XM Cyber | SOLUTION BRIEF

XM Cyber Cloud Exposure Management

Prevent Cloud Breaches By Proactively Eliminating Exposures And Validated Attack Paths That Put Your Business-Critical Workloads At Risk.

Many organizations view cloud as an environment that can and should be managed in a silo, with dedicated tools, teams and processes. The challenge with this approach is that attackers don't work in silos. Many cloud breaches are a result of lateral movement stemming from a compromised on-prem asset, highlighting the importance of understanding how hybrid environments interconnect and viewing exposures through the eyes of an attacker.

XM Cyber empowers organizations to see their infrastructure exactly as an attacker does, continuously mapping potential paths from compromised endpoints to critical cloud workloads. We move beyond scoring findings and assuming toxic combinations by validating exploitability and highlighting where every attack path converges to distinguish between theoretical noise and actual danger. This enables your team to proactively disrupt the attack chain, preventing lateral movement and securing business-critical data before a breach occurs.

SOLUTION BENEFITS

Continuous Discovery

Maintain continuous visibility into cloud accounts and resources running across multicloud environments with agentless posture assessment and automatic mapping of controls to common industry standards and best practices.

Context-driven Prioritization

Focus remediation efforts on exposures that put business-critical cloud resources and data at risk, highlighting choke points where multiple attack paths converge.

Attack Graph Analysis and Validation

Automatically map every potential attack path within and across cloud and hybrid environments, testing whether exploitability conditions are met to eliminate false positives and shut down lateral movement.

How XM Cyber Protects Cloud Environments

XM Cyber leverages Attack Graph Analysis™ to provide end-to-end visibility and exploitability-based exposure prioritization within and across dynamic multi and hybrid cloud workloads. Here's how it works:

Cloud Exposure Management

Proactively eliminate exposures from your cloud environments, understanding how cloud risk findings interconnect to form attack paths that put mission-critical cloud resources and data at risk.

Cloud Security Posture Management

Continuous visibility into cloud resources and workloads with a real-time understanding of their current configuration and security posture, mapped to common industry best practices and regulatory standards.

Cloud Vulnerability Management

ontinuously assess hosts and containers for lnerabilities, prioritize remediation efforts ased on validated exploitability and track mediation progress over time.

Cloud Infrastructure Entitlement Management (CIEM)

Track cloud accounts and permissions usage across your multicloud environments, identifying potential for privilege escalation and lateral movement and helping enforce LPA policies.

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.