Use Case

XM Cyber | See All Ways™

XM Cyber for Amazon Web Services (AWS)

Gain Full Visibility into Potential Attacks Across Cloud and On-Premise Environments

Consider all the components required to build a successful AWS infrastructure: virtual machines, databases, connections to multiple services, as well as security roles and policies. There are many opportunities to make mistakes or misconfigure accounts and permissions.

XM Cyber helps you understand your use of AWS from the attacker's perspective through via the Attack Path Management platform.

As more and more data are migrated to the cloud, new risks emerge making it critical for companies to assess their risk posture and understand how attackers can operate within their cloud environment. Organizations relying on the cloud must now understand how their new hybrid environment can be attacked from on premise devices that link to cloud data.

Continuously Apply Risk-Free Attack Simulation Across Your Cloud Environments

If you are assessing your on-prem risk separately from your cloud risk, you have no way of knowing what risks they pose to each other. XM Cyber closes the loop between on-prem and cloud risk assessment via its patented, Attack PAth Management platform.

The XM Cyber platform audits AWS configurations via AWS API and uses that information to calculate different attack vectors. By simulating attacks on an organization's AWS infrastructure, it is possible to find misconfigurations leading to risks such as IAM privileges escalations, access token theft or leveraging of the Cloud Instance Metadata API to pivot across the cloud.

XM Cyber reduces cybersecurity risk by continuously simulating advanced persistent threats against an organization's critical assets, identifying security gaps, and prioritizing remediation. Implementing in an AWS environment is a simple process requiring less than an hour.

Secure your AWS Migration

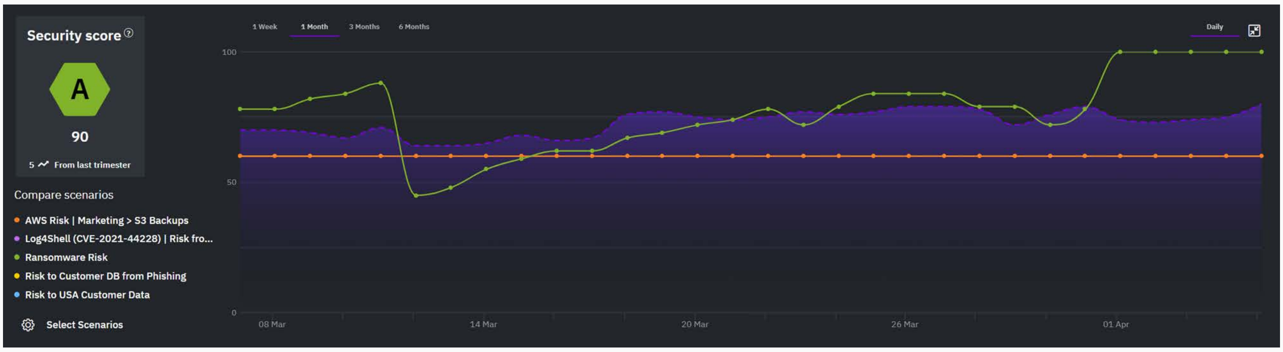
Most organization are still in migration mode. It is critical for organizations to deploy XM Cyber while they are migrating to the cloud, not just afterwards. Attacks can happen during migrations, and mistakes that happen throughout the migration process must be identified and fixed. The benefit is you can confidently build your AWS infrastructure in a fully secure manner that will not require a re-architecture at a later date.

Key Benefits

- Identify security gaps in AWS implementations resulting from mistakes, misconfigurations and poor IT hygiene.
- Apply during migrations to eliminate security risks throughout the process
- Identify hybrid attack possibilities where on
- Run 24/7 continuous attack simulations to spot security issues as they happen
- Protect critical assets stored in AWS by identifying every attack vector available to hackers
- Add context to incident and alert data based on simulated attack risk analysis to prioritize responses and optimize resources

Are Your Critical Assets Really Secure On-Prem And in The Cloud?

Rely on XM Cyber for attack path management that closes security gaps in your hybrid cloud network. Customers can rapidly identify and respond to cyber risks affecting their business-sensitive systems because the platform continuously calculates every potential attack path. Detailed remediation options are prioritized based on the potential impact, including exploitable vulnerabilities and credentials, misconfigurations, and user activities. XM Cyber eliminates 99% of its customer's cyber risk by focusing IT and security operations on the one percent that represents the greatest threat.



About XM Cyber

XM Cyber is a leading hybrid cloud security company that's changing the way innovative organizations approach cyber risk. Our attack path management platform continuously uncovers hidden attack paths to your critical assets across cloud and on-prem environments, so you can cut them off at key junctures and eradicate risk with a fraction of the effort. This approach is a complete game-changer, which is why some 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.

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

XM Cyber