XM Cyber | See All Ways™

Risk Exposure Reduction and Vulnerability Prioritization

A Buyer's Guide for
Attack Path Management

Table Of Contents:

01 Executive Summary

In a positive trend, cybersecurity teams are becoming increasingly mature and more aware of the threats they face today. To that end, there is now a greater understanding that protecting the organization's critical assets from sophisticated bad actors requires constant identification of, and remediation of, the most critical cyber exposures and how they combine together across these environments to put critical assets at risk.

Organizations that enable Attack Path Management across their on-prem, SaaS, and Cloud environments can continuously reduce their risk exposure by uncovering hidden attack paths to businesses' critical assets, identifying security controls gaps, and prioritizing security exposures so organizations can focus remediation activities.

Attack Path Management goes beyond identifying different technical weaknesses such as vulnerabilities, misconfigurations, and identity exposures by determining how attackers can use their various attack techniques to find a path to exploit critical business assets. Identifying the high-priority attack vectors and attack paths reduces risk and has the added benefit of reducing overall remediation efforts because lowly scored risk patching may be deprioritized.

With a proper solution in place, research shows a 90% reduction in likelihood of a severe breach due to the wide coverage across on-prem, Cloud and SaaS of attack path management and an ROI of up to 400%[1].

This guide describes how organizations can reduce their cyber exposures, details the emerging Attack Path Management technology, and shares why many organizations are implementing it. It also delivers advice on how to evaluate APM solutions and justify purchasing an APM solution.

02 How Do Organizations Manage Attack Paths and Reduce Their Risk Exposure?

What is an Attack Path?

It is the path across entities that the attacker takes from the breach point to your critical asset. At each step in the path, the attacker uses a technique to compromise the entity, and uses that entity to step to the next entity in the path. Research revealed in less than 4 hops, 94% of critical assets can be compromised from the initial breach point[2].

To clearly understand an attack path, there is a prerequisite – knowledge of what an attack vector is. An attack vector is a method that cyber-attackers use to compromise a system. Although the terms are sometimes mixed, attack vectors are not to be confused with an attack surface, which is best defined as every possible point where an adversary can attempt to enter your network or system.

An attack path is a visualization of the chain of events that occurs when attack vectors are exploited. In this sense, an attack vector acts as a doorway, while an attack path is a map that shows how an adversary entered the door and where that adversary went. Malware, ransomware, or phishing are all examples of common attack vectors.

While cloud attack vectors can be used to target a security gap within your network or system, vectors can also be leveraged to exploit human error. Adversaries will often take advantage of multiple vectors when conducting an attack. When you combine multiple attack techniques together, you can create an attack vector and when you combine multiple attack vectors together you can create an attack path. It's also important to know that attack vectors may exist even when they appear to be mitigated. For example, creating an extremely strong password won't help much if you don't realize that password is available on the dark web, just waiting for an attacker to use it against you.

Why is Attack Path Management Critical?

Compared to two years ago, cyber-risks are increasing. According to ESG research, 82%[3] of organizations say that cyber-risk has increased over the past two years. This increase is due to factors such as an increase in cyber-threats, greater dependence on IT to fulfill its business mission, and an increase in the number of assets on the attack surface. Recognizing this trend, executives and corporate boards are pressuring CISOs to improve cyber risk mitigation—but there's a problem. Many organizations lack the right level of risk context. In other words, they don't understand whether increasing exposures places their critical assets at risk. This situation poses a real conundrum for CISOs since they can't communicate an accurate cyber-risk status to business managers, and they aren't sure how to prioritize investments for risk mitigation.

Cyber-risk leads directly to cyber-attacks. While organizations use multiple siloed tools and manual processes to address cyber-risk management, adversaries use automated tools to continually scan the attack surface for user and business-critical vulnerabilities. The result can be classified as a mismatch—two-thirds of organizations have experienced a cyber-attack resulting from an unknown, mismanaged, or poorly managed internet-facing asset. And once adversaries compromise a system, it's easy for them to move laterally across networks. These incidents include ransomware attacks, data breaches, and regulatory compliance violations.

Key challenges facing organizations today:

Cybercriminals keep getting better and are acting more frequently.

Other than penetration testing, other solutions evaluate individual assets without effectively evaluating pathways and the relationship to critical assets.

Penetration testing is only done periodically due to cost, business disruption, and labor requirements.

Organizations have a constant list of thousands, to hundreds-of thousands of patches.

A constantly changing IT infrastructure creates new paths and opportunities for cybercriminal attacks.

03 What is Attack Path Management (APM)

What are the key aspects of an APM solution

Every organization wants to reduce their cyber-risk. Attack Path Management creates an ongoing process for identifying and remediating exploitable attack paths to critical assets. APM can help organizations identify their most critical exposures like misconfigurations, risky users, and software vulnerabilities across the hybrid environment, apply cost effective remediation actions by directing resources to fix choke points (those junctures where many attacks paths traverse through), communicate business risks, identify risk mitigation strategies, and track success over time.

APM solutions should:

Provide an automated methodology to frequently analyze the security exposures across the organization's entire infrastructure without outages, disruptions, or performance issues.

Understand cyberattack pathways and identify security issues creating the greatest exposure to critical infrastructure.

Provide out-of-the-box scenario analyses as well as custom scenarios based upon unique customer experiences or specific threats, such as malware or zero-day vulnerabilities.

Reduce the requirement for other vulnerability management activities, most notably pen testing.

Breach Points

Every campaign starts at a compromised endpoint called a breach point. A breach point may be an endpoint with a high probability to get infected, as the initial foothold of an attack.

Critical Assets

An entity in the network that has possible value to an attacker or the organization (which makes it a point of interest to an attacker). A critical asset can be one of the following:

Device: An endpoint in the network
Data: A file type found on any of the endpoints
Network: A network-related entity - like a certain segment, subnet, etc.
Cloud: There are multiple cloud entity types, such as S3, Lambda, roles, etc.

Campaigns

An attack scenario executed by the virtual hacker. It contains the loaded APT capabilities and the current state of all sensors in the network -- compromised, discovered, undiscovered or disabled. Every campaign runs with its configuration defined in its parent scenario.

Scenarios

A set of rules created by a user running a campaign. The rules determine such things as the scope of campaigns, breach points, the type of devices to be included, as well as campaign frequency and duration.

Choke Points

The entity presents the greatest risk to the critical assets and the rest of the environment as well. The greater number of attack paths the entity plays a step in, the more the entity is a choke point.

Other Evaluation Considerations

Breach and Attack Simulation (BAS)

Solutions that automate security posture assessments by continuously validating technical and procedural security controls between different segments of internal and external networks.

What type of security controls do BAS solutions test? And what don't they test? EPP, Email Gateways, IPS, IDS solutions and Secure Web Gateways are some of the controls being tested. More importantly, what is not being tested are risks in PAM solutions (Privileged Access Management), misconfigurations in Active Directory, and potential risk of identities and vulnerabilities. With exposures from unmanaged activities like misconfigurations, shared credentials, and poor user activities, attackers can leverage the security gaps to compromise critical assets.

Vulnerability Scanners

A regular process of identifying, assessing, reporting, managing and remediating security vulnerabilities and missing patches across internal and external endpoints and systems.

Vulnerability management as it stands today is ineffective primarily throughout its entire processes of vulnerability discovery, prioritization, and remediation. With so much vulnerability data, the combination of infrequent scanning with pen tests not being integrated, leaves gaps and blind spots, is limited to the context of the environment and many critical vulnerabilities are still missing from the assessment.

Traditionally, solutions look for exploitable vulnerabilities using CVSS scoring focused on the risk on the critical asset -- and not the risk towards the critical asset. It becomes nearly impossible to prioritize risk exposure without an understanding of the pre/post conditions, the attack paths, and no view of choke points to cut off attack paths at key junctures.

Penetration Testing

Security gaps often develop as the result of flawed software code, operating system backdoors, improper configurations, and other similar issues. During a pen test, an attempt will be made to discover problems such as these by targeting servers, wireless networks, mobile devices and other possible points of entry for attackers. As you might imagine, manual pen testing is usually resource intensive, lacks prioritization and the results are often out of date as soon as they are published. Most organizations must hire trained, third-party white hat pen testing or red team pen testing experts to conduct the exercise. Alternatively, they may create their own red, blue or purple teams from internal staff members, should they have the institutional expertise. Penetration testing results will deliver highly confident results for a limited scope, but with a highly manual effort. With an Attack Path Management solution in place, organizations can reduce their penetration testing costs of up to $1.4 million over three years[4].

Attack Surface Management (ASM)

Attack surfaces have been rapidly expanding in recent years, thanks in part to the cloud and the increased popularity of remote work. This has given attackers a target-rich environment in which to operate. ASM solutions are used by organizations to discover, analyze, categorize, and manage externally facing assets.

Classifying and monitoring an ever-growing attack surface is not easy — most organizations report that they make no effort to do so. Some monitor just a small part of their attack surface, and a disturbingly large number of organizations have Internet-connected devices within their networks of which they are not even aware. One of the best ways to achieve strong ASM cybersecurity is by adopting some core security frameworks that help reduce the creation of new misconfigurations/vulnerabilities such as a Zero Trust framework across the organization.

Examples from the Real-World: Risk Exposures Discovered by Attack Path Management

1

"An exposure at a global company gave unprivileged users the ability to compromise admin accounts. With the ZeroLogon vulnerability, it could compromise the Active Directory in the company's Asia location, which had trust established with all the other ADs in the organization".

Manager of Technical Enablement

2

"Every admin had a single login for every administrative task. User management, database, etc. This is a bad practice since if the account gets compromised, the attacker has free reign. Attack Path Management solutions can show how credentials can be dumped, leading to compromise of critical assets".

Technical Director

3

"In a manufacturing environment, you can wind up with health and safety issues, not only security problems. With the attack paths found, an attacker could compromise a server responsible for controlling unscrewed/unmanned vehicles, which were responsible for transporting manufacturing goods from A to B in the factory. With access, an attack could gain control of the devices, causing physical harm and damage".

Technical Director

4

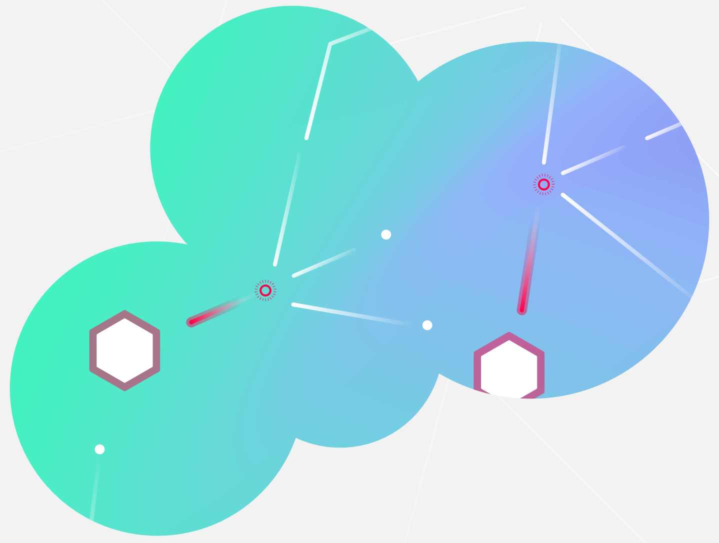
"Discovered an attack path that used a development server that could compromise most of the organization's network. After looking at the server, they decided to turn it off rather than path it as it wasn't serving any purpose".

Customer Success Team Leader

5

"The most interesting attack paths combine multiple categories of telemetry. This path used 3; local credentials were captured and then leveraged to pivot over to another Windows machine. The attacker was then strategically positioned on the network where they could respond to a proxy broadcast from the critical asset. The new network positioning meant they could intercept a misconfigured Windows update request and leverage a vulnerability present on the critical asset to compromise the machine".

Director of Sales Engineering



04 Key Features and Capabilities to Evaluate for APM Solutions

Contextualization

Gives context to misconfigurations, vulnerabilities, and risky users and how they can all be leveraged to compromise critical assets across on-prem, Cloud and SaaS environments.

Prioritization

Looks at all risks and prioritizes them by the impact they pose to critical assets, so you know what to fix to disrupt the most damaging attack paths first.

Continuous

The modern attack surface is dynamic and changes constantly. Constantly understands attack paths, and how easy they are to update with the latest vulnerabilities and attack techniques, as well as the operational effort required to run continuously.

Operational Safety & Impact

This has 2 areas of focus. Firstly, how risky the tools are to run in production environments, e.g. by deploying live exploits! Secondly, how easy the tools are to manage operationally and the level of planning and resource it takes to operate the tool.

Comprehensive

The solution should consider all workstations, entities, virtual machines, containers, user activity, and configurations, etc. as part of attack path analysis to ensure you can see all ways your organization is at risk to plan prioritized remediation efforts.

Resolution

Save analyst time by cutting off attack paths at key junctures a.k.a. choke points, with a least-cost, maximum-impact approach. Using Attack Path Management, organizations can avoid costs of remediation, fines, customer costs, revenue lost, and brand rebuilding of up to $12.4 million over three years[5]. Organizations reduce the frequency and severity of cybersecurity attacks by utilizing Attack Path Management to prioritize focus on security exposures and remediation activities on issues associated with critical assets.

Improvement

With automated remediation planning that's embedded into your operation you can help drive business decisions and see that your security investments are paying off. Using a least-cost, maximum-impact approach like Attack Path Management, research shows organizations in fact have 80% fewer issues to remediate by knowing where to disrupt attack paths[6].

Board-level Reporting

Accurately assesses risk and can help support executive and operational reporting processes. Allows boards to quickly grasp how their organization can be attacked, how improvements are occurring over time because of security investment, changes in processes or implementation of environment hardening, and most importantly, how much risk exists for critical assets.

05 Business Drivers to Reduce Risk Exposure with APM

Hybrid Cloud Security

Organizations are moving critical assets to the cloud yet they can't see how these assets can be attacked!

Supply Chain and Third-Party Risk

know that your business partners will be compromised. But you can't see how that places your business at risk!

Vulnerability Assessment & Vulnerability Management

Organizations struggle to know which vulnerabilities can be leveraged to compromise their critical assets.

Ransomware Readiness

You know attackers will establish the initial foothold, but you don't know how this will impact your critical assets.

Cyber Risk Reporting

Businesses everywhere don't know how to answer the most important question: Are our critical assets protected?

Mergers & Acquisitions

Organizations need to consolidate and integrate infrastructure but can't see how all the change places the program at risk.

Operationalization

See your hybrid attack surface to lower risk and speed up digital transformation.

OT Security

Detect security gaps and correlations between environments to pinpoint hardening efforts.

06 How Vendors Stack Up

Use Cases and Initiatives	XM Cyber	Cloud Security	Breach and Attack Simulation	Vulnerability Prioritization
Preventing cyber security exposure based on actual risk exploitability and remediation effort across hybrid cloud	●	◕	◑	◑
Detecting Anomalous behavior	○	◑	◔	○
Risk visibility and prioritization for business critical assets	●	◔	◔	◑
Chaining together misconfigurations, user behavior and vulnerabilities to identify hidden attack paths	●	◕	◑	◔
Understanding risk to critical assets through enterprise risk scoring	●	◑	◕	◔
Support for scale of large infrastructure (non-intrusive, no malicious code in production, no alert fatigue)	●	●	◔	◕
Remediation-centric approach for increased security posture	◕	◑	◑	◔
Security Posture Scoring aligned with actual risk showing trends over time	●	◑	◕	○

Capability	Cloud Security				
	XM Cyber	Wiz	Orca	PAN	Check Point
Single view of all attack paths across on-prem and cloud environments	●	○	○	○	○
Choke Point analysis for cost-effective remediation	●	○	○	○	○
Cloud Security Posture Management (CSPM)	●	●	●	●	●
Holistic view of risk exposure across the hybrid environment with security score and trends over time	●	◕	◕	◕	◕
Easily define risk scenarios with attack paths focused on critical assets to spot security gaps and reduce risk exposures	●	◑	◑	○	○

Capability	Breach & Attack Simulation				
	XM Cyber	Cymulate	SafeBreach	Pentera	Picus Security
Coverage to provide constant scenario simulations, reducing pen testing activities	●	◑	◑	●	◔
Continuous and safe simulation	●	◑	◑	◔	◑
Security Control Validation and automated penetration testing	◑	●	●	●	●
Attack path analysis for Active Directory across the hybrid cloud environment	●	◔	○	◔	○
Wide range of use cases including third party risk management, business risk profiling, and proactive exposure reduction	●	◕	◕	◔	◕

Capability	Vulnerability Prioritization				
	XM Cyber	Tenable.io	Microsoft Defender VM	Qualys VMDR	Rapid 7 Insight VM
Prioritize vulnerabilities based on riskiest assets and CVE exploitability	●	●	●	●	●
CVE prioritization based on attack path exploitability	●	○	○	○	○
Asset Discovery across the network	◑	●	●	●	●
Combine multiple types of exposures beyond CVEs to know what is attackable	●	●	●	●	●
Efficient remediation based on choke point analysis	◕	◕	●	●	◕

○ ◔ ◑ ◕ ●

← Weak ___Strong →

07 Key Questions to Ask Vendors

CISOs can identify their critical risk exposures with Attack Path Management solutions, as they combine many functions into a single platform. Attack Path Management takes an adversary perspective to answer questions such as: “How can I be attacked?”, “Which of my critical assets are at risk?”, and “How can I mitigate these risks with minimal effort?”

Armed with this knowledge, CISOs can identify their most critical exposures like misconfigurations, risky users, and software vulnerabilities across on-prem, Cloud, and SaaS. CISOs can also apply cost effective remediation actions by directing resources to fix choke points — those junctures where many attack paths traverse through. These actions can help CISOs to detect and communicate business risks, identify risk mitigation strategies, and track success over time.

What is my security score?

What needs to be fixed so my business won't be compromised?

Which of my critical assets are at risk, and what exposures need to be fixed?

Where are my security gaps?

References:

1 Forrester Total Economic Impact Study, 2022
2 XM Cyber Attack Path Management Impact Report, 2022
3 ESG "A CISO's Guide to Reporting Cyber Risk to the Board", 2022
4 Forrester Total Economic Impact Study, 2022
5 Forrester Total Economic Impact Study, 2022
6 XM Cyber Attack Path Management Impact Report, 2022

About XM Cyber

XM Cyber, a Schwarz Group company, is a leading hybrid cloud security company that's changing the way innovative organizations approach cyber risk. By continuously uncovering hidden attack paths to businesses' critical assets and security controls gaps across cloud and on-prem environments, it enables security teams to remediate exposures at key junctures and eradicate risk with a fraction of the effort. Many of the world's largest, most complex organizations choose XM Cyber to help eradicate risk. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, and Israel. XM Cyber was acquired by the fourth largest retailer in the world, Schwarz Group in November 2021.

Tel-Aviv:	+972-3-978-6668
New-York:	+1-866-598-6170
London:	+44-203-322-3031
Neckarsulm:	+49-7132-30485600
Paris:	+33-1-70-61-32-76

xmcyber.com

XM Cyber