Karamba Security Expands its Autonomous Cybersecurity Technology to Protect Enterprise Edge, Industry 4.0 and IoT Smart Devices

Partnership with Wind River to accelerate market adoption of embedded security solutions to prevent mass scale cyberattacks

BLOOMFIELD HILLS, Michigan & HOD HASHARON, Israel – May 14, 2019 – Karamba Security, a world-leading provider of embedded cybersecurity for the automotive industry, today announced that its autonomous security solution is being used to protect connected devices and systems across a broad spectrum of vertical markets facing similar large-scale cybersecurity threats.

Following successful deployments of Karamba's embedded, self-protecting and auto-recovery software technology in the automotive industry -- including more than 32 engagements with car manufacturers and tier-1 automotive suppliers -- manufacturers in other vertical markets have sought out Karamba's technological offering. Manufacturers of enterprise edge devices, Industry 4.0 controllers and other connected systems have engaged with Karamba, using its runtime integrity software to provide an active hardening layer to their connected, massively deployed devices.

In a world where everything is connected – cars, factories, homes, enterprise edge devices, to name a few – widespread attacks on connected machines threaten to disrupt everyday life and put businesses at risk. Connected system providers are required to offer secured devices to protect their customers against brand damage, liability risks and revenue loss that can result from large-scale cyberattacks.

"These attacks have a potential to disable transportation fleets, disrupt national power grids or use in-home surveillance cameras to violate privacy," says Ami Dotan, Karamba Security co-founder and CEO. "Connected system providers are working harder than ever to ensure that their products are safe and secure. Embedding Karamba's software into their existing infrastructures offers a new level of protection against hackers trying to exploit connected devices on a grand scale."

In conjunction with this market expansion, Karamba also announced a go-to-market partnership with embedded software firm Wind River to help automotive, aerospace, defense, industrial, medical and network providers to automatically embed self-protection security in their connected devices. With their successful collaboration for the automotive industry, the two companies launched an initiative to expand the use of built-in, embedded, runtime integrity in the connected systems world.

"Karamba's focus on protecting the runtime and software integrity in critical applications makes them a natural Wind River partner to expand our safe and secure product offering for customers across the markets we serve," said Michel Genard, vice president of product at Wind River. "Cybersecurity is increasingly becoming a top priority across critical infrastructure sectors where embedded protection against cyberattacks is a must have. Together with Karamba, we are contributing to the evolution of connected devices and systems with a preventative solution against advanced attacks."

Karamba's technology automatically hardens the full image of the connected system and prevents modification of the factory settings. The embedded security is always on, assuring the software integrity during runtime and preventing attackers from taking control of the connected system. This way developers, providers, manufacturers and vendors can offer products that are self-protected against cyberattacks.

“Connected devices of all types need protection for both their functionality and their data,” said Steve Hoffenberg, a director at industry analyst firm VDC Research. “Connectivity increases the number of potential attack vectors, and hackers have dramatically improved their attack skills. Device makers need to up their defensive game in response, enabling devices to protect themselves without imposing onerous constraints on legitimate users.”

“We quickly recognized that demand for our automated device hardening technology applies to multiple markets and a myriad of products,” said Ami Dotan. “The mandate for security is being driven by manufacturers, suppliers and business users alike, and we are able to offer a proven, production ready solution that is automated, pragmatic and simple. Offering automatically embedded security to software defined products in automotive, Industry 4.0, IoT and other products fit well with our partnership with Wind River.”

About Karamba Security
Karamba Security provides industry-leading embedded cybersecurity solutions for connected systems. Product manufacturers in automotive, Industry 4.0, IoT, and enterprise edge rely on Karamba’s automated runtime integrity software to self-protect their products against Remote Code Execution (RCE) cyberattacks with negligible performance impact. After 32 successful engagements in automotive and other industries, product providers trust Karamba’s award-winning solutions to increase their brand competitiveness and protect their own 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
amir.einav@karambasecurity.com
214-620-7320

Media Contact:
PAN Communications
Kyle Tildsley
Karamba@pancomm.com
617.502.4300