XM Cyber | SOLUTION BRIEF

Security Controls Monitoring

Continuously assess tool configuration, optimize defenses and streamline compliance.

Many organizations find themselves managing increasingly large tool stacks as they add additional security, business productivity and IT tools to meet business and compliance needs.

This introduces challenges such as ensuring that initial and ongoing configuration is optimal and maximum value is being delivered from each tool. With dozens of tools to manage, identifying which issues are most critical is difficult, even more so when layering in audit and compliance needs and associated costs.

XM Cyber helps organizations address these problems by continuously assessing tool security controls from deployment through day-to-day usage - proving that they are being used optimally. Issues are prioritized by severity, enabling busy teams to proactively close security exposures before they can be exploited and frameworks are mapped to specific controls making compliance simple.

SOLUTION BENEFITS

Continuously Assess Security Controls

Consolidate disparate tools into one console, assess configuration from deployment and maximize ROI

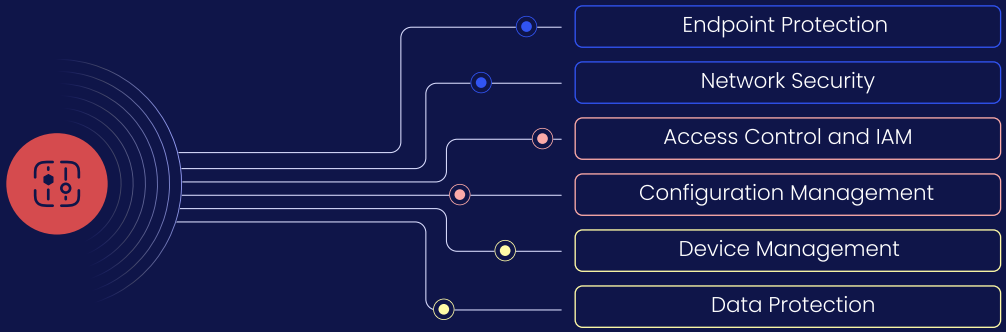
Proactively Optimize Defenses

See and close security weak spots before they can be identified and exploited by fast-moving attackers

Streamline Regulatory Compliance

Align with critical requirements, continuously support audit readiness and cut manual effort

Streamline Control Assessment and Compliance



XM Cyber: Optimizing Security Posture and Speeding Compliance

XM Cyber continuously monitors a wide range of tools used by businesses, as well as core Active Directory and cloud providers. Here are some of the key features:

Security Controls Monitoring

Critical security controls are continuously assessed across your tool stack, transforming lists of issues into a prioritized action plan managed from one dashboard. Ongoing monitoring identifies configuration drift and gives an up-to-date view of your security posture.

Broad Tool Coverage

A wide range of tools are covered across security, business productivity and IT categories. For example, endpoint security, network security, identity and access management, data protection, device management and many more.

Compliance Mapping to Controls

Where relevant frameworks and regulations are mapped to specific tools and frameworks, significantly reducing manual effort. Examples include BSI C5, CIS controls, FedRAMP, GDPR, ISO 27001, NIST CSF, PCI-DSS, SOC2 and more.

Hybrid Environment Support

Modern organizations operate hybrid environments to maximize operational benefits and the same is true of the tools they use. Unlike many other vendors, XM Cyber supports control assessment for tools deployed on-premises, in the cloud and SaaS.

Active Directory and Cloud Security Posture

Active Directory and cloud deployments are monitored for issues such as misconfigurations and excessive permissions, strengthening the security of your core services.

Guided Remediation

Remediation guidance aligns with CIS best practices and includes the specific steps that need to be taken for a fix to be implemented, with alternatives where needed. This facilitates fast communication, justification and rapid deployment of remediation efforts.

XM Cyber

As the pioneer of exposure management, XM Cyber delivers a continuous and actionable understanding of cyber risk across the entire attack surface, including hybrid, cloud, on-prem, OT, legacy, AI, and container environments. Powered by proprietary Attack Graph Analysis™, the platform continuously validates exploitable exposures against a digital twin of your production environment, applying nearly a decade of offensive security expertise. By revealing the critical choke points where multiple attack scenarios converge, XM Cyber directs security teams to the remediation actions that eliminate the most risk with the least effort. The result is measurable improvement in security posture through prioritized, high-impact remediation, along with clear, business-contextual reporting that enables leaders to communicate risk effectively and demonstrate security ROI.