XM Cyber for Ransomware

Stop ransomware before it happens by closing all the gaps that hackers can use to infiltrate your network

Ransomware attackers don't care about your company, your customers or your intellectual capital. They only want to cripple you so they can extract a ransom. And the number of attacks is growing rapidly (Mandiant ransomware investigations increased 860% from 2017 to 2019). Endpoint defenses are no longer sufficient in stopping these malicious actors from penetrating your network. In fact, they do not even have to reach your critical assets – just shut down your operations by limiting access and encrypting your data.

BYOD, VPNs, RPDs and a host of new cloud and software tools have been introduced recently as enterprises around the world send employees home to work. This constant change exposes your company in ways that traditional security controls can't identify. The only answer is to deploy pre-emptive security that identifies gaps and helps you remediate them on a continuous basis.

Now is the time to build XM Cyber Attack-Centric Exposure Prioritization Platform (ACEPP) into your ransomware defense program. XM Cyber identifies for you the exposures within your network that can be used to attack your company -- misconfigurations, open credentials, poor user behavior, and vulnerabilities generally caused by poor IT Hygiene. Now you have a continuous view of your risk and a prioritized list of remedial actions to take.

Stop them before they have the chance by knowing in advance how they can penetrate your network.

Do You Have a RansomwareStrategy?

XM Cyber customers know ransomware is real. Here are their top concerns and how XM Cyber is stopping ransomware before it gets a foothold in your network:

Constantly changing networks open holes that attacks can use. At any given moment, changes in your environment can have a domino effect that put your critical business assets, if not your entire network, at risk of a ransomware attack. Penetration testing is only good for the time period it evaluates. Vulnerability tools only identify single points of failure. You need XM Cyber to continuously show you what would happen if a ransomware attacker gain access.

Identifying attack paths an attacker might use is difficult. Your analysts can easily create an attack scenario in XM Cyber to simulate what would happen if that particular asset is breached. By simulating an attack, XM Cyber shows what would happen if an attacker had access to any particular asset. As a result, you analysts can be much more efficient in their ransomware prevention activities.

Hybrid attacks can go unnoticed by analysts and other security controls. Acting as a virtual hacker, the XM Cyber platform shows all possible steps that can be taken from a machine that is compromised, including hybrid attacks that move from on-premises devices to cloud-based assets.

Lateral movement prevention is difficult to find and stop. By constantly examining your environment for weaknesses, XM Cyber helps your team identify service accounts, domain accounts, vulnerabilities open to exploitation, local configurations, and other key configurations that would allow attackers to move with ease.

No ability to identify choke points. XM Cyber clearly identifies assets that can affect multiple other assets, essentially creating a choke point. By eliminating the vulnerability of just one asset, the risk to the entire network can be greatly reduced.

XM Cyber Helps Prevent Ransomware Attacks Before They Happen

XM Cyber provides advanced preventative measures via its advanced ACEPP capabilities, allowing analysts to reduce the risk of ransomware attacks. You can count on these unique features only found in the XM Cyber Platform:

- Ability to answer with a simple Yes or No whether business critical assets are susceptible for breach
- Prioritized and actionable. XM Cyber expedites the entire exposure, assessment and remediation cycle. This empowers the security team to focus on the most important issues.
- Choke point identification. XM Cyber identifies assets on the network that can affect other assets. The more links to other assets, the greater the risk and the higher the priority must be to remediate.
- Continuous operation. Manual testing is not effective enough because your network is constantly changing. To truly understand your risk, you need to run 24/7 in your production environment, constantly improving your security posture.
- Improved investigative process. If suspicious activity is discovered, the XM Cyber Platform explores and identifies the potential impact. By clearly identifying critical assets, the XM Cyber Platform assists customers in fully understanding how from a particular breach point the adversary might move laterally, reach other systems, or compromise critical assets.
- Attack path visualization. At the core of XM Cyber is the visual battleground that automatically generates a network map and displays assets and the chronological flow of possible attack paths within your live environment. Your security teams can drill down for asset discovery or to identify the exact technique used by the virtual hacker to move from one step to the other.
- Weighted scoring based on asset criticality. Combining efforts with threat and vulnerability management, machine tagging is used to incorporate the risk appetite of an individual asset into the exposure score calculation. Therefore, machines marked as “high value” will receive more weight in the exposure score calculation.
- Attack Simulation from any breach point. XM Cyber runs attack simulations automatically starting from the identified breach point showing you where an attack could go.
- Flexible architecture. Quick, easy deployment on premise or in the cloud.
- Comprehensive and up-to-date attack scenarios using the latest hackers' techniques and methods. XM Cyber gives you the ability to run multiple and simultaneous attack scenarios, including the latest attacks from XM Labs and the MITRE ATT&CK framework.

Are You Asking Your Network and Security These Important Questions to Stop Ransomware?

Are business-critical assets secured?

How do you find those attack paths?

How would an attacker stage a ransomware attack in my environment, and how far would they get?

How can you measure to see how an attack could get from your HR device to your critical backups?

How do you find out how an attacker in your network can stage a ransomware attack before pushing out the payload?

Can you prioritize which vulnerabilities to fix and their location?

Can you see where your administrators are using their credentials and where they can be harvested, i.e., their vulnerabilities?

How about those service accounts that were set up years ago without a password expiration that use an interactive logon?

Is your network segmentation intact, or is there a way that it can be circumvented?

How can you monitor this daily when your network and cloud are constantly changing?

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
info@xmcyber.com

XM CYBER