CYBER INSIGHTS

LloydSadd

NAVACORD®

Attack Surface Management Explained

Attack surfaces refer to the total possible entry points (also known as attack vectors) for unauthorized access into any system.

The recent rise of remote and hybrid work combined with the shift to the cloud and widespread implementation of software-as-a-service applications have made attack surfaces increasingly prominent, complex and difficult to defend against cyberattacks. Fortunately, attack surface management (ASM)—the continuous monitoring of potential attack vectors—can provide organizations with an inventory of exposed assets to accelerate responses to cyber threats. ASM entails the following automated core processes:

1. **Asset discovery**—This is a continuous process that scans for potential entry points for cyberattacks. These assets may include subsidiary assets, third-party or vendor assets, unknown or non-inventoried assets, known assets, or malicious or rogue assets.
2. **Classification and prioritization**—Assets are analyzed and prioritized by the likelihood that hackers could use them as a target. They're inventoried by their connections to other assets in the IT infrastructure, such as IP address, identity and ownership. Assets are also analyzed for exposures such as missing patches, coding errors and potential attacks, including ransomware or malware. Each vulnerable asset is assigned a risk score or security rating.
3. **Remediation**—Potential vulnerabilities are remediated in order of priority. It may be necessary to apply software or operating system patches, debug application codes or use stronger data encryption. Previously unknown assets may need new security standards, or it may be necessary to integrate subsidiary assets in organizations' cybersecurity strategies.
4. **Monitoring**—Security risks change whenever a new asset is deployed or existing assets are used in new ways. Networks and their inventoried assets are continuously monitored for vulnerabilities to allow ASM to find attack vectors in real-time and give organizations a chance to neutralize threats.

ASM not only protects organizations from cyberattacks, but it's also frequently required by underwriters to obtain cyber insurance, making it all the more vital.

If you have questions specific to your business, or would like additional information, please reach out to your Lloyd Sadd Advisor.

LET US HELP YOU MANAGE YOUR RISK

Edmonton: 1.800.665.5243
Calgary: 1.866.845.8330
Kelowna: 1.800.665.5243

lloydsadd.com
info@lloydsadd.com