XM Cyber | SOLUTION BRIEF

XM CYBER CONTINUOUS EXPOSURE MANAGEMENT

Securing the Global Economic Infrastructure

Prevent attacks targeting the critical financial systems, customer data, and hybrid infrastructures that power global markets.

Modern financial services delivery has evolved into a highly interconnected ecosystem, generating vast amounts of sensitive data including PII, PCI, and proprietary financial records, all while relying on a complex mix of multi-cloud environments, legacy infrastructure, and third-party tools. Traditional tooling and proactive security approaches fail to provide the attack surface coverage and context needed to effectively prioritize the exposures that actually threaten financial stability, regulatory compliance, and customer trust.

XM Cyber provides the exposure intelligence needed to see every exposure and attack path across your hybrid environment, from third-party integrations to core banking systems. The platform builds a dynamic digital twin of the entire IT estate, discovering and validating exposures and attack paths, and prioritizing those that put financial operations and service delivery in jeopardy. This approach eliminates wasted effort by pinpointing the specific exposures and paths that attackers can actually weaponize to compromise critical financial systems or nonpublic data.

SOLUTION BENEFITS

See Every Exposure, Every Path

Dynamically map the entire attack surface from internal networks to connected devices, uncovering every path an attacker could take to compromise core financial systems and SWIFT terminals.

Act for Impact, Not Just Severity

Eliminate noise and wasted effort by focusing on validated exposures and attack paths that actually jeopardize liquidity, capital reserves, or trading integrity.

Articulate Risk, Drive Remediation

Quantify risk and prove regulatory compliance with validated exposure intelligence to drive action among cross-functional stakeholders and ensure alignment with risk, compliance and audit teams.

XM Cyber: The Cure for Blind Spots and Missing Exposure Context

XM Cyber leverages Attack Graph Analysis™ to provide end-to-end visibility and exploitability-based exposure prioritization across dynamic hybrid environments. Here are some of the key benefits for financial services organizations:

Secure Legacy Core Banking Systems and Processes

Move beyond unpatchable systems by identifying attack paths that lead to the core and implementing compensating controls that don't require downtime.

Prove Compliance with Security and Regulatory Policies and Frameworks

Satisfy strict global requirements such as DORA, PCI DSS, and SWIFT CSP by continuously validating that your security controls actually work, providing empirical evidence for audits and board-level reporting.

Protect Distributed Payment and Transaction Terminals

Secure connected endpoints like ATMs and POS systems by ensuring a breach at the edge cannot pivot into your central financial ledgers.

Prevent Ransomware Attacks and Ensure Business Continuity

Identify and close the lateral movement paths used in ransomware campaigns to ensure zero downtime for mission-critical trading and consumer banking platforms.

Safeguard M&A and Facilitate Secure Cloud Migration

De-risk complex integrations and ensure that hybrid-cloud migration doesn't provide a direct, unmonitored road to your sensitive financial data by gaining instant visibility into how inherited exposures create new attack paths into your production environment.

Enable AI Adoption and Innovation without Introducing Risk

Secure the rapid adoption of AI banking tools by discovering "Shadow AI" workloads and validating that new AI integrations don't create unintended paths into your sensitive production and financial data.

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.