

XM Cyber Security Controls Monitoring

For BeyondTrust Privileged
Password Management (PAM)



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.



+



**Ensure the integrity of
your identity-centric
security posture by
protecting the paths to
privileged access**

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.

XM Cyber SCM and BeyondTrust seamlessly integrate together, enabling organizations to effectively design, implement and monitor the specific CSCs needed to optimize the deployment and operation of the full spectrum of identity, access and security to eliminate blindspots and prevent attacks.

Introducing: BeyondTrust

Protecting the Paths to Privilege Access

BeyondTrust is the global cybersecurity leader protecting Paths to Privilege™ with an identity-centric approach. Offering the full spectrum of identity, access, and security to create seamless and efficient solutions that combat internal and external threats.

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 Hardening

Optimize the availability and integrity of your enterprise-wide access control policies through an identity-centric approach that provides unparalleled situational awareness of privileged and remote access management. Minimize the risk of unauthorized access to critical systems.

Security Configuration Optimization

Establishing a sound foundation of privileged access management is essential to reducing the attack surface and onward threat propagation. Implement best practices and extend your zero trust network to all resources and critical systems, by ensuring you have full coverage of your BeyondTrust deployments.



Safeguard Security Defences

Monitor divergence from security baseline to detect unwanted configuration changes

Configuration Drift Management

Security teams gain a comprehensive view of all privileged access activities across the network. To help maintain their desired access control framework. Tracking key security controls such as password change frequency, max concurrent connections for privileged access, and monitoring for password changes outside of expected timeframes.

Anomaly Detection

Ongoing monitoring and recording of all privileged access sessions, allowing rapid detection of suspicious behavior and ensure the alignment with expected activities and operating patterns. Detect deviations from the baseline and alert when thresholds are exceeded, enabling immediate response to potential security threats.



Continuous Compliance Reporting

Simplify and increase adherence to leading industry compliance and regulations

Audit Readiness

Effective implementations of privilege access control are fundamental to a broad variety of regulatory compliance requirements and security frameworks. Continuous monitoring of policies and privileged use helps organizations comply with even the most stringent of regulations by providing detailed audit trails of privileged access actions.

Compliance Risk Reporting

Privileged identities hold the keys to critical systems and services, and require comprehensive awareness and management to protect their integrity and help organizations adhere to compliance frameworks. Detailed reports on access policies are generated, allowing organizations to demonstrate compliance with relevant regulations.

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 BeyondTrust PAM:



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 access control 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 BeyondTrust

BeyondTrust fights every day to secure identities, intelligently remediate threats, and deliver dynamic access to empower and protect organizations around the world. Our vision is a world where all identities and access are protected from cyber threats. Our innovative approach goes beyond just PAM to find, manage, and protect the Paths to Privilege™.

BeyondTrust's identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

Gain visibility and control over privileged identities, accounts, access, and pathways to privilege across your environment. Simplify deployments, reduce costs, improve usability, and supercharge your existing investments with the deepest set of privileged access management (PAM) and identity security capabilities.

[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.