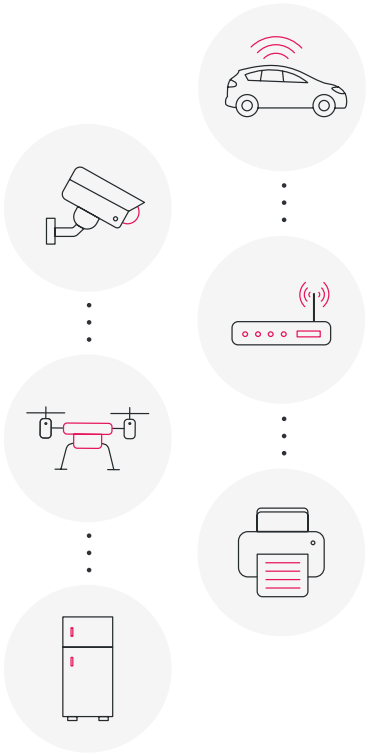
XGuard Suite™

Karamba Security | THE EMBEDDED SECURITY POWERHOUSE.

Erstklassige Selbstverteidigung

Karamba Security's Runtime Integrity für eingebettete Systeme härtet vernetzte Geräte automatisch und verhindert so, dass Hacker sie während des gesamten Produktlebenszyklus kompromittieren können. Die Software von Karamba Security verhindert Angriffe während der Laufzeit – von bösartigen Dateien und Skripten bis hin zu dateilosen Angriffen, die Pufferüberläufe und andere Memory-Schwachstellen ausnutzen.

Die eingebettete Runtime Integrity-Technologie umfasst sowohl Control Flow Integrity (CFI) als auch Application Whitelisting. Beide kombiniert schützen vor der Ausnutzung von Zero-Day- und Day-One-Schwachstellen – und das ganz ohne Fehlalarme. Die Laufzeitschicht ist komplementär zur statischen Code-Analyse und kann die fortschrittlichsten Angriffe auf kritische vernetzte Systeme wie Netzwerkkomponenten, Enterprise Edge, Kfz-Steuergeräte und IoT-Geräte blockieren.



Wie verhindert Karamba Security's Software die Kompromittierung von Geräten?

Selbstschützende Software

Die Sicherheitsrichtlinie wird während des Entwicklungsprozesses automatisch in die Geräte-Firmware eingebettet. Entscheidungen zur Erkennung und Vermeidung werden lokal auf dem Gerät getroffen. Es ist keine Vernetzung erforderlich.

Keine Fehlalarme

Patentierte deterministische Algorithmen stellen sicher, dass – basierend auf den Werkseinstellungen – nur legitime Funktionsaufrufe und legitime Binärdateien in den Systemspeicher geladen werden können. Alles andere wird blockiert.

Vernachlässigbare Performanceeinbußen

Die eingebettete Sicherheitsrichtlinie prüft die Integrität aller Operationen während der Laufzeit und benötigt dafür weniger als 5% der CPU-Auslastung und des Memory-Footprints. Es ist kein Hardware-Upgrade erforderlich.

Unterstützt alle Gerätetypen

Unterstützt werden ARM, Intel, PowerPC und Infineon Prozessoren, Linux, VxWorks, QNX und RTOS Betriebssysteme. Jeder Controller kann geschützt werden.

Keine Updates der Blacklist erforderlich

Die Sicherheitsrichtlinien basieren auf den Werkseinstellungen. Es ist nicht notwendig, die Richtlinie mit neuen, Anti-Malware-Signaturen zu aktualisieren. OTA-Funktionalität wird unterstützt.

Kein Eingriff von Entwicklern nötig

Patentierte Algorithmen generieren automatisch die Sicherheitsrichtlinie und betten diese während des Software-Image-Builds in die Gerätesoftware ein.

www.karambasecurity.com | contact@karambasecurity.com

Karamba Security USA
Tel: +1 248 574 5171

Karamba Security Germany
Tel: +49 151 1471 6088

Karamba Security Israel
Tel: +972 9 88 66 113