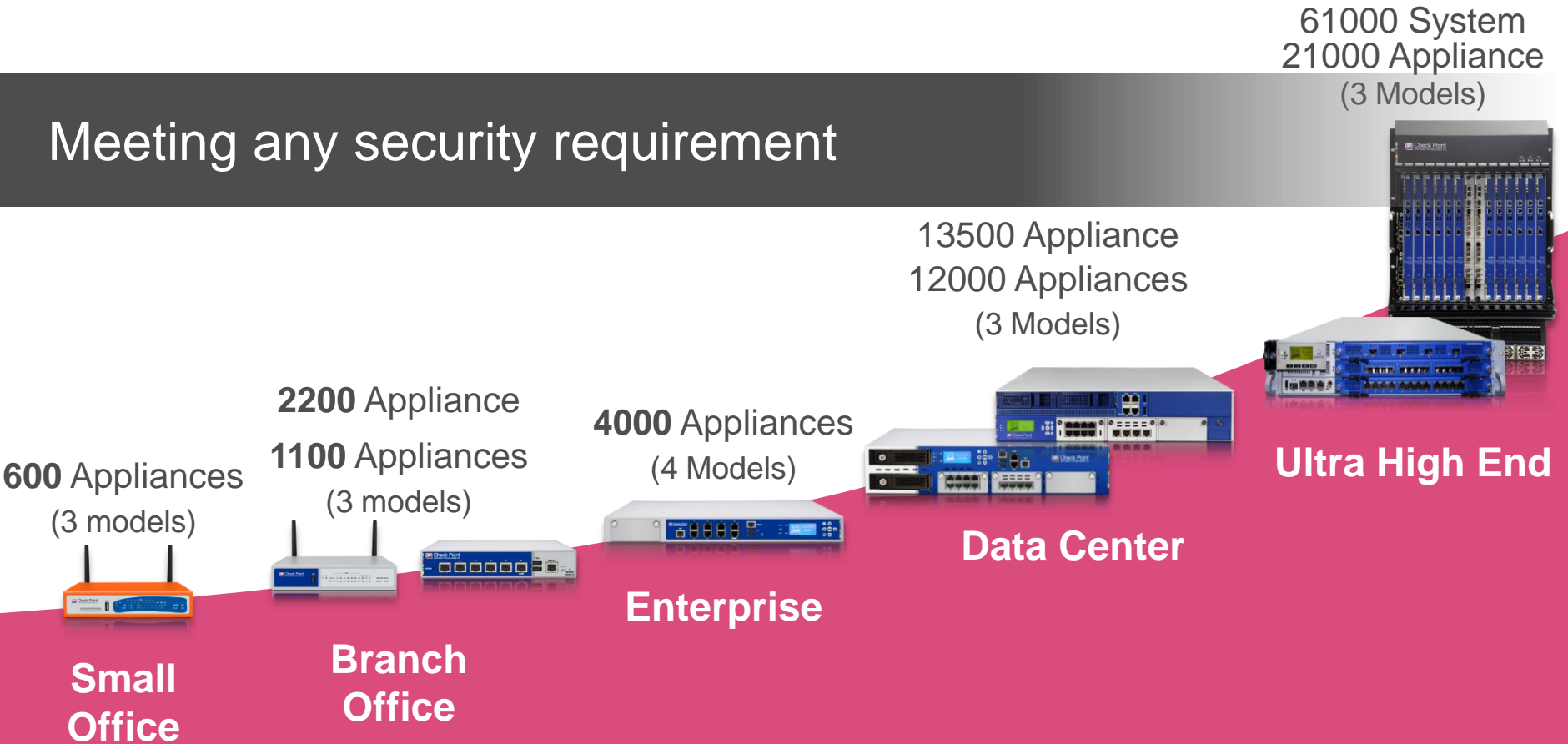
ENFORCEMENT LAYER

Of Check Point



SECURITY GATEWAYS

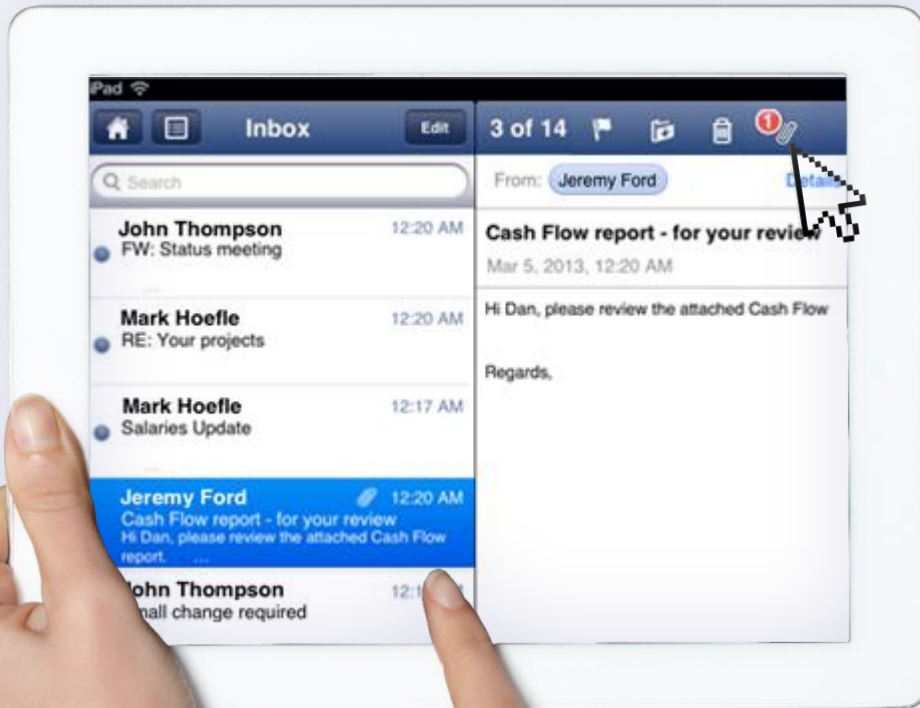
Meeting any security requirement





Use Business Data within a Secure Business Application

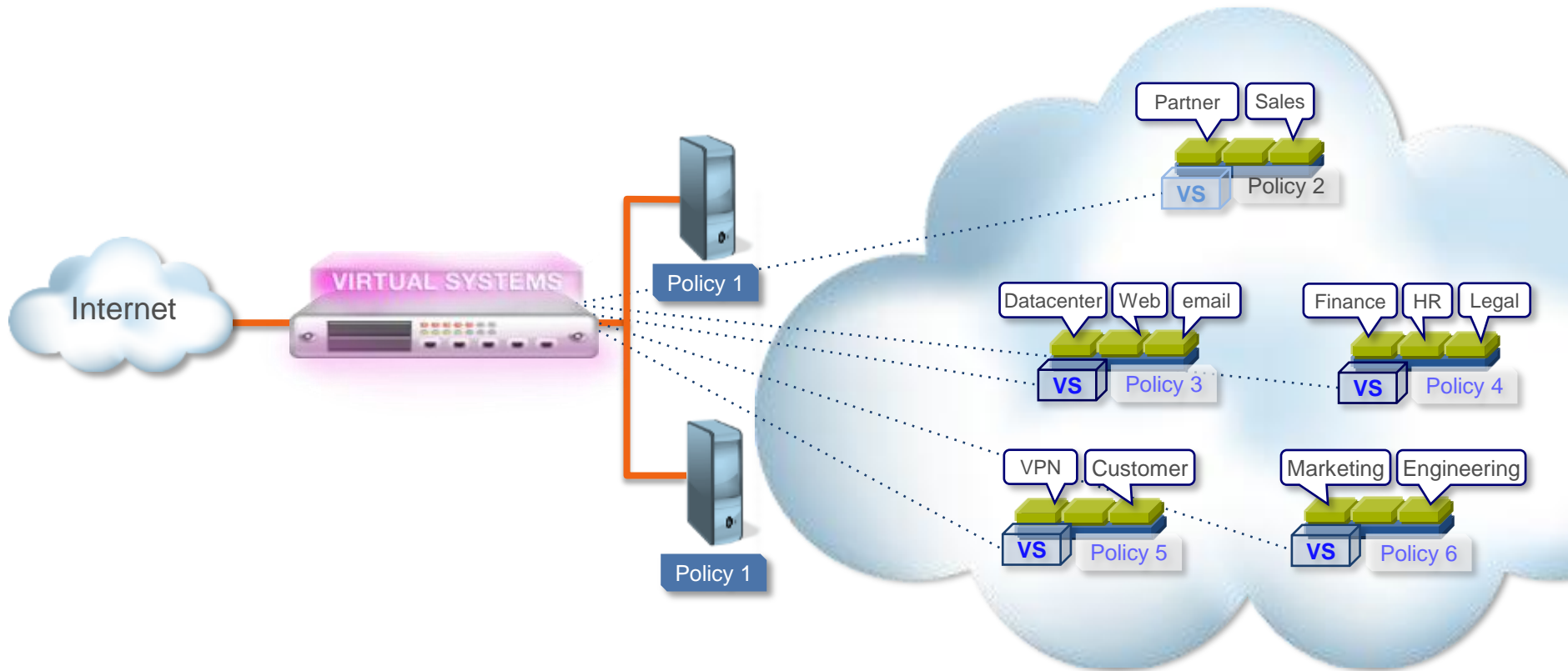
Only Authenticated Users
Access the Business Container



Use Business Data within a Secure Business Application

Use Emails Securely

Use Documents Securely

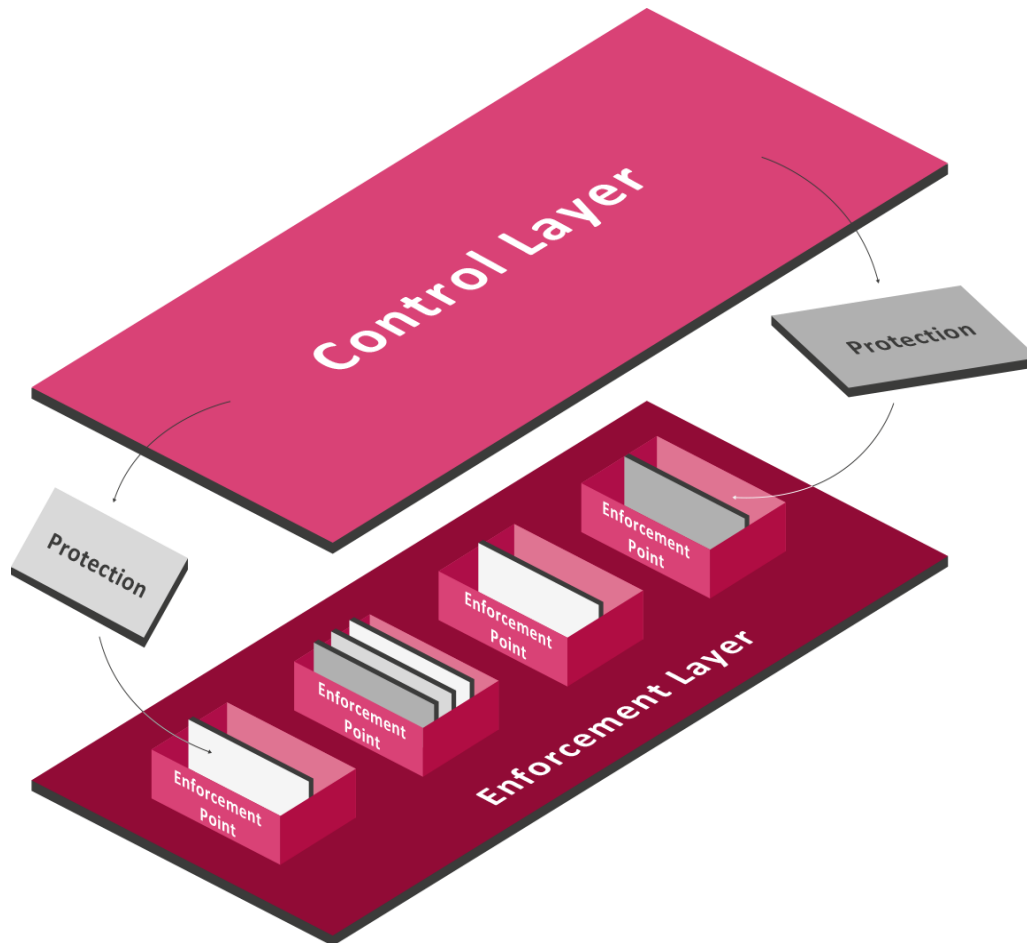


Virtualized Gateways Simplify Private Cloud Security

CONTROL LAYER

CONTROL LAYER

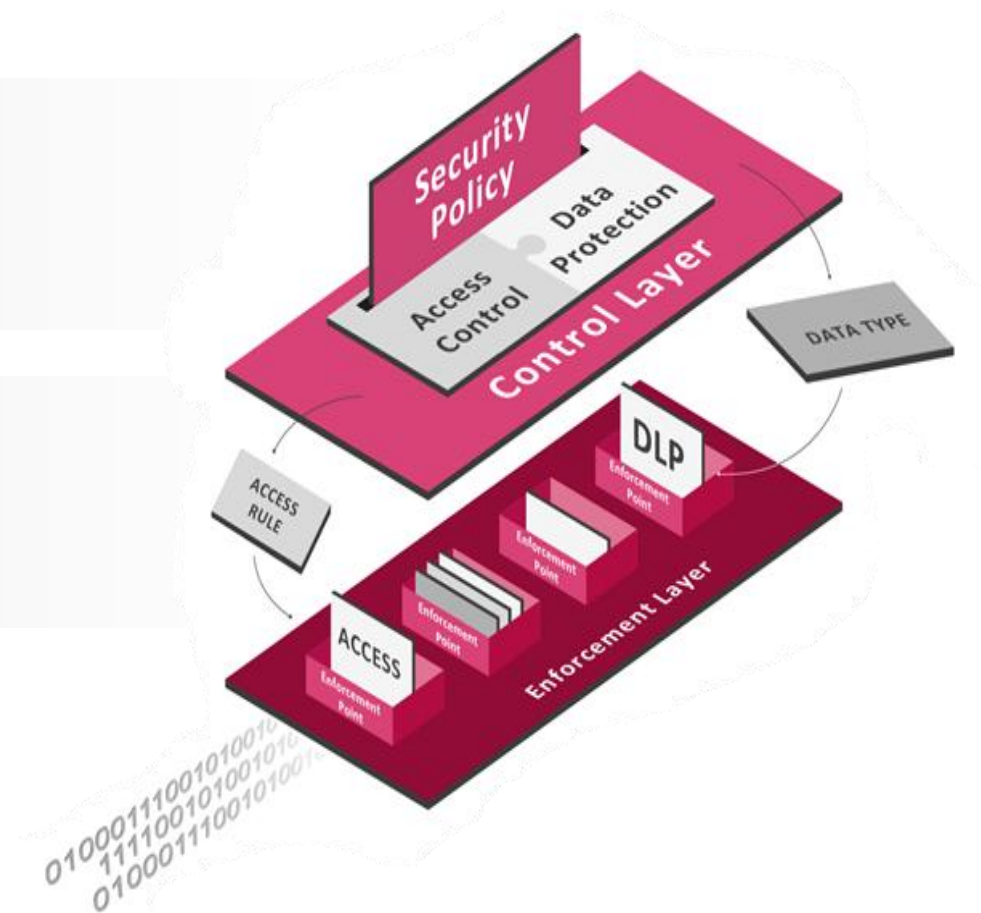
Generate PROTECTIONS



ACCESS CONTROL AND DATA PROTECTION

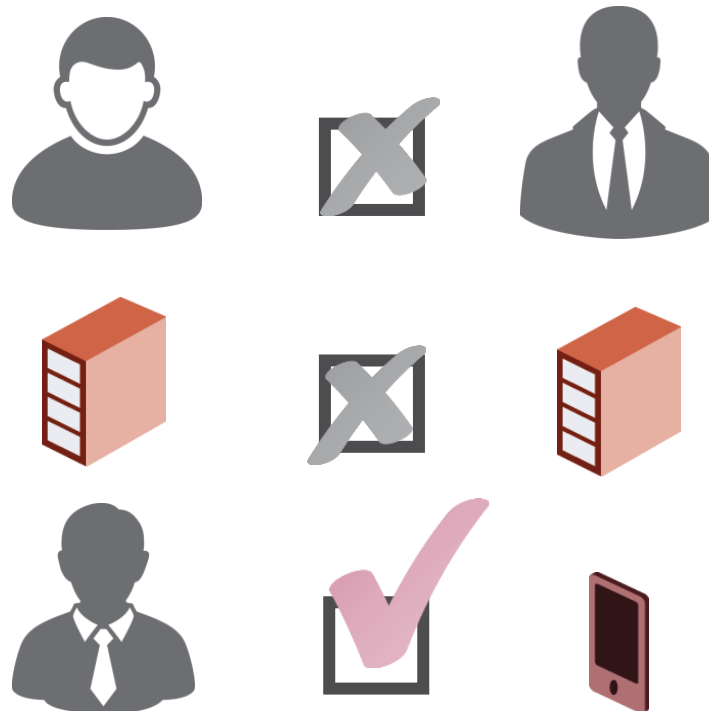
Control interactions
between users, assets,
data and applications

Protect data in
motion and at rest



NEXT GENERATION FIREWALL

Controls interactions between **USERS, ASSETS, DATA** and **APPLICATIONS**



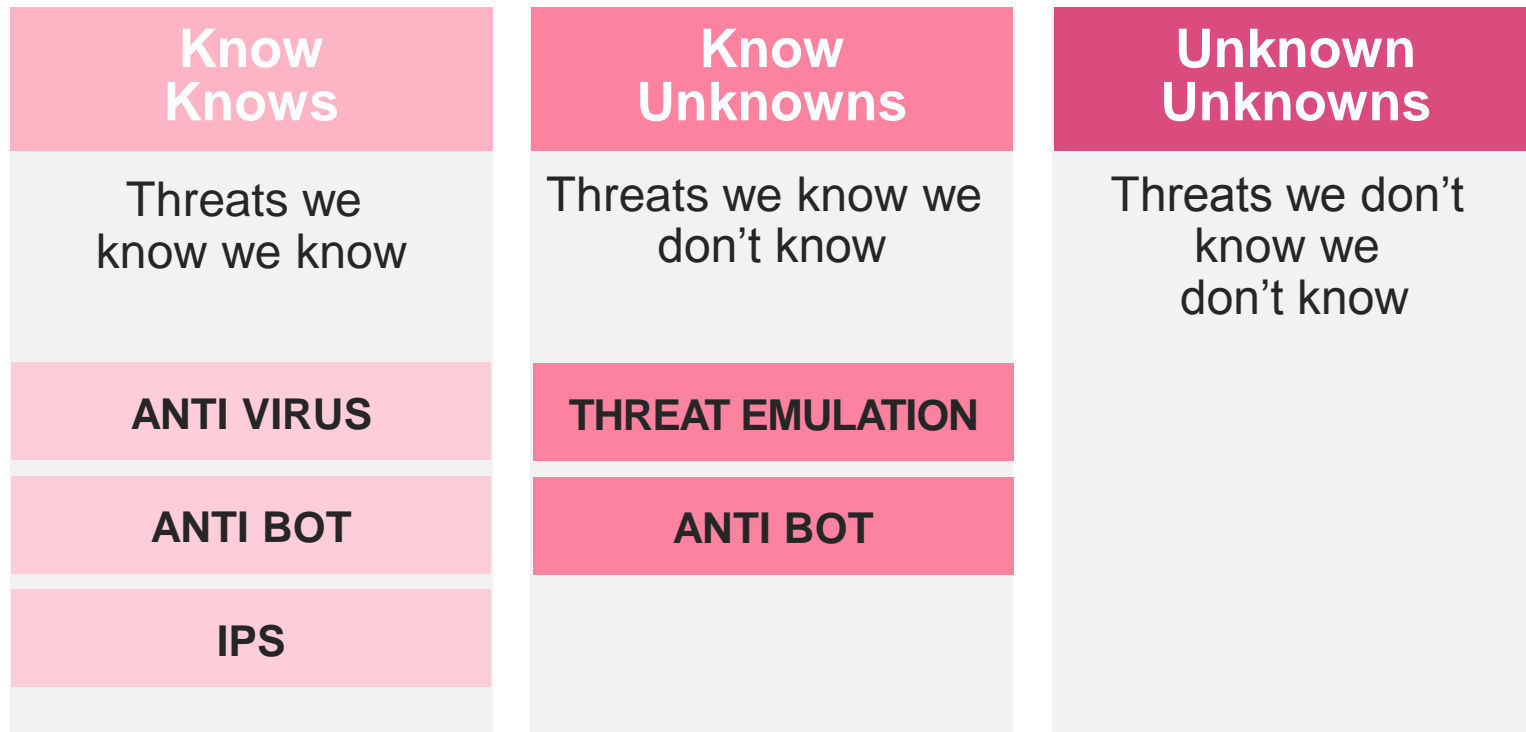
**MOST ORGANIZATIONS ARE
USING FIREWALLS TODAY
AND IT WORKS QUITE
WELL...**

BUT...



WHAT ABOUT PROTECTING AGAINST THE BAD GUYS?

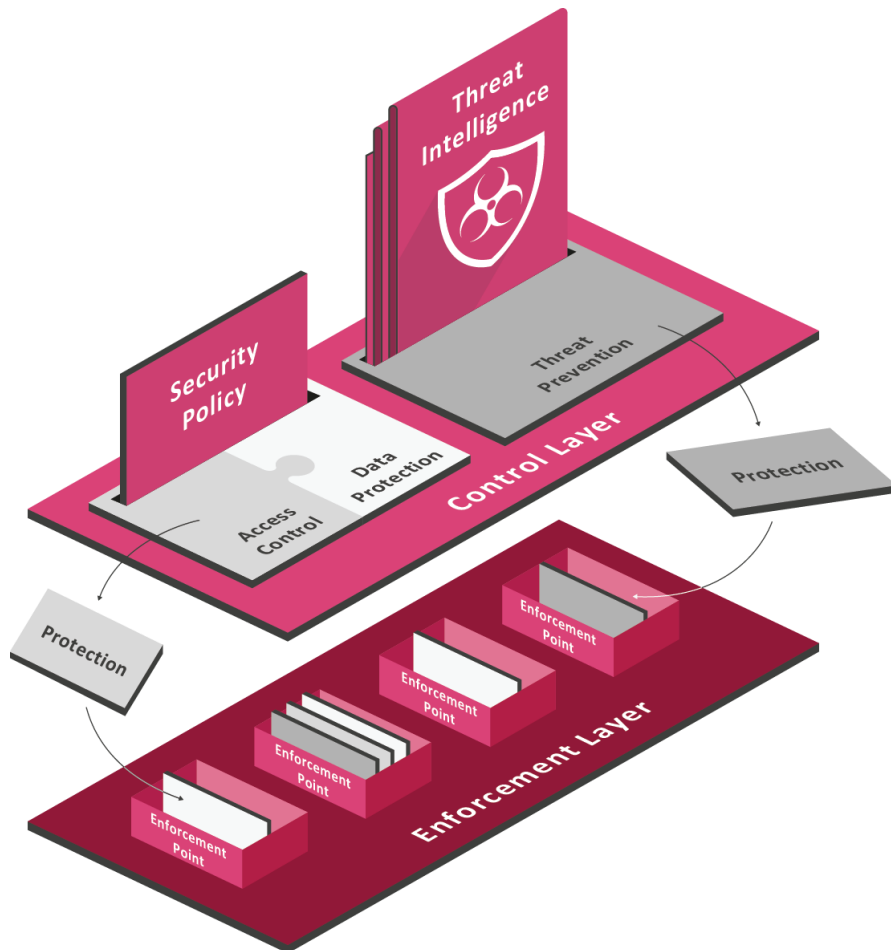
THE THREATS WE NEED TO PREVENT



WHAT IS NEEDED?

THREAT PREVENTION

Updated protections in **REAL-TIME**



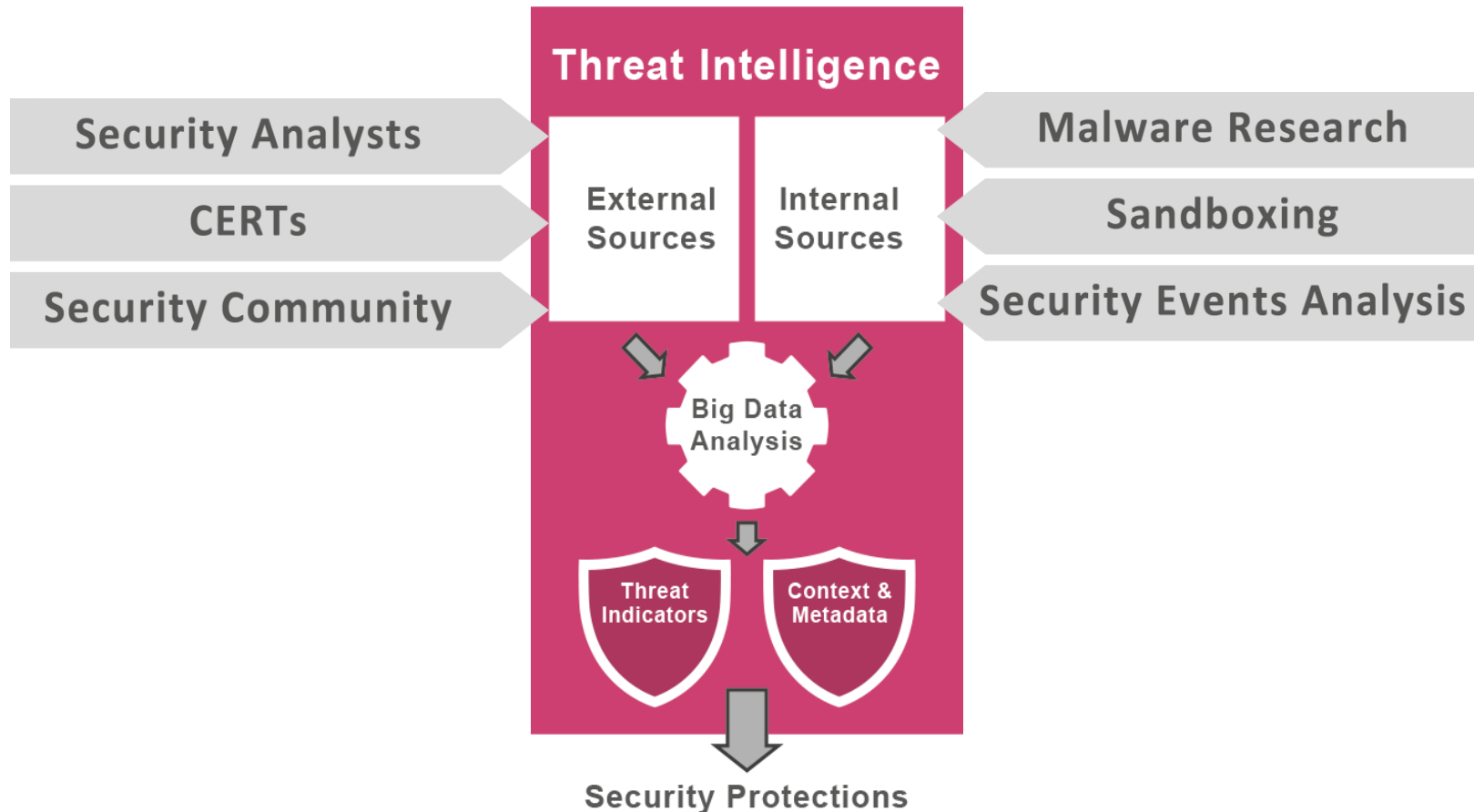
Utilizing the same enforcement points for real time dynamic Threat Prevention protections

EFFCTIVE THREAT PREVENTION IS BASED ON INTELLIGENCE



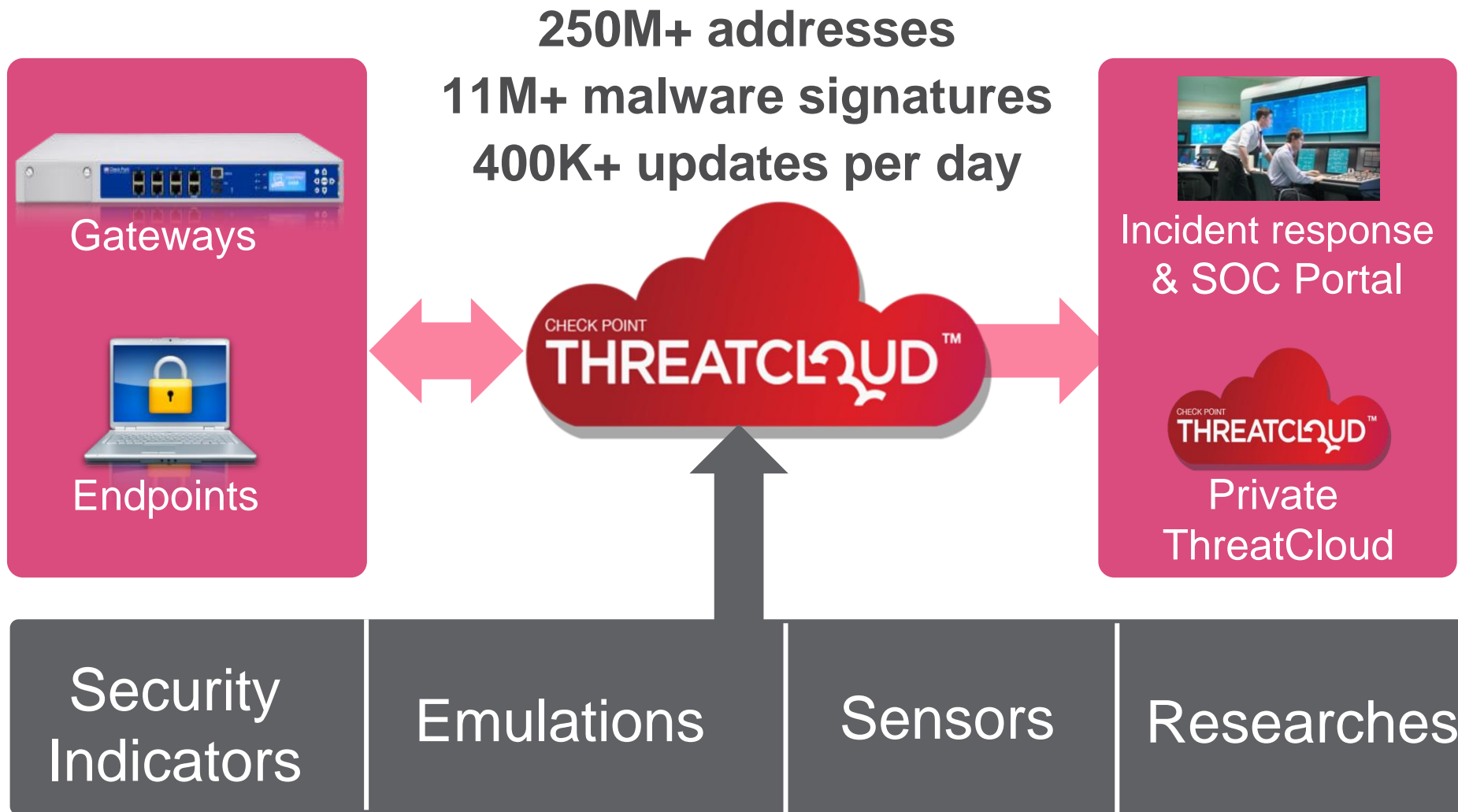
THREAT INTELLIGENCE

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



ThreatCloud

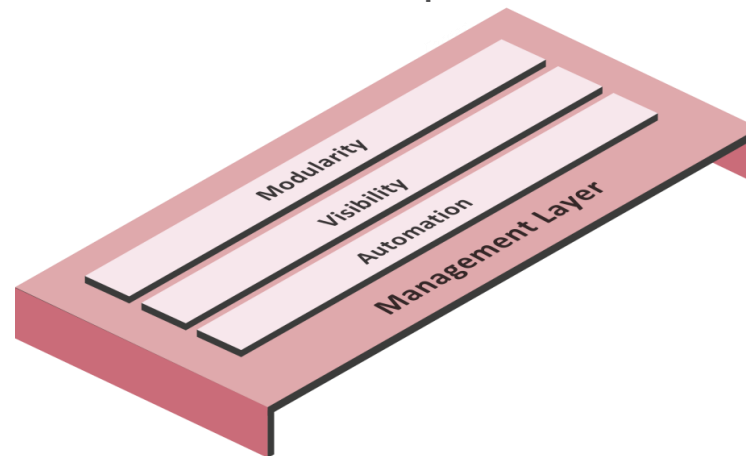
Global collaboration to fight threats



MANAGEMENT LAYER

MANAGEMENT LAYER

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



MODULARITY

AUTOMATION

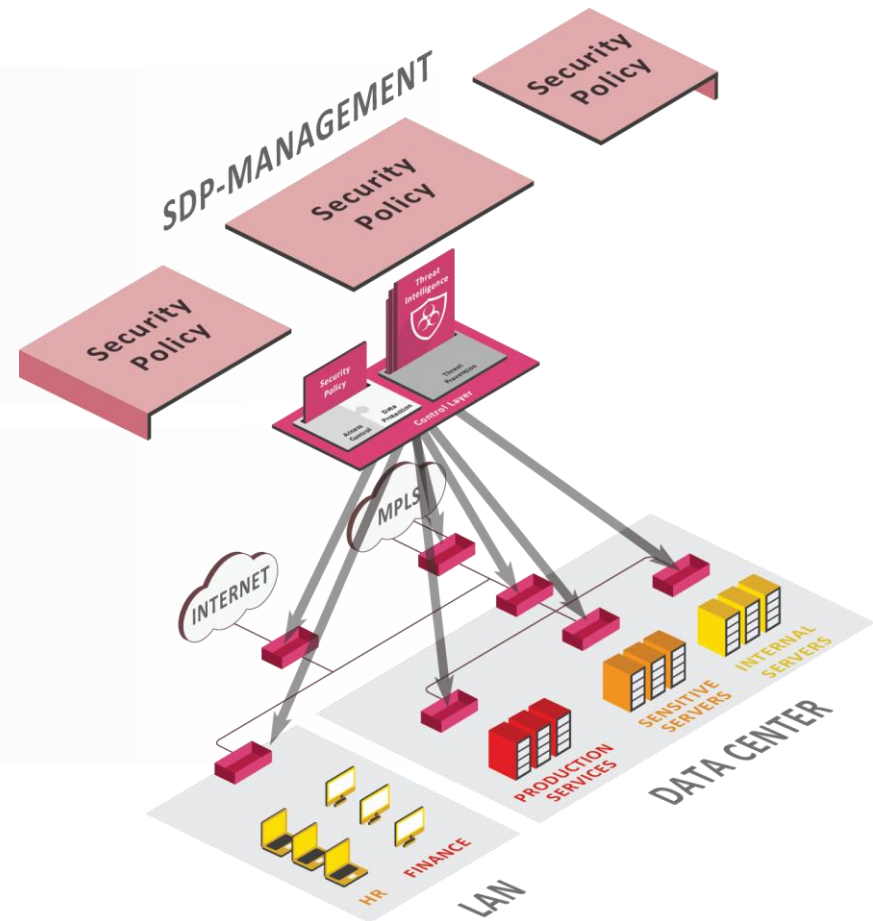
VISIBILITY

MODULARITY

ENDLESS FLEXIBILITY with LAYERS of POLICIES

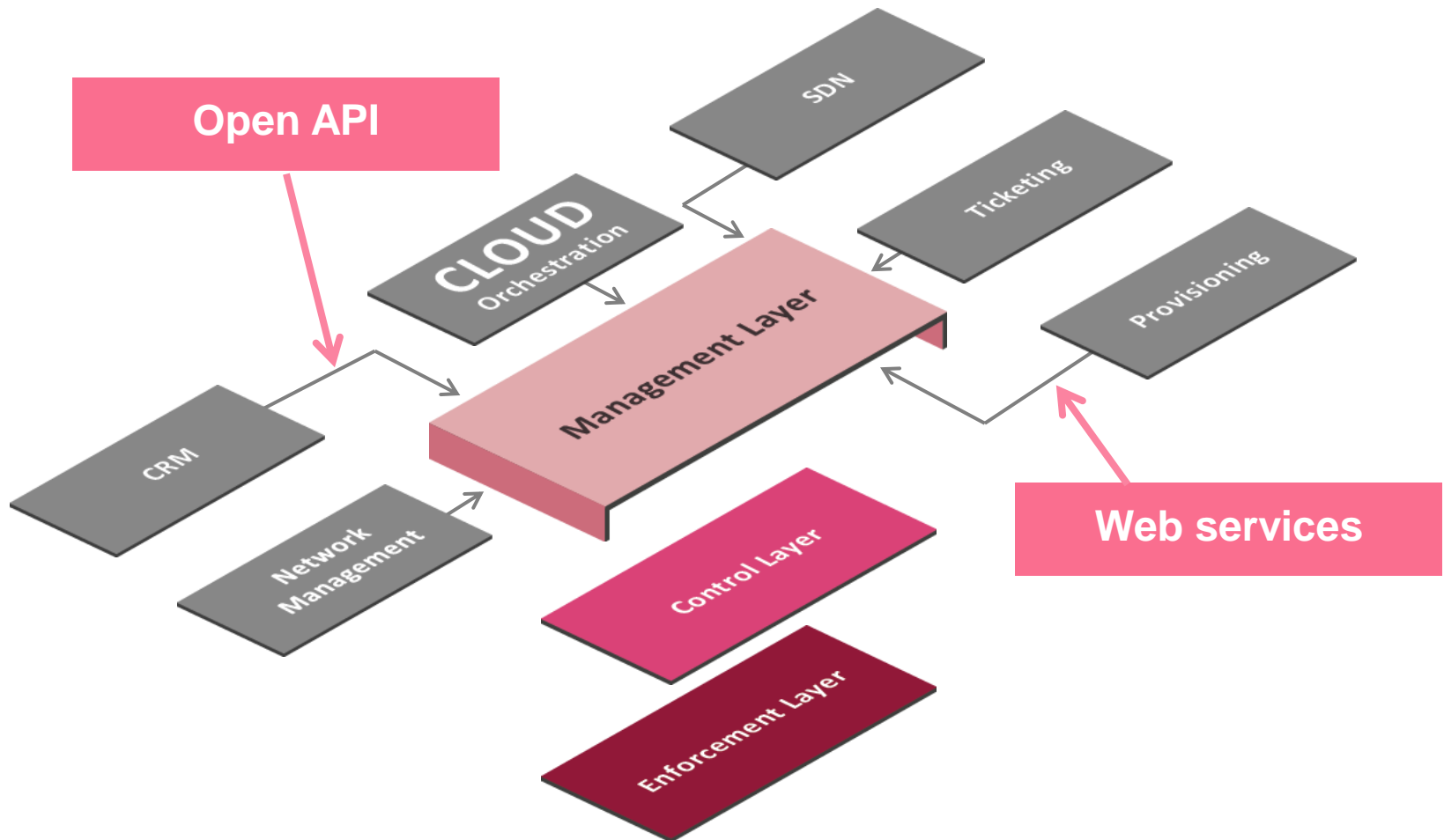
Management modularity provides the flexibility to manage each segment and control

Segregation of duties
Layers of policy



AUTOMATION

OPEN INTERFACES support business process changes



SDP AND SDN WORKING IN SYNERGY

SDN

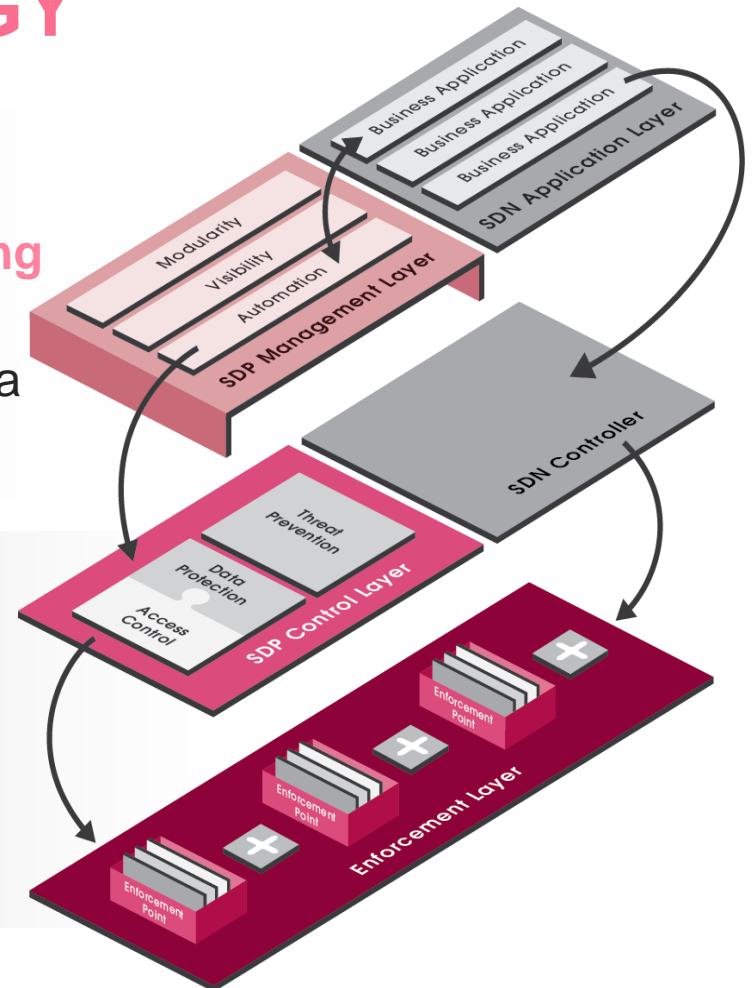
An emerging network architecture, decoupling network control and data planes.

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

SDP

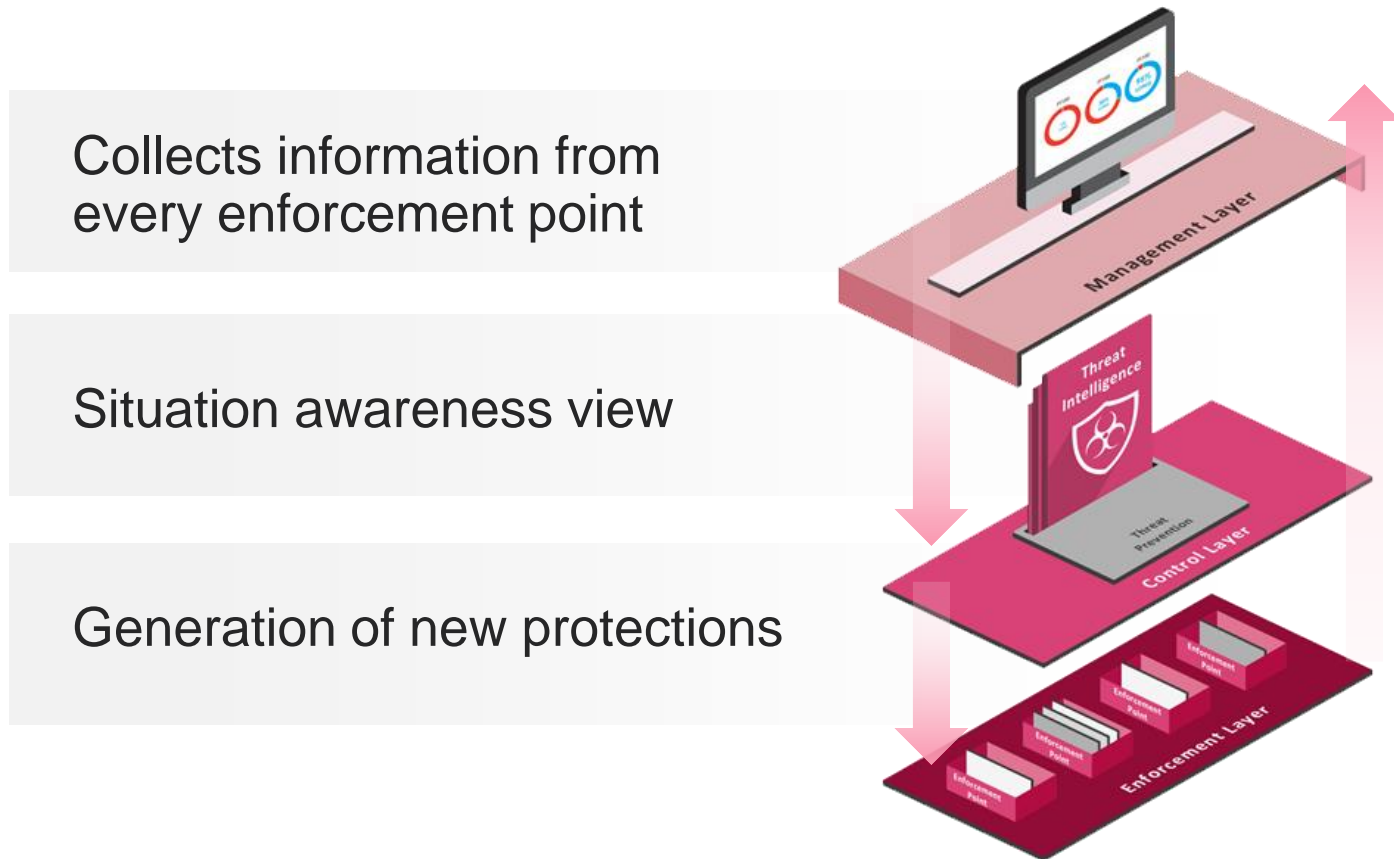
An overlay architecture enforcing security traffic flows within an SDN network

Data flows are programmed to pass through SDP enforcement points



VISIBILITY

SITUATION AWARENESS & INCIDENT RESPONSE



Delegation and Segregation of Duties

Granular Privileges

No.	Name	Protected Scope	Protection/Site	Action	Track	Install On
1	Secure network with all threat capabilities	RNDNetwork	N/A	Recommended_Profile ⌵ ⌵ ⌵	Log	* Policy Targets
2	Threat emulation special rule for Sales server	SalesServer	N/A	Threat Sales Profile ⌵ ⌵ ⌵	Log	* Policy Targets



Can manage IPS only

No.	Name	Source	Destination	Services	Action
1	all web traffic	* Any	* Any	TCP HTTP_and_...	⊕ Accept
2	Allow Michael access to BYC Site	Michael	BYCSite	* Any	⊕ Accept
3	allow 4 admins reach everything	Billi Alex John Bob	* Any	* Any	⊕ Accept



Can manage Branch Office Access Policy only

Simultaneous Admins

9	Drop other connectivity to perimeter gateway	* Any	Perimeter-GW	* Any	Drop
10	allow LAN and gateway access to	Perimeter	* Any	TCP http	⊕ Accept
9	Drop other connectivity to perimeter gateway	* Any	Perimeter-GW		
12	allow Corporate Email access to Anti-Spam	MailServer	COMAntiSPAM	TCP smtp	⊕ Accept
13	allow NY office all access	RemoteO...	* Any	* Any	⊕ Accept
14	allow LAN to remote office NY	LANsGroup	RemoteOffic...	* Any	⊕ Accept
15	allow Bob and Alice access NY Office	Alice Bob	RemoteOffic...	* Any	⊕ Accept

Locked By Current Session

Locked Object
Locked By: ariel
Locked On: 19/12/2013 08:31:33



Connected Admins & Chat

Check Point SmartConsole

Standard Package

Policy Overview

Access

Network

Web Content

NAT

Threat Prevention

1. Network 2. Web Content

Search Policy...

No.	Hits	Name	Source	Destination	VPN	Services	Action	Time	Track	Install C
1	0	all web traffic	* Any	* Any	* Any	TCP HTTP_and_...	Accept	* Any	Comple...	* Po
2	0	Allow Michael access to BYC Site	Michael	BYCSite	* Any	* Any	Accept	* Any	Log	* F
3	0	allow 4 admins reach everything	Billi Alex John Bob	* Any	* Any	* Any	Accept	* Any	Log	* F
4	0	allow 2 admins reach Cellarix via AOL	Jessica Bob	Cellarix	* Any	TCP AOL	Accept	* Any	Log	* Po
5	0	allow 2 admins reach Bosa Server	Alice Shannon	Bosa	* Any	* Any	Accept	* Any	Log	* Po
6	0	allow exchange to use smtp	ExchangeOWA	* Any	* Any	TCP smtp	Accept	* Any	Log	* Po
7	0	Drop connectivity to the Exchange Server	* Any	ExchangeOWA	* Any	TCP ssl_v3 TCP imap	Drop	* Any	Log	* Po

Details Logs

all web traffic 0

Source	Hits	Destination	Hits	Services	Hits	Install On
* Any		* Any		TCP HTTP_and_HTTPS_proxy (8080) 243		* Policy Targets

Created by: aa

Created on: Dec 17, 2013

Expiration time: Jun 10, 2014

Performance impact: Low

Ticket number: 123456

Rule requester: Johan Smith

Online Users

Joe

E-mail

Mobile

ariel

E-mail

Mobile

Did you create the new rule 177?

Enter your command or 'help' for usage

No Tasks In Progress

Joe 2 online users

172.23.26.11



Sessions Management

Recognized * Any * All

You have 4 Active Sessions

Continue Current Session
Ticket 87-598-45A

Recent Sessions (4)

Create New Session...

Search

Applications	Service
Any Recognized	* Any
Any Recognized	TCP HTTP
Any Recognized	* Any
Any Recognized	TCP TCP
	TCP HTTP
Any Recognized	* Any

12:35
Changed IP of Network object R&D network from 192.168.32.0 to 192.174.54.0

12:35
Added Tag VIP to host object CEO Host

Very SmartWorkflow

Robert R.
11/7/13
Added service:
http_and_https_proxy

Rule	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
3	Remote Access	Mobile-vpn-user@Any	* Any	RemoteAccess	CIFS TCP http TCP https TCP imap TCP http_and_https_proxy	Accept	Log	* Any	* Any
3	Remote Access	Mobile-vpn-user@Any	* Any	RemoteAccess	CIFS TCP http TCP https TCP imap	Accept	Log	* Any	* Any

Robert R.
11/7/13
Added destination:
Corporate-mis

Rule	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
7	Critical Subnet	Corporate_internal_net	Corporate-finance Corporate-hr Corporate-qa Corporate-rmd Corporate-mis	* Any	* Any	Accept	Log	Corp. GW	* Any
7	Critical Subnet	Corporate_internal_net	Corporate-finance Corporate-hr Corporate-qa Corporate-rmd	* Any	* Any	Accept	Log	Corp. GW	* Any

12.10.10.1



Decisions tools

Check Point SmartConsole | Demo Mode

VPN Access Policy 1 | NY VPN Access Policy 2 | Identity Based Policy | Common Policy - All Sites

Access 201 | Nat 49 | Threat Prevention 12

MONITOR 7 | Tech Support 3 | Finance All 18

Summary | Details | Logs

Source

- IT-Group
 - Remote-1-gw | 172.16.2
 - Remote-2-gw | 192.168
 - Remote-3-gw | 172.16.1
 - Net-6 | 10.14.1
 - Finance-net

Expire rules with no hits
 automatically expired rules after 6 months with no hits

Time Period

Start

- Immediately
- At: 08/01/2014 14:28

End

- Never
- At: 08/01/2014 14:28
- After: 6 months with no rule hits

Recurring (Advanced)

Add Tag

OK Cancel

Date created: 10/5/2013

Expiration Time: After 6 months with no hits

Hit Count: 20M

Josh Green | 192.10.10.1

Enter script or your commands

Tasks 5 | Josh Green | 192.10.10.1



Automation – using the Rest API

Sample API: Policy

https://172.23.26.11:8443/sample1/

Check Point Rule Base Client Demo R80

Add Rule Status: Disconnect Refresh Publish

Add a new rule

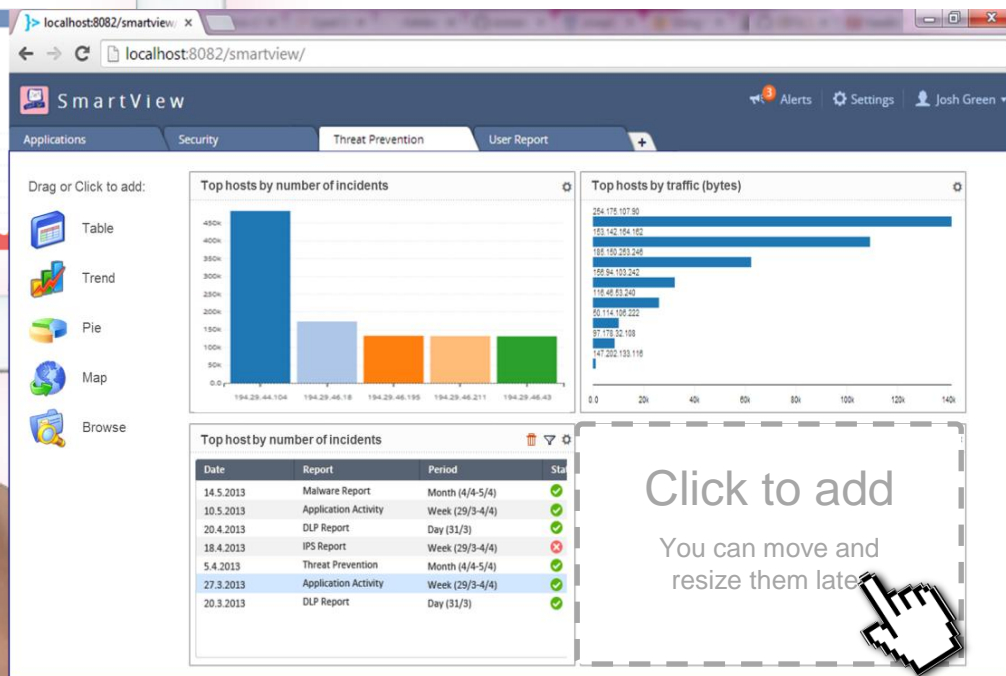
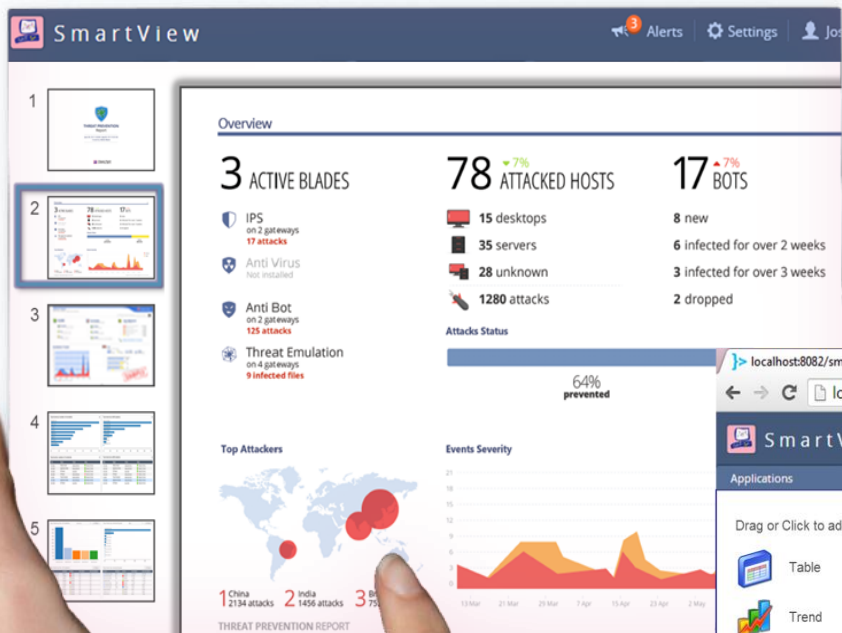
#	Name	Source	Destination	VPN	Service	Action	Options
1							Delete
2	Rule Name	Any	Any	Any	Any	drop	Delete
3	connectivity to the Exchange Server						Delete

Add Rule Cancel



Web-based monitoring and reporting system

Customized views
Logs and Reports
Access from PC and
Tablets



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

THANK YOU!