

Compliance Software Blade

Frequently Asked Questions

General Information about Compliance

Q: What is Compliance?

A: Compliance is a process by which an organization checks itself against best practices and legal or regulatory requirements.

Q: How do I ensure I am compliant?

A: Check Point provides automated regulatory compliance reporting highlighting what is being checked and tested, as well as regulations that are at risk of being breached.

Q: Isn't Compliance an annual activity?

A: No. Organizations need to ensure they are constantly in compliance. The Compliance Software Blade automates this process and monitors the security policy in real-time and on an on-going basis.

Q: What if I don't need to be compliant with regulations? Can I still use our Compliance Software Blade?

A: Definitely. Non-regulated companies can use the security best practices that will help them improve their overall security. Many of the Early Availability participants had minimal regulatory exposure yet still found immense value from the best practices.

Regulations and Standards

Q: Which standards does the Compliance Software Blade cover?

A: Please refer to CP Wiki page: [Compliance Software Blade - Supported Regulations](#).

Q: Where can I find the latest and new standards the Compliance Software Blade covers?

A: Please refer to Checkmates [Toolbox Repository](#). You may download an XML which you can then import into the Compliance dashboard.

Q: How can future regulations or standards be added?

A: The Compliance team is constantly looking for new regulations and standards to include. If you have suggestions, send them through to compliance@checkpoint.com.

Sales and Positioning

Q: How is Check Point's 3D Security vision related to compliance?

A: 3D Security is about People, Policy and Enforcement. The Compliance Software Blade is a key component that adds value to any company in understanding and managing its overall security policy against Check Point best practices and security regulations.

Q: Does Compliance Software Blade run on the security gateway?

A: No. The Compliance Software Blade is a Management Software Blade and runs on the management environment and not on the gateway.

Q: If a customer has a Firewall Management solution, for example, AlgoSec or Tufin, will they still benefit from the Compliance Software Blade?

A: Yes. Those solutions provide compliance reporting for firewalls only, and their security checks are mapped to a limited set of regulations. The Check Point Compliance Software Blade has coverage of all the Network Security Software Blades and has much broader regulatory coverage too.

Q: Will it require the users of the Compliance Software Blade to invest a lot of time in set up and configuration? And on an on-going basis?

A: The Compliance Software Blade is non-intrusive. This is a real benefit to the customer as once the Software Blade is turned on, it constantly monitors the security architecture with next to zero investment on the part of the user.

Q: Can this tool be used as a reference for auditors?

A: Definitely. There are a number of pre-defined reports. The compliance summary report shows all the security best practices and the scoring. The regulation report shows all the checked regulatory requirements and itemizes what has been checked. This is a valid piece of documentation for any auditor.

Q: Can the Compliance Software Blade be of interest for CISOs?

A: Yes. Since CISOs are in charge of the company's overall security strategy, they will get a lot of value from the tool, as it provides a clear picture on Check Point's security recommendations and compares it to their current architecture, without any additional work.

Q: Which data will be presented, if the customer doesn't have all Check Point's blades?

A: The Compliance Software Blade presents the status of relevant security best practices according to the installed Software Blades. Security best practices for non-installed Software Blades can be viewed in a comprehensive table within the Compliance Software Blade. The purpose is to highlight to the customer what they could be monitoring if they had more blades from Check Point.

Working with non-Check Point Products

Q: Is it possible to interface the Compliance Software Blade with other products (such as PAN and Juniper products)?

A: No.

Best Practices

Q: What is a “best practice”?

A: A best practice is a specific recommendation developed by Check Point which defines the optimal way to configure the Check Point security and management blades. Best practices receive a compliance status that allows you to understand how well the best practice is currently implemented in your own environment.

Q: Is it possible to add new automated security best practices?

A: Check Point’s compliance team is currently authoring new content. Check Point will manage new content requests coming from Check Point SEs. Check Point is also exploring the possibility of allowing customers to write their own security checks and to define the automation rules from within.

Exclude

Q: Is it possible to exclude non-relevant gateways or clusters from the Compliance Software Blade?

A: The customer can decide which gateways and clusters are relevant and can exclude all others, ensuring minimal degradation in the overall security grade.

Q: Is it possible to exclude a specific security best practice from the Compliance Software Blade?

A: Yes. Sometimes, organizations have certain constraints that prevent them from configuring a Check Point Software Blade according to the recommendation. The Compliance Software Blade allows individual checks to be excluded along with the reason why the check should be excluded and for which period of time.

Technical Information

Q: Does the Compliance Software Blade only check the firewall for compliance?

A: No. The Compliance Software Blade supports all of the Network Security Software Blades: Firewall, IPS, IPSec VPN, Application Control, URL Filtering, Identity Awareness, Anti-Bot, Antivirus, Mobile Access, Anti-Spam and Email Security, and DLP.

Q: Does the Compliance Software Blade have any performance impacts?

A: There is a nightly re-scan of the management which takes approximately 10 minutes. During this time, the Compliance Software Blade cannot be used but the other Software Blades can.