FOR IMMEDIATE RELEASE

Contact: Jenn Jones
Phone: 857-328-0173
Email: press@cyberriskalliance.com

CRA Study: Piecemeal Approaches to API Security put Organizations in the Crosshairs

Application development and APIs have become critical to many organizations, which has put APIs in the crosshairs of sophisticated cybersecurity attacks

New York, NY, July 5, 2022 – Many security teams struggle to achieve the visibility and maturity needed to minimize risks and protect against sophisticated attacks such as bots and distributed denial of service (DDoS), according to a new report from CRA Business Intelligence, the research arm of cybersecurity data and insights company CyberRisk Alliance.

The data and insights in this report are based on an online survey conducted in early 2022 among 250 IT and cybersecurity decision-makers and influencers from companies of all sizes. The survey was underwritten by ThreatX, provider of a platform that protects APIs from all threats, including DDoS attempts, bot attacks, API abuse, exploitations of known vulnerabilities, and zero-day attacks.

Although many organizations have various API standalone protection tools in place, many of the respondents often regarded these solutions as ineffective and incomplete, particularly when tracking undocumented (rogue or shadow) APIs and expired (zombie) APIs.

Among the survey findings:

- Organizations lack an overall strategy to guide API efforts and, perhaps, to support advocacy for additional resources: 56% of respondents said their organizations have an effective API protection strategy
- In 59% of organizations, responsibility for API protection rests with developers and/or DevOps teams. While there may be functional benefits to such arrangements, these teams may lack the security expertise, skills or time to enforce security adequately — where fully managed API attack protection platforms can fill this gap.
- Resources for API security are deemed insufficient at many organizations, although that may be starting to shift: Most respondents are optimistic their organizations will increase API security budgets in 2022.
- While an overarching API security strategy is beneficial on its own, it can also serve as a driver for the purchase or upgrade of API protection solutions. Approximately half of the

respondents said that supporting such a strategy would be a primary reason to invest in an API protection tool or platform.

"As organizations continue their journey to the cloud, API security is an increasing area of concern, especially when 31% of organizations' APIs are undocumented (shadow or rogue)," said Matt Alderman, Executive Vice President, Foresight at CyberRisk Alliance. "This ThreatX research highlights the need for a fully managed API attack protection platform. Organizations should focus on real-time attack monitoring and blocking, attack details, and attacker behavioral analytics as key features for these platforms."

As the practice of API security matures, organizations should focus on developing a deeper understanding of their API environments, together with potential vulnerabilities throughout the API development life cycle.

Managing and maturing API security strategy has become the next essential task for the modern enterprise: leveraging technology and managed services to close security gaps and protect critical assets.

The full research report is available for **download here**.

About CyberRisk Alliance
CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, SecurityWeekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. Click here to learn more.

About ThreatX
ThreatX's API protection platform and managed services make the world safer by protecting APIs from all threats, including DDoS attempts, botnets, zero-days and multi-mode attacks. ThreatX applies AI and ML to detect and respond to even the slightest indicators of suspicious activity in real-time, protecting companies in every industry globally.