XM Cyber

Continuous Exposure Management Platform

Prevent Attacks that Put Your Business at Risk.

As hybrid environments grow more complex, organizations are overwhelmed by a staggering volume of exposures. Traditional tools flag thousands of issues but fail to identify the few that actually threaten business-critical assets. Solutions that ingest exposures from disparate tools merely centralize findings, and can't check exploitability, reachability, and the effectiveness of security controls as they relate to your environment. Teams end up with long lists of non-viable exposures, chasing the wrong priorities. With **agentic AI** accelerating exploitation from weeks to hours, security teams can't afford to chase non-viable exposures and need to eliminate the routes attackers can take before any compromise.

XM Cyber continuously uncovers what attackers can really do by integrating all exposure types into a single Attack Graph. By analyzing the paths attackers can take to critical assets, XM Cyber shuts down risks that truly impact your business before they are exploited.

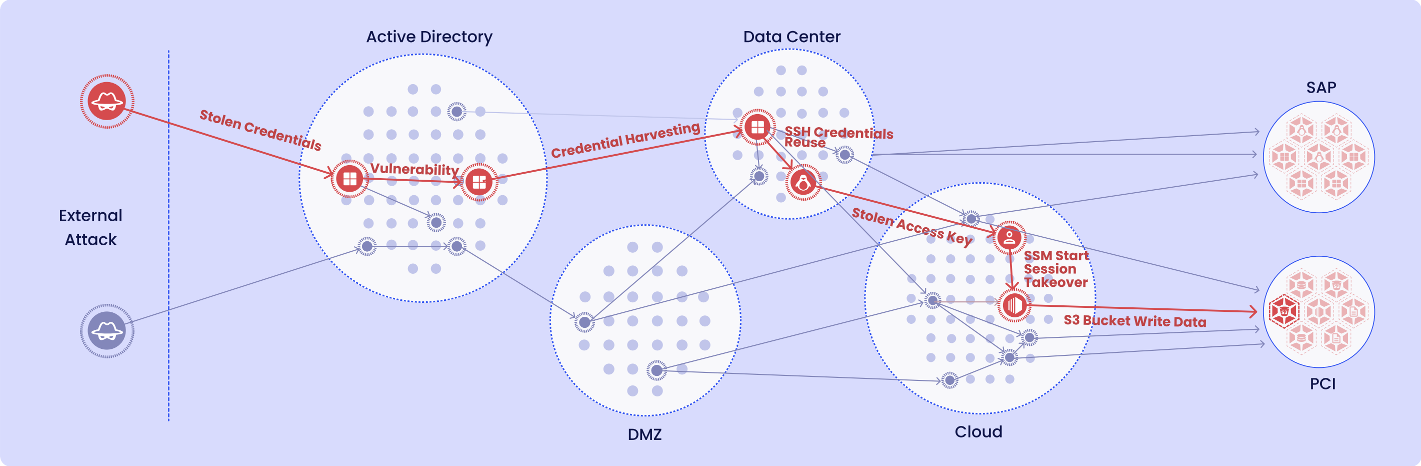
> "XM Cyber enabled us to move past raw vulnerability counts and understand what was truly exploitable. This allowed us to direct IT teams with precision, reducing time spent debating priorities and accelerating remediation."
>
> **John Meakin, CISO, Equiniti**

Benefits

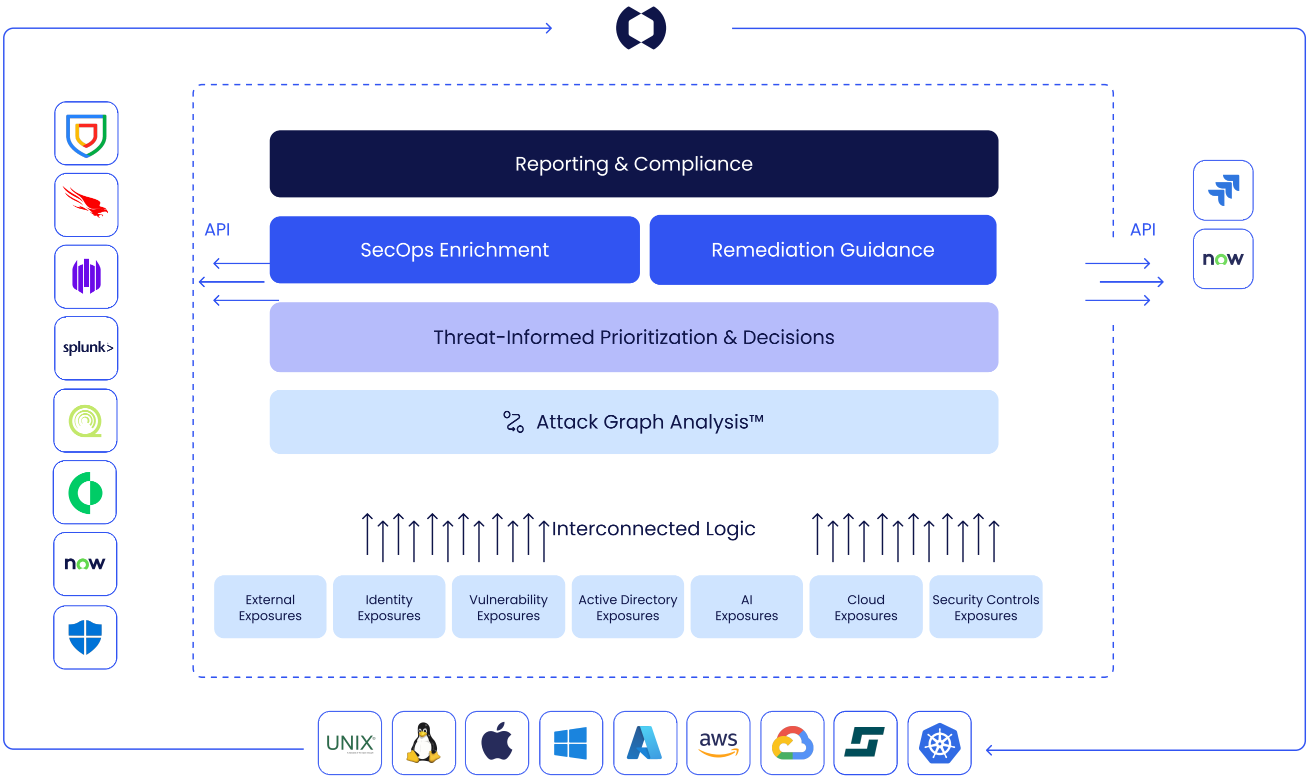
See Every Exposure, Every Path
Uncover validated exposures across the entire attack surface and eliminate all viable attack paths before attackers use them.

Act for Impact, Not Just Severity
Focus on fixing exploitable exposures on Choke Points to cut off multiple attack paths at once, improving remediation efficiency.

Prove Urgency, Drive Remediation
Communicate risk context effectively to align across teams and prove security posture and ROI to leadership.



Continuous Exposure Management Platform



Continuous Exposure Management Across the Full Attack Surface

XM Cyber operationalizes exposure management end-to-end, connecting diverse exposure types (vulnerabilities, misconfigurations, identity and access exposures, exposed credentials, AI exposures, etc.) to map how they form validated attack paths, from external exposures to the internal network, and across on-prem and multi-cloud environments.

True Validation of Exposures to Filter Out Noise

XM Cyber builds a digital twin of your overall environment to test multiple exploitability and reachability conditions for every exposure, taking into account active security controls in your environment.

Meaningful Risk and Compliance Reporting

With XM Cyber you can report on meaningful reduction of risk to business-critical processes and assets, prove effective security operations to leadership, and achieve continuous audit readiness by monitoring assets and security controls for policy violations.

Business-Driven Prioritization & Remediation

XM Cyber prioritizes remediation based on rich business impact context: the exposures that compromise the highest number of critical assets and are at intersections of multiple attack paths (Choke Points) are top priority – so a single fix eliminates many paths.

> “XM Cyber helped us go from thousands of critical vulnerabilities to just a handful of key fixes, reducing our exposure from 98% to 2%. That’s a game-changer for us.”
>
> **Ilaria Buonagurio, Head of CIS Prevention, Global Luxury Retail**