Sectigo and Green Hills Software Partner to Help Manufacturers Protect Endpoint Devices

Submitted by: Sectigo
Monday, 2 November 2020

Green Hills to Offer Sectigo Embedded Firewall Products, Integrated and Optimized with Its Portfolio of Internet-Connected Platform Solutions

ROSELAND, NJ and SANTA BARBARA, CA – November 2, 2020 – Sectigo® (https://sectigo.com/), a leading provider of automated digital identity management, embedded security, and web security solutions, and Green Hills Software (https://www.ghs.com/), the worldwide leader in high-assurance operating systems, today announce a global reseller agreement. The agreement enables Green Hills Software to offer Sectigo's Icon LabsTM Embedded Firewall, integrated and optimized for use with Green Hills Software's INTEGRITY® real-time operating system (RTOS) and its embedded high-performance TCP/IP v4/v6 host and router networking stack.

The pairing strengthens Green Hills Software's internet-connected platform solutions with the expanded networking security required in today's connected systems responsible for critical functions for automotive, industrial, medical, transportation and mil/aero industries.

"Most cyberattacks on embedded systems remain undetected until it is too late. Early detection is critical as it maximizes the safety of products while helping to prevent the loss of IP, disruption of services, and attacks proliferating to other portions of the system or network," explained Alan Grau, VP of IoT/Embedded Solutions, Sectigo. "Green Hills Software's integration of our embedded firewall with their proven and mature INTEGRITY RTOS will provide customers worldwide with a powerful combination of experience and security technology that sounds the alarm, then stops the attack."

The INTEGRITY RTOS (https://www.ghs.com/products/rtos/integrity.html) microkernel architecture is designed for critical embedded systems demanding proven separation, security, and real-time determinism. The operating system's separation architecture helps manufacturers safely and securely partition software running at different levels of criticality. For critical functions, INTEGRITY assures secure and real-time execution by means of impenetrable partitions that deliver freedom-from-interference and guaranteed system resources.

The Sectigo Icon LabsTM Embedded Firewall (https://sectigo.com/enterprise/sectigo-iot-platform) enjoys widespread global adoption, combining numerous powerful and configurable features to detect and contain cyberattacks.

Configurable filtering policies — Uses configured filtering rules to control the filtering engine. The rules provide complete control over the type of filtering performed and the specific criteria used to filter packets. Rules can be configured for:

Static filtering rules for IP address, MAC address, port number, and protocol number
Block list and allow list filtering modes
DPI filtering rules for message type, message contents, and message source
Threshold-based filtering criteria

Independently enabling and disabling static filtering, dynamic filtering, DPI filtering, and threshold-based filtering

EDSA Compliance support — Serves as an important building block for achieving EDSA compliance for embedded devices, providing support for many capabilities mandated by EDSA-311:

Protocol fuzzing and replay attack protection
Data flooding protection
Denial of service protection
Notification of attacks
Disabling of unused ports

Logging and alerting — Maintains a log of security events and policy violations, enabling command audits and forensic investigation to determine the source of an attack.

Management system integration — Incorporates an agent that enables remote management from an enterprise security manager system, or to other Security Information and Event Management (SIEM) systems. This integration provides:

Centralized management of security policies
Situational awareness and device status monitoring
Event management and log file analysis

Intrusion detection and prevention — Blocks all unused ports and protocols, limiting the attack surface hackers can exploit. Logging packets that violate configured filtering rules enables detection of unusual traffic patterns, traffic from unknown IP addresses, and other suspicious behavior.

“Green Hills is pleased to be adding this additional cybersecurity capability to our portfolio of industry-leading foundational security offerings,” said Dan Mender, VP of Business Development, Green Hills Software. “Protecting critical internet-connected solutions is paramount for our customers, and Sectigo’s Icon Labs Embedded Firewall capability extends our customers’ ability to design purpose-built secure solutions in automotive, industrial, medical, transportation and mil/aero markets.”

Green Hills Software’s internet-connected platforms are integrated and optimized with Sectigo’s embedded firewall and are available today. For more information, contact info@ghs.com or visit our website at https://www.ghs.com/go/icon-labs (https://www.ghs.com/go/icon-labs).

About Green Hills Software

Founded in 1982, Green Hills Software is the worldwide leader in embedded safety and security. In 2008, the Green Hills INTEGRITY-178 RTOS was the first and only operating system to be certified by NIAP (National Information Assurance Partnership comprised of NSA & NIST) to EAL 6+, High Robustness, the highest level of security ever achieved for any software product. Our open architecture integrated development solutions address deeply embedded, absolute security and high-reliability applications for

the military/avionics, medical, industrial, automotive, networking, consumer and other markets that demand industry-certified solutions. Green Hills Software is headquartered in Santa Barbara, CA, with European headquarters in the United Kingdom. Visit Green Hills Software at https://www.ghs.com (https://www.ghs.com).

Green Hills, the Green Hills logo and INTEGRITY are trademarks or registered trademarks of Green Hills Software LLC, in the U.S. and/or internationally. All other trademarks are the property of their respective owners.

About Sectigo

Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As the world's largest commercial Certificate Authority with more than 700,000 customers and over 20 years of experience in online trust, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions for securing webservers, user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow. For more information, visit www.sectigo.com (http://www.sectigo.com/) and follow @SectigoHQ.

UK Media Contacts:

Ines Mitsou
Positive
020 3637 0640
imitsou@positivemarketing.com

Max Bailey
Positive
020 3637 0640|07933318525
mbailey@positivemarketing.com

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of Sectigo

Copyright © 1999-2026 ResponseSource, Northburgh House, 10 Northburgh Street, London, EC1V 0AT, UK

e: info@responsesource.com t: 020 3426 4051 f: 0345 370 7776 w: https://www.responsesource.com