Karamba Security Survey: Consumers Hold Vendors Accountable for Their Devices' Cybersecurity

A 1,000-User Poll Exhibits Public Pressure on Vendors of Connected Devices

Karamba Security will unveil at CES 2020 a product and service portfolio that enables vendors to seamlessly cyber-protect their connected devices throughout the device lifecycle

BLOOMFIELD HILLS, MI, and HOD HASHARON, Israel – Karamba Security, a world-leading provider of embedded cybersecurity for connected devices, today released a report revealing that nearly three quarters of consumers expect manufacturers of connected IoT devices to protect their devices from hacks. This view is in sharp contrast to today's datacenter best practices, which require users to deploy their own measures of cyber protection, such as antivirus software.

The report, "Consumer Attitude Towards IoT Security," surveyed 1,000 consumers in the United States on connected device security ahead of the CES 2020 conference, which in an average year reveals hundreds to thousands of new connected devices. The survey results show consumers are increasingly concerned about hacks of such connected devices and demand manufacturers embed high-level security in their connected products.

In the survey, 87% of respondents said they believe connected device manufacturers should be responsible for securing products from hacks. Nearly three-quarters of the respondents went a step further: 72% said they would refuse to use a connected IoT device if they found out it wasn't equipped with embedded security.

"The survey results clearly show that consumers aren't willing to compromise when it comes to securing connected devices," said Ami Dotan, Karamba Security CEO and Co-founder. "As connected devices like Amazon Alexa, smart home appliances, and connected cars become more popular, hackers grow more and more sophisticated, finding ways to exploit vulnerabilities and infiltrate their targets for economic gains. Manufacturers need to step up to the challenge and provide their customers with the protection they deserve."

The Karamba Security survey showed most consumers are concerned about the future of IoT security. A total of 81% think IoT devices will become more of a target for hackers in the next five years. When asked whether they were more concerned about a thief breaking into their home or a hacker breaching one of their connected devices, responses were even – 50% for each.

Karamba Security will unveil at CES2020 a portfolio of products and services that enables vendors to seamlessly protect their connected devices. The portfolio covers the entire device lifecycle, from design to post-production. The portfolio does not require changes to R&D processes and has a feather-light footprint on the device itself, in order to not derail the device performance.

"Device manufacturers need to be armed with powerful tools to meet connected device security threats to consumers head-on," Dotan said. "Customers are demanding security that is embedded into the connected device itself. Our research reflects this sentiment, and to help both the device manufacturers and consumers, we plan to announce new products at CES that provide a comprehensive solution that seamlessly and automatically embeds tamper-proof cybersecurity from the design through the post-production stage for connected devices. It's a win-win for manufacturers and consumers of their products".

Karamba Security will present this portfolio of security solutions at CES 2020, North Hall, Booth #5931, January 7-10, in Las Vegas. Joining Karamba's portfolio of runtime integrity in production, the new product suite will arm manufacturers with the security validation they need to ensure that their

connected devices are secured during the design development phase. Another part of the offering will communicate with the cloud and continuously detect threat indicators. This intelligence alerts the security operations center of suspicious behavior on the device and fleet level.

About Karamba Security
Karamba Security is the embedded security powerhouse, providing industry-leading embedded cybersecurity solutions for connected systems. Connected device manufacturers in automotive, Industry 4.0, enterprise edge, and IoT rely on Karamba's portfolio and experts to protect their connected devices against Remote Code Execution (RCE) and Command Injection. After over 50 successful engagements with Fortune 100 companies, automotive OEMs, tier-1 providers and other device manufacturers, connected device providers worldwide trust Karamba's award-winning solutions for compliance and brand competitiveness when protecting their customers against cyberthreats.

More information is available at www.karambasecurity.com and follow us on Twitter @KarambaSecurity.

Karamba Security Business Contact:
Amir Einav, VP of Marketing
+1-214-620-7320

Media Contact:
PAN Communications
Kyle Tildsley
Karamba@pancomm.com
+1-617-502-4352