

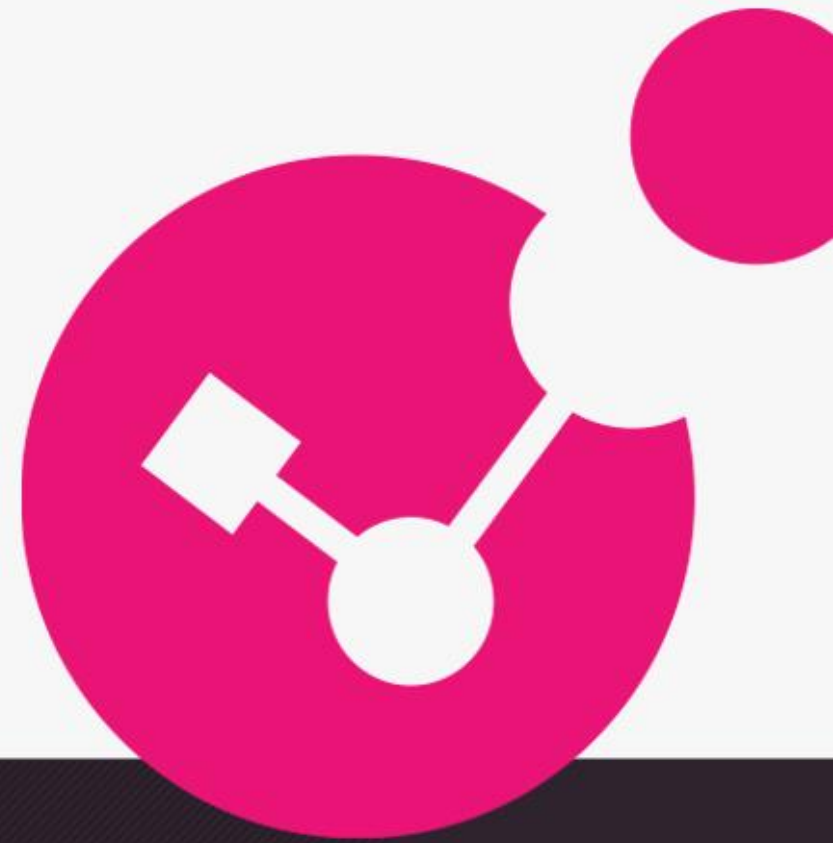


COMPLIANCE BLADE

Check Point GRC

Roberto Quiñones-Cruz | Technical Account Manager

Email us at - compliance@checkpoint.com



YOU DESERVE THE BEST SECURITY

Agenda

1. Compliance Blade

- How align with Check Point security best practices.
- How to comply with industry regulations (ISO, PCI, LGPD, etc)

2. SmartEvent

- Gain visibility with Smart Event
- Learn about SmartView and Smart Event Policy

Why Use The Compliance Blade?

- Making sure you're getting the most security out of your CP Platform.



Increased Security Scores

- Eliminating Poor Configurations
 - Rules using any, any, accept
 - Anti-spoofing is disabled
 - Expired or unused rules
 - Uncommented or undocumented rules
- 300+ Predefined Check Point Security Best Practices
- Customizable best practices to match your environment
- Monitoring changes in real-time



Detect Human Errors

- Misconfiguration of Gaia OS parameters
- Building non-compliant firewall rules
- Adhering to company configuration standards
- Auditable changes



Mistakes happen, but mistakes can be detrimental to your security posture!

Regulatory Compliance

- Translates thousands of complex regulatory requirement into actionable Security Best Practices
- 39 Built In Check Point Regulations
- Build custom compliance regulations for your environment and import



Check Point SmartConsole

Discard Session Publish

Log General Overview Compliance

Overview

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

Security Best Practices Compliance

214 Best Practices monitored across

1 Gateway

8 Blades

Secure	63%
Good	4%
Medium	4%
Poor	29%

Gateways

Top 5 Bottom 5 Favorites

HomeGW 74%

Blades

Firewall	92%
Gaia OS	79%
URL Filtering	47%
IPSec VPN	82%
IPS	56%

Action Items and Messages

Pending Action Items

0 Overdue items 2 Upcoming items 0 Future items 78 Unscheduled items

2 Security Alerts

December 15th 2020 16:05
Change made by admin on Firewall Blade violates with ISO 27002, NIST 800-53, ISO 27001, PCI DSS 2.0, DSD, HIPAA Security, GLBA, NIST 800-41, Firewall STIG, CobiT 4.1, MAS TRM, GPG13, NERC CIP, FIPS 200, SOX, Katakri 3.0, CJIS, PCI DSS 3.0, PPG 234, Protection of Personal Information Act, 2013, Statement of Controls (ISAE 3402), IT Grundschutz - Security Gateway, GDPR, New York State Cybersecurity Regulation, PCI-DSS 3.2, SANS Top 20, Customer Security Programme (CSP) regulations

December 15th 2020 08:50
Change made by admin on IPSec VPN Blade violates with ISO 27002, ISO 27001, PCI DSS 2.0, HIPAA Security, GLBA, NIST 800-53, CobiT 4.1, Firewall STIG, MAS TRM, NERC CIP, FIPS 200, SOX, CJIS, Katakri 3.0, NERC CIP (v.5), PCI DSS 3.0, PPG 234, Protection of Personal Information Act, 2013, Statement of Controls (ISAE 3402), IT Grundschutz - Security Gateway, GDPR, New York State Cybersecurity Regulation, PCI-DSS 3.2, SANS Top 20, Customer Security Programme (CSP) regulations

2 System Messages

January 3rd 2021 17:57
The Compliance Blade update package has succeeded. Security Best Practices and Regulations will be updated automatically

August 25th 2020 10:52
The Compliance Blade update package has failed. Please check the DNS and Proxy configuration on the Gateway or contact Check Point support

Regulatory Compliance

64% Compliant	GDPR	4 requirements
87% Compliant	HIPAA	15 requirements
93% Compliant	ISO 27002	142 requirements
97% Compliant	NIST 800-41	22 requirements
84% Compliant	PCI 3.2	28 requirements
93% Compliant	SOX	13 requirements

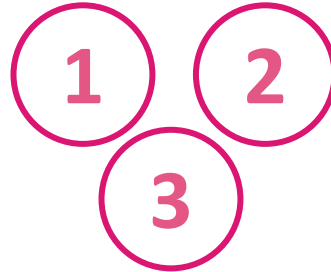
Object Categories

- Network Objects: 2772
- Services: 519
- Applications/Categories: 8821
- VPN Communities: 2
- Data Types: 62
- Users: 6
- Servers: 3
- Time Objects: 3
- UserCheck Interactions: 13
- Limit: 4
- Updatable Objects: 98

Commercial Model



Annuity Blade



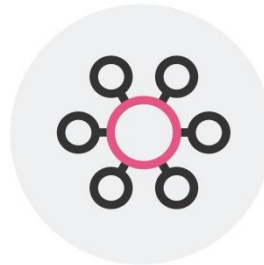
**Multi-year
Options**



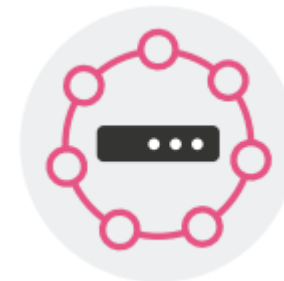
**Management
License**



**GW-based,
not Container**





**Multi-Domain
Pricing**



**Management
1st Year Free**

Check Point Differentiation

	
<p>Covers CP Products (FW, Blades, Management, GAIa,etc.)</p>	<p>Covers Firewall Only</p>
<p>Fully Integrated into Management</p>	<p>Third Party analysis (i.e. you need to buy another tool)</p>
<p>Find issues in real-time BEFORE you push policy</p>	<p>Run analysis reports after the fact</p>
<p>Used every day</p>	<p>Maybe used two to four times a year</p>

SmartEvent: Full Threat Visibility



**Customizable
Visibility**



**Real-Time Forensic &
Event Investigation**



**Unified
Views**

What is SmartView?

- SmartView is an application of the SmartEvent server
- SmartView is used for analytical purposes
- Consists of widgets

Each widget performs an independent query

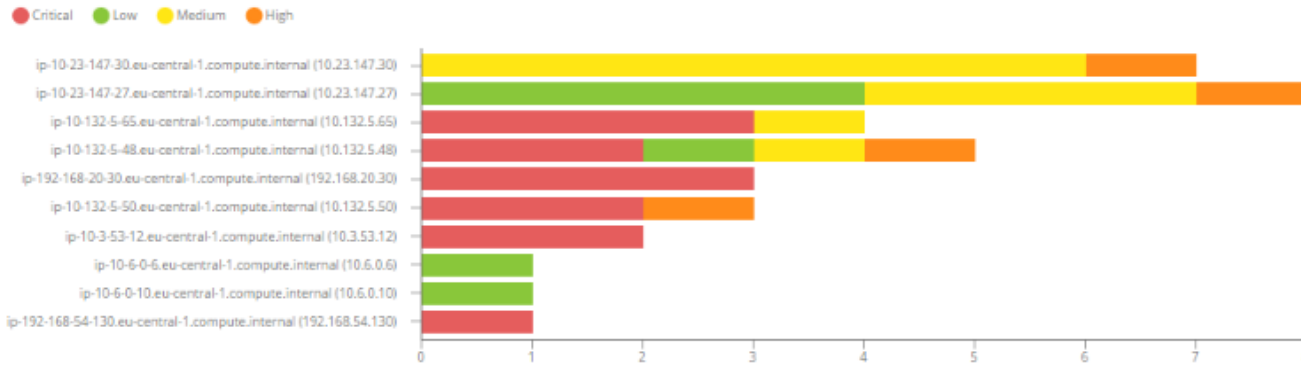
Generates a graphical presentation (such as maps, timelines, graphs, tables etc.) of the relevant information selected in the widget

Easily Customize your Reports

Hosts

13

Top Hosts by No. of Incidents



Top Hosts by No. of Incidents

Source	Severity	Blade	Protection Name	Protection Type	Action
ip-10-132-5-50.eu-central-1.compute.internal (10.132.5.50)	Critical	Threat Emulation	Exploited doc document Exploited pdf document	HTTP Emulation SMTP Emulation	Detect Prevent
ip-10-3-53-12.eu-central-1.compute.internal (10.3.53.12)	Critical	Threat Emulation	Exploited doc document Exploited pdf document	HTTP Emulation	Prevent
ip-10-132-5-65.eu-central-1.compute.internal (10.132.5.65)	Critical	Anti-Bot Anti-Virus Threat Emulation	Backdoor.Win32.Taldoor.A Exploited doc document Malicious Binary.balmbij Virus.WIN32.Eicar-Modified-Test-File	Emulation Signature	Detect Prevent

THREAT PREVENTION Report

Feb 14, 2018 12:00 AM - Feb 21, 2018 6:15 PM

Accessible from any device



Management



Helpdesk



Auditor

APPLICATION and URL FILTERING

General Activity

High Risk Applications

High Risk Users

High Bandwidth Applications

High Bandwidth Categories

High Bandwidth Users

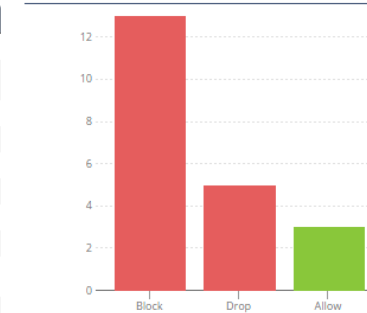
- Endless possibilities of reporting styles
- Generate reports for any audience
- Create your own templates

High Risk Applications

List of High Risk Applications

Application Name	Application Category	Risk	Action	Traffic	Logs
OpenVPN	Anonymizer	5 Critical	Block	22.4KB	1
Dropbox	File Storage and Sharing	4 High	Block	336.4KB	19
facetz.net	High Risk	4 High	Block	0B	17
LogMeIn rescue	Remote Administration	4 High	Allow	2.2GB	10
kitcode.net	High Risk	4 High	Block	0B	10
iMesh	P2P File Sharing	4 High	Drop	4.2KB	10
www.childabuse.com	Child Abuse	4 High	Drop	0B	9
www.walla.co.il	High Risk	4 High	Drop	0B	9
content.yieldmanager.edgesuite.net	High Risk	4 High	Block	0B	6
LogMeIn	Remote Administration	4 High	Allow	2.5MB	5
data.24smi.net		4 High	Block	0B	5
pages.um-per.com		4 High	Block	0B	4
www.bit.com	Gambling	4 High	Drop	0B	4
Remote Desktop Protocol	Remote Administration	4 High	Allow	23.2MB	4
Mobile Spy	Spyware / Malicious Sites	4 High	Drop	1.1KB	3
BitTorrent Protocol	P2P File Sharing	4 High	Block	0B	3
Bezeq Cloud	File Storage and Sharing	4 High	Block	0B	3
foxnews.demdex.net		4 High	Block	0B	2
Crashplan	File Storage and Sharing	4 High	Block	3.2KB	2
Proxy based anonymizers	Anonymizer	4 High	Block	0B	1
adtpix.com		4 High	Block	0B	1

High Risk Applications By Action



Allowed High Risk Applications

Application Name	Risk
LogMeIn rescue	4 High
LogMeIn	4 High
Remote Desktop Protocol	4 High

- Edit
- Restore Defaults
- Copy Report
- Hide Identities
- Export to Excel
- Export to PDF
- Export Template
- Report Filter
- Report Settings

What are events?

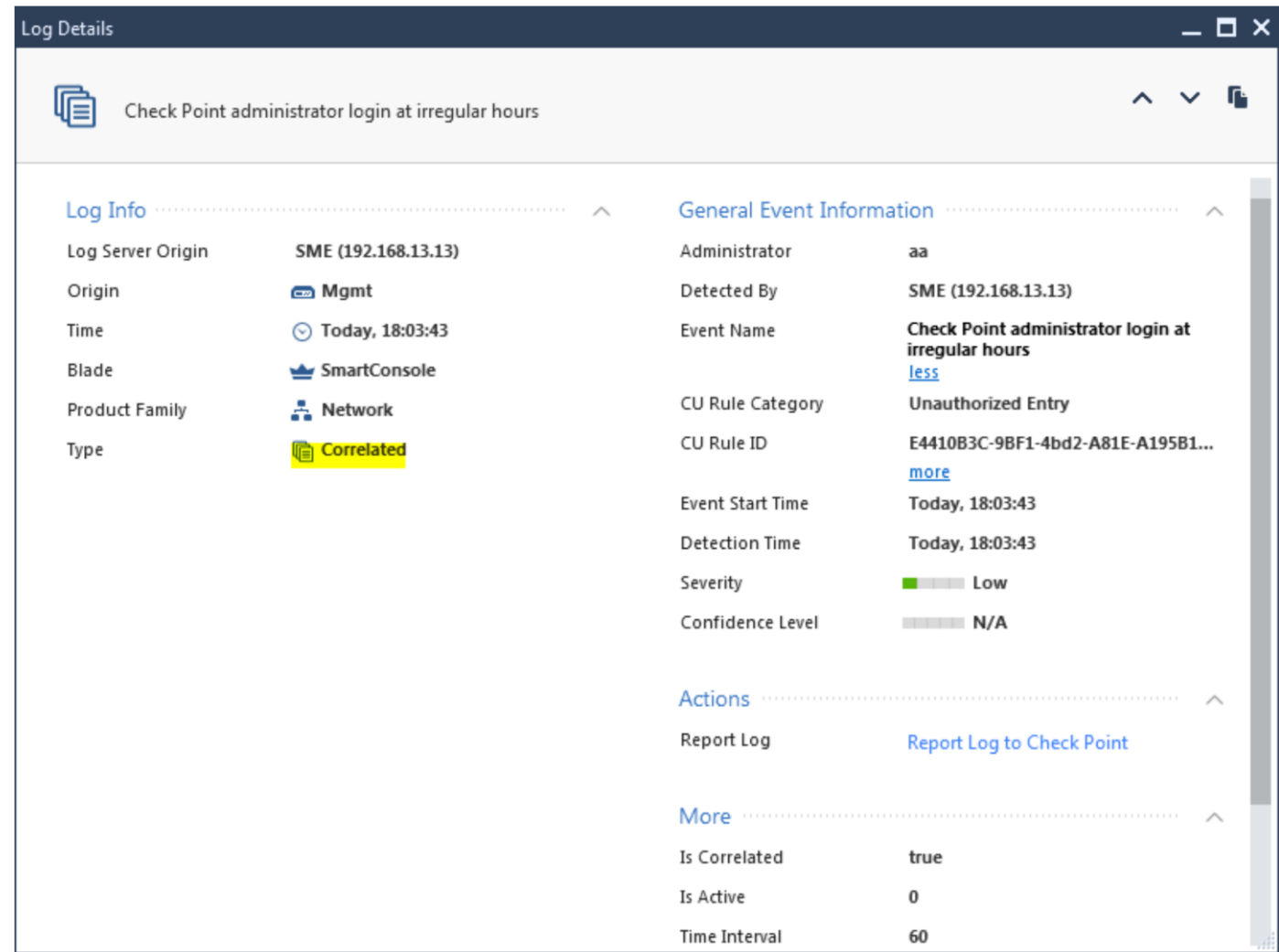
- Events are predefined or user defined filters and thresholds for certain values for fields such as action, protection name, blade etc.
- If traffic (or audit) logs has reached the threshold – an event is generated.
- We can add the following features to most events
 - Automatic reactions
 - Mail
 - External script
 - Block source
 - Block event activity
 - SNMP trap
- Exclusions
- Exception
- Time objects

What are events?

Example for audit event: CP admin login at irregular hours.

In this event there's a time object defining what are the regular working hours.

Logging out of this range will produce this event.



The screenshot displays the 'Log Details' window for a Check Point event. The event title is 'Check Point administrator login at irregular hours'. The interface is divided into several sections:

- Log Info:**
 - Log Server Origin: SME (192.168.13.13)
 - Origin: Mgmt
 - Time: Today, 18:03:43
 - Blade: SmartConsole
 - Product Family: Network
 - Type: Correlated
- General Event Information:**
 - Administrator: aa
 - Detected By: SME (192.168.13.13)
 - Event Name: Check Point administrator login at irregular hours
 - CU Rule Category: Unauthorized Entry
 - CU Rule ID: E4410B3C-9BF1-4bd2-A81E-A195B1...
 - Event Start Time: Today, 18:03:43
 - Detection Time: Today, 18:03:43
 - Severity: Low
 - Confidence Level: N/A
- Actions:**
 - Report Log: Report Log to Check Point
- More:**
 - Is Correlated: true
 - Is Active: 0
 - Time Interval: 60

What are events?

Example of a DLP traffic event:

This DLP event was created as a result of a DLP incident.

The screenshot displays a 'Log Details' window for a 'Detect' event. The event is titled 'DLP Detect DLP Data Type Name: Inappropriate Language'. The interface is divided into several sections: 'Log Info', 'Policy', 'Data Loss Prevention', and 'General Event Information'. The 'Log Info' section includes details such as Log Server Origin (SME), Origin (GW), Time (Today, 12:55:20), Blade (DLP), Product Family (Network), and Type (Correlated). The 'Policy' section shows the Action (Detect), DLP Rule UID, and DLP Rule Name (Inappropriate Language). The 'Data Loss Prevention' section provides details on the DLP Transport (FTP), DLP Action Reason (Rule Base), Original e-mail (View email...), DLP Relevant Data Types (Inappropriate Language), DLP Data Type Name (Inappropriate Language), Data Type UID, Matched File Percentage (0), Matched File Text Segm... (0), DLP Words List (blurred), and Scanned Data Fragment (DLPtest.txt). The 'General Event Information' section includes the Description (DLP Detect DLP Data Type Name: I...), Detected By (SME), Event Name (DLP Incident), CU Rule Category (Legacy;Check Point DLP Events), CU Rule ID, Event Start Time (Today, 12:55:19), Event End Time (Today, 12:55:20), Detection Time (Today, 12:55:20), and Last Update Time (Today, 12:55:20).

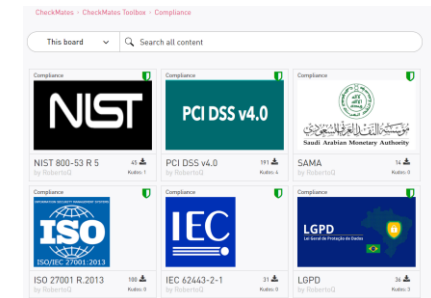
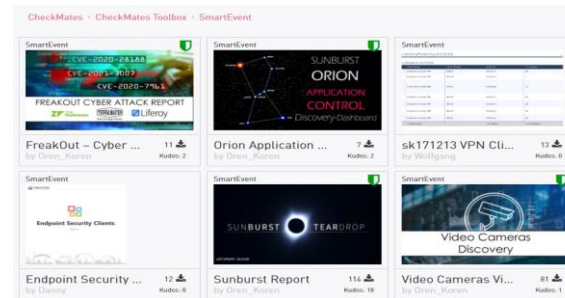
Log Info		Policy	
Log Server Origin	SME (192.168.13.13)	Action	Detect
Origin	GW	DLP Rule UID	9781FB42-E2D0-4F10-96BC-7EBDF6...
Time	Today, 12:55:20	DLP Rule Name	Inappropriate Language
Blade	DLP	Data Loss Prevention	
Product Family	Network	DLP Transport	FTP
Type	Correlated	DLP Action Reason	Rule Base
General Event Information		Original e-mail	View email...
Description	DLP Detect DLP Data Type Name: I...	DLP Relevant Data Types	Inappropriate Language
Detected By	SME (192.168.13.13)	DLP Data Type Name	Inappropriate Language
Event Name	DLP Incident	Data Type UID	79EF8572-A412-40BF-8ECA-86E78E9...
CU Rule Category	Legacy;Check Point DLP Events	Matched File Percentage	0
CU Rule ID	D3250971-7268-43B8-AB84-2006834...	Matched File Text Segm...	0
Event Start Time	Today, 12:55:19	DLP Words List	[blurred] [2 matches], [blurred] [2..
Event End Time	Today, 12:55:20	Scanned Data Fragment	DLPtest.txt
Detection Time	Today, 12:55:20	Actions	
Last Update Time	Today, 12:55:20		

Additional Resources (CheckMates ToolBox)

- Compliance Blade



- Smart Event



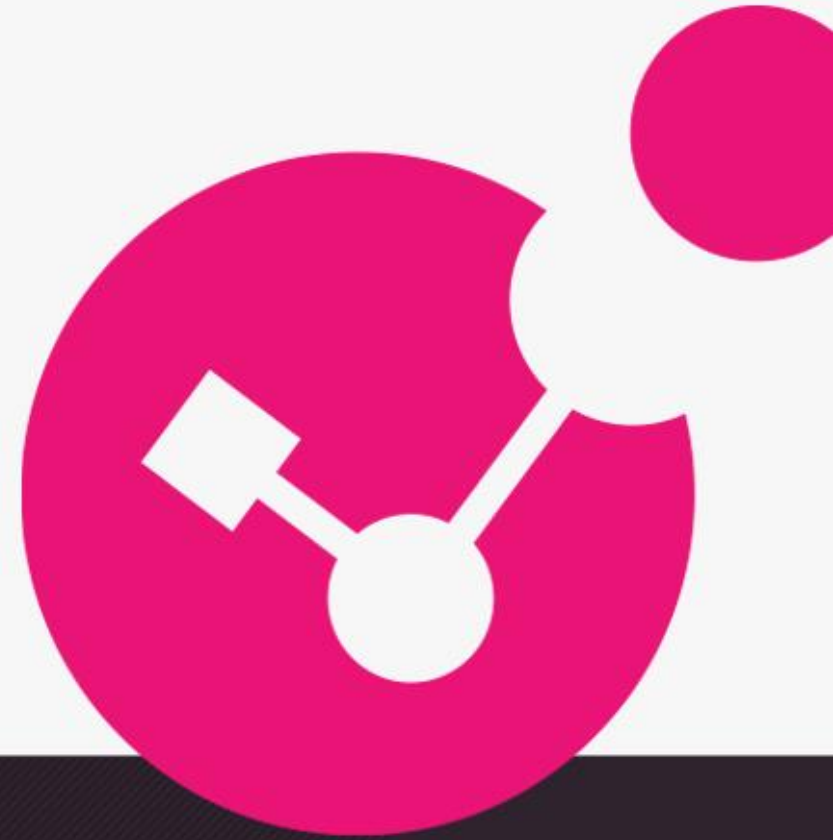
Summary

- Compliance Blade is EASY to use and customizable
- Can help detect and fix misconfiguration
- Generate audit reports (ISO, GDPR, SOX, PCI DSS and more)
- Smart Event Provides full threat visibility (SmartView and Events)



Thank you!

Email us at - compliance@checkpoint.com



YOU DESERVE THE BEST SECURITY