CONTINUOUS MONITORING SOLUTION FOR GOVERNMENT AGENCIES

Organizations today demand continuous evidence that the Network Security environment is configured correctly and in line with best practice recommendations. Yet the reality is that this is a time consuming, complex and costly endeavor. The lack of available resources in security teams typically doesn't allow focusing on anything that isn't a core network security activity. As such, compliance reporting is often perceived as an unnecessary burden on an already overworked team.

The Continuous Diagnostics and Mitigation (CDM) program, launched by the Department of Homeland Security, is a dynamic approach to strengthening the cybersecurity of networks and systems, enabling network administrators to know the state of their respective networks at any given time and mitigate flaws at near-network speed. It is designed to deal with the challenge of what happens in-between audits, allowing administrators to understand what is occurring on a continuous basis. This shift in approach significantly alters the way organizations collect information and requires data collection to become fully automated.

SOLUTION

The Check Point Continuous Monitoring Solution provides Federal Agencies with real-time configuration monitoring against a library of security best practice diagnostics to ensure the configuration of Check Point is fully in line with expert recommendations. Check Point's Continuous Monitoring provides security and network administrators with detailed security status analysis against the recommended baseline and actionable guidance on how to remedy security weaknesses.

Check Point's Continuous Monitoring solution is fully integrated into Check Point Software Blade Architecture. Violation notifications highlight potential security and compliance violations, reducing the time required and errors associated with manual change management, providing you with control over your security environment at all time.

PRODUCT FEATURES

- Policies configurations are compared against a library of security best practices leveraging rich security expertise
- Customizable Federal policies in addition to Check Point's security baseline
- Constantly monitors gateway configuration with security best practices
- Security is checked with every change for all Network Security Software Blades
- Notifies on security policy changes negatively impacting security
- Easy to implement actions and recommendations
- Automated reporting

PRODUCT BENEFITS

- Real-time monitoring of Federal IT environments against regulatory standards and best practices
- 360 degree visibility of security status across Check Point Network Security Environment

SECURITY BEST PRACTICES

At the heart of Check Point's Continuous Monitoring solution lays a library containing hundreds of security diagnostics and best practices that define and recommend the optimal configuration for the Check Point Management, Software Blades and Security Gateways. The library of best practices have been defined and refined by Check Point security experts, leveraging Check Point's decades of security expertise. The best practices cover Check Point's Network Security suite, including Firewall Policy, Firewall and Gateway configuration, IPS, IPSec VPN, Mobile Access, Application Control, URL Filtering, Anti-Virus, Anti-Bot, DLP and more.

REGULATORY COMPLIANCE

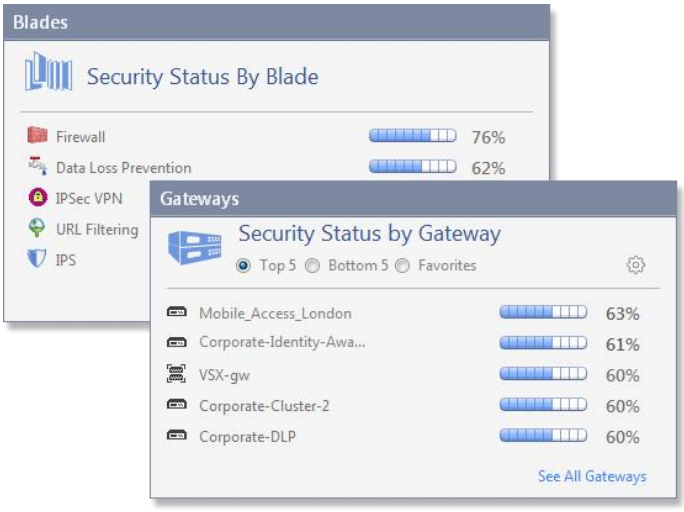
Check Point has created an extensive mapping that reflects the relationships between the Check Point Best Practices, and specific requirements within different regulatory frameworks. Check Point covers NIST 800-53, NIST 800-41, and the Network Firewall STIG published by DISA as part of its regulatory coverage. This mapping allows regulatory and audit reports to be produced constantly and at a click of a button. This can be extended and allows Federal Agencies to create a security policy within the Check Point Continuous Monitoring solution and define the relationships between the individual policy requirements and the Check Point Security Best Practices.

AUTOMATED SECURITY ALERTS

Check Point's Security Violations technology performs real-time simulation analysis before the change is installed as policy, providing Administrators the peace of mind that all changes made will be scanned against Check Point's Best Practice Diagnostics and will generate violation notifications in the event that a change is in breach of recommendations. Violation notifications highlight potential security and compliance violations, reducing the time required and errors associated with manual change management, providing you with control over your security environment at all time.

RECOMMENDATIONS AND ACTION MANAGEMENT

All security best practices have corresponding recommendations, assisting security managers in understanding what actions need to be taken to improve compliance and security. The Continuous Monitoring solution enables effective management of actions and recommendations, and facilitates prioritization and scheduling of action items.



CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com