Check Point
SOFTWARE TECHNOLOGIES LTD.

R80 SECURITY MANAGEMENT

The Future of Security Management

©2016 Check Point Software Technologies Ltd.

Managing Security Today is COMPLEX

PEOPLE	PROCESS	TECHNOLOGY
Fewer resources	Multiple security solutions	Mobile
More tickets	Manual processes	Cloud
Greater expertise	Lack of integration	On-Demand Services

©2016 Check Point Software Technologies Ltd.

Check Point
SOFTWARE TECHNOLOGIES LTD.

The key to managing complexity
is security **consolidation**

INTRODUCING...

R80

SECURITY MANAGEMENT

R80

THE PLATFORM TO CONSOLIDATE ALL YOUR SECURITY

Unified Policy Management

Efficient, Automated Operations

Integrated Threat Management

©2016 Check Point Software Technologies Ltd.

R80

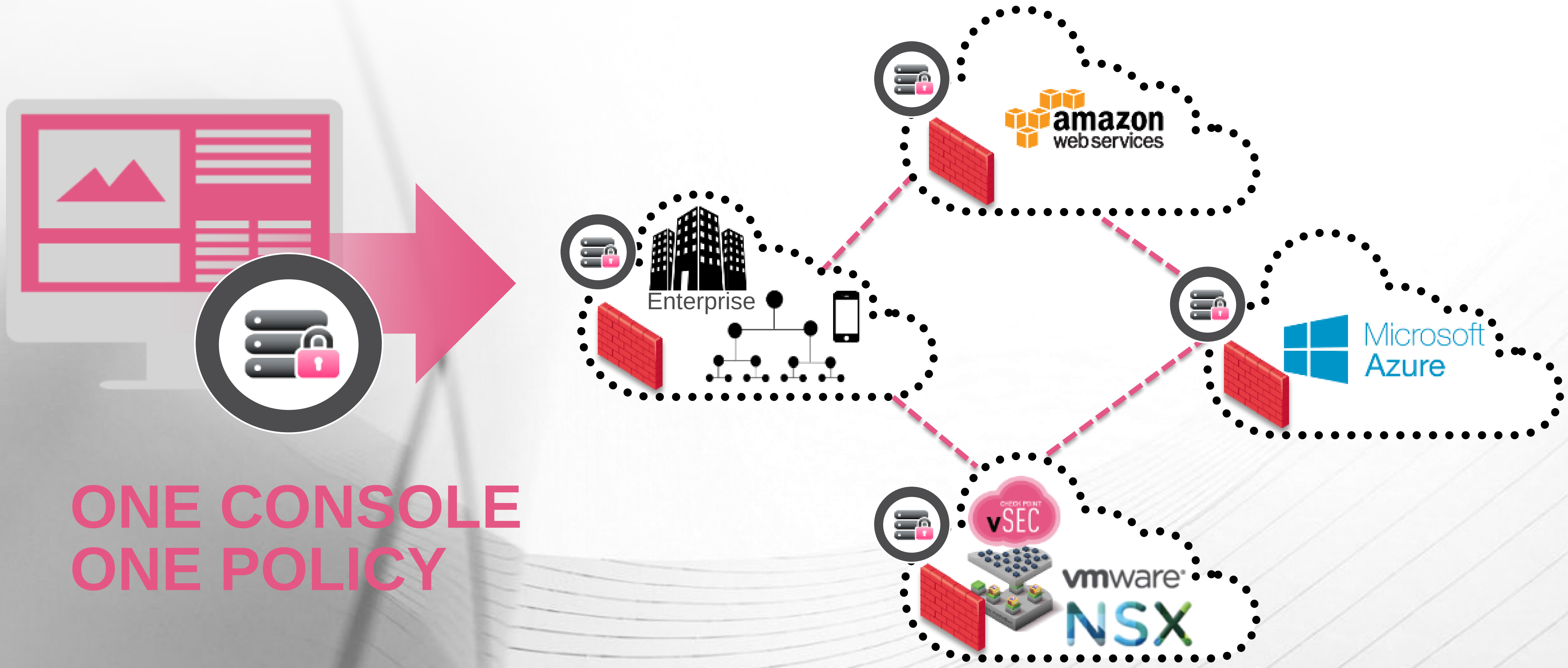
CHANGE THE WAY
YOU **MANAGE SECURITY**

Check Point
SOFTWARE TECHNOLOGIES LTD.

UNIFIED POLICY MANAGEMENT

One Console to Manage Everything

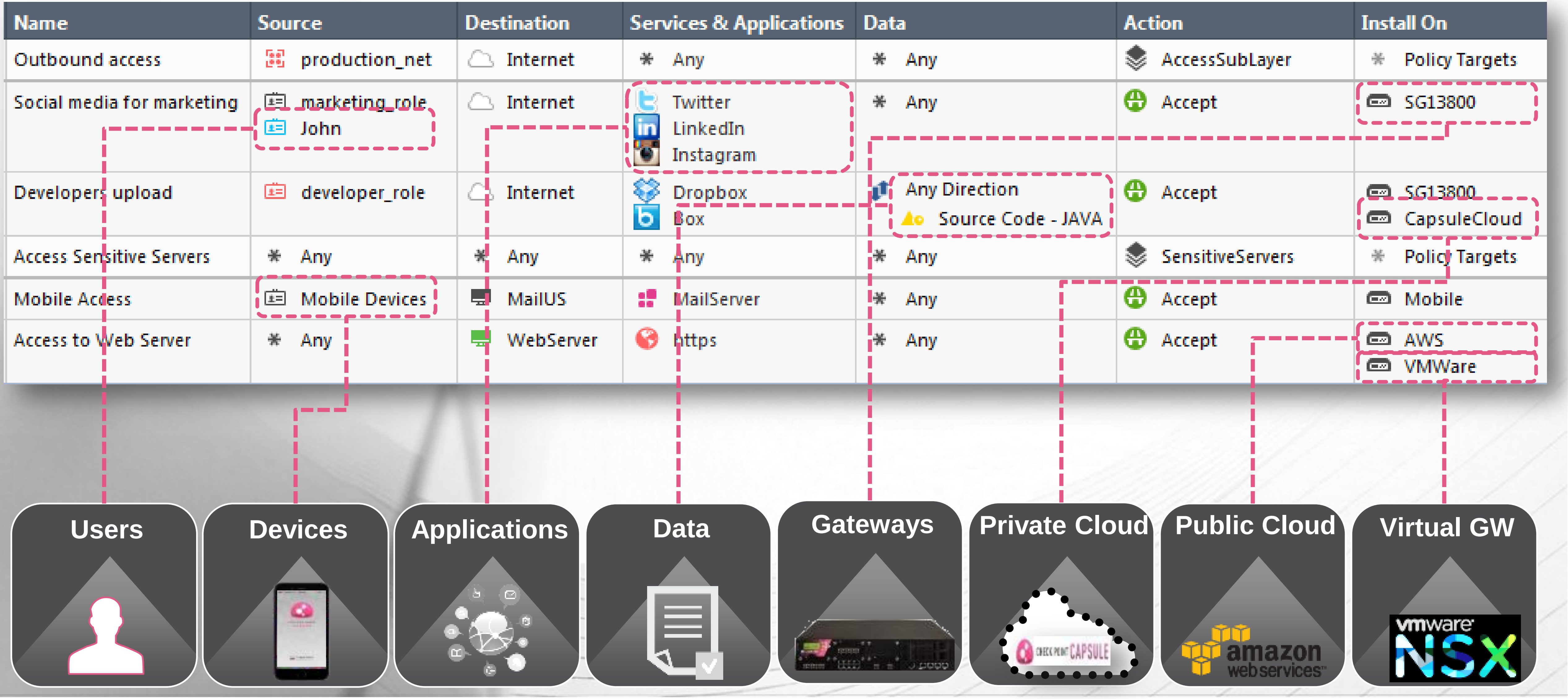
Check Point
SOFTWARE TECHNOLOGIES LTD.



ONE CONSOLE
ONE POLICY

©2016 Check Point Software Technologies Ltd.

One Policy to Manage Everything



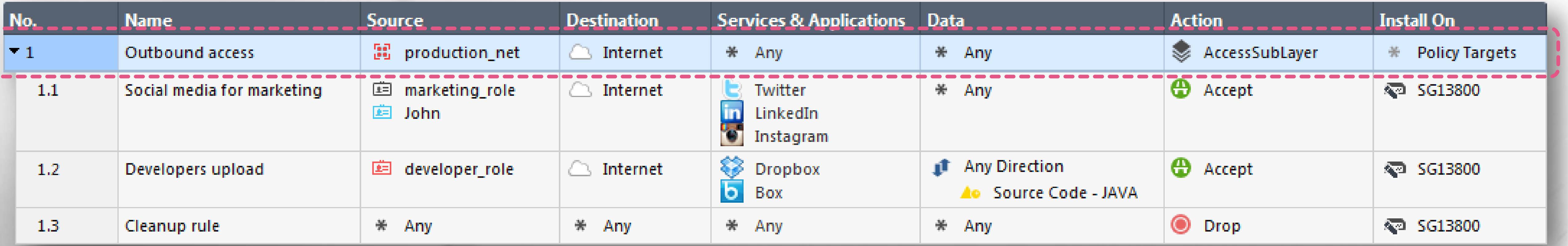
Name	Source	Destination	Services & Applications	Data	Action	Install On
Outbound access	production_net	Internet	Any	Any	AccessSubLayer	Policy Targets
Social media for marketing	marketing_role John	Internet	Twitter LinkedIn Instagram	Any	Accept	SG13800
Developers upload	developer_role	Internet	Dropbox 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

©2016 Check Point Software Technologies Ltd.

Unparalleled Policy Granularity & Control

Check Point
SOFTWARE TECHNOLOGIES LTD.

Control all traffic from the production network to the Internet



No.	Name	Source	Destination	Services & Applications	Data	Action	Install On
▼ 1	Outbound access	production_net	Internet	Any	Any	AccessSubLayer	Policy Targets
1.1	Social media for marketing	marketing_role John	Internet	Twitter LinkedIn Instagram	Any	Accept	SG13800
1.2	Developers upload	developer_role	Internet	Dropbox Box	Any Direction Source Code - JAVA	Accept	SG13800
1.3	Cleanup rule	Any	Any	Any	Any	Drop	SG13800

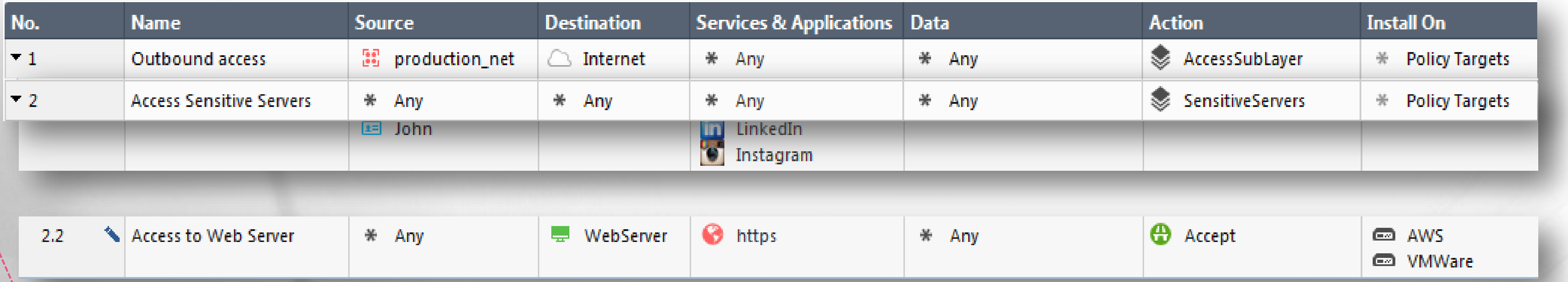
Allow developers to upload and download JAVA source code to Dropbox and Box

©2016 Check Point Software Technologies Ltd.

Easily Segment Policy for Better Manageability and Control

Ann

Walter



No.	Name	Source	Destination	Services & Applications	Data	Action	Install On
▾ 1	Outbound access	production_net	Internet	Any	Any	AccessSubLayer	Policy Targets
▾ 2	Access Sensitive Servers	Any	Any	Any	Any	SensitiveServers	Policy Targets
		John		LinkedIn Instagram			
2.2	Access to Web Server	Any	WebServer	https	Any	Accept	AWS VMWare

Duties separated based on IT role

Each policy segment can be delegated to distribute workload

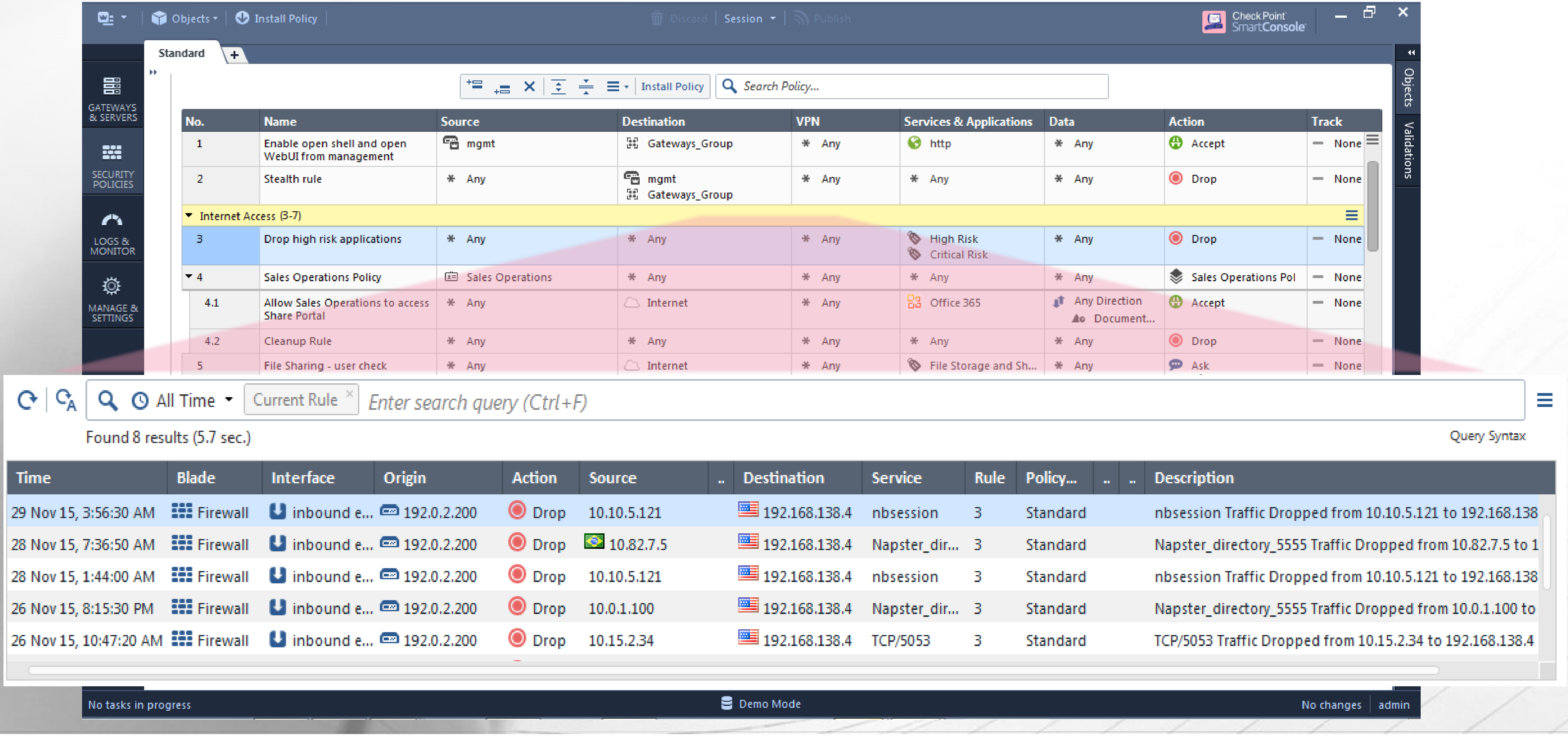
©2016 Check Point Software Technologies Ltd.

R80 CHANGE THE WAY YOU **WORK AND COLLABORATE**

Check Point SOFTWARE TECHNOLOGIES LTD.

EFFICIENT AND AUTOMATED OPERATIONS

With one click, access all logs and rule details



No.	Name	Source	Destination	VPN	Services & Applications	Data	Action	Track
1	Enable open shell and open WebUI from management	mgmt	Gateways_Group	Any	http	Any	Accept	None
2	Stealth rule	Any	mgmt Gateways_Group	Any	Any	Any	Drop	None
Internet Access (3-7)								
3	Drop high risk applications	Any	Any	Any	High Risk Critical Risk	Any	Drop	None
4	Sales Operations Policy	Sales Operations	Any	Any	Any	Any	Sales Operations Pol	None
4.1	Allow Sales Operations to access Share Portal	Any	Internet	Any	Office 365	Any Direction Document...	Accept	None
4.2	Cleanup Rule	Any	Any	Any	Any	Any	Drop	None
5	File Sharing - user check	Any	Internet	Any	File Storage and Sh...	Any	Ask	None

Found 8 results (5.7 sec.)

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	nbsession	3	Standard			nbsession 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	nbsession	3	Standard			nbsession 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

©2016 Check Point Software Technologies Ltd.

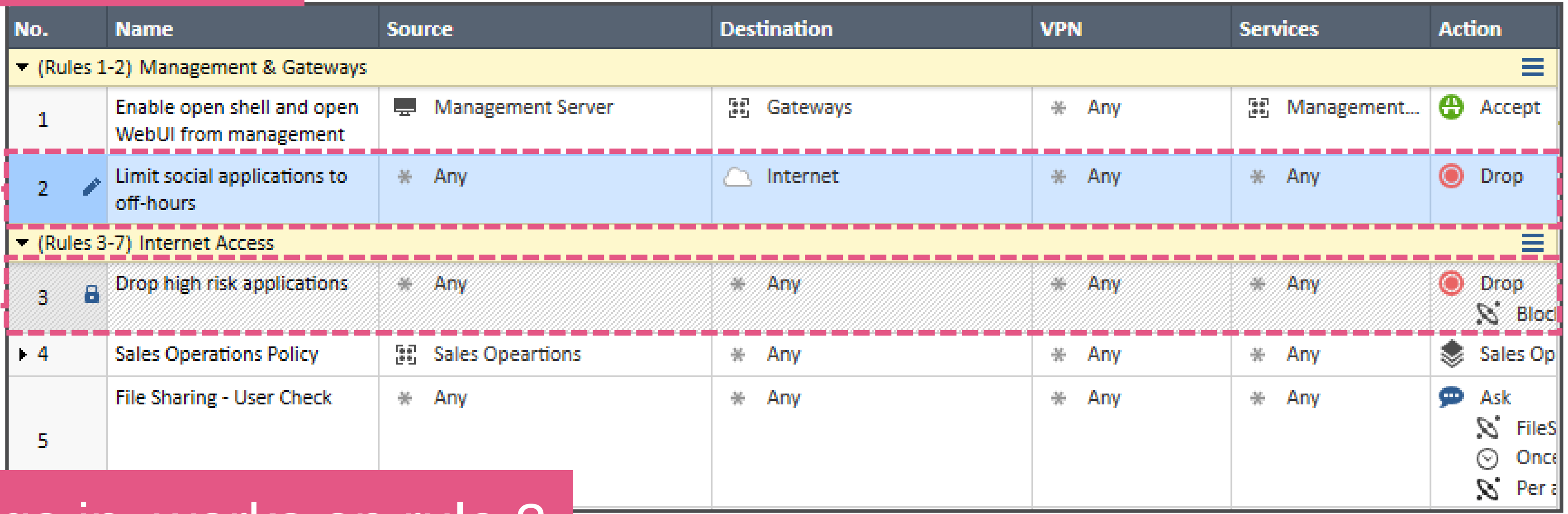
Admin Concurrency Increases Team Productivity

Check Point
SOFTWARE TECHNOLOGIES LTD.

Ann

Ann logs in, sees rule 3 locked

Ann works on rule 2

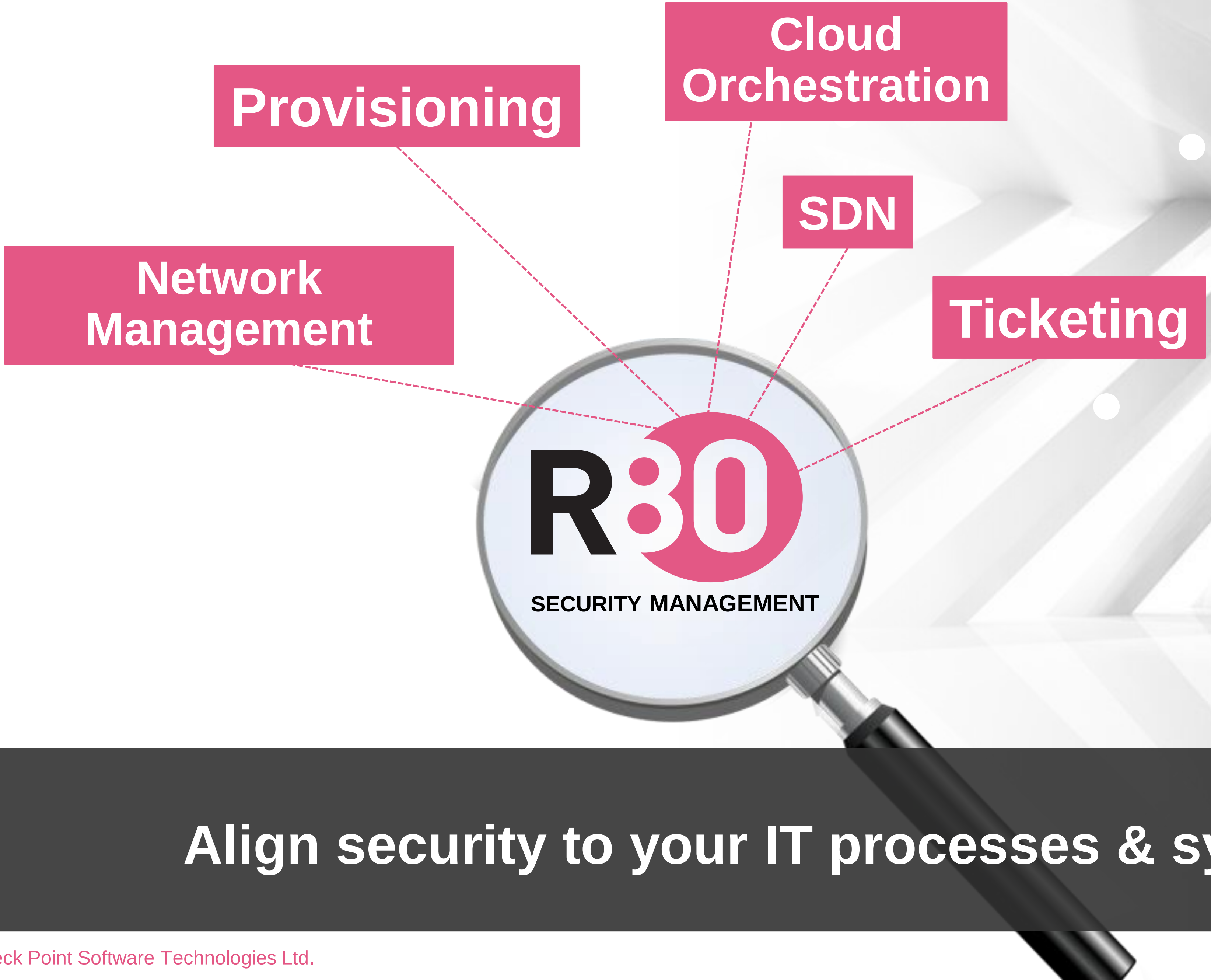


No.	Name	Source	Destination	VPN	Services	Action
(Rules 1-2) Management & Gateways						
1	Enable open shell and open WebUI from management	Management Server	Gateways	Any	Management...	Accept
2	Limit social applications to off-hours	Any	Internet	Any	Any	Drop
(Rules 3-7) Internet Access						
3	Drop high risk applications	Any	Any	Any	Any	Drop Bloc
4	Sales Operations Policy	Sales Opeartions	Any	Any	Any	Sales Op
5	File Sharing - User Check	Any	Any	Any	Any	Ask FileS Once Per a

Walter logs in, works on rule 3

Walter

Multiple admins can work on same policy without conflict



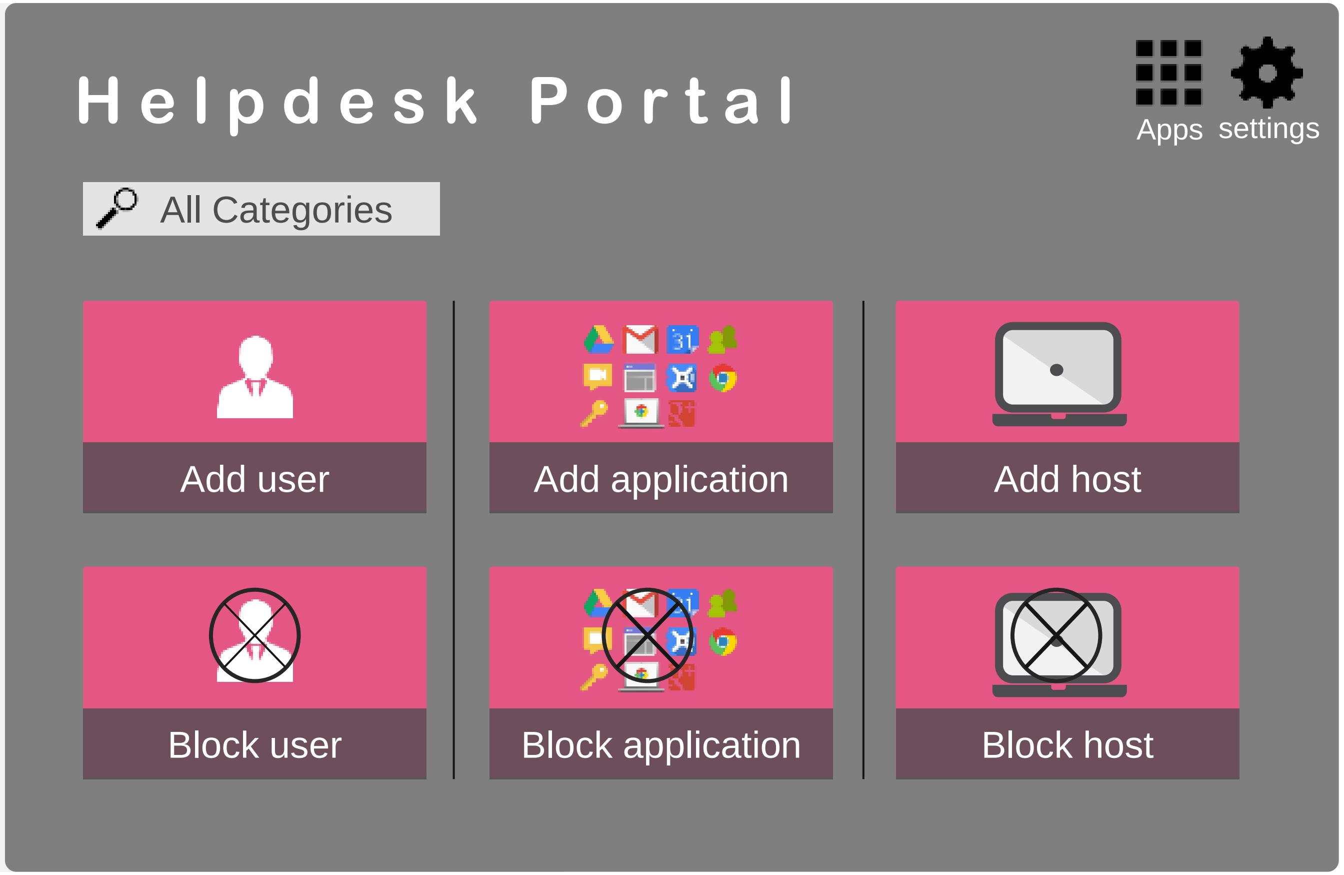
Align security to your IT processes & systems

©2016 Check Point Software Technologies Ltd.

Empower Self-Service Security

Use R80 API to automate routine Helpdesk security tasks

Reduce Security team workload overhead

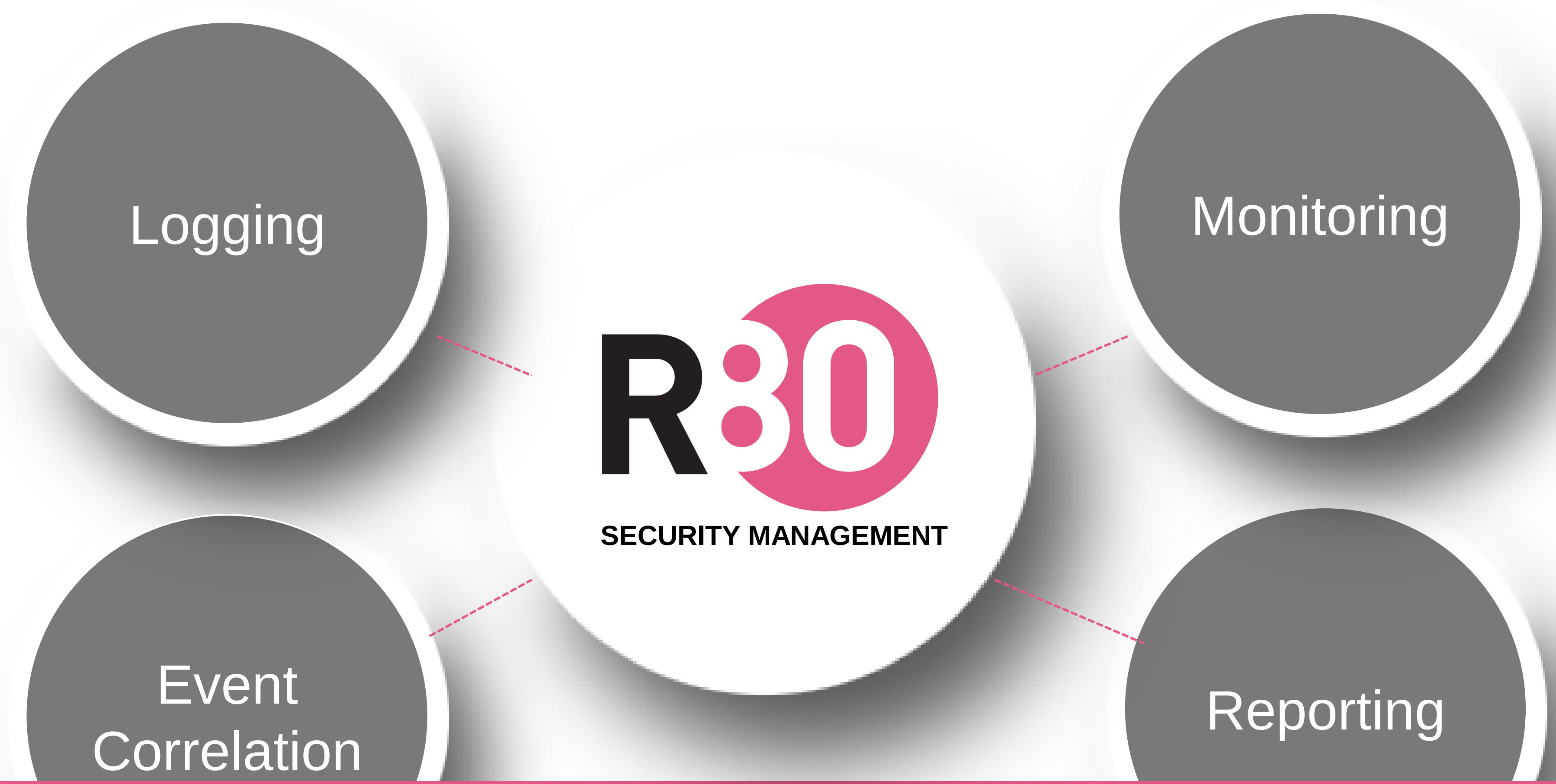


R80 CHANGE THE WAY YOU **MANAGE RISK**

Check Point
SOFTWARE TECHNOLOGIES LTD.

INTEGRATED THREAT MANAGEMENT

Fully Integrated Threat Management



Logging

Monitoring

R80
SECURITY MANAGEMENT

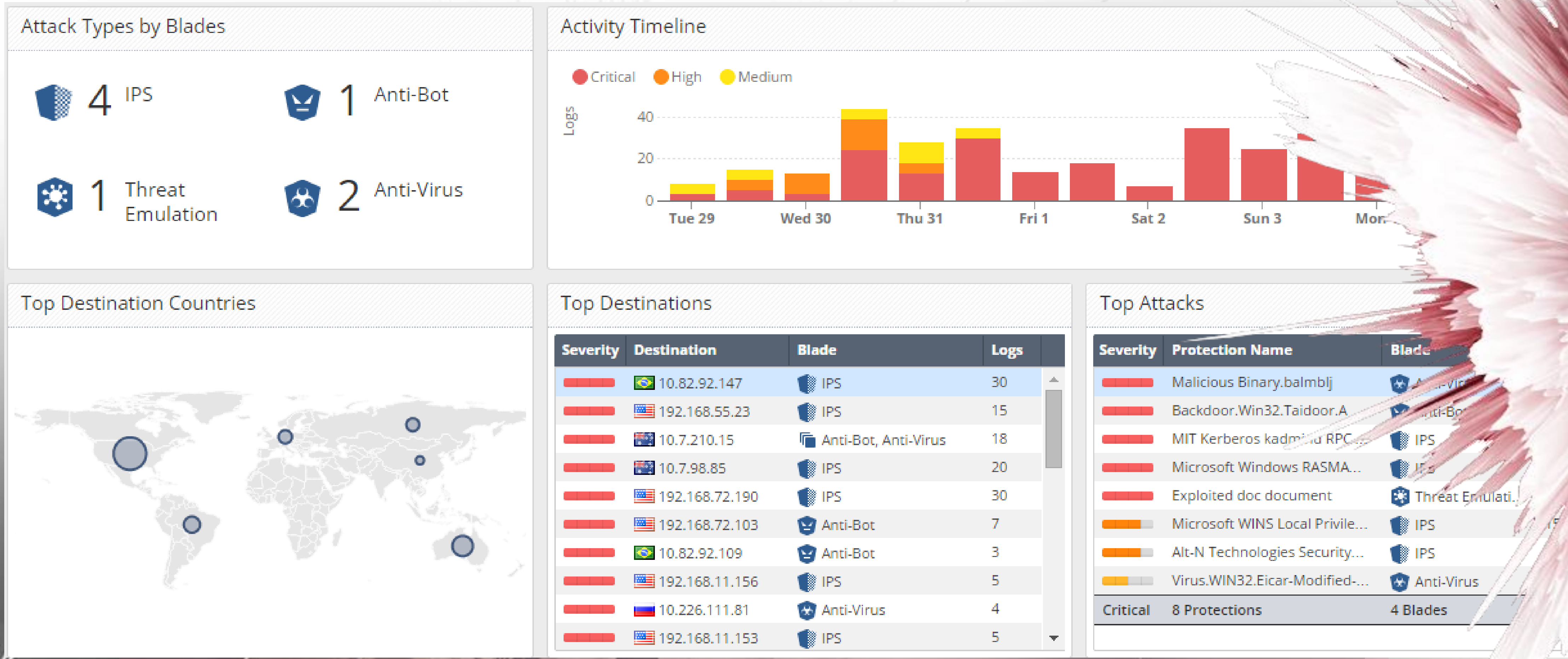
Event Correlation

Reporting

For Full Visibility Across Your Network

©2016 Check Point Software Technologies Ltd.

A Single View into Security Risk



Attack Types by Blades

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

Activity Timeline

Top Destination Countries

Top Destinations

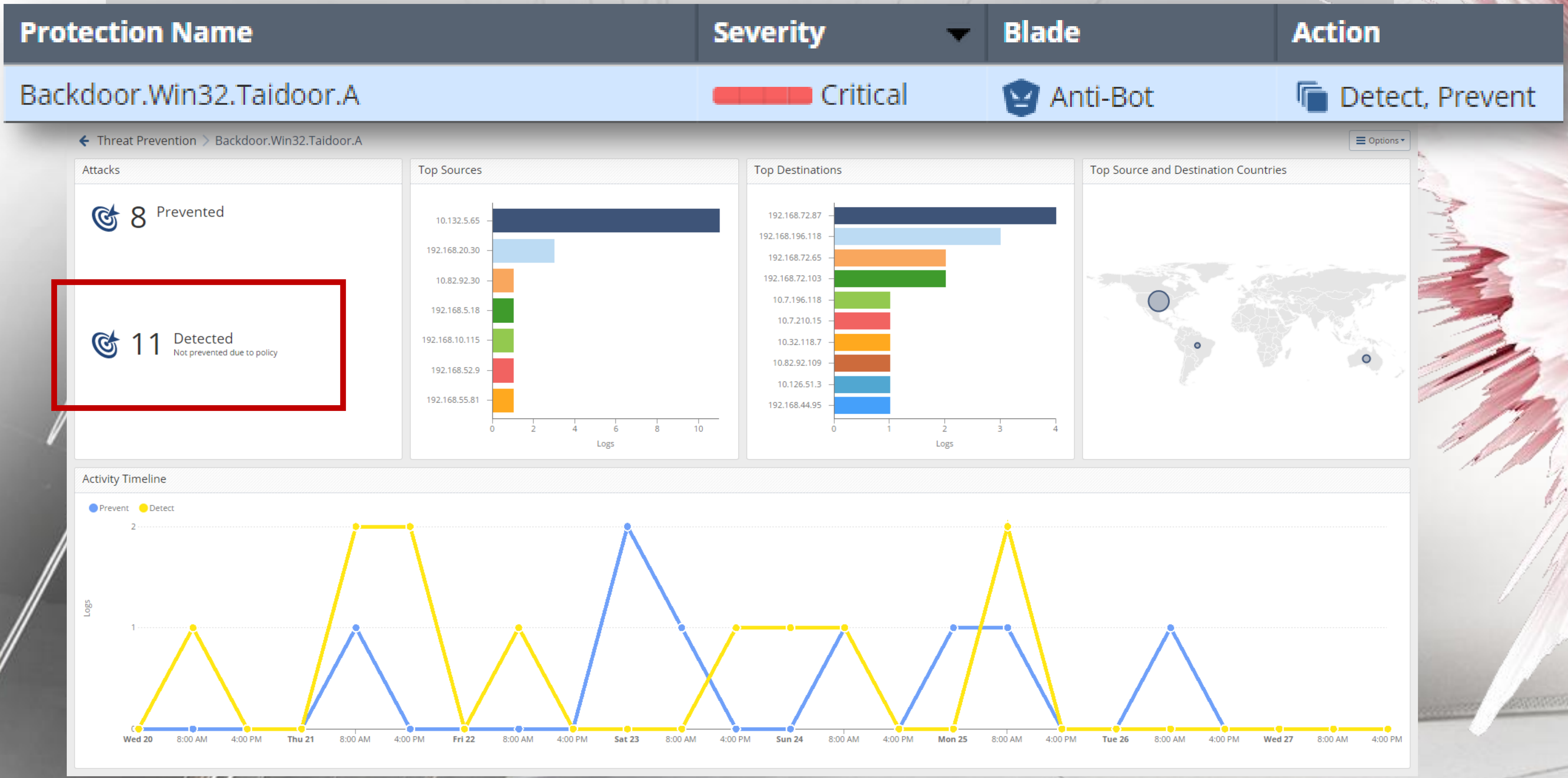
Severity	Destination	Blade	Logs
■■■■	10.82.92.147	IPS	30
■■■■	192.168.55.23	IPS	15
■■■■	10.7.210.15	Anti-Bot, Anti-Virus	18
■■■■	10.7.98.85	IPS	20
■■■■	192.168.72.190	IPS	30
■■■■	192.168.72.103	Anti-Bot	7
■■■■	10.82.92.109	Anti-Bot	3
■■■■	192.168.11.156	IPS	5
■■■■	10.226.111.81	Anti-Virus	4
■■■■	192.168.11.153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

Top Attacks

Severity	Protection Name	Blade
■■■■	Malicious Binary.balmblj	Anti-Virus
■■■■	Backdoor.Win32.Taidoor.A	Anti-Bot
■■■■	MIT Kerberos kadmind RPC...	IPS
■■■■	Microsoft Windows RASMA...	IPS
■■■■	Exploited doc document	Threat Emulati...
■■■□	Microsoft WINS Local Privile...	IPS
■■■□	Alt-N Technologies Security...	IPS
■■□□	Virus.WIN32.Eicar-Modified-...	Anti-Virus
Critical	8 Protections	4 Blades

©2016 Check Point Software Technologies Ltd.

Investigate the Threat



Protection Name	Severity	Blade	Action
Backdoor.Win32.Taidoor.A	🟥 Critical	Anti-Bot	Detect, Prevent

Threat Prevention > Backdoor.Win32.Taidoor.A

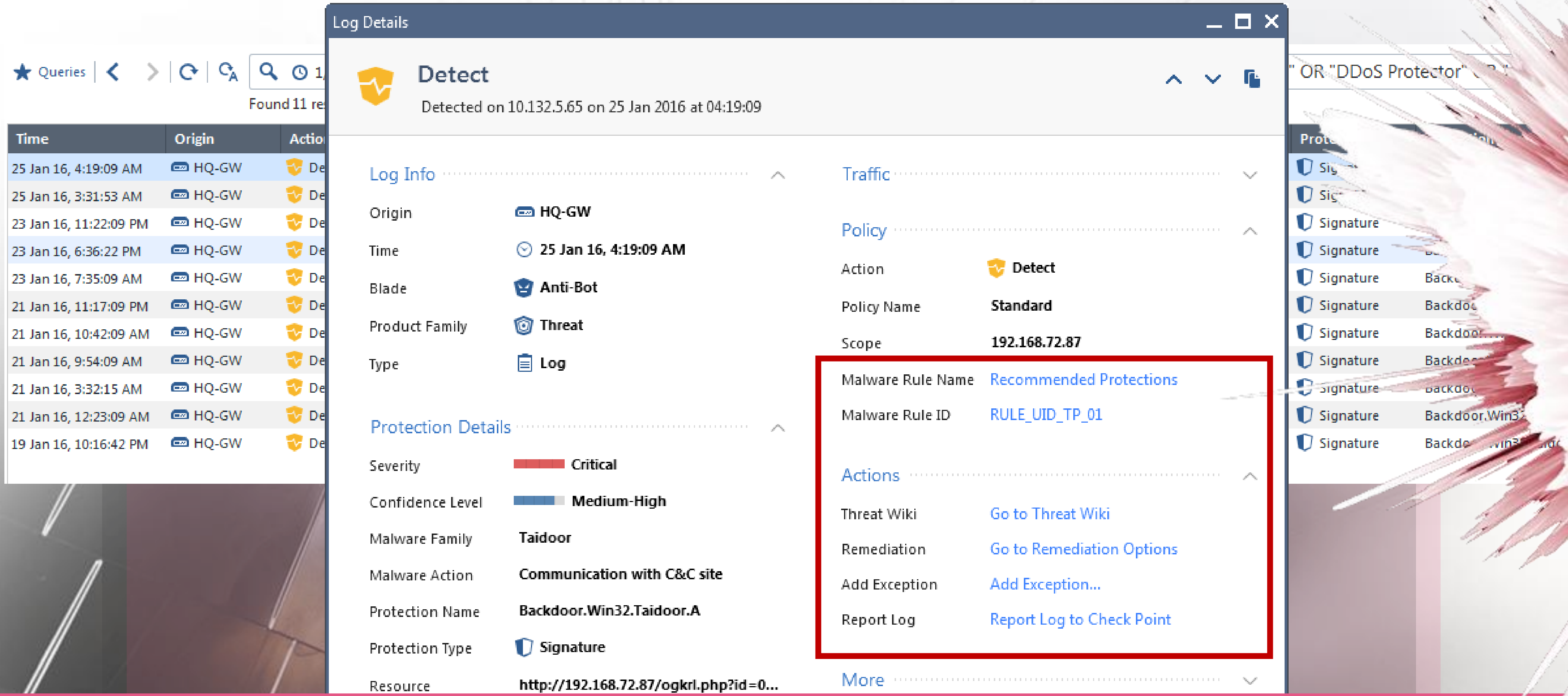
Attacks

8 Prevented

11 Detected
Not prevented due to policy

©2016 Check Point Software Technologies Ltd.

From View to Action



Time	Origin	Actio
25 Jan 16, 4:19:09 AM	HQ-GW	De
25 Jan 16, 3:31:53 AM	HQ-GW	De
23 Jan 16, 11:22:09 PM	HQ-GW	De
23 Jan 16, 6:36:22 PM	HQ-GW	De
23 Jan 16, 7:35:09 AM	HQ-GW	De
21 Jan 16, 11:17:09 PM	HQ-GW	De
21 Jan 16, 10:42:09 AM	HQ-GW	De
21 Jan 16, 9:54:09 AM	HQ-GW	De
21 Jan 16, 3:32:15 AM	HQ-GW	De
21 Jan 16, 12:23:09 AM	HQ-GW	De
19 Jan 16, 10:16:42 PM	HQ-GW	De

Log Details

Detect

Detected on 10.132.5.65 on 25 Jan 2016 at 04:19:09

Log Info

Origin	HQ-GW
Time	25 Jan 16, 4:19:09 AM
Blade	Anti-Bot
Product Family	Threat
Type	Log

Protection Details

Severity	Critical
Confidence Level	Medium-High
Malware Family	Taidoor
Malware Action	Communication with C&C site
Protection Name	Backdoor.Win32.Taidoor.A
Protection Type	Signature
Resource	http://192.168.72.87/ogkrl.php?id=0...

Traffic

Policy

Action	Detect
Policy Name	Standard
Scope	192.168.72.87
Malware Rule Name	Recommended Protections
Malware Rule ID	RULE_UID_TP_01

Actions

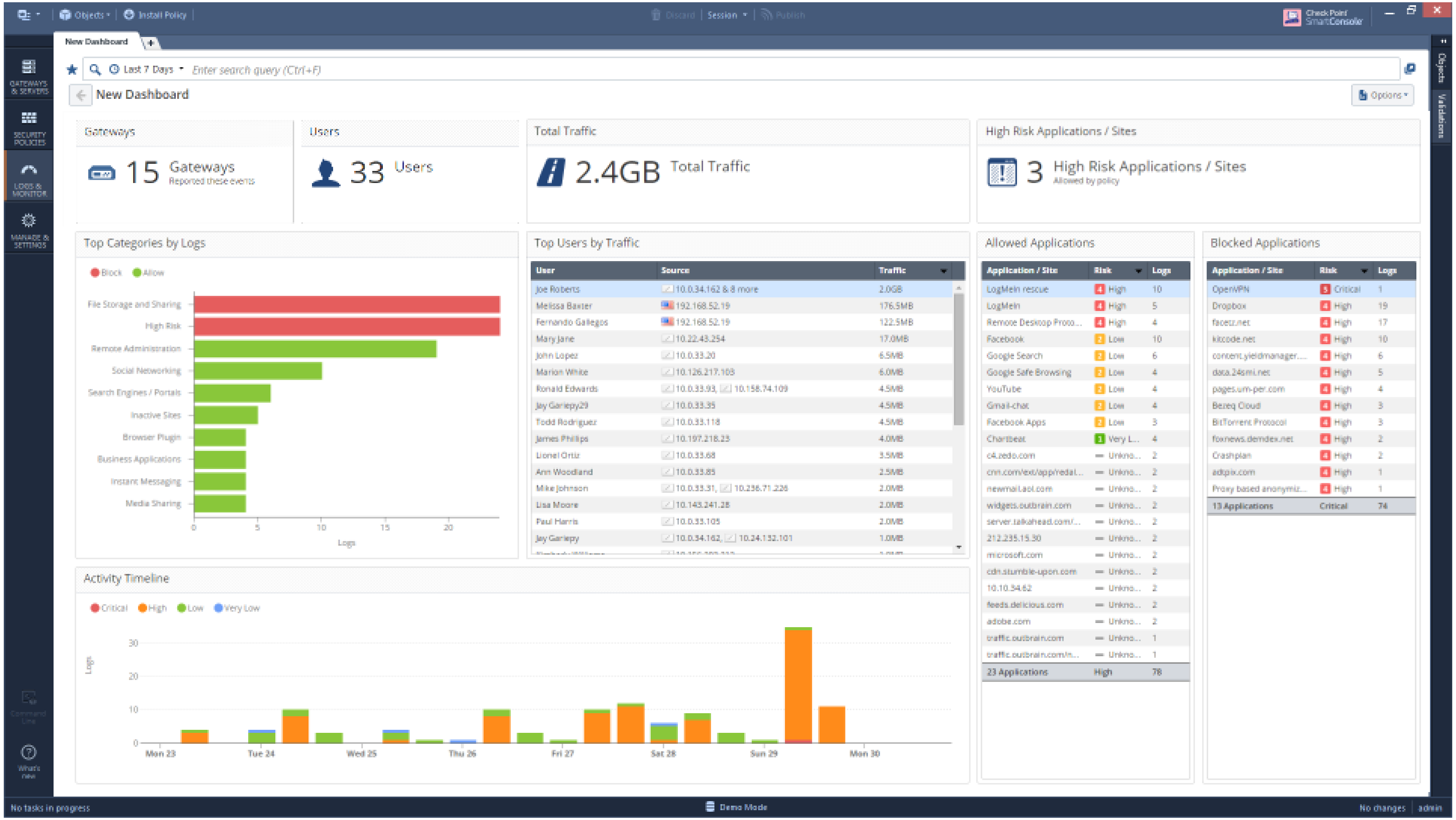
Threat Wiki	Go to Threat Wiki
Remediation	Go to Remediation Options
Add Exception	Add Exception...
Report Log	Report Log to Check Point

More

Respond to security incidents immediately and prevent the next attack

©2016 Check Point Software Technologies Ltd.

Easily Customizable, Monitor What’s Important



New Dashboard

Gateways: 15 Gateways — Reported these events

Users: 33 Users

Total Traffic: 2.4GB Total Traffic

High Risk Applications / Sites: 3 High Risk Applications / Sites — Allowed by policy

Top Users by Traffic

User	Source	Traffic
Joe Roberts	10.0.34.162 & 8 more	2.0GB
Melissa Baxter	192.168.52.19	176.5MB
Fernando Gallegos	192.168.52.19	122.5MB
Mary Jane	10.22.43.254	17.0MB
John Lopez	10.0.33.20	6.5MB
Marion White	10.126.217.103	6.0MB
Ronald Edwards	10.0.33.93, 10.158.74.109	4.5MB
Jay Gariepy29	10.0.33.35	4.5MB
Todd Rodriguez	10.0.33.118	4.5MB
James Phillips	10.197.218.23	4.0MB
Lionel Ortiz	10.0.33.68	3.5MB
Ann Woodland	10.0.33.85	2.5MB
Mike Johnson	10.0.33.31, 10.236.71.226	2.0MB
Lisa Moore	10.143.241.28	2.0MB
Paul Harris	10.0.33.105	2.0MB
Jay Gariepy	10.0.34.162, 10.24.132.101	1.0MB

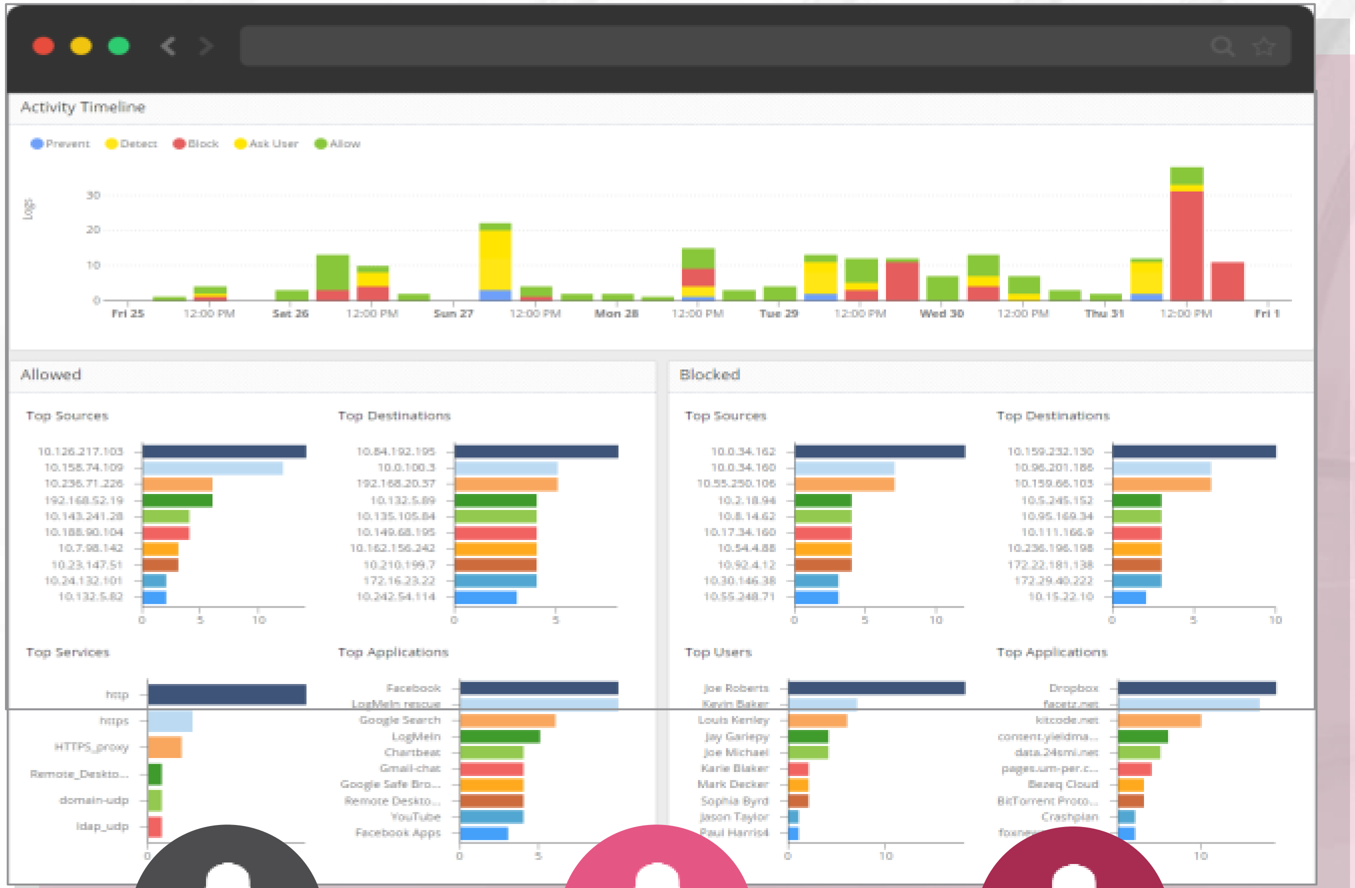
Allowed Applications

Application / Site	Risk	Logs
LogMeIn rescue	4 High	10
LogMeIn	4 High	5
Remote Desktop Proto...	4 High	4
Facebook	2 Low	10
Google Search	2 Low	6
Google Safe Browsing	2 Low	4
YouTube	2 Low	4
Gmail-chat	2 Low	4
Facebook Apps	2 Low	3
Chartbeat	1 Very L...	4
c4.zedo.com	Unkno...	2
cnn.com/ext/app/redal...	Unkno...	2
newmail.aol.com	Unkno...	2
widgets.outbrain.com	Unkno...	2
server.talkahead.com/...	Unkno...	2
212.235.15.30	Unkno...	2
microsoft.com	Unkno...	2
cdn.stumble-upon.com	Unkno...	2
10.10.34.62	Unkno...	2
feeds.delicious.com	Unkno...	2
adobe.com	Unkno...	2
traffic.outbrain.com	Unkno...	1
traffic.outbrain.com/n...	Unkno...	1
23 Applications	High	78

Blocked Applications

Application / Site	Risk	Logs
OpenVPN	5 Critical	1
Dropbox	4 High	19
facetz.net	4 High	17
kitcode.net	4 High	10
content.yieldmanager....	4 High	6
data.24smi.net	4 High	5
pages.um-per.com	4 High	4
Bezeq Cloud	4 High	3
BitTorrent Protocol	4 High	3
foxnews.demdex.net	4 High	2
Crashplan	4 High	2
adtpix.com	4 High	1
Proxy based anonymiz...	4 High	1
13 Applications	Critical	74

Easily Customize Your Reports



Accessible from any device

Management

Helpdesk

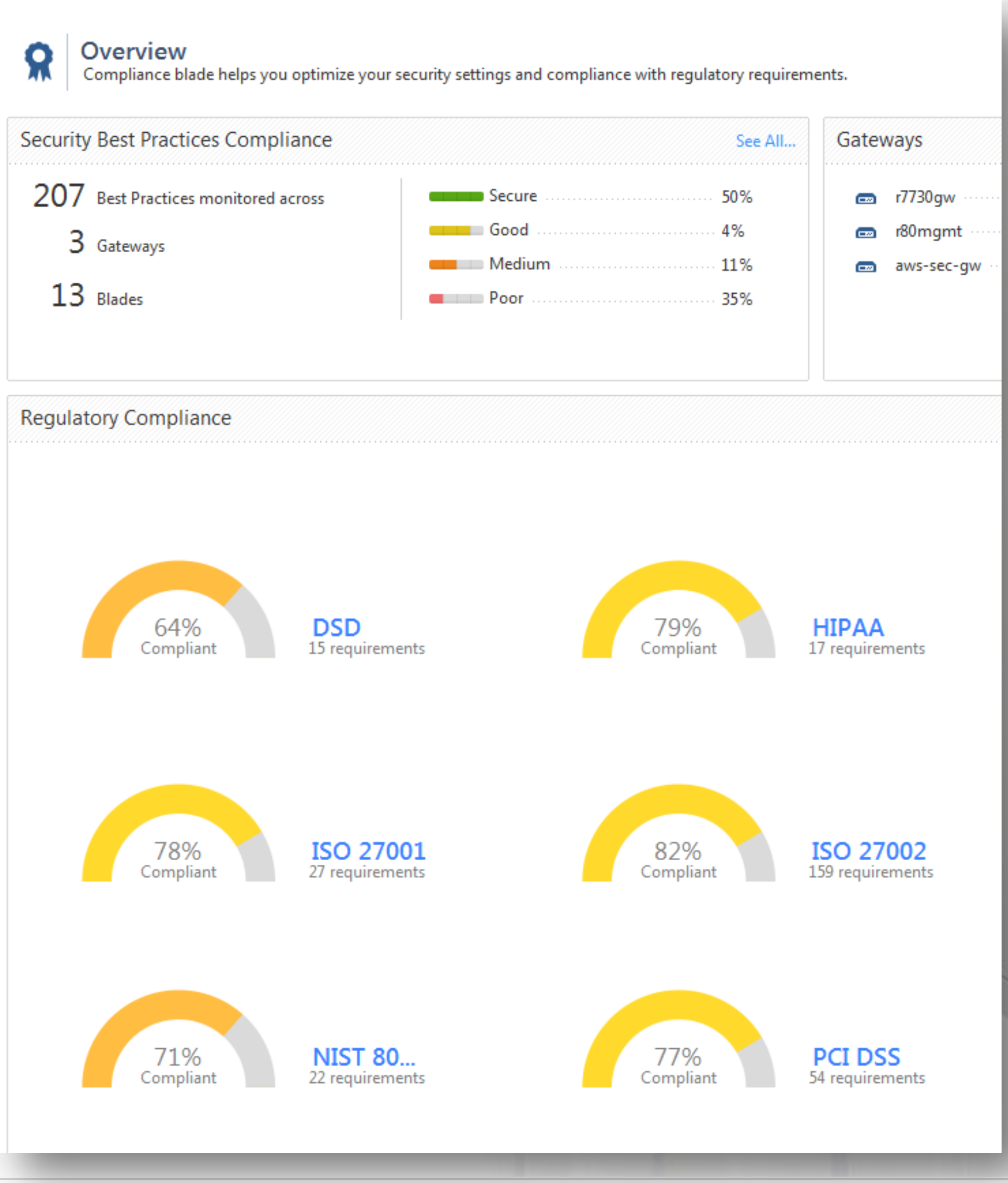
Auditor

©2016 Check Point Software Technologies Ltd.

Keep Your Security Compliant

Compliance Overview

Helps you optimize your security settings & compliance



Overview

Compliance blade helps you optimize your security settings and compliance with regulatory requirements.

Security Best Practices Compliance

See All...

207 Best Practices monitored across

3 Gateways

13 Blades

Secure	50%
Good	4%
Medium	11%
Poor	35%

Gateways

- r7730gw
- r80mgmt
- aws-sec-gw

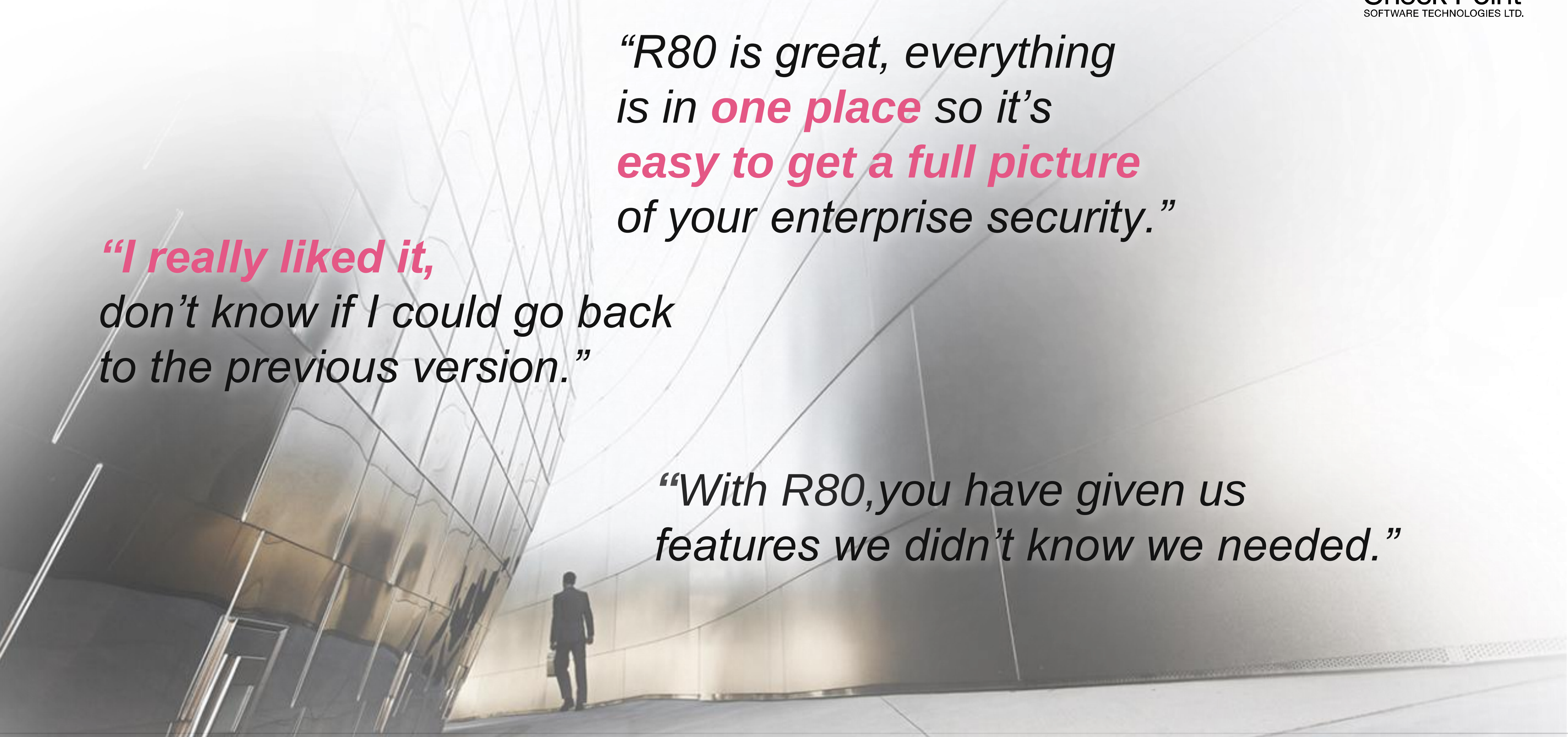
Regulatory Compliance

64% Compliant	DSD	15 requirements
79% Compliant	HIPAA	17 requirements
78% Compliant	ISO 27001	27 requirements
82% Compliant	ISO 27002	159 requirements
71% Compliant	NIST 80...	22 requirements
77% Compliant	PCI DSS	54 requirements

©2016 Check Point Software Technologies Ltd.

What Our Customers Are Saying

Check Point
SOFTWARE TECHNOLOGIES LTD.



“R80 is great, everything is in ***one place*** *so it’s* ***easy to get a full picture*** *of your enterprise security.”*

“I really liked it, *don’t know if I could go back to the previous version.”*

“With R80,you have given us features we didn’t know we needed.”

©2016 Check Point Software Technologies Ltd.

R80 THE FUTURE OF SECURITY MANAGEMENT

Check Point
SOFTWARE TECHNOLOGIES LTD.

Consolidate all your security

Keep pace with **dynamic** environments

Deploy security without **impeding innovation**

Gain **full visibility** to prevent the next attack

COMMUNITY. CHECKPOINT.COM

Check Point
SOFTWARE TECHNOLOGIES LTD.

R80

Ask questions. Share code. Stay up-to-date.

Customers

Partners

Experts

Check Point
SOFTWARE TECHNOLOGIES LTD.

THANK YOU

©2016 Check Point Software Technologies Ltd.