차세대보안 구축 청사진

SOFTWARE-DEFINED PROTECTION

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

CHECK POINT

$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)

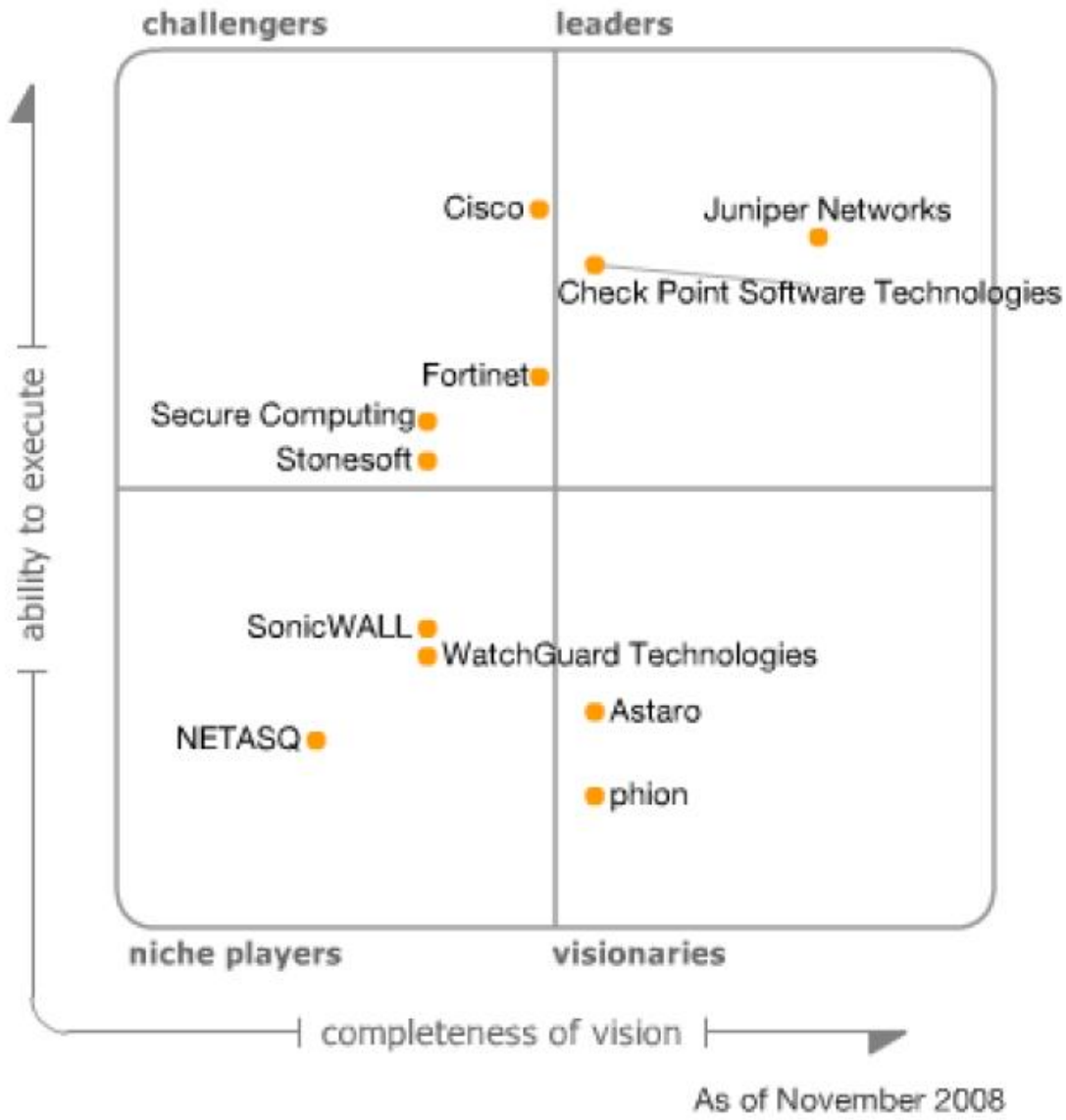
Top Ranked NGFW by NSS Labs, Gartner, SC Magazine

“Leader” in Gartner Enterprise Firewall for 17th year

가트너 매직 쿼드런트

Check Point SOFTWARE TECHNOLOGIES LTD.

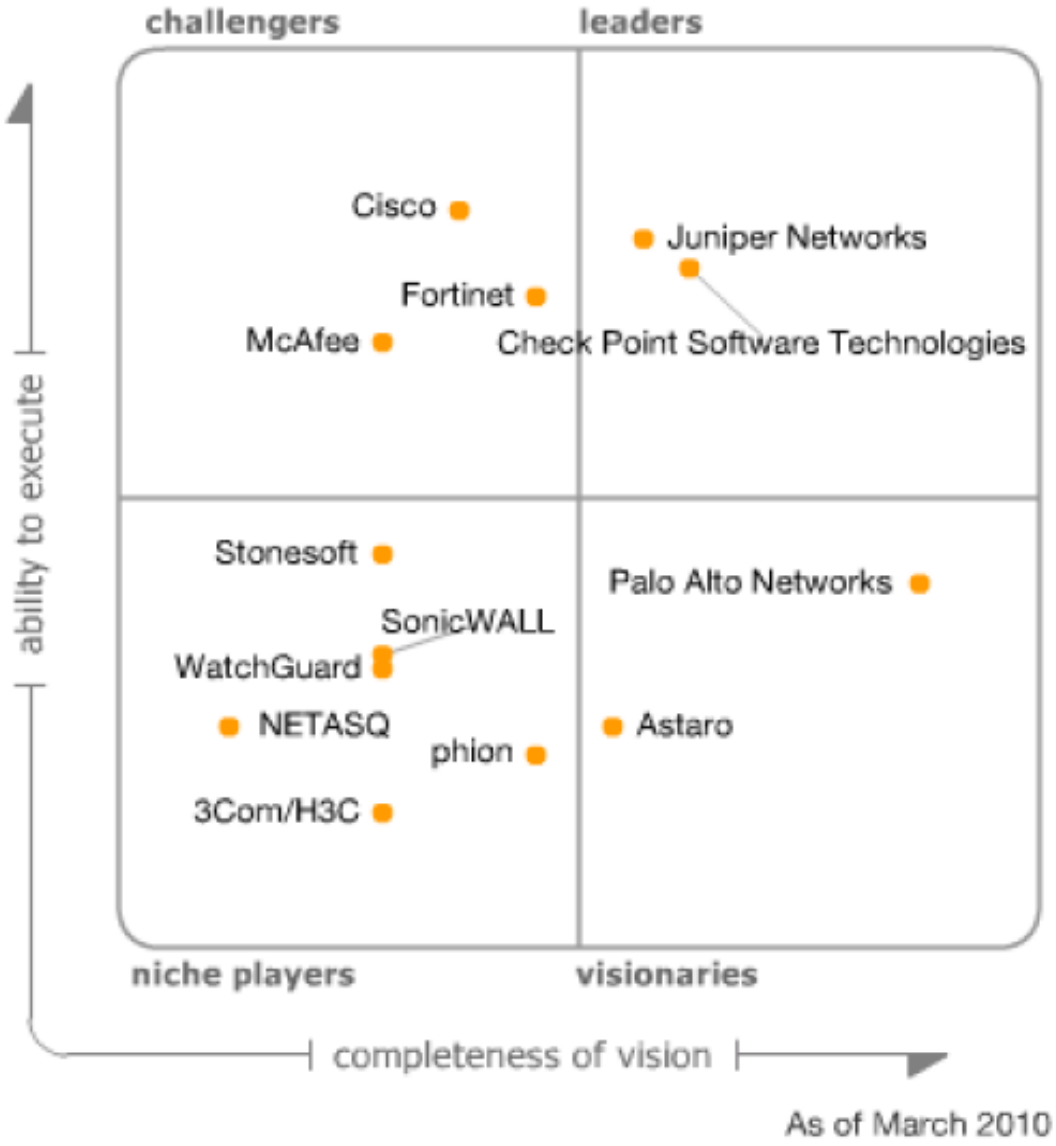
. Magic Quadrant for Enterprise Network Firewalls



가트너 매직 쿼드런트

Check Point SOFTWARE TECHNOLOGIES LTD.

. Magic Quadrant for Enterprise Network Firewalls



가트너 매직 쿼드런트

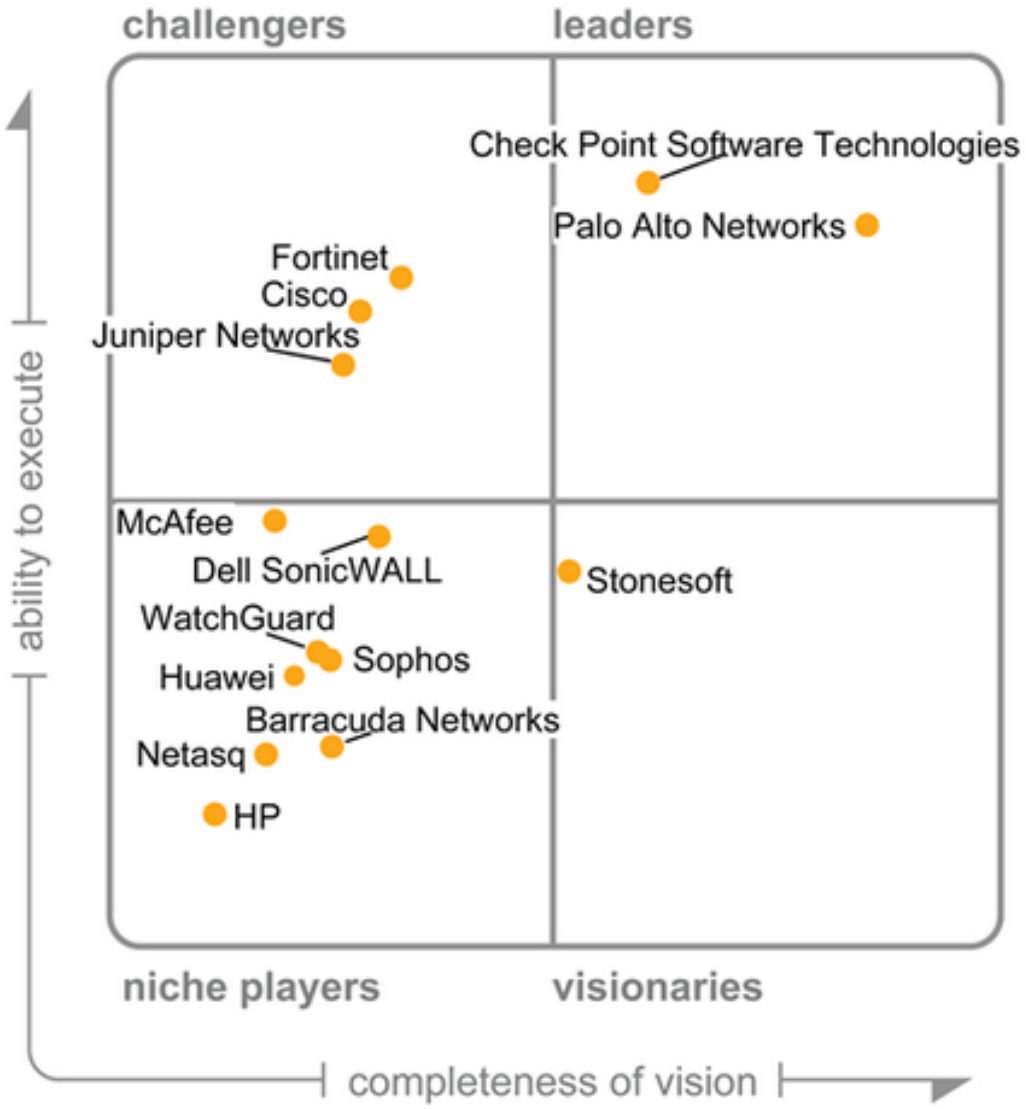
Check Point SOFTWARE TECHNOLOGIES LTD.

. Magic Quadrant for Enterprise Network Firewalls

가트너 매직 쿼드런트

Check Point SOFTWARE TECHNOLOGIES LTD.

. Magic Quadrant for Enterprise Network Firewalls



As of February 2013

가트너 매직 쿼드런트

Check Point SOFTWARE TECHNOLOGIES LTD.

Figure 1. Magic Quadrant for Enterprise Network Firewalls

Source: Gartner (April 2014)

Who should you trust to secure your business?

SOFTWARE-DEFINED PROTECTION

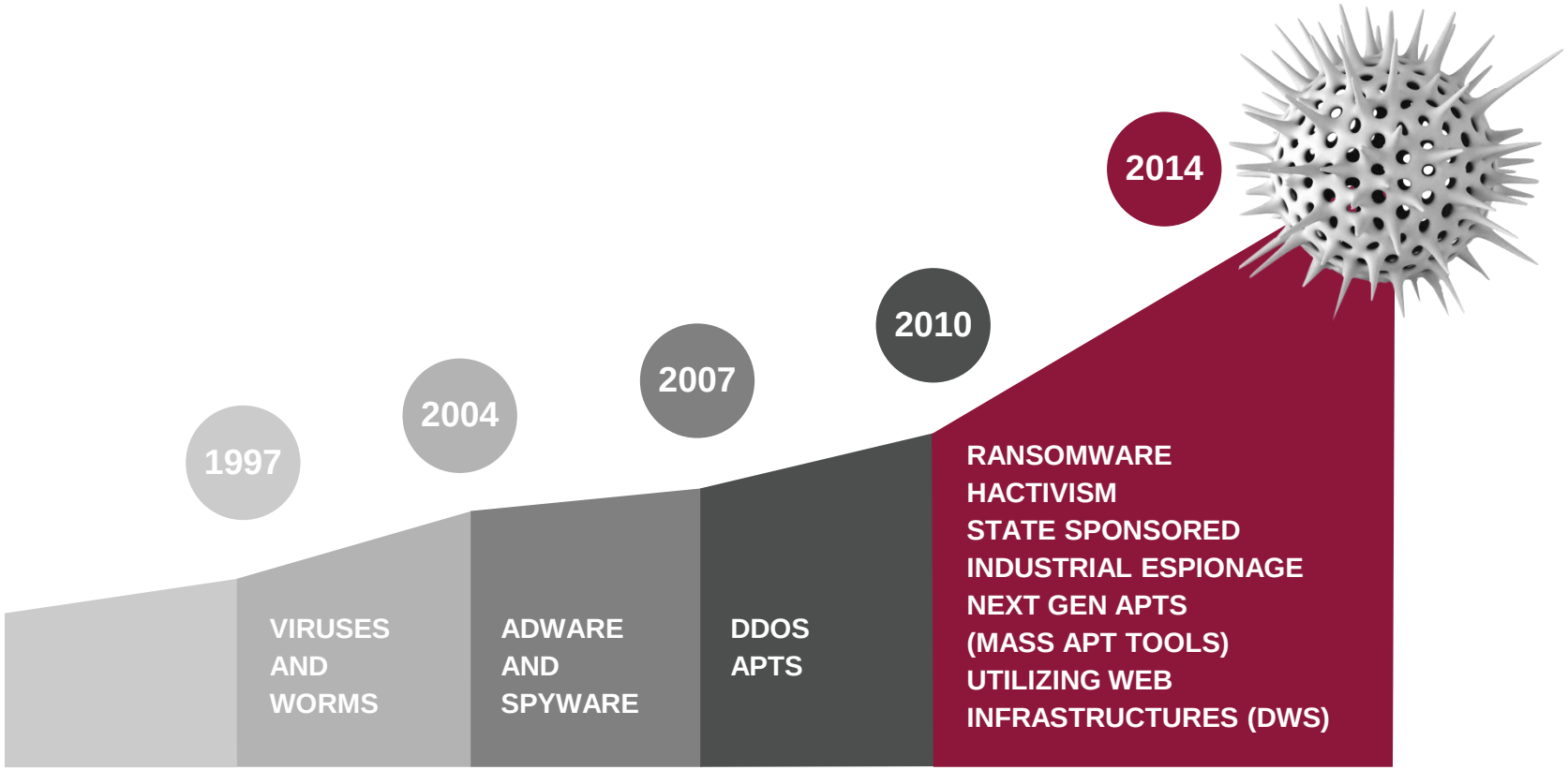
Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

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

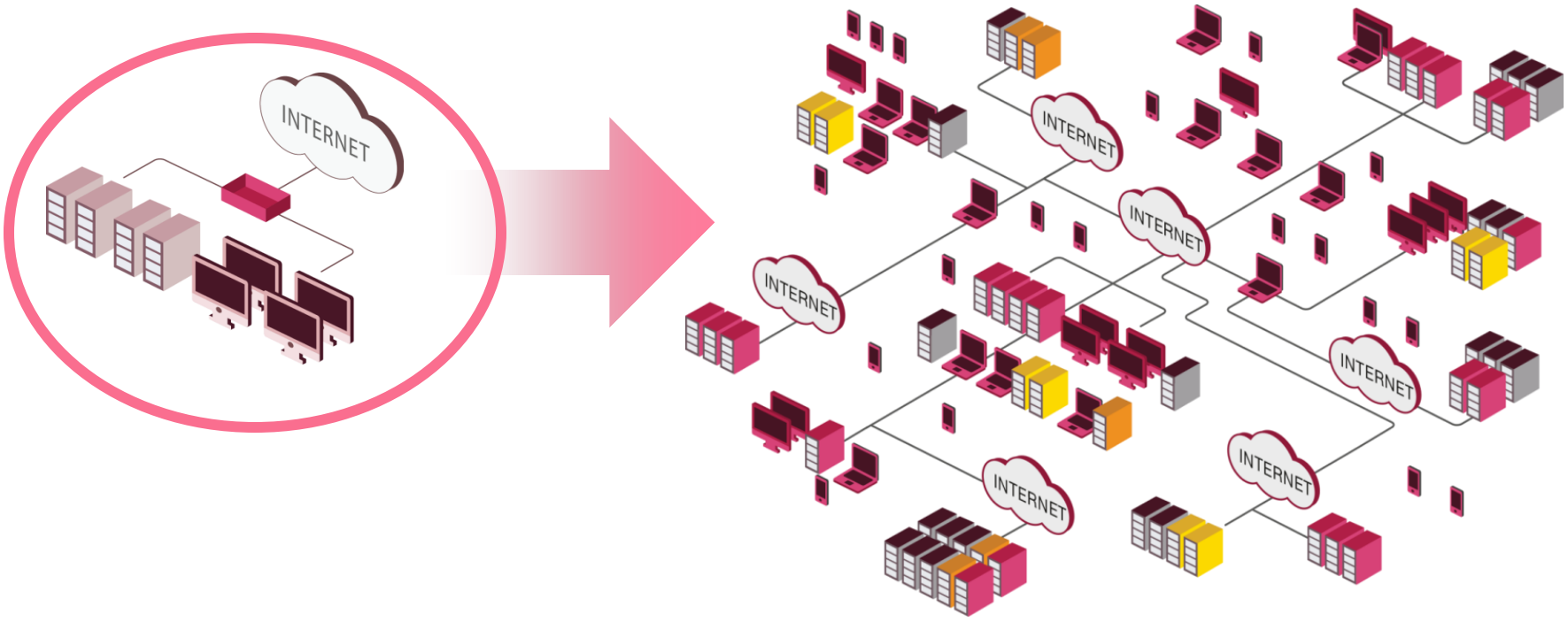
ZERO-DAY EXPLOITS PRICE LIST

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?

Check Point
SOFTWARE TECHNOLOGIES LTD.

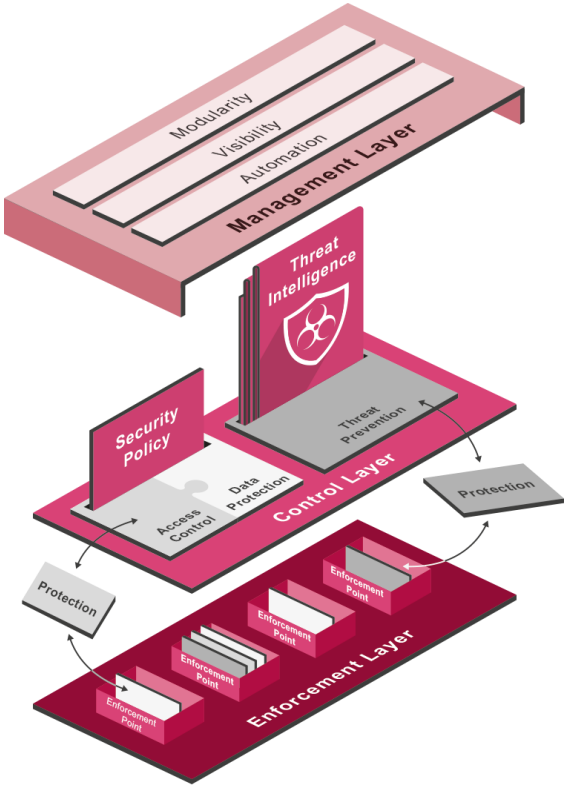
WE NEED SECURITY
that is

MODULAR
AGILE
SECURE!!!

Introducing

SOFTWARE –DEFINED PROTECTION

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

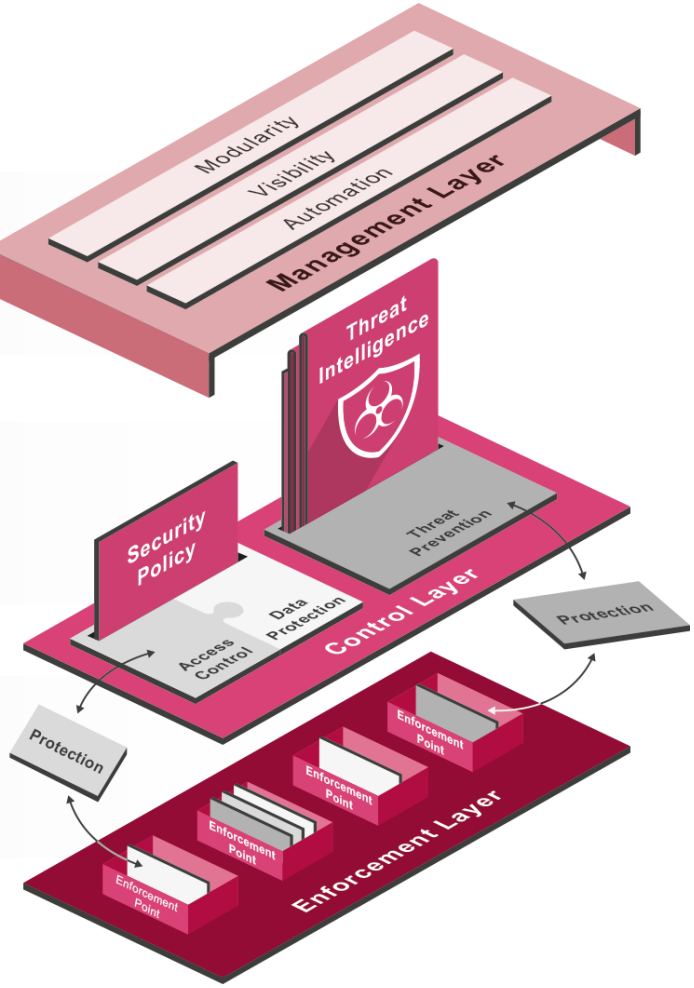


SOFTWARE – DEFINED PROTECTION

MANAGEMENT LAYER
Integrates security with business process

CONTROL LAYER
Delivers real-time protections to the enforcement points

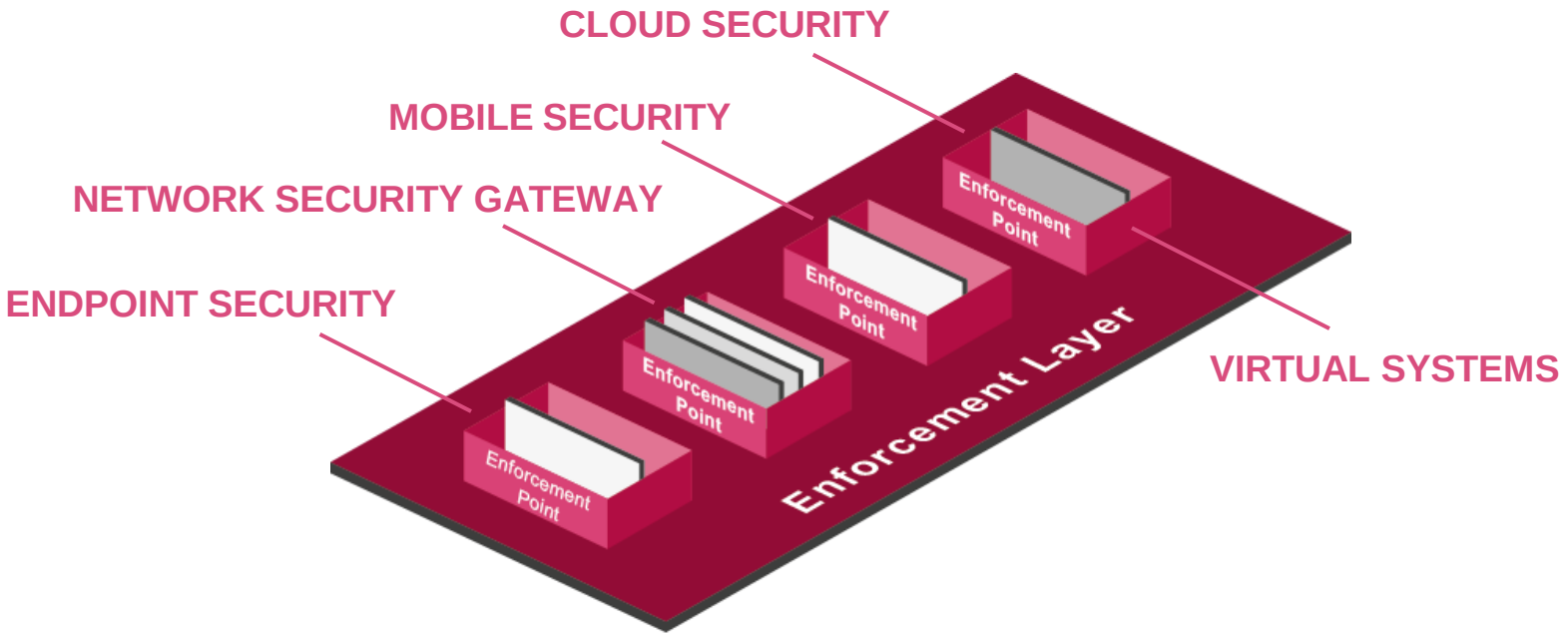
ENFORCEMENT LAYER
Inspects traffic and enforces protection in well-defined segments



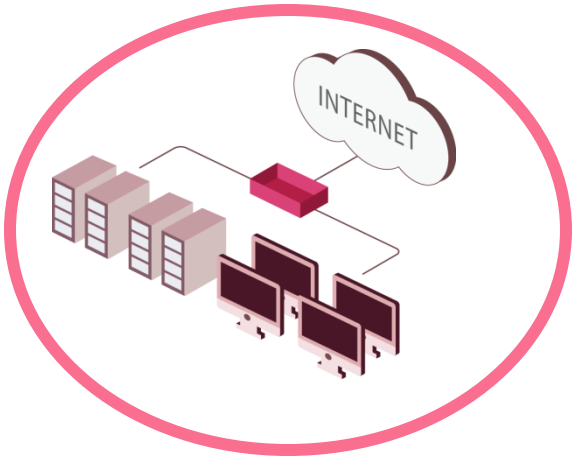
ENFORCEMENT LAYER

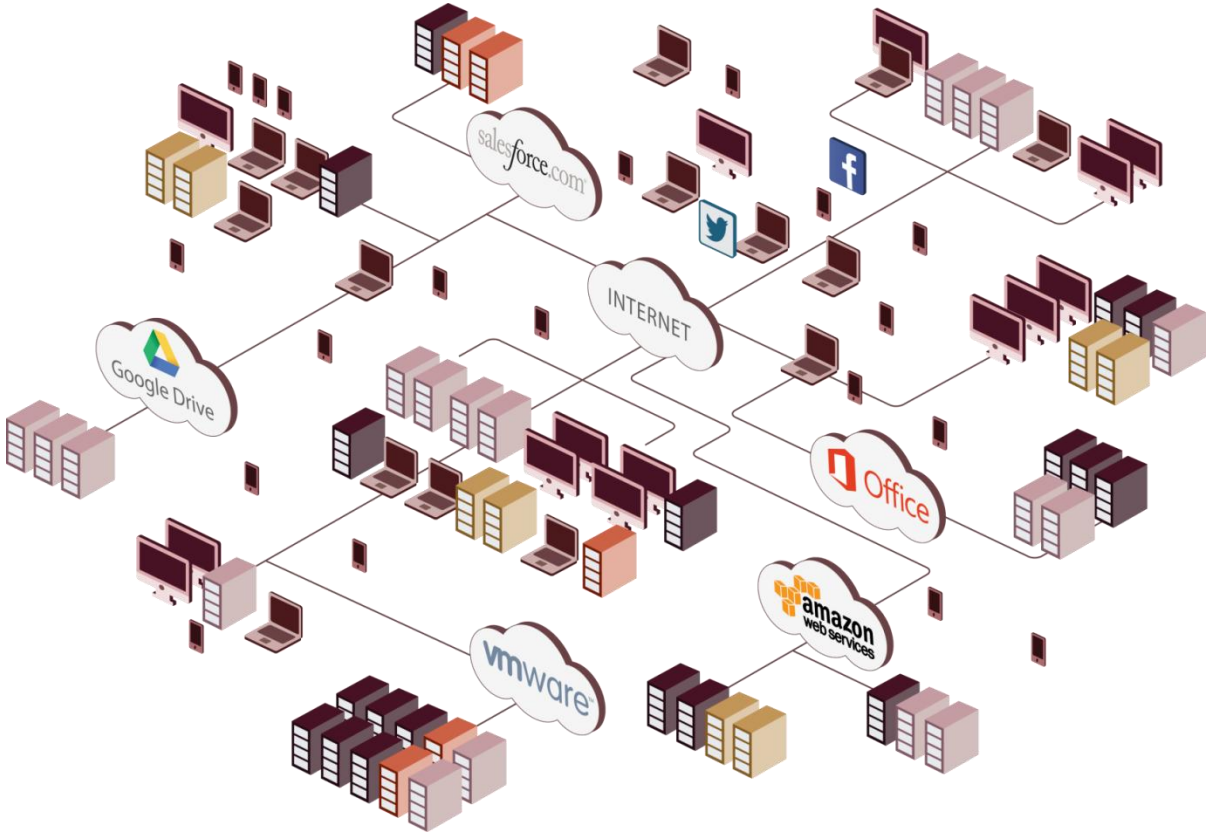
ENFORCEMENT LAYER

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

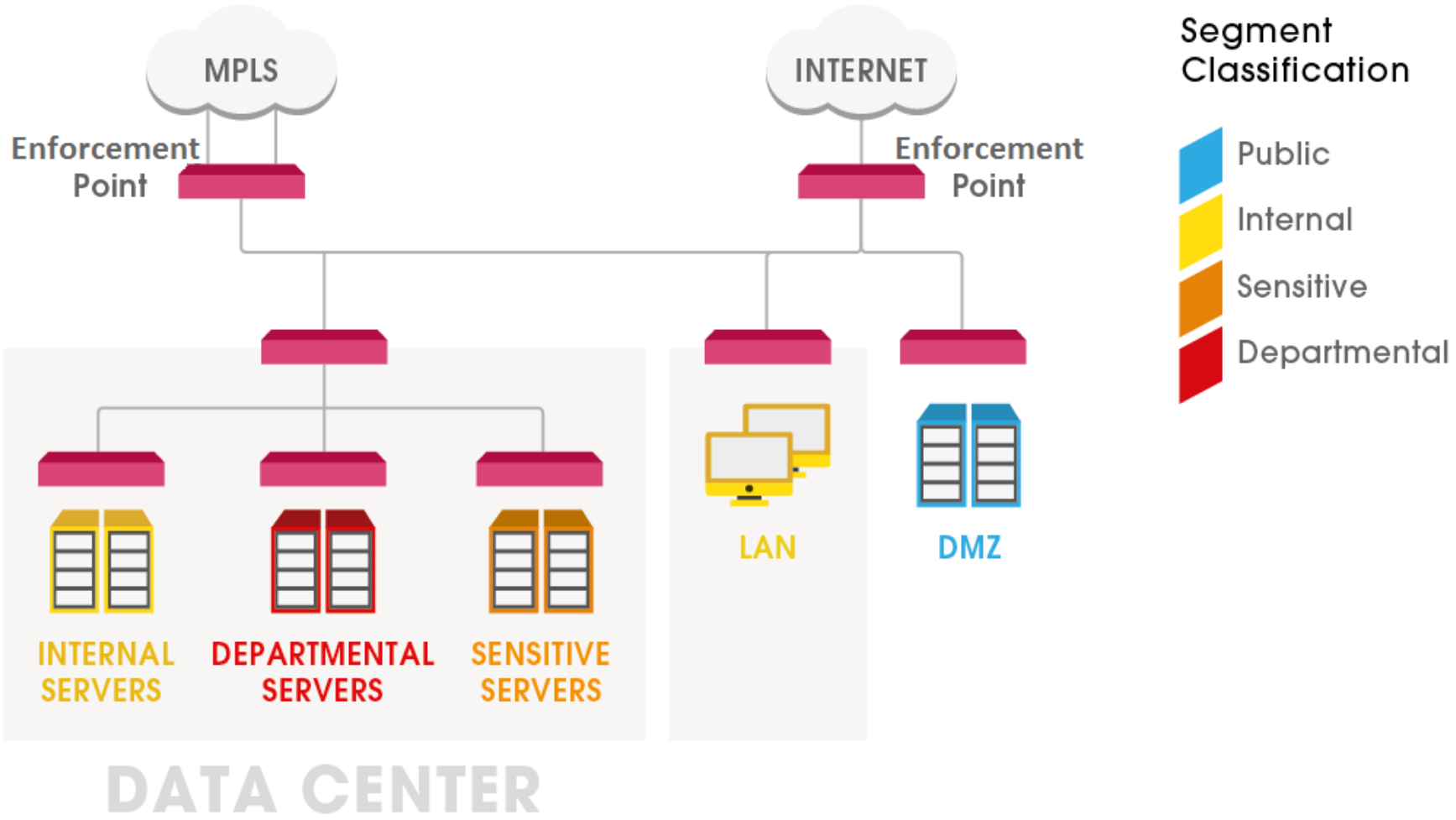


SEGMENTATION IS THE NEW PERIMETER





SEGMENTATION IS THE NEW PERIMETER



ENFORCEMENT LAYER

Of Check Point

SECURITY GATEWAYS

Check Point SOFTWARE TECHNOLOGIES LTD.

Meeting any security requirement

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 System
21000 Appliance
(3 Models)

Ultra High End

MOBILE SECURITY

Use Business Data within a Secure Business Application

Only Authenticated Users Access the Business Container

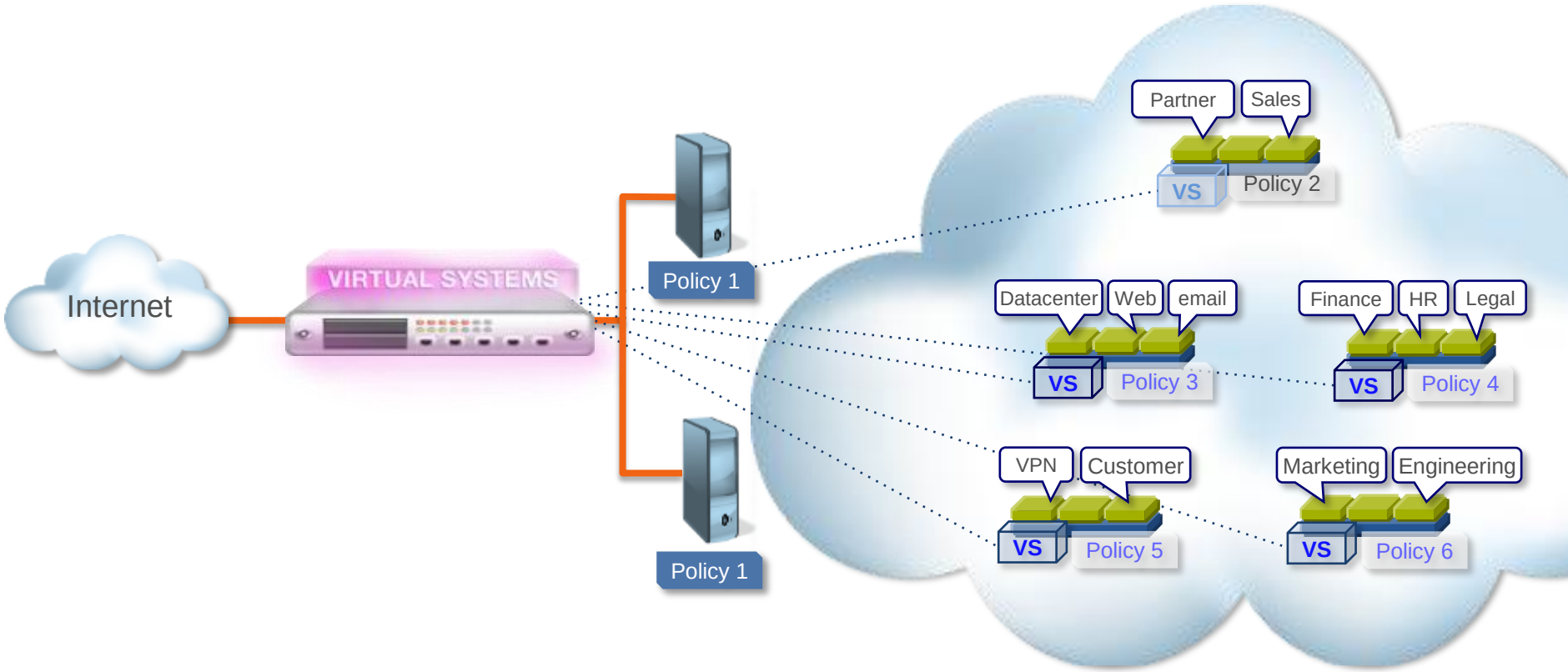
MOBILE SECURITY

Use Business Data within a Secure Business Application

Use Emails Securely

Use Documents Securely

CLOUD SECURITY

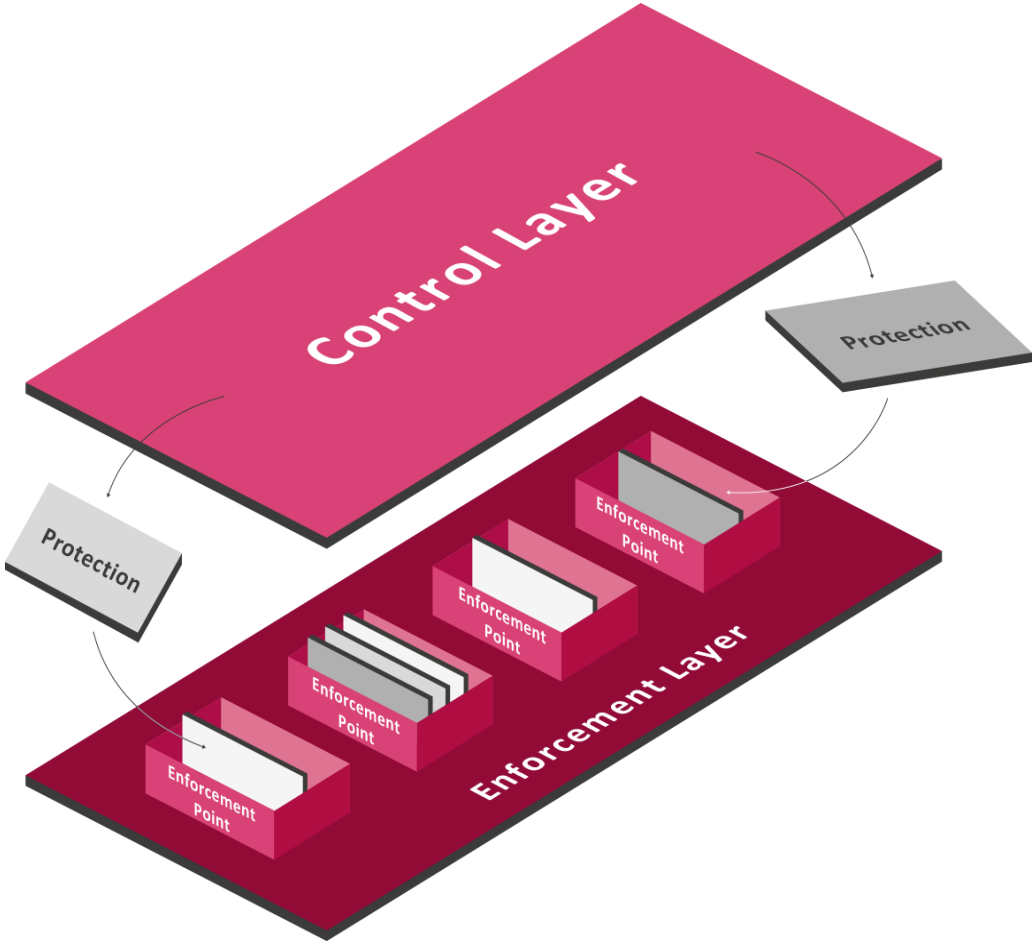


Virtualized Gateways Simplify Private Cloud Security

CONTROL LAYER

CONTROL LAYER

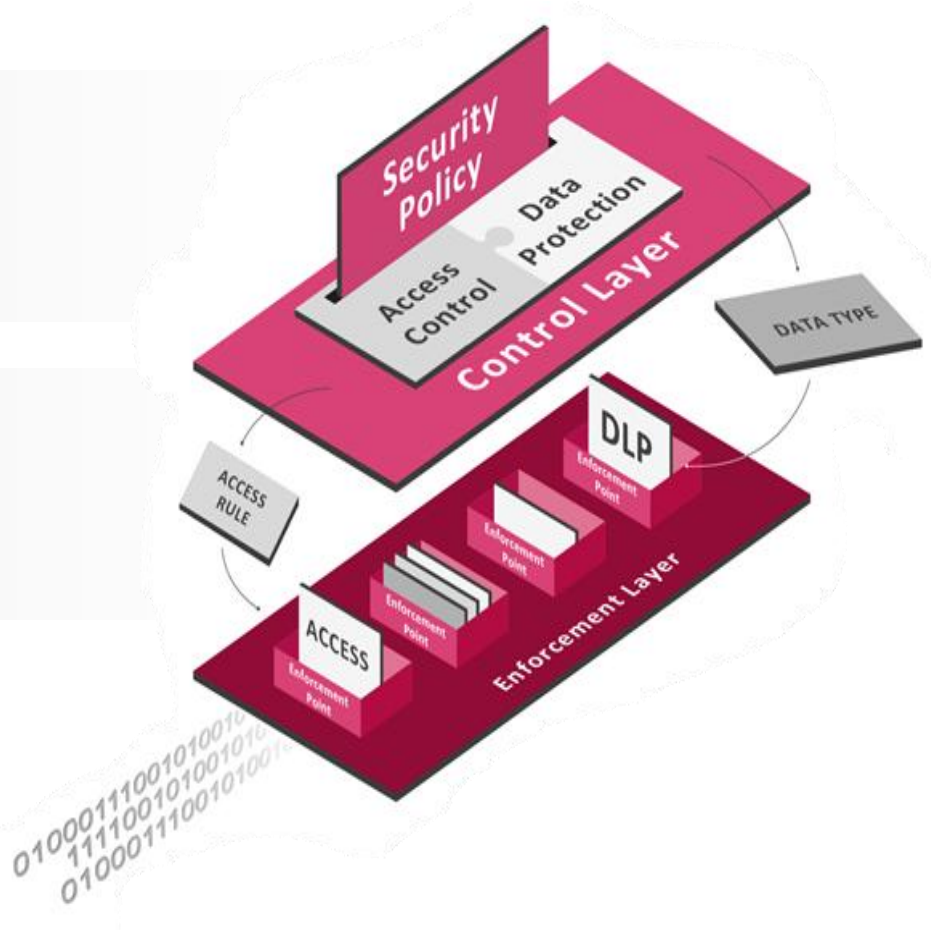
Generate **PROTECTIONS**



ACCESS CONTROL AND DATA PROTECTION

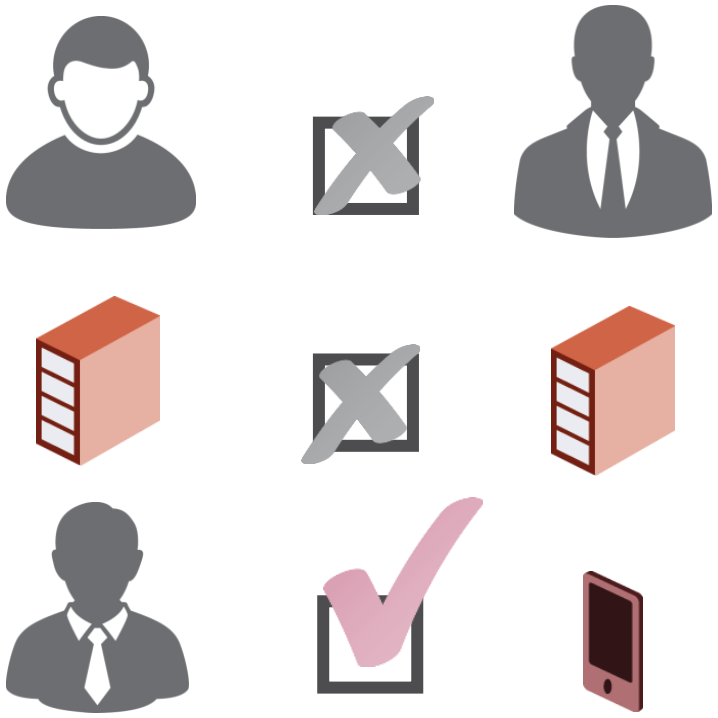
Control interactions between users, assets, data and applications

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?

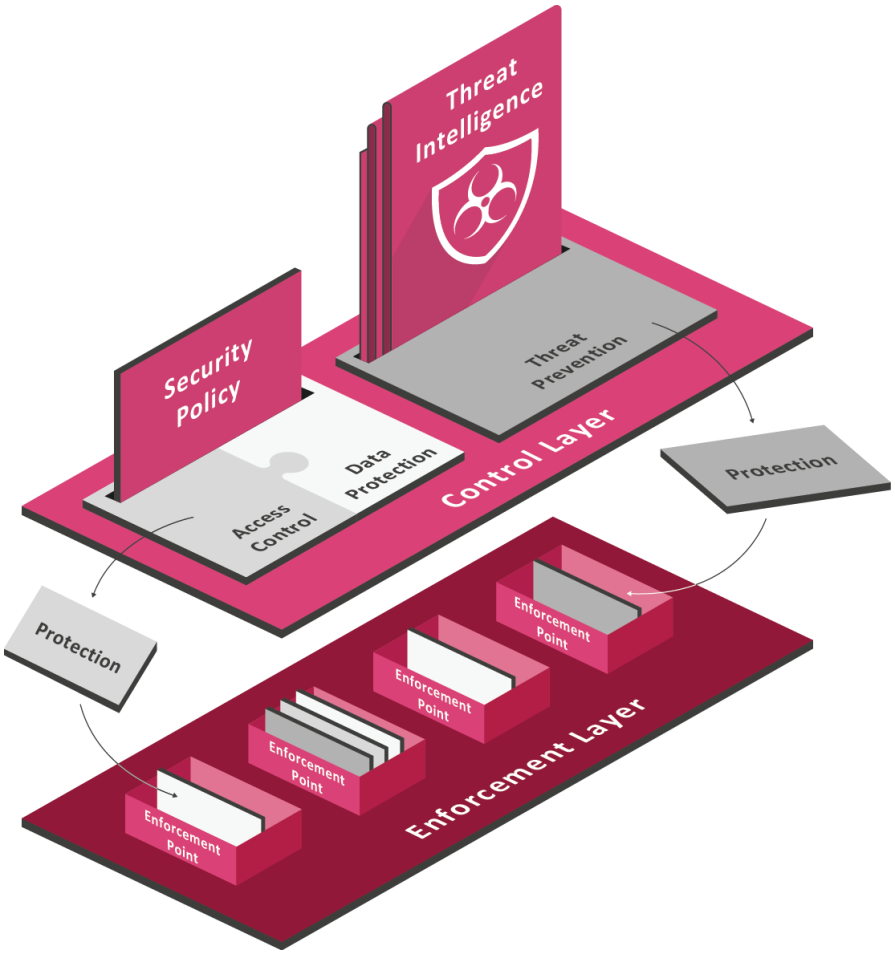
THE THREATS WE NEED TO PREVENT

Know Knows	Know Unknowns	Unknown Unknowns
Threats we know we know	Threats we know we don't know	Threats we don't know we don't know
ANTI VIRUS	**THREAT EMULATION**	
ANTI BOT	**ANTI BOT**	
IPS		

WHAT IS NEEDED?

THREAT PREVENTION

Updated protections in **REAL-TIME**

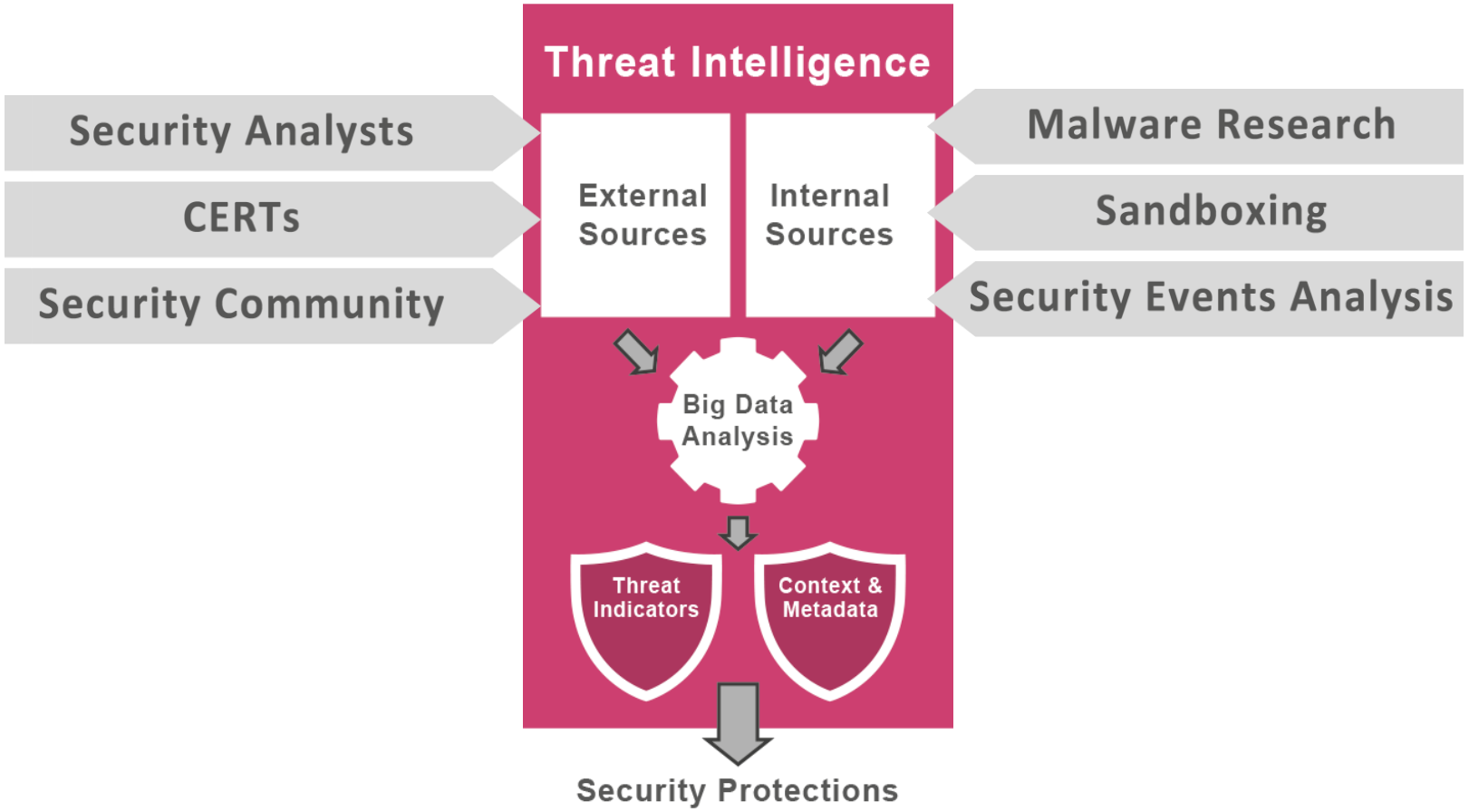


Utilizing the same enforcement points for real time dynamic Threat Prevention protections

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

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

Gateways

Endpoints

CHECK POINT THREATCLOUD™

Incident response & SOC Portal

CHECK POINT THREATCLOUD™

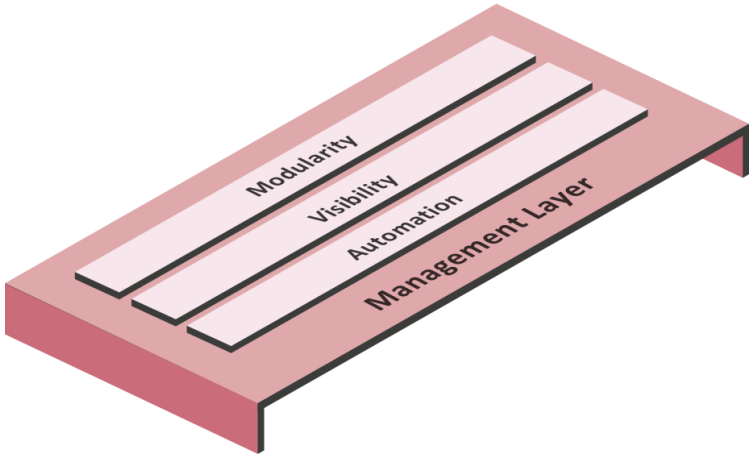
Private ThreatCloud

Security Indicators | Emulations | Sensors | Researches

MANAGEMENT LAYER

MANAGEMENT LAYER

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



MODULARITY

AUTOMATION

VISIBILITY

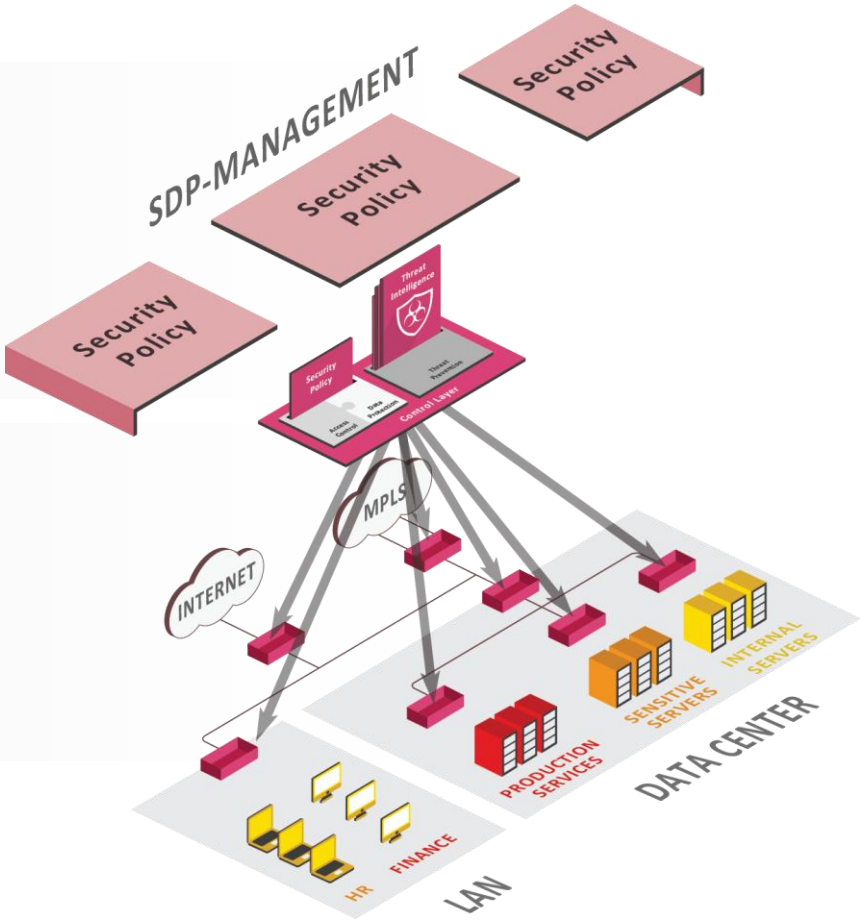
MODULARITY

ENDLESS FLEXIBILITY with LAYERS of POLICIES

Management modularity provides the flexibility to manage each segment and control

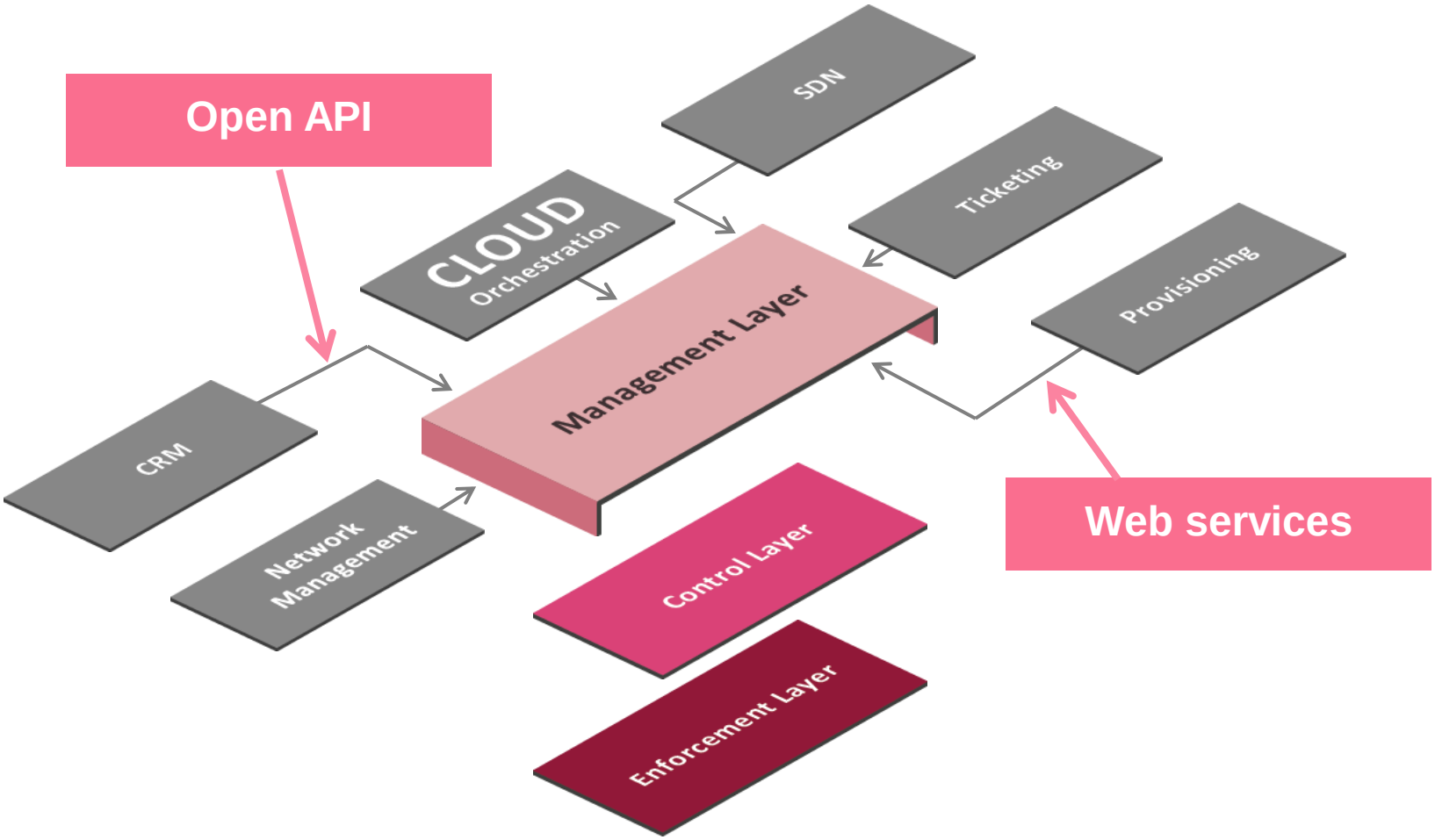
Segregation of duties

Layers of policy



AUTOMATION

OPEN INTERFACES support business process changes



SDP AND SDN WORKING IN SYNERGY

SDN

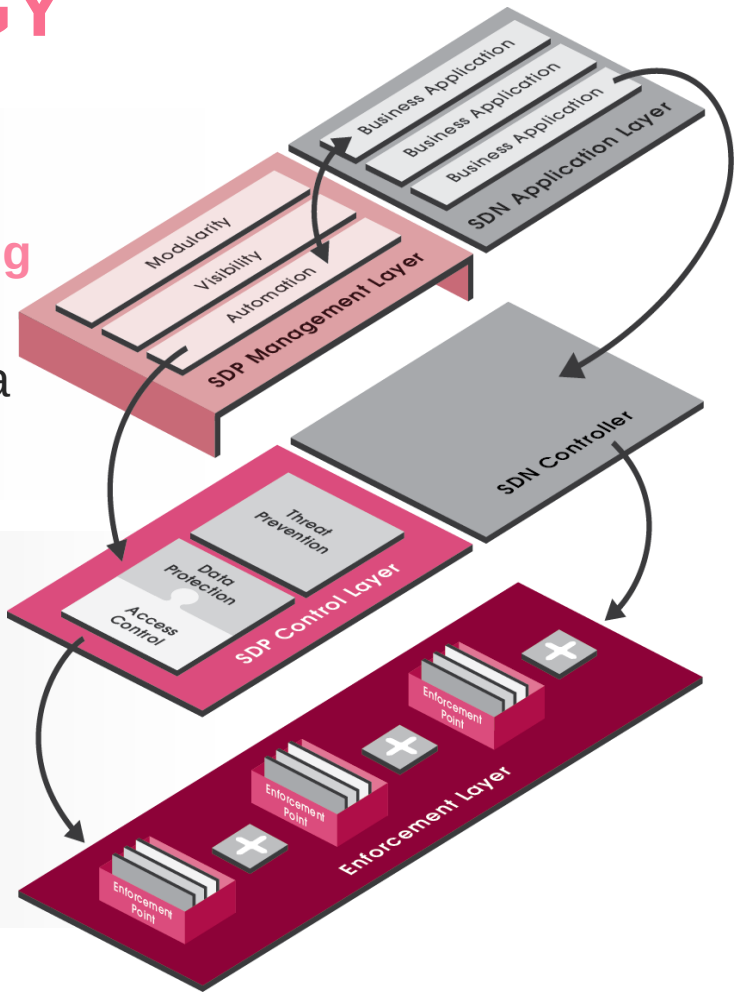
An emerging network architecture, decoupling network control and data planes.

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



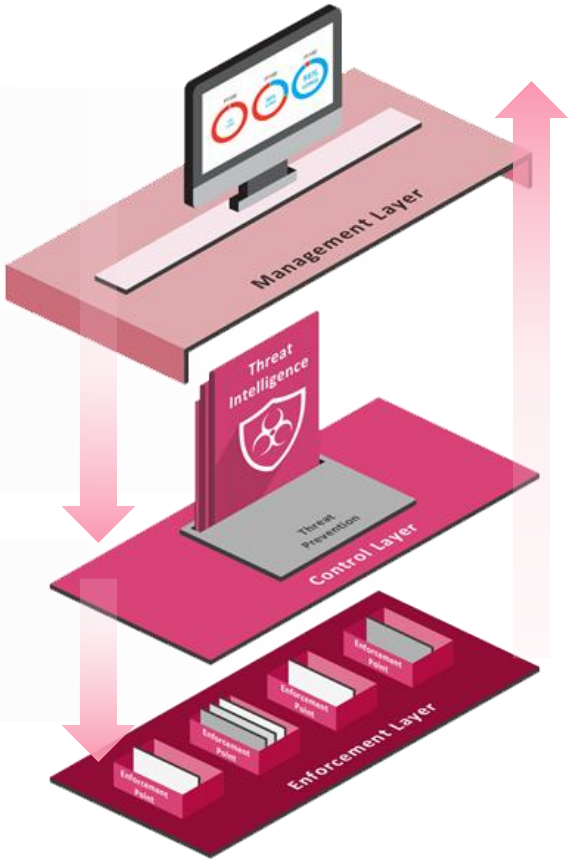
VISIBILITY

SITUATION AWARENESS & INCIDENT RESPONSE

Collects information from every enforcement point

Situation awareness view

Generation of new protections



Delegation and Segregation of Duties

Granular Privileges

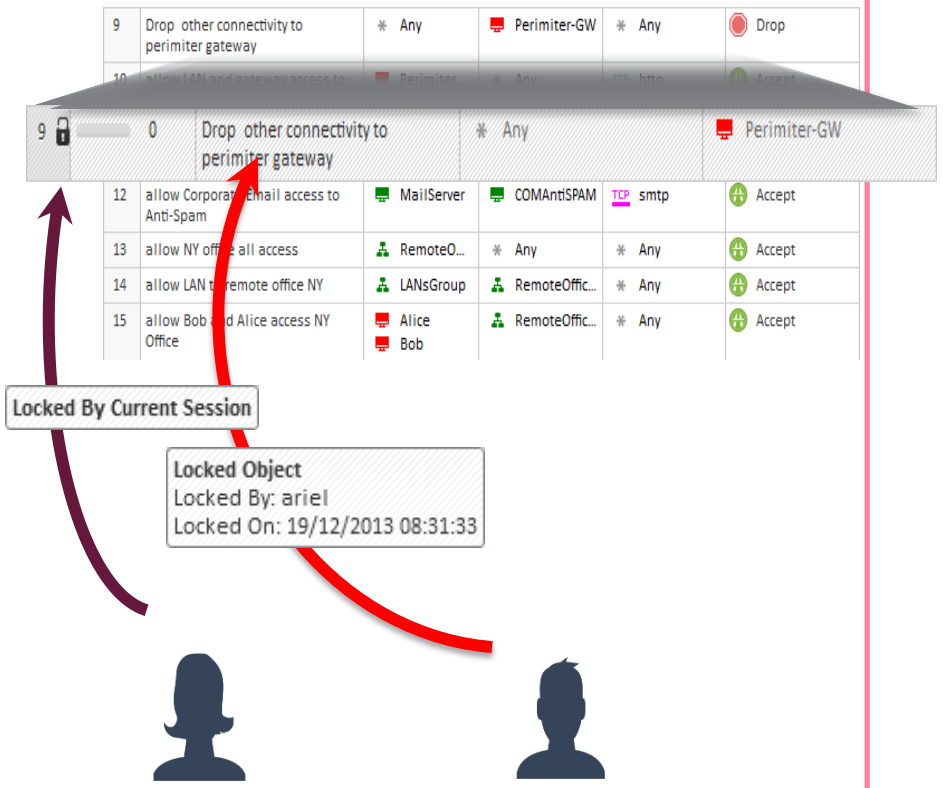
No.	Name	Protected Scope	Protection/Site	Action	Track	Install On
1	Secure network with all threat capabilities	RNDNetwork	N/A	Recommended_Profile	Log	Policy Targets
2	Threat emulation special rule for Sales server	SalesServer	N/A	Threat Sales Profile	Log	Policy Targets

Can manage IPS only

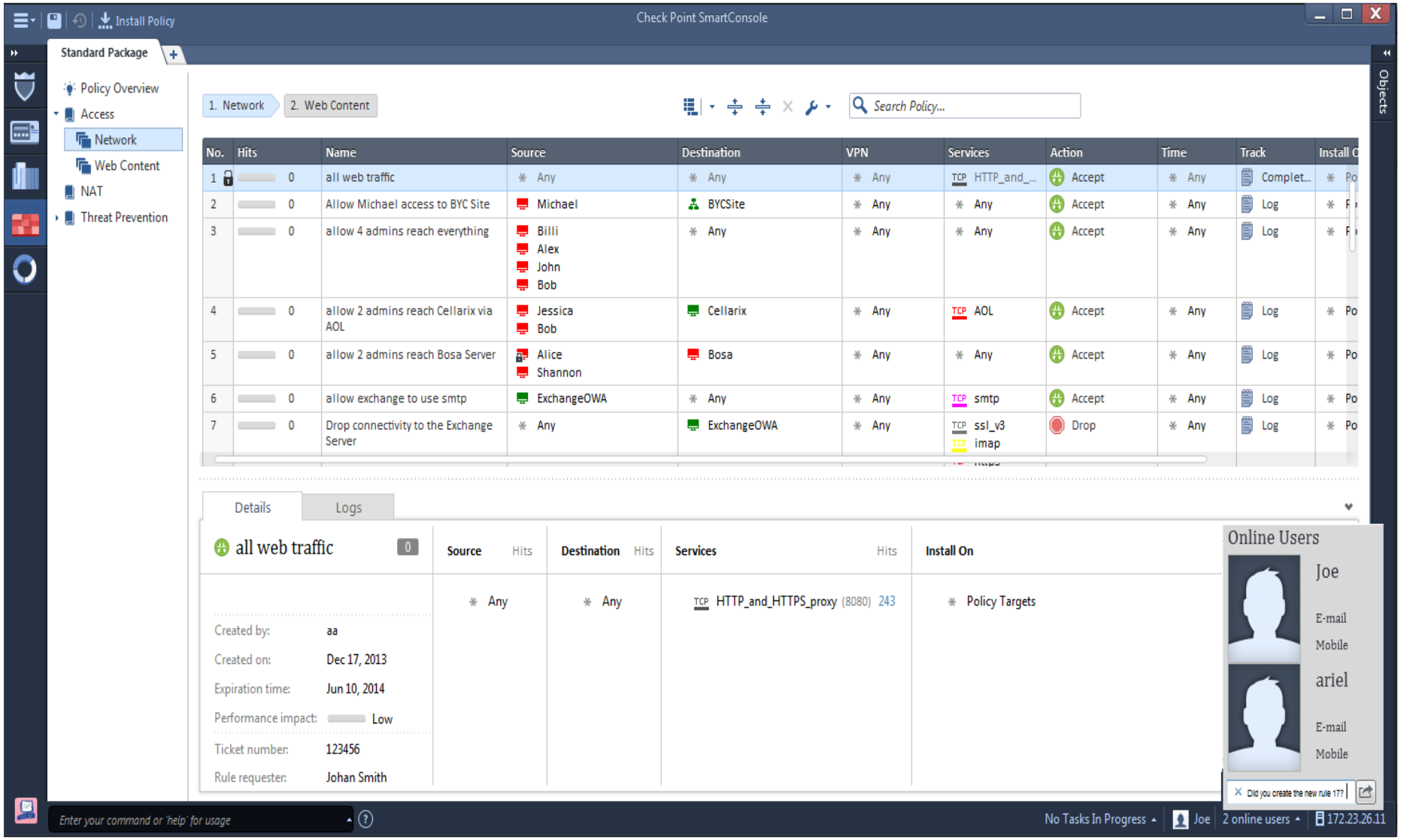
No.	Name	Source	Destination	Services	Action
1	all web traffic	Any	Any	HTTP_and_...	Accept
2	Allow Michael access to BYC Site	Michael	BYCSite	Any	Accept
3	allow 4 admins reach everything	Billi Alex John Bob	Any	Any	Accept

Can manage Branch Office Access Policy only

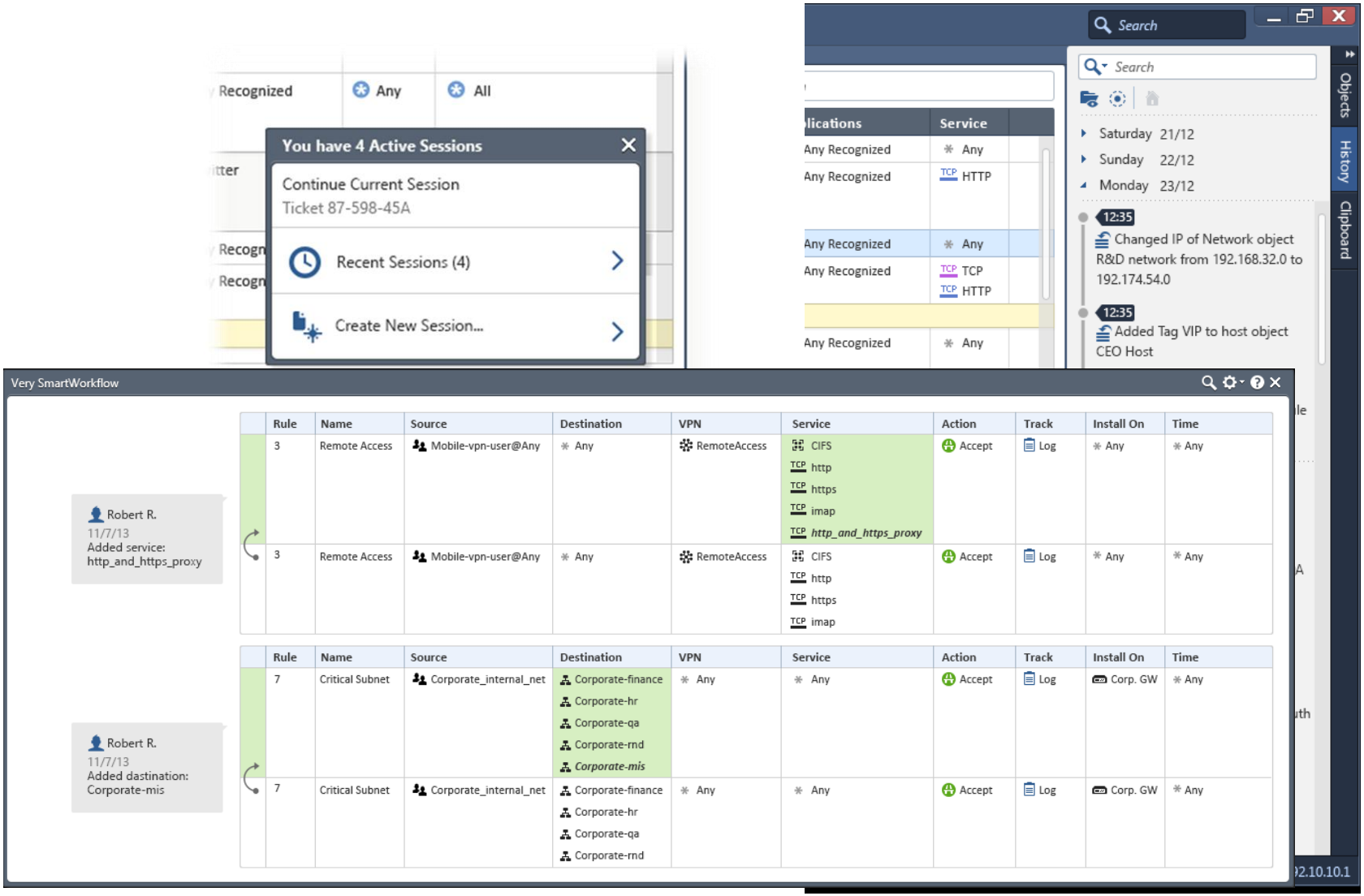
Simultaneous Admins



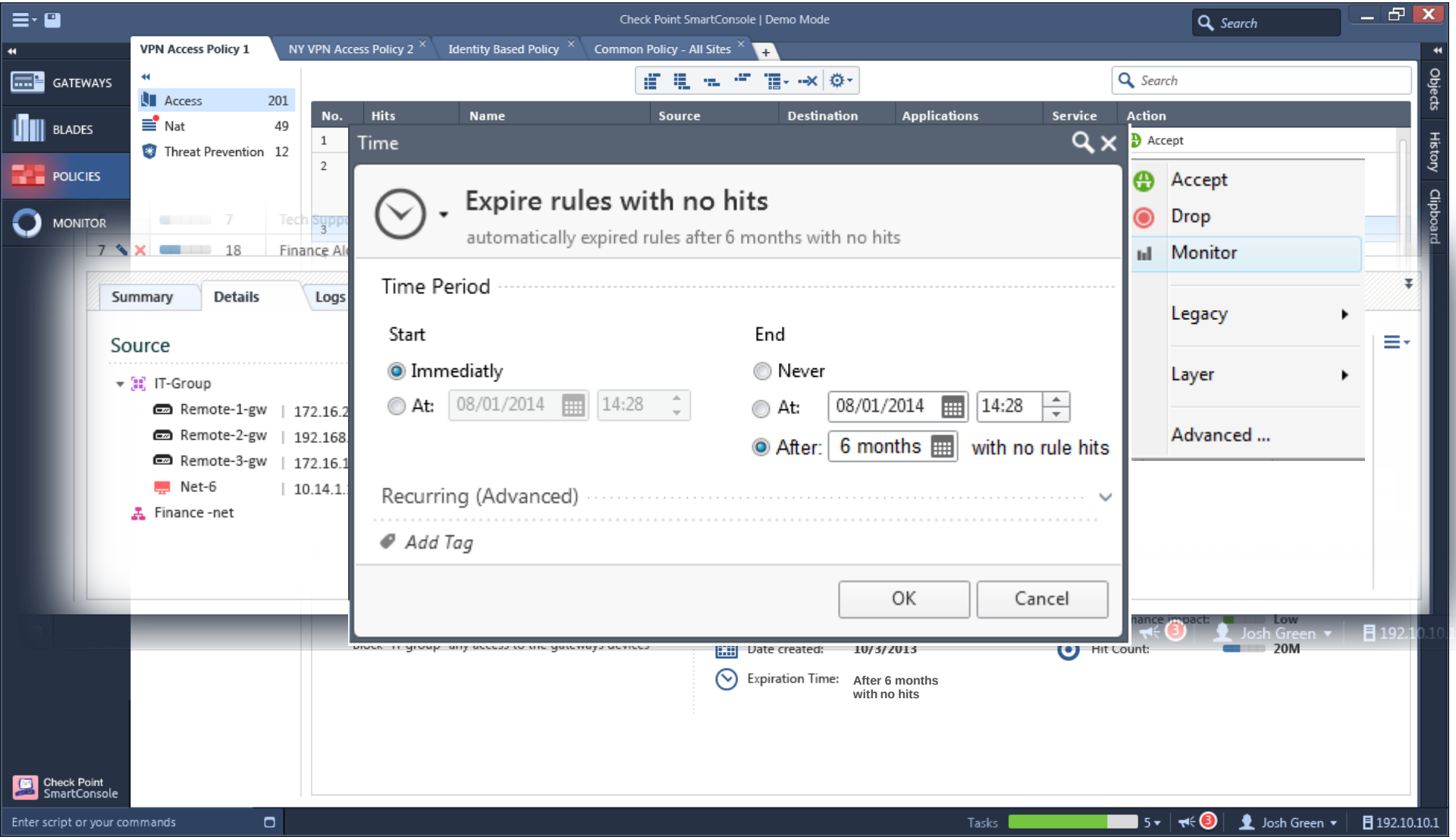
Connected Admins & Chat



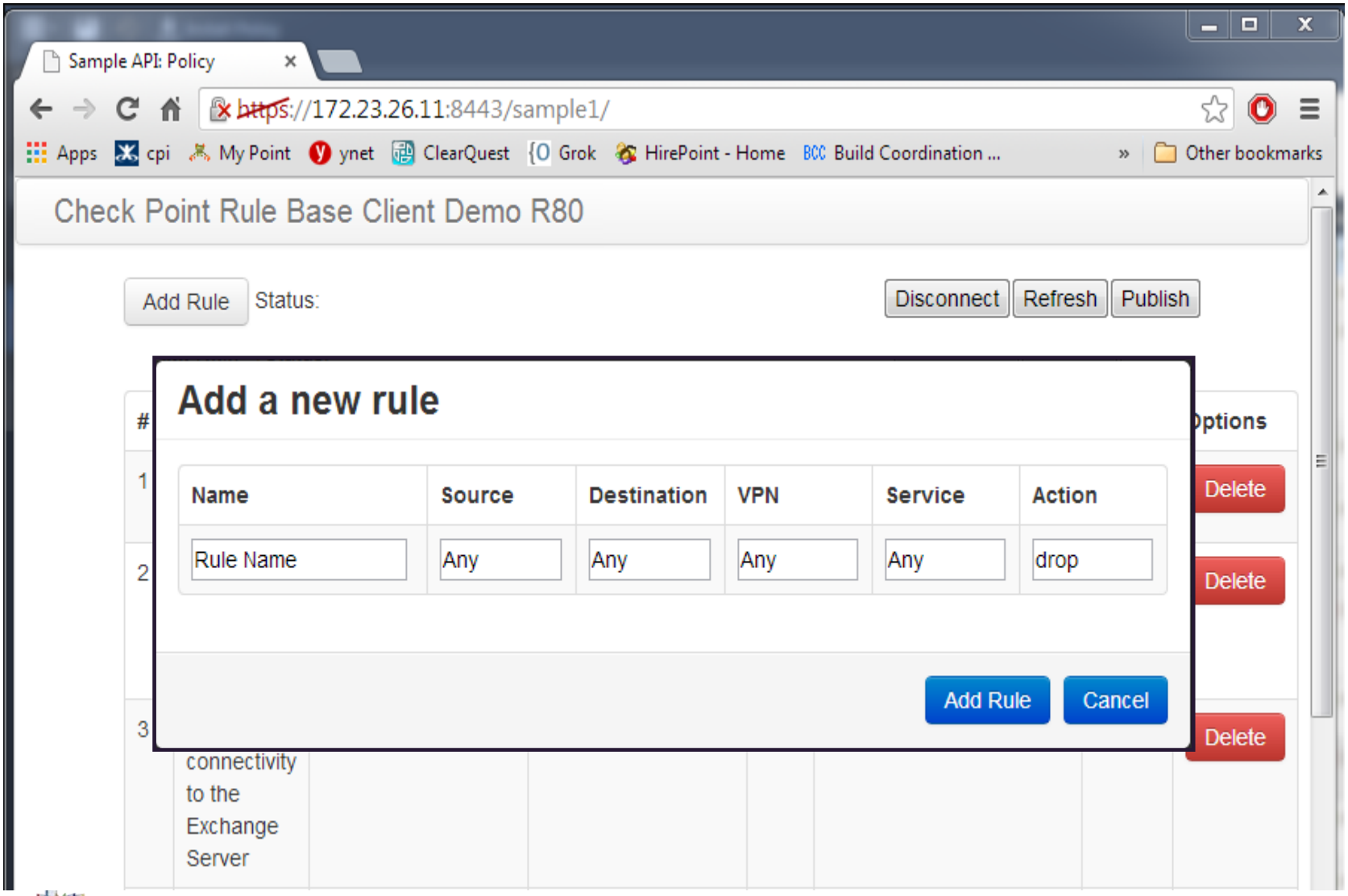
Sessions Management



Decisions tools

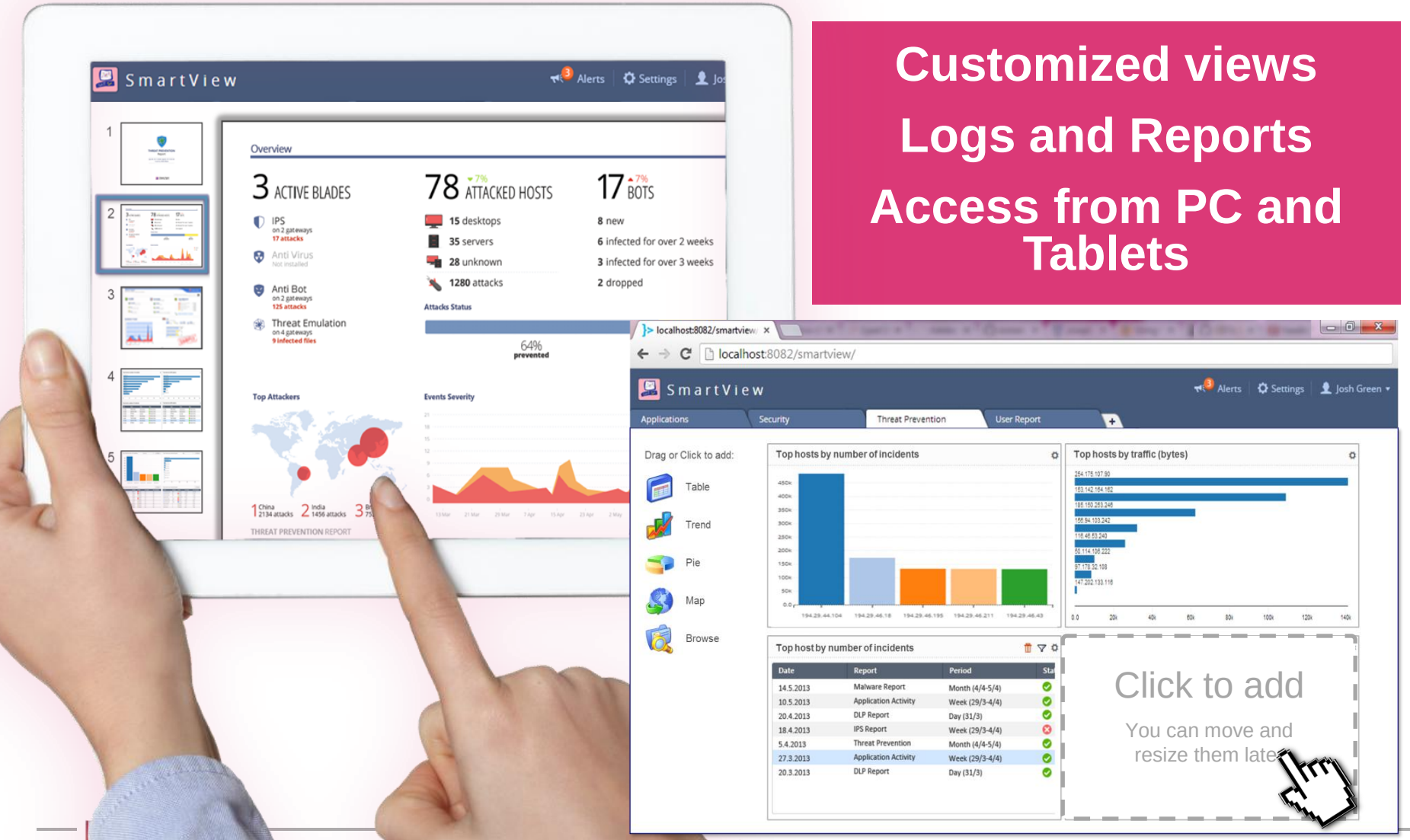


Automation – using the Rest API



Web-based monitoring and reporting system

Check Point SOFTWARE TECHNOLOGIES LTD.



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!

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.