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. In fact, Gartner predicts that by 2020, 95 percent of all cloud security incidents will be the customer’s fault. The result might expose your critical data to a wide audience outside your network. XM Cyber helps you understand your use of AWS from an attacker’s perspective through an innovative Attack-Centric Exposure Prioritization (ACEP) 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, automated Attack-Centric Exposure Prioritization (ACEP) 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 organizations 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.
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.

**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-premise and cloud infrastructure connect
- 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

XM Cyber continuously evaluates your environment for high-risk exposures due to misconfigurations, vulnerabilities and human error that could be used in combination to open access to your most critical assets. By identifying and prioritizing security that protects the most important data, XM Cyber customers optimize their existing security investments and significantly reduce risk and the impact of a breach.

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

Rely on XM Cyber for Attack-Centric Exposure Prioritization that closes gaps in cloud and physical network security. 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.