



Mastering Compliance

Unveiling the power of Compliance Blade

Roberto Quinones-Cruz

4-17-2024

YOU DESERVE THE BEST SECURITY

Agenda

- Introduction to the Compliance Blade
- Key features
- Technical Dive and How-To
- Demo
- Roadmap
- Conclusion and Q&A

Compliance Blade – Introduction

Compliance Blade lives in Security Management 

Helps you get the most security from your Check Point Platform



**Increased
Security Scores**



**Detects
Human Error**



**Regulatory
Security Compliance**

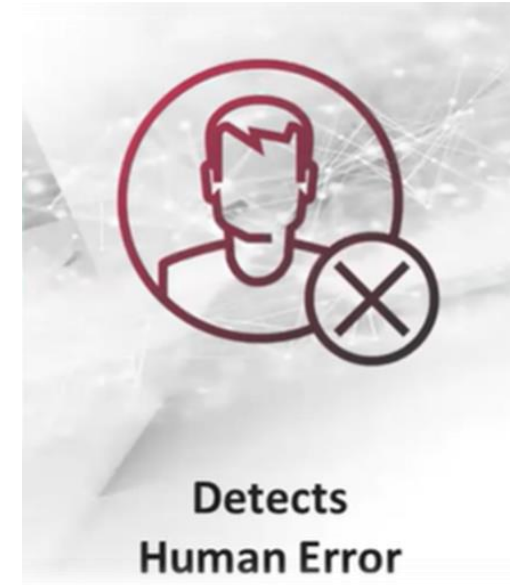
Configuration Management

- 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 Changes

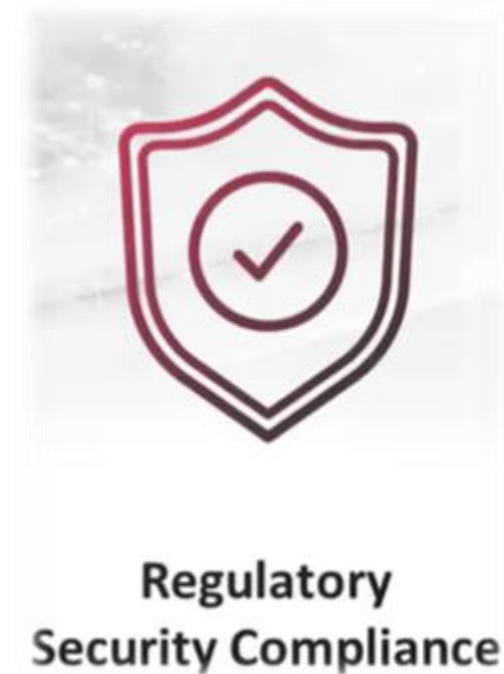
- Misconfiguration of Gaia OS parameters
- Building non-compliant firewall rules
- Adhering to company configuration standards
- Auditable changes



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

Regulatory Compliance

- Translates thousands of complex regulatory requirement into actionable Security Best Practices
- Built In Check Point Regulations
- Build custom compliance regulations for your Business Requirements



Compliance Blade View – Technical Dive

General Properties

- Network Management
- NAT
- Logs
- Other

Machine

Name: MGMT Color: Black

IPv4 Address: 172.23.51.213 [Resolve from Name]

IPv6 Address:

Comment:

Secure Internal Communication: Trust established [Communication...]

Platform

Hardware: Open server Version: R80.40 OS: Gaia [Get]

Management (7)

- Network Policy Management
 - Secondary Server
- Endpoint Policy Management
- Logging & Status
 - Identity Logging
- Workflow
 - User Directory
- Provisioning
- Compliance
- SmartEvent**
 - SmartEvent Server
 - SmartEvent Correlation Unit

Network Policy Management

Comprehensive security policy management using SmartDashboard - a single, unified console for all security functionalities.

[OK] [Cancel]

Overview

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

Security Best Practices Compliance [See All...]

214 Best Practices monitored across

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

1 Gateway

8 Blades

Gateways [Top 5] [Bottom 5] [Favorites] [See All...]

HomeGW: 74%

Blades [See All...]

- 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 [See All...]

- 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, CIJS, 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, 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 [See All...]

- 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 [See All...]

- GDPR**: 64% Compliant (4 requirements)
- HIPAA**: 87% Compliant (15 requirements)
- ISO 27002**: 93% Compliant (142 requirements)
- NIST 800-41**: 97% Compliant (22 requirements)
- PCI 3.2**: 84% Compliant (28 requirements)
- SOX**: 93% Compliant (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: 90

Policy Best Practice

Security Best Practices

Blade:Firewa

Active	Blade	ID	Name	Status
<input checked="" type="checkbox"/>	Firewall	FW102	Check that Anti-Spoofing has been activated on each Gateway	Poor
<input checked="" type="checkbox"/>	Firewall	FW103	Check that Anti-Spoofing is set to Prevent on each Gateway	Poor
<input checked="" type="checkbox"/>	Firewall	FW107	Check that there is an additional log server defined for each Gateway for the storage of Firewall logs	Poor
<input checked="" type="checkbox"/>	Firewall	FW150	Check the Expiration settings for User Accounts	Poor
<input checked="" type="checkbox"/>	Firewall	FW153	Check that each rule has a Comment defined	Poor
<input checked="" type="checkbox"/>	Firewall	FW156	Check the Expiration settings for Administrator Accounts	Poor
<input checked="" type="checkbox"/>	Firewall	FW108	Check that Firewall runs a script before deleting old log files	Medium
<input checked="" type="checkbox"/>	Firewall	FW116	Check that NAT/PAT is enabled in the Gateway Properties	Medium
<input checked="" type="checkbox"/>	Firewall	FW130	Check that 'Stealth Rule' is Defined in Access Policy	Medium
<input checked="" type="checkbox"/>	Firewall	FW143	Check the Hit Count data configuration	Medium

Relevant Objects: 1 out of 2 items are secure

Active	Rulebase	Rule Index
<input checked="" type="checkbox"/>	Corporate_Policy/Network	
<input checked="" type="checkbox"/>	Branch_Office_Policy/Branch_Office_Policy Netwo	3

Security Alert Details

Change Details

Date: 13/3/2024 18:36
 Host: 172.23.51.1
 User: admin

Security Best Practice Details

ID: FW130
 Title: Check that 'Stealth Rule' is Defined in Access Policy

Previous status: Secure

New status: Poor

Action Item: The 'Stealth Rule' in the Access Policy needs to be defined as follows: Source= Any; Destination= Security Gateway ; Service= Any; Action= Drop; Track= Not None ; Install on= Policy Target ; Time= Any. Note that the Stealth rule should be set in the top part of the policy. The Compliance Blade scans the top 30% of each Access Policy when searching for the Stealth rule.

No.	Name	Source	Destination	VPN	Service
Security Gateways Access (1-2)					
1	Administrator Access to Gateways	Admins	Corporate-GW	* Any	
2	Stealth Rule	* Any	Corporate-GW	* Any	* Any

Accept Log * Policy Targets

Configuration Best Practice

General Properties

- Network Management
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- ICAP Server
- Anti-Bot and Anti-Virus
- Threat Emulation
- Platform Portal
- UserCheck
- Mail Transfer Agent
- IPS
- IPSec VPN
- VPN Clients
- Logs
- Fetch Policy
- Optimizations
- Hit Count
- Other

Activation Mode

According to Threat Prevention policy

Detect only

Bypass Under Load

Bypass IPS inspection when gateway is under heavy load

Track:

Check Point ThreatCloud Information

Help Improve Check Point Threat Prevention product by sending anonymous information about feature usage, infections details and product customizations. [Learn More...](#)

IPS Update Policy

The gateway automatically updates the IPS protections. See sk120255

Use IPS management updates

IPS protections are updated according to the IPS update policy, under Threat Prevention Policy -> Threat Tools -> Updates

Security Best Practice #IPS111: Check that IPS protections per Gateway activated according to the IPS policy

Best Practice Details

- Description:**
This test checks all IPS gateways that their protections have been activated according to the policy.
- Action Item:**
The IPS Protections should be activated according to the policy.
Action Due Date: [Schedule Now](#)

Relevant Objects: 9 out of 10 items are secure

Active	Relevant Object	Status
<input checked="" type="checkbox"/>	Remote-3-gw	Secure
<input checked="" type="checkbox"/>	Remote-5-gw	Secure
<input checked="" type="checkbox"/>	Remote-1-gw	Secure
<input checked="" type="checkbox"/>	Remote-2-gw	Secure
<input checked="" type="checkbox"/>	Remote-4-gw	Secure
<input checked="" type="checkbox"/>	HQgw	Secure
<input checked="" type="checkbox"/>	Corporate-GW	Secure
<input checked="" type="checkbox"/>	RemoteBranchGw	Secure
<input checked="" type="checkbox"/>	EuropeBranchGw	Secure
<input checked="" type="checkbox"/>	BranchOffice	Poor

Security Alert Details

Change Details

Date: 10/4/2024 17:38
Host: 172.23.51.1
User: admin
Description: Engine mode: changed from 'by_policy' to 'detect_only'

Security Best Practice Details

ID: IPS111
Title: Check that IPS protections per Gateway activated according to the IPS policy
Previous status: Secure
New status: Poor
Action Item: The IPS Protections should be activated according to the policy.

Regulatory and Frameworks

The screenshot displays the Check Point Compliance Blade interface for ISO27001:2022. The main view shows a table of compliance items with their IDs, statuses, and names. A search bar and 'Generate Report' button are visible at the top right.

ID	Status	Name
8.13	Poor	Information backup - Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.
8.7	Medium	Protection against malware - Protection against malware should be implemented and supported by appropriate user awareness.
8.19	Medium	Installation of software on operational systems - Procedures and measures should be implemented to securely manage software installation on operational systems.
8.23	Medium	Web Filtering - Access to external websites should be controlled.
8.1	Good	User Endpoint Devices - Information stored on, and accessed from, user endpoint devices should be protected.
8.2	Good	Privileged access rights - The allocation and use of privileged access rights should be controlled.
8.5	Good	Secure Authentication - Secure authentication should be implemented.
8.9	Good	Config management - Configurations, including software, should be managed.
8.15	Good	Logging - Logs that record activities, exceptions, errors and failures should be generated, stored and protected.
8.20	Good	Network security - Networks and network devices should be protected.

Below the table, a section titled 'Relevant Security Best Practices: 0 out of 1 items are secure' shows a table with one item:

ID	Name	Blade	Status
FW107	Check that there is an additional log server defined for each Gateway for the storage of Firewall logs	Firewall	Poor

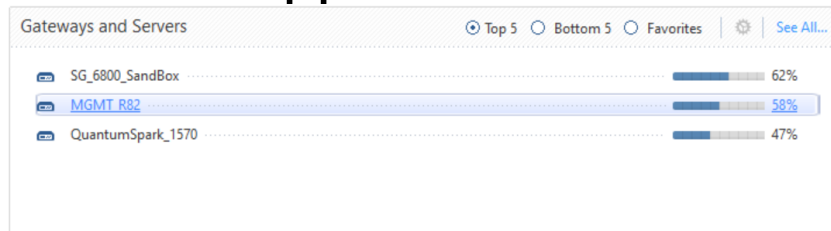
The right-hand side of the interface shows a 'Report' for 'Compliance Report ISO27001:2022', generated on April 10, 2024. It features a '73% Compliance' badge and a '75 Action Items' section with a pie chart showing 75 items are 'Unscheduled'. Below this, there are three summary charts:

- 186 Security Best Practices related to this regulation:** 50% Secure, 4% Good, 10% Medium, 24% Poor.
- 10 Regulatory Requirements:** 0 Compliant, 6 Good, 3 Medium, 1 Poor.
- Blades Security Status by Blade:** Firewall (82%), URL Filtering (57%), IPSec VPN (85%), IPS (46%).

Demo

Roadmap Compliance Blade R82 Management

Added support for Quantum Maestro and Quantum Spark Appliances:



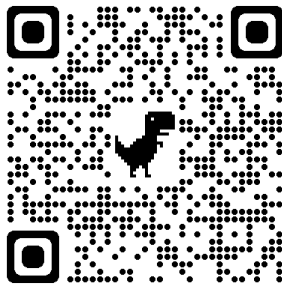
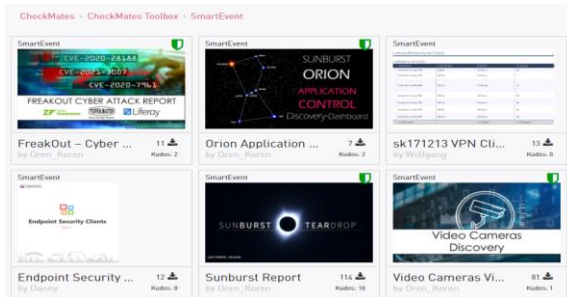
Status	Name	IP	Version	Active Blades	Hardware	CPU Usage
✓	MGMT_R82	192.168.100.19	R82	👑 🛡️ 📄 📄	Open server	2%
✓	QuantumSpark_1570	192.168.100.21	R80.20	📄 📄 📄	1570/1590 Appliances	0%
✓	SG_6800_SandBox	192.168.100.25	R81.20	📄 📄 📄	Maestro	0%

- Gaia OS Best Practice support for Maestro Security Groups by checking each Security Group Member individually and presenting a consolidated Best Practices status.
- Applying relevant Gaia OS Best Practices on Quantum Spark Appliances.
- Added Gaia OS Best Practice support for Log Servers.

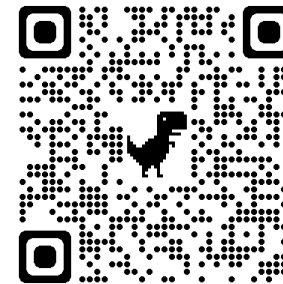
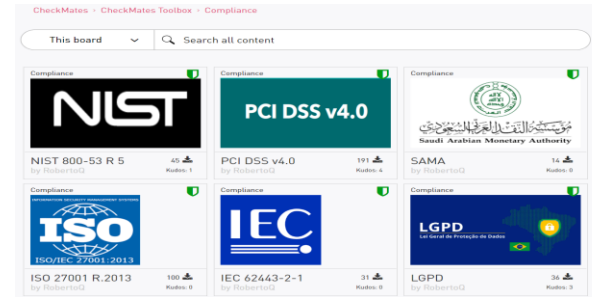
Additional Resources



SmartEvent



Compliance Blade



Summary

Q&A

- Compliance Blade is EASY to use and customizable
- Can help detect and fix misconfigurations
- Generate Compliance reports (ISO, GDPR, SOX, PCI DSS and more)



Thank You!

YOU DESERVE THE BEST SECURITY