Ransomware Attack Prevention

Discover cyber exposures that lead to successful ransomware attacks and prevent them in advance, with Attack Path Management

Ransomware groups are looking for ways to reach your critical assets, to increase their chances of getting a higher ransom payout. For the same reason, they have begun employing the double extortion technique, where before encrypting your data, they exfiltrate it and then threaten to leak it online. Searching for routes to reach your critical assets, attackers are lying low, propagating the network as a result of misconfigurations, unpatched vulnerabilities and mismanaged credentials.

Existing security controls are often siloed and provide fragmented visibility of your critical assets and the attacker's journey. Attackers take time to explore your cyber exposures but knowing which exposures put your critical assets at risk above others is challenging. Knowing what to fix first and which junctions in your network can be more damaging than others as many attack paths traverse through these is key to sabotaging any attack. Focusing on the attacker's path results in better resilience as well as better ROI from your existing security tools.

Get the attackers' perspective of your environment

The XM Cyber Attack Path Management Platform runs continuous and safe ransomware attack modeling, enabling you to see your environment through the eyes of the attackers and to gain complete visibility of the actual attack surface. By assuming breach, the platform highlights the cyber exposures that enable attackers to stealthily move within your network, on their path to take control of your critical assets, and to exfiltrate and encrypt data.

Early visibility of all possible ransomware attack paths and cyber exposures in your network will help you prioritize and focus resources on fixing the security issues that have the biggest impact on the success or failure of a ransomware attack.

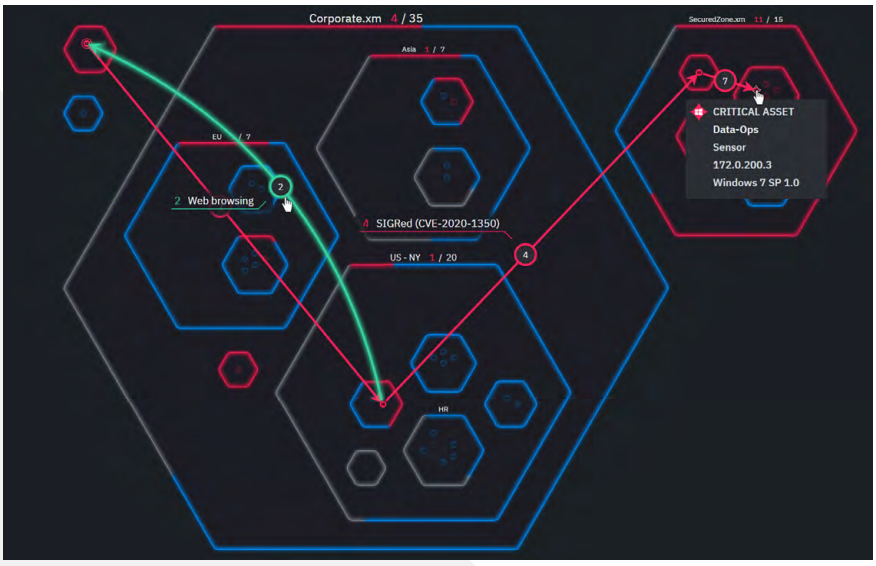


Fig. 1 Map all attack paths across the environment via XM Cyber's Battleground

- Illuminate and disrupt ransomware attack paths, in the cloud or on premises
- Close the gaps ransomware groups can use to compromise your network
- Continuously monitor and know what to fix first to prevent attacks
- Efficiently reduce the risk and impact of ransomware attacks

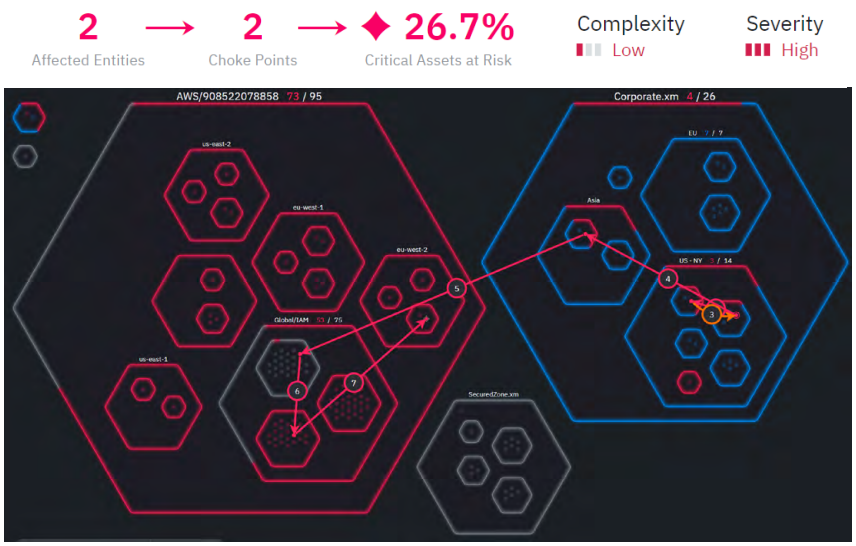
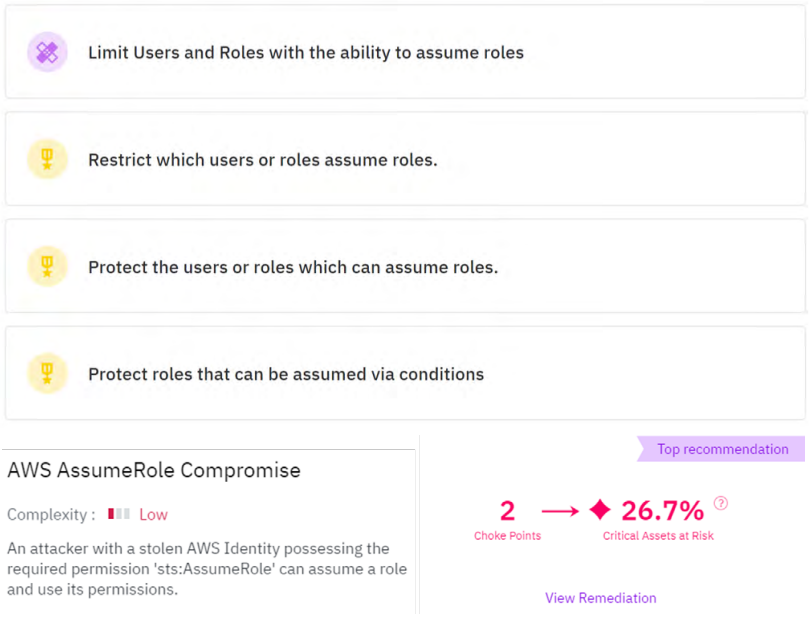


Fig. 2 Choke points automatically detected in XM's Attack Path Management Solution for prioritized remediation

Highlight choke points - the key devices and entities that many attack paths traverse through and facilitate access to your critical assets and data.

Ensure safe, fast and cost-effective remediation

XM Cyber Attack Path Management solution automatically generates an actionable remediation plan that prioritizes the required actions for cost-effective, safe and speedy disruption of current and future ransomware threats. Follow the step-by-step guidance to ensure optimized use of resources for fixing exposures, as well as continuous enhancement of your security resilience and improved operation of your existing security tools. It could be as simple as removing a user from the directory.



Follow the step-by-step remediation plan to harden your environment and improve your security posture.

The XM Cyber Attack Path Management Platform proactively makes it harder for ransomware and malicious groups to access, exfiltrate and encrypt your data, by greatly reducing the attack surface, disrupting attacks in the making and enhancing your resilience.

About XM Cyber

XM Cyber is the global leader in attack path management. XM Cyber brings a new approach that uses the attacker's perspective to find and remediate critical attack paths across on-premises and multi-cloud networks. 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 attack paths putting mission-critical systems at risk, providing context-sensitive remediation options. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, and Israel.

XM CYBER

Tel Aviv +972 3 978 6668
New York +1 866 598 6170
London +44 203 322 3031
Munich +49 163 6288041
info@xmcyber.com