XM Cyber

Digital Risk Assessment for Your M&A Growth Strategy

Continuous Exposure Management for Mergers and Acquisitions

Identify and close security gaps at every stage of the M&A lifecycle - before attackers exploit them.

M&A deals carry hidden security risks. The environment you're acquiring can include legacy systems, misconfigured assets, systems with excessive privileges, and credentials that attackers have already stolen. Yet many of these threats never show up during the due diligence process.

That means your security teams are making critical decisions based on incomplete information – usually under tight timelines. What's more, confidentiality limits what you can even start to assess before the deal closes. And after the deal, integration pressure limits how much you can fix before the networks connect.

XM Cyber continuously discovers and validates the exposures that M&A introduces - across every phase of the deal lifecycle. The platform scans external attack surfaces and exposed credentials before the deal closes, maps real attack paths across the acquired environment pre- integration and keeps exposure management running continuously once the two environments merge - so your team knows what to fix first and how to protect against opportunistic exploits.

More Informed Due Diligence

Better visibility into external exposures and exposed credentials of the target company before the deal closes.

More Secure Integration

Prioritize and remediate validated, high-impact risks for faster and more secure integration.

Unified Resilience

Continuously monitor the merged environment and report risk based on a shared baseline.

CEM for M&A: Resilience Across the M&A Stages

DUE DILIGENCE

Stealth Risk Assessment

Confidential, non-intrusive scans of the external attack surface.

PRE-INTEGRATION

Effective Risk Mitigation

Risk assessment across the hybrid environment and prioritization of what to fix first

POST-MERGER

Integration & Continuous Governance

Continuous discovery, prioritization, and remediation of the highest impact exposures

How XM Cyber Secures the M&A Lifecycle

XM Cyber Continuous Exposure Management platform provides a dedicated solution for enterprises that grow through acquisitions and need to streamline their security assessment throughout the M&A lifecycle. The CEM for M&A solution discovers, prioritizes, and drives remediation of the validated highest impact exposures across the hybrid environment at every step of the program, before attackers can exploit them.

Assess External Exposures

Discover internet-facing assets, outdated systems, and exposed credentials of the target company - all through passive, non-intrusive scanning that keeps due diligence confidential.

Quantify Risk for Decision Making

Score what you find against real-world exploitability so your team can make informed decisions about deal terms and integration planning.

Prioritize Integration Risks

Map validated attack paths across on-premises and cloud segments of the acquired entity and focus remediation on the exposures that carry the most business risk.

Establish Continuous Monitoring

Deploy unified exposure management for the combined environment to maintain security and compliance post integration.

Operationalize Repeatable M&A

Build a consistent security process across every deal - from technical kickoff and scope definition to KPI tracking and full deployment.

Report Risk to Leadership

Give leadership a shared risk baseline across both environments with clear, business-contextual security reporting they can act on.

Acquire the Business. Not the Liabilities.

Enhancing the M&A Security Lifecycle Workshop by XM Cyber

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.