XM Cyber

XM VRM Datasheet

XM VRM
Vulnerability Risk Management

Focus Efforts. Resolve Vulnerabilities.

Comprehensive Vulnerability Prioritization for the Hybrid World

The next generation of risk-based vulnerability management is here, with dynamic and continuous CVE mapping that allows you to seamlessly pivot security context from a traditional to a transformative RBVM construct. Prioritize your viewpoint of vulnerabilities from exploit likelihood to business impact risk and streamline the mobilization of remediation efforts, with rich contextual guidance, to justify action and proactively accelerate security operations.

The Problem with Traditional Vulnerability Management

Diverse asset types, spread across a distributed attack surface, along with the growing severity of vulnerabilities all culminate in a widening remediation deficit.

Traditional tools with inaccurate scanning methodologies generate high volumes of false positives that contain limited, if any, context for action.This means even the most well-defined operating processes are difficult to put into action.

Solutions that continue to view risk posture by an individual asset context or that fail to consider compensating controls result in flawed and ineffective prioritization logic, and offer little in the way of real-world validation.

Unclear ownership of assets and the lack of justification for action make it challenging for security teams to prioritize efforts based on their limited understanding of the business risk presented by each vulnerability.

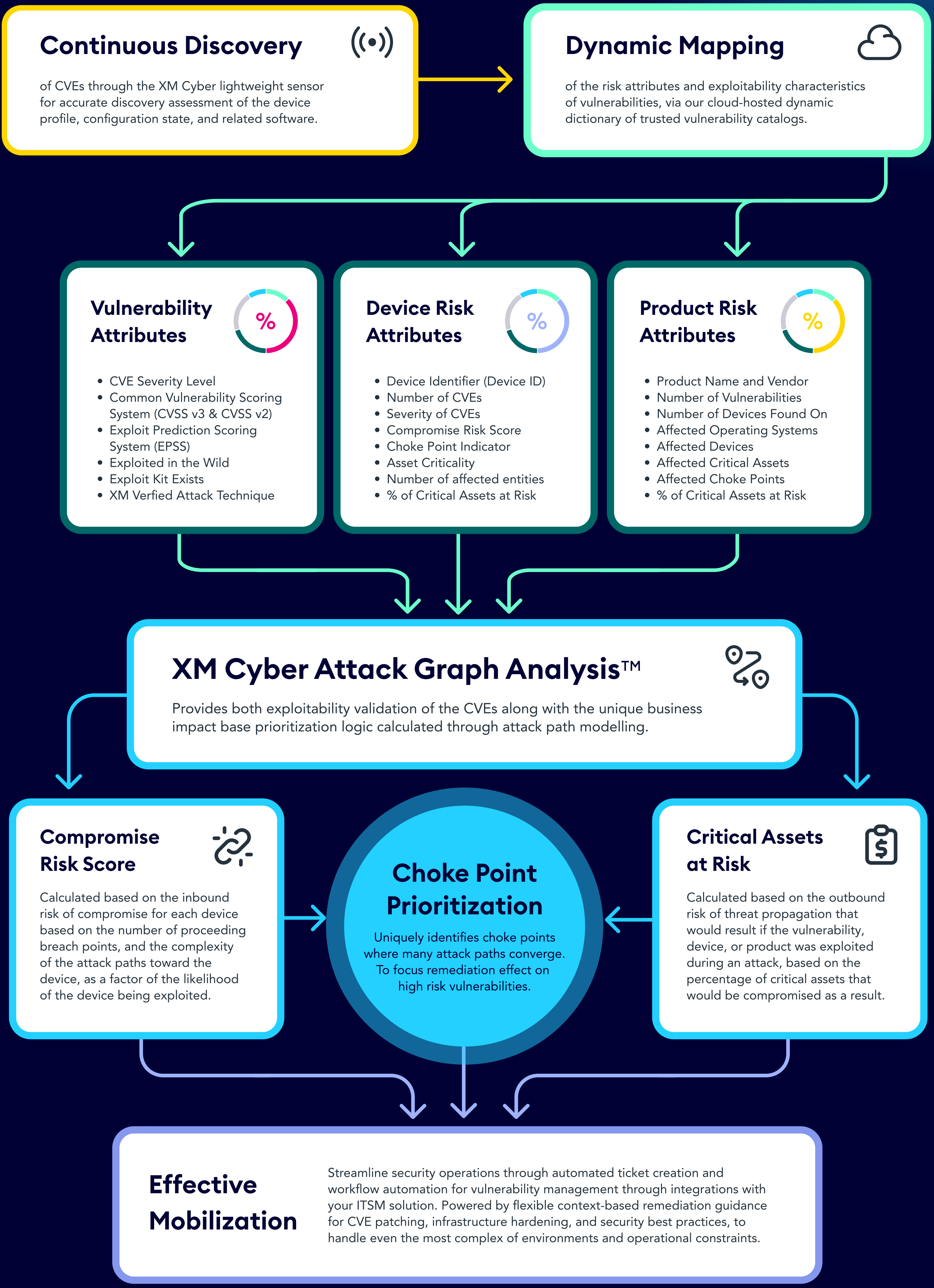
KEY CAPABILITIES

It's Time for a New Approach to Vulnerability Management

Revolutionize vulnerability management processes with contextual risk quantification that uniquely correlates intrusion likelihood with validated business impact risk, enabling you to focus remediation and patching efforts on high-impact vulnerabilities.

- **Innovative Discovery and Dynamic Mapping:** Continuous and dynamic discovery of vulnerabilities across hybrid infrastructure that ensures accurate CVE mapping to diverse risk attributes.
- **CVE Exploitability Validation:** Take the guess work out of CVE risk analysis, by correlating exploit kits and attack techniques to CVEs and validating their exploitability in your environment.
- **Impact-based Risk Prioritization:** Know where to focus, with the complete picture of vulnerability risk based on the impact to business critical assets.
- **Traditional to Transformative Risk Context:** Seamlessly pivot security context from intrusion risk to business impact risk, based on the true exploitability of an individual CVE, device, or product.
- **Remediation Mobilization:** Ensure your teams have the justification, prioritization, and remediation guidance they need to accelerate closed-loop vulnerability patch management.

XM VRM Technology Flow



Continuous Discovery

of CVEs through the XM Cyber lightweight sensor for accurate discovery assessment of the device profile, configuration state, and related software.

Dynamic Mapping

of the risk attributes and exploitability characteristics of vulnerabilities, via our cloud-hosted dynamic dictionary of trusted vulnerability catalogs.

Vulnerability Attributes

- CVE Severity Level
- Common Vulnerability Scoring System (CVSS v3 & CVSS v2)
- Exploit Prediction Scoring System (EPSS)
- Exploited in the Wild
- Exploit Kit Exists
- XM Verfied Attack Technique

Device Risk Attributes

- Device Identifier (Device ID)
- Number of CVEs
- Severity of CVEs
- Compromise Risk Score
- Choke Point Indicator
- Asset Criticality
- Number of affected entities
- % of Critical Assets at Risk

Product Risk Attributes

- Product Name and Vendor
- Number of Vulnerabilities
- Number of Devices Found On
- Affected Operating Systems
- Affected Devices
- Affected Critical Assets
- Affected Choke Points
- % of Critical Assets at Risk

XM Cyber Attack Graph Analysis™

Provides both exploitability validation of the CVEs along with the unique business impact base prioritization logic calculated through attack path modelling.

Compromise Risk Score

Calculated based on the inbound risk of compromise for each device based on the number of proceeding breach points, and the complexity of the attack paths toward the device, as a factor of the likelihood of the device being exploited.

Choke Point Prioritization

Uniquely identifies choke points where many attack paths converge. To focus remediation effect on high risk vulnerabilities.

Critical Assets at Risk

Calculated based on the outbound risk of threat propagation that would result if the vulnerability, device, or product was exploited during an attack, based on the percentage of critical assets that would be compromised as a result.

Effective Mobilization

Streamline security operations through automated ticket creation and workflow automation for vulnerability management through integrations with your ITSM solution. Powered by flexible context-based remediation guidance for CVE patching, infrastructure hardening, and security best practices, to handle even the most complex of environments and operational constraints.

Continuous Discovery

The XM Cyber Vulnerability Risk Management module utilizes a lightweight sensor to dynamically assess the configuration state and registry settings of devices, software and products on a continuous basis, to dynamically map vulnerabilities and CVEs via a cloud-hosted dynamic dictionary.

Taking a Traditional Approach to Vulnerability Prioritization

Flexible contextual views of vulnerabilities by CVE, Device, or Product context allows IT operations teams to prioritize vulnerabilities based on the risk attributes in line with a traditional approach to vulnerability management.

For individual CVEs, prioritization is provided through risk attributes such as CVSS Severity or EPSS Score. The Prioritization logic also includes CVEs with a known Exploit Kit, or have been exploited in the wild. All these risk attributes count towards the individual exploit likelihood of the CVE.

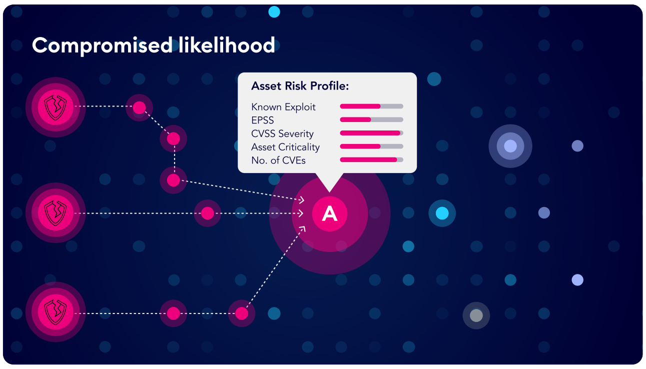
Operators can see the distribution of each CVE across devices to help assess the remediation effort, or to pivot their viewpoint to that of the device or product context.

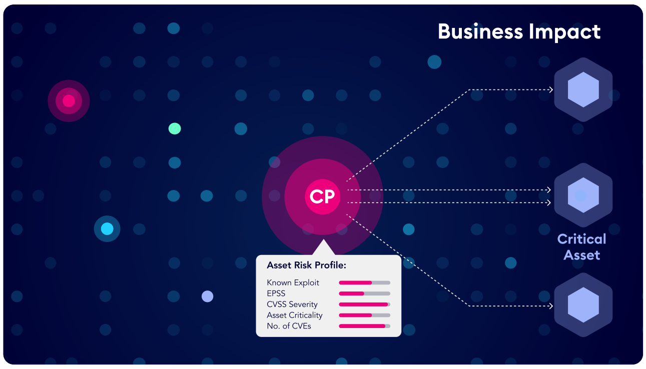
By focusing on devices, IT Operations can now understand the overall risk presented by a device based on the number and severity of the CVEs related to its Operating Systems, underlying hardware, and the software products installed.

Switching to a Transformative Approach to Vulnerability Prioritization

All exposures discovered by the XM Cyber CEM platform, including CVEs, are continuously analyzed through XM Attack Graph Analysis™ to see how they chain together into attack paths that target critical assets. For Vulnerabilities, the first step in this process is to map CVEs with exploit kits and their associated attack techniques, and then verify their exploitability on the individual device. Once identified as exploitable, all potential lateral movements from the device are then verified via the XM Sensor. This unique attack path validation can then be utilized for enhanced prioritization logic:

- **Attack Technique** – Where a known exploitable vulnerability has been proven to be exploitable in your specific environment.
- **Compromise Risk Score** – The inbound risk of compromise based on the number of breach points available and the complexity of hops required by an attacker to reach and exploit the device.
- **Affected Entities** - The number of entities an attacker can directly compromise by exploiting the vulnerabilities on the device.
- **Critical Assets at Risk** – The outbound or onward business impact risk based on the percentage of critical assets that would result from an attacker exploiting the device.



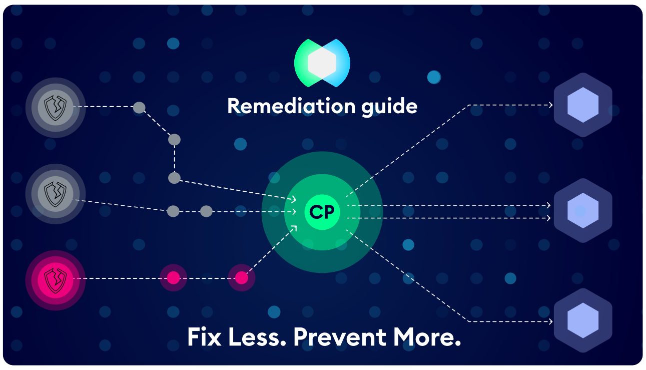


These unique risk attributes enable SecOps Teams to see their environment through the eyes of an attacker and transform their approach to vulnerability prioritization, based on validated exploitability and business impact risk.

Effective Mobilization

After the validation of exploitability and the prioritization of vulnerabilities through the XM Attack Graph Analysis™, the XM Cyber platform goes a step further by providing remediation guidance in the form of playbooks that can be used by IT Operations teams to implement the required actions.

If the CVE can be patched, a remediation guide outlines where the patch can be found, and how it should be applied. However, not all vulnerabilities can be patched, either due to the reliance on legacy systems, limited maintenance windows, or when a patch is simply not yet available. In these cases, the XM Cyber Platform provides two additional types of playbooks, either in the form of a hardening guide or a best practices guide, each of which contains a combination of information and guidance from the specific vendor, along with insights from the XM Cyber security research experts.



Workflow automations can be initiated through the XM Cyber Platform integrations with leading ITSM tools, ticketing solutions, and SOAR platforms. Operators can create a new task from any remediation guidance in the platform, assign the ticket to the relevant teams, and attach the XM Cyber remediation guide, to ensure the right people have the information they need to implement effective remediation and response actions to critical and high-risk vulnerabilities.

Business Value Outcomes

XM Cyber Vulnerability Risk Management provides an innovative new approach to discover, quantify, and reduce risk presented by vulnerabilities, which combines with the XM Attack Graph Analysis™ for enhanced exploitability validation, enabling a more effective approach to vulnerability management.

Transformative
Vulnerability Remediation

Flexible contextual views of vulnerabilities with unique prioritization and validation logic, that allows you to seamlessly pivot your security viewpoint from traditional to transformative Risk-Based Vulnerability Management.

Impact-Based
Risk Reporting

Comprehensive vulnerability risk quantification that validates which vulnerabilities present the greatest risk to the business, based on both the inbound compromise risk score, and the onward Impact risk towards critical assets.

Collaborative
Security Optimization

Foster a culture of collaboration and accelerate closed-loop vulnerability patch management, with the justification, prioritization, and remediation guidance needed to ensure the effectiveness of defensive strategies.

THE XM CYBER PLATFORM

Stop Wasting Time on Fixes that Don’t Impact Risk

XM Cyber

XM Cyber Vulnerability Risk Management is an add-on module to the XM Cyber Continuous Exposure Management Platform, that transforms the way organizations approach cyber risk.

XM Cyber gives you the context you need to make faster and more confident decisions about which exposures to fix and which to safely ignore. Automatically discover all the attack paths in your environment to clearly see which vulnerabilities, misconfigurations, and identities chain together to pose the greatest risk.

Now you can stop wasting time on exposures that don't open attack paths to critical assets - the dead ends. Instead, leverage the power of attack graphs to automatically pinpoint the exact spots - the choke points - where you can disrupt the attacker's path. See all ways, and accelerate remediation efficiency, by ensuring your IT and Security Operations teams have the guidance they need to mobilize effective remediation strategies, helping you. **Fix Less. Prevent More.**