Use Case

XM Cyber | See All Ways™

XM Cyber for Continuous Vulnerability Prioritization

The smarter way to identify and remediate risks to your digital world

Complex, constantly changing digital networks represent an ongoing risk to most organizations. Information technol-ogy and cyber security teams are overwhelmed with alerts, software updates and new vulnerabilities. The only solution is to automate and integrate the right information at the right time to give clear direction across management, security and operations on where to focus. The end goal is to reduce risk associated with the most critical assets and optimize investments in capital and operating expense.

Not all vulnerabilities are created equal. XM Cyber combines advanced vulnerability scanning and patch management capa-bilities with its patented Attack Path Management platform to expose and remediate the greatest risks to your digital world. By adding additional context of how a particular vulnerability can be leveraged to compromise your critical assets, XM Cyber maximizes the effectiveness of your team's ability to proactively secure what matters most.

The Challenges of Finding and Fixing

Identifying and remediating vulnerabilities is a constant problem. To stay ahead of attackers, your cybersecurity program must become an ongoing process that relies on automation and intelligent analysis to support your security and IT responsiveness.

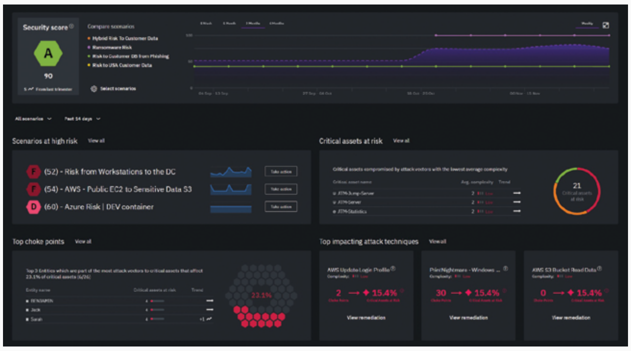
The first step is to continuously scan your network for potential risk. Typically, security teams scan for vulnerability data and then request the IT teams update or patch the affected systems. Sounds easy but in larger organizations, this can represent hundreds or thousands of common vulnerabilities and exposures (CVEs). Each one must be researched and prioritized. In some cases, the issue is low risk or only impacts a minimal number of low-risk systems. Sometimes the fix is a patch that has been superseded by another patch. The IT team has no means of prioritizing.

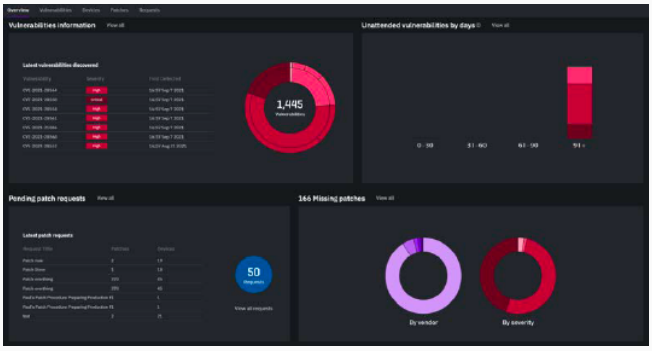
The Difference Between Risk-On and Risk-To Your Critical Assets

Your vulnerabilities represent risks associated with a particular asset. What's more important however, is identifying vulnerabilities that allow attack paths that lead to your critical assets. By prioritizing based on risks to versus risks on, you and your teams can pinpoint exactly the remedial activities required to close the complete attack chain related to your most critical assets. Ultimately, you lower or even eliminate risk while optimizing your team's time and effort.

Attack Path Management Optimizes Risk Reduction

Using attack path modeling in conjunction with vulnerability scanning, XM Cyber delivers the next generation in vulnerability management. Now security and IT teams can work together, relying on additional context to evaluate the criticality of each vulnerability to prioritize and manage updates and patching. The benefit to customers is a continuous approach to vulnerability management that reduces risk while also reducing man hours and improving processes between security and operations.


Security score
A
90
Compare scenarios
Hybrid Risk To Customer Data
Ransomware Risk
Risk to Customer DB from Phishing
Risk to USA Customer Data
Select scenarios
All scenarios
Past 54 days
Scenarios at high risk
View all
F (52) - Risk from Workstations to the DC
F (54) - AWS - Public EC2 to Sensitive Data S3
D (60) - Azure Risk | DEV container
Take action
Critical assets at risk
View all
Critical assets compromised by attack vectors with the lowest average complexity
21
Critical assets at risk
Top choke points
View all
23.1%
Top impacting attack techniques
View all
AWS Update Login Profile
PrintNightmare - Windows ...
AWS S3 Bucket Read Data
2 → 15.4%
30 → 15.4%
0 → 15.4%
View remediation



Let XM Cyber's Attack Path Management Solve These Key Challenges:

There are too many vulnerabilities to manage and patch. By combining data from the VM module with XM Cyber's attack path management continoually models attacks to show you exactly the highest priority vulnerabilities based on their actual impact to your company, making sure your critical assets are patched. By focusing on the most critical patches, operations can reduce their immediate workload by as much as 90 percent because they only must focus on the 10 percent of CVEs that matter most.

How do I bridge the gap between security and operations? We know there is a big gap between what security is finding from vulnerabilities and what the IT or operations team is asked to do to fix those vulnerabilities. Looking up solutions to vulnerabilities is burdensome on operations. XM Cyber identifies not only the most important areas to remediate, but also provides you with information on the relevant and most recent patches, and where to deploy them.

There's too many scans and noise on the network from security tools. Our lightweight sensor gives you full vulnerability assessment and attack simulation with very low impact to the performance of your endpoints.

It's difficult to understand the risks affecting the network. XM Cyber not only gives you the most current list of vulnerabilities affecting your environment, including all the latest vulnerabilities, but it also analyzes misconfigurations and human error to understand all possible open pathways towards your critical assets.

There's too much data to analyze. XM Cyber helps you and your teams easily understand the connection between a vulnerability, the devices it affects and the patches that can fix it to understand the scope of the problem and how to remediate it across your organization.

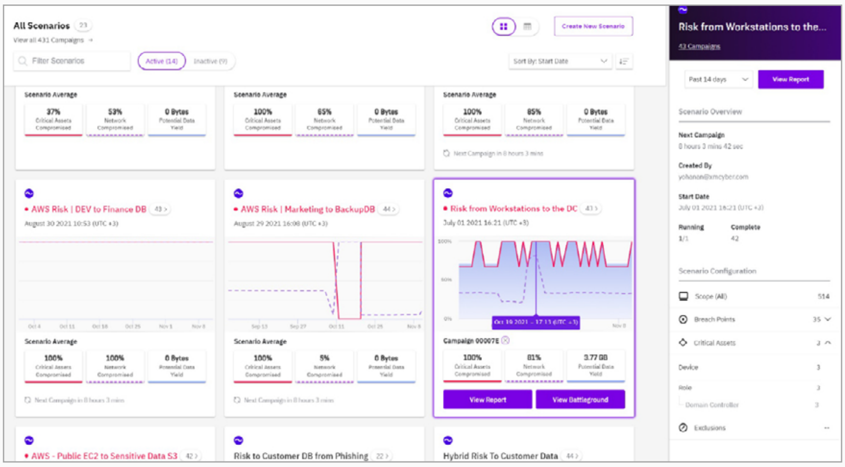
I can't assign tasks to various teams. XM Cyber gives you the option to create a request for specific patches or devices and pass it to your teammates, executives or IT teams to act on it, with ability to keep and track the outbound requests to make sure nothing is missed or forgotten.

Key Benefits of XM Cyber Attack Path Management

- Move risk AWAY from critical assets
- Focus on business impacting vulnerabilities
- Manageable vulnerability volumes for IT
- Optimise resource and remediation process ∫ Prioritize with context, always
- Continuous visibility of all vulnerabilities in your envionrment

Achieve Continuous Vulnerability Management

Our security solutions streamline the process from identifying, classifying, and addressing vulnerabilities to avoid threat actors exploiting gaps in time between security vulnerability reports and remediation. IT teams can easily import vulnerability scan results taken by Security teams. Quickly view the identified CVEs and associated patches and publish or approve any missing patches for deployment and save significant time.


All Scenarios 23
View all 431 Campaigns →
Filter Scenarios
Active (14) Inactive (9)
Create New Scenario
Sort By: Start Date

Scenario Average
37% Critical Assets Compromised | 53% Network Compromised | 0 Bytes Potential Data Yield

Scenario Average
100% Critical Assets Compromised | 65% Network Compromised | 0 Bytes Potential Data Yield

Scenario Average
100% Critical Assets Compromised | 85% Network Compromised | 0 Bytes Potential Data Yield
Next Campaign in 8 hours 3 mins

AWS Risk | DEV to Finance DB 43
August 30 2021 10:53 (UTC +3)
Scenario Average
100% Critical Assets Compromised | 100% Network Compromised | 0 Bytes Potential Data Yield
Next Campaign in 8 hours 3 mins

AWS Risk | Marketing to BackupDB 44
August 29 2021 16:08 (UTC +3)
Scenario Average
100% Critical Assets Compromised | 5% Network Compromised | 0 Bytes Potential Data Yield
Next Campaign in 8 hours 3 mins

Risk from Workstations to the DC 43
July 01 2021 16:21 (UTC +3)
Oct 19 2021 – 17:13 (UTC +3)
Campaign 00007E
100% Critical Assets Compromised | 81% Network Compromised | 3.77 GB Potential Data Yield
View Report | View Battleground

AWS - Public EC2 to Sensitive Data S3 42
Risk to Customer DB from Phishing 22
Hybrid Risk To Customer Data 44

Risk from Workstations to the...
43 Campaigns
Past 14 days | View Report
Scenario Overview
Next Campaign: 0 hours 3 mins 42 sec
Created By: yohanan@xmcyber.com
Start Date: July 01 2021 16:21 (UTC +3)
Running: 1/1 | Complete: 42
Scenario Configuration
Scope (All) 514
Breach Points 35
Critical Assets 3
Device 3
Role 3
Domain Controller 3
Exclusions --

You'll improve the experience and productivity of IT teams that previously spent many hours researching, deduplicating, and preparing a patch group of updates manually.

About XM Cyber

XM Cyber is the global leader in Attack-Centric Exposure Prioritization, which is also known as Risk-Based Vulnerability Management (RBVM). The XM Cyber platform enables companies to rapidly respond to cyber risks affecting their business-sensitive systems by continuously finding new exposures, including exploitable vulnerabilities and credentials, misconfigurations, and user activities.
XM Cyber constantly simulates and prioritizes the attack paths putting mission-critical systems at risk, providing context-sensitive remediation options. XM Cyber helps to eliminate 99% of the risk by allowing IT and Security Operations to focus on the 1% of the exposures before they get exploited to breach the organization's "crown jewels" – its critical assets.
XM Cyber was founded by top executives from the Israeli cyber intelligence community and has offices in North America, Europe, and Israel.

Tel-Aviv:	+972-3-978-6668
New-York:	+1-866-598-6170
London:	+44-203-322-3031
Munich:	+49-163-6288041
Paris:	+33-1-70-61-32-76

xmcyber.com