XM Cyber

Integration Solution Brief

XM Cyber Security Controls Monitoring

For Checkpoint New Generation Firewall

Executive Summary

To enable the modern business to be successful, IT services must enable the business to work at the speed they need, while optimizing service delivery and ensuring business continuity and customer satisfaction. To do this organizations must implement and maintain a complicated, and constantly developing connected IT infrastructure. As these services evolve and transform, they also suffer from the growing security risk.

To address this and better defend the business from threat actors and adversaries, while ensuring the smooth running of business-critical systems and services, many CISOs are seeking to understand and then improve the security posture of their attack surface.

Enabling this requires a centralized viewpoint of all their security systems, control policies, and processes, that provide awareness of the current state, and the guidance needed to implement more effective security, without causing unnecessary friction to the business. To do this, they need a Security Controls Monitoring platform that integrates seamlessly with their existing cybersecurity ecosystem, and provides unique insights to optimize their primary security solutions.

CHECK POINT

+

Proactive security validation, instantly exposing misconfigurations and policy gaps to ensure your defense is always at its strongest.

The Need For Comprehensive Security Controls Monitoring

When cybersecurity responsibilities are dispersed throughout the organization, it is nearly impossible to comprehend how secure your organization is. Aligning effective security controls to security benchmarks, recommendations, regulations, and best practices can be very complex. Maintaining business continuity while under constant and increasing risk in an ever-evolving threat landscape, further compounds the strain on IT Security resources and personnel.

Effective cybersecurity requires synergy between people, processes, and technology. As such the purpose of continuous security controls monitoring is to ensure that each component is operating effectively and aligned to the same outcomes. Achieving this requires the design, implementation and testing of Critical Security Controls (CSCs), across your security stack.

With XM Cyber SCM, Security Operations teams can monitor and manage the high-performance capabilities and rich features of the Checkpoint NGFW as a crucial component in an organization’s cybersecurity strategy. This means teams can safeguard sensitive data, prevent data breaches, and ensure compliance with security policies.

Introducing: CHECK POINT

Check Point's Next-Generation Firewall (NGFW),

Quantum Force Security Gateways & Hybrid Mesh Firewalls, is an advanced security gateway that combines traditional firewall functions with unified threat management features like intrusion prevention (IPS), anti-malware, sandboxing for zero-day protection, and application control to prevent sophisticated Gen V cyberattacks.

Introducing: XM Cyber

XM Cyber Security Controls Monitoring (XM SCM) solution is a cybersecurity awareness and compliance management platform that acts as a single source of truth for the security posture of your entire hybrid infrastructure. It provides visibility, validation and monitoring of all security tools, critical security controls (CSCs), and their alignment to common security frameworks and regulatory compliance standards.

Solution Benefits by Use Case:

Security Posture Management

Establish a security posture baseline for Cloud to Core infrastructure and security tools

Infrastructure Management

Integrating XM Cyber SCM with Checkpoint NGFW significantly enhances infrastructure hardening by continuously monitoring firewall rules and settings for potential vulnerabilities. The solution collects critical information, including any-accept rules, disabled rules, and expired rules, which helps organizations identify overly permissive configurations that could lead to unauthorized access. By addressing these vulnerabilities in real time, organizations can strengthen their defenses and mitigate the risk of potential attacks.

Security Configuration Optimization

The integration enables organizations to optimize their security configurations by identifying misconfigurations and applying best practices. XM Cyber SCM can highlight issues such as logging disabled on cleanup rules, anti-spoofing settings not being enforced, or management gateways having weak password policies. By addressing these configurations, organizations can enhance the effectiveness of their firewall solutions, leading to better security outcomes.

Safeguard Security Defences

Monitor divergence from security baseline to detect unwanted configuration changes

Configuration Drift Management

Configuration drift can create security gaps as firewall settings change over time without proper oversight. By integrating Checkpoint NGFW with XM Cyber SCM, organizations gain the ability to track changes to firewall rules and settings consistently. This oversight enables security teams to quickly identify any deviations from established security policies and remediate them, ensuring that the firewall remains compliant with best practices.

Anomaly Detection

The integration enhances anomaly detection capabilities by monitoring firewall logs for unusual patterns of activity or unauthorized access attempts. XM Cyber SCM can flag instances such as excessive failed login attempts or improper access configurations, enabling security teams to respond swiftly to potential threats. This continuous monitoring helps organizations identify and address anomalies before they escalate into significant security incidents.

Continuous Compliance Reporting

Simplify and increase adherence to leading industry compliance and regulations

Audit Readiness

Integrating XM Cyber SCM with Checkpoint NGFW supports organizations in achieving audit readiness by maintaining comprehensive documentation of firewall configurations and security events. By tracking critical parameters such as admin roles, password policies, and firewall rules, organizations can quickly provide evidence of compliance during audits. This level of preparedness streamlines the audit process and reinforces trust in the organization's overall security posture.

Compliance Risk Reporting

The integration facilitates comprehensive compliance risk reporting by generating insights into firewall security configurations and user account statuses. XM Cyber SCM highlights potential compliance gaps, such as weak password policies and accounts with excessive permissions, enabling organizations to proactively address risks. By producing detailed reports that outline compliance with regulatory mandates, organizations can ensure that they meet necessary security standards and maintain confidence in their governance practices.

Access Control and IAM · Endpoint Security · Data Protection · **Network Security** · Config Management

Email Security · Remote Access · Vuln Management · Device Management · Web Services

Virtualization · Security Rating · SSPM Cloud Services · SIEM / SOC · IT Management

Business Value Outcomes Of Technology Integration:

Ensure Continuous Security Posture Validation and Optimization for Checkpoint NGFW:

Reduce Operational Overhead

Effectively align cybersecurity technology, people, and processes to remediate exposures and implement proactive critical security controls.

Identify, track, and validate CSC indicators across all cybersecurity tools to correct misconfiguration, malfunctions, or security gaps in critical functionality.

Increase Security Posture & Cyber Hygiene

Ensure effective cyber hygiene that minimizes an attacker's ability to gain unauthorized access to your network and applications.

Comprehensive and continuous analytics that detect deviations from normal behavior and align access control policies to your desired security state.

Accelerate Adherence to Compliance Frameworks

Understand & report your security risk posture, to ensure the alignment of <PRODUCT SPECIFIC> configuration and policies to common compliance frameworks.

Out-of-the box CSC's and reporting, that drive your alignment to regulatory compliance frameworks, to simplify audit readiness.

About Check Point

Check Point Software Technologies Ltd. is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times.

Find out more

About XM Cyber

XM Cyber is a leading Continuous Exposure Management company that transforms the way organizations approach cybersecurity risk mitigation.

Uniquely combine continuous security control validation with XM Attack Graph Analysis™ capability to discover CVEs, misconfigurations, and identity issues, along with weaknesses in cybersecurity posture across the full attack surface.

It analyses how attackers can chain exposures together, or evade security defences, to reach and then compromise critical assets. The platform then provides detailed remediation guidance and recommendations to increase security posture and reduce cyber risk, enabling security teams to prevent more attacks with 75% less remediation effort.

Find out more

Stop wasting time on fixes that don't impact risk

XM Cyber gives you the context you need to make faster and more confident decisions about your security posture. Understand what critical security controls you have in place and how they are helping you align to best practices and regulatory compliance frameworks.

Now you can achieve continuous compliance across your dynamic Infrastructure, helping you reduce operational overhead and more effectively align cybersecurity technology, people and processes to remediate misconfigurations and implement proactive critical security controls.

The platform enables you to report compliance risk, by first understanding and then validating your security risk posture and it's alignment to common compliance and regulatory frameworks. Which in turn minimizes the attackers' ability to evade your security defences and increases your overall security posture.

It's time to change how you work, by ensuring your IT and Security Operations teams have the guidance they need to design and optimize effective critical security controls, while also mobilizing effective remediation strategies, helping you
Fix Less. Prevent More.