XM Cyber

Integration Solution Brief

XM Cyber Security Controls Monitoring

For Zscaler Internet Access

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.

zscaler™

+

Accelerate digital transformation and ensure the integrity of your Cloud-Native Secure Service Edge

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. Which requires the design, implementation and testing of Critical Security Controls (CSCs).

XM Cyber SCM and Zscaler seamlessly integrate together, enabling organizations to effectively design, implement and monitor the specific CSCs needed to embrace cloud native zero trust and accelerate digital transformation so that customers can be more agile, efficient, resilient, and secure.

Introducing: zscaler

Zscaler Internet Access (ZIA) - Embrace cloud native zero trust

Zscaler Internet Access™ delivers the world's most deployed security service edge (SSE), built on a decade of SWG leadership.

Replace your legacy network security solutions with zero trust for secure connectivity, a great user experience, and administrative visibility and control.

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. Providing 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

In todays connected world, the delivery of secure internet access is essential for the protection of users, devices, and business services. Ensuring the integrity of the Zscaler platform, administrator roles, privileges, and the configuration of policy settings within it are of upmost importance, when globally deploying your zero trust network, and connected services.

Security Configuration Optimization

Establishing a sound foundation of internet access policies, web filtering, and exclusions across your transient workforce and remote infrastructure is essential for their protection and to minimize the risk of unauthorized access. Integrating with XM SCM helps you deisgn and implement best practices policies for internet use without causing unnecessary friction to the business.

Safeguard Security Defences

Monitor divergence from security baseline to detect unwanted configuration changes

Configuration Drift Management

Tracking configuration changes and modifications to web filtering policies, including policy additions, deletions, and blocking settings, helps avoid weaknesses and gaps that could be exploited via phishing or social engineering. These configurations are reviewed continuously to observe changes in how internet access is delivered, maintained, and regulated.

Anomaly Detection

Making sure everyone can securely access web apps and cloud services from anywhere, while staying safe from ransomware and threats is a priority for security teams. Being able to detect unexpected modifications to web filtering policies, traffic volumes, and observing unusual patterns helps track shifting threat levels in web activity to help prevent data loss or other malicious access events.

Continuous Compliance Reporting

Simplify and increase adherence to leading industry compliance and regulations

Audit Readiness

Web security configurations, policy changes, and administrative settings are documented for auditing purposes. Tracking updates to filtering rules provides insight into how security policies evolve. Maintaining records of security events supports compliance monitoring.

Compliance Risk Reporting

Security events and policy configurations are reviewed to identify areas where compliance may not align with defined security standards. The presence of filtering rules not fully enforced across users, groups, or locations is observed. Monitoring security data related to web filtering policies provides details on regulatory and security conformance.

Access Control | Endpoint Security | Data Protections | Network Security | Config Management

Email Security | **Remote Access** | Vuln Management | Device Management | **Web Services**

Virtualization | Security Rating | CSPM & SSPM | SIEM / SOC | IT Management

Business Value Outcomes Of Technology Integration:

Ensure Continuous Security Posture Validation and Optimization for Zscaler Internet Access:

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 secure internet access 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 Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure.

The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location.

Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest in line cloud security platform. Learn more at zscaler.com or follow us on X (Twitter) @zscaler.

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 combining continuous security control validation with its XM Attack Graph Analysis™ capability, to discover CVEs, misconfigurations, and identity issues, along with weaknesses in cybersecurity posture across on-premise and all major cloud environments.

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.