IoT Security Assessment

Better security for a connected world

The Problem

As the deployment of IoT devices continues to accelerate, their impact on critical sectors such as infrastructure, healthcare, automotive, and government operations becomes more profound. These IoT devices — responsible for powering cities, monitoring patient health, managing critical systems, and safeguarding sensitive data — are increasingly targeted by cyberattacks, posing significant risks to national security, public safety, and operational continuity.

Consider the energy grid as an example. In 2023, a critical vulnerability (CVE-2023-28489) was discovered in Siemens Remote Terminal Units (RTUs), widely used in industrial control systems. Exploiting this flaw could allow attackers to take complete control of these devices, potentially destabilizing power grids and causing blackouts by altering critical automation parameters.[1]

Beyond the energy grid, risks extend to other life-critical and mission-critical systems, including:

- **Medical devices:** In 2022, researchers identified vulnerabilities in widely used infusion pumps in hospitals, including leakage of sensitive information, unauthorized access, and overflow. These flaws could be exploited to alter medication delivery, posing serious risks to patient safety.[2]
- **Automotive systems:** In 2024, a vulnerability in Kia's web portal allowed researchers to hack and track millions of vehicles, enabling unauthorized control over features like unlocking doors and starting ignitions.[3]

Adding to these risks is the issue of transparency in IoT device firmware. Many IoT devices are built using complex, multi-layered software stacks often containing third-party and open-source components. Without a comprehensive Software Bill of Materials (SBOM), organizations struggle to identify and track vulnerabilities within their IoT ecosystems. For example, vulnerabilities in widely used open-source libraries embedded in firmware can remain undetected for years, allowing attackers to exploit them at a scale.

The scale of these threats is staggering. A report from April 2023 revealed that the number of IoT-related cyberattacks reached over 10.54 million by the end of 2022.[4] These attacks not only endanger lives and operations but also impose legal and reputational risks on manufacturers and service providers, as regulatory frameworks for IoT security — such as those requiring SBOM generation and management— become increasingly stringent.

For organizations in critical sectors, maintaining the security of IoT devices, ensuring compliance with emerging standards, and managing SBOM complexities can be overwhelming. Many lack the specialized expertise, tools, and bandwidth to address these challenges effectively.

[1] https://www.securityweek.com/critical-siemens-rtu-vulnerability-could-allow-hackers-to-destabilize-power-grid/
[2] https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities/
[3] https://www.wired.com/story/kia-web-vulnerability-vehicle-hack-track/
[4] Monthly number of IoT attacks global 2022 | Statista

The Solution

In the face of this growing cyber threat and as IoT cybersecurity testing requirements intensify and compliance deadlines loom, are you ready? Are you adequately equipped to conduct comprehensive testing of IoT devices? Failing to do so could result in significant costs.

Backed by decades of security testing and research, the Keysight IoT Security Assessment is here to help you. We make it easy and cost-effective for you to improve the cybersecurity of IoT devices and align with various IoT labeling standards.

We provide an IoT cybersecurity testing platform that automates validation through a point-and-click user interface (UI) or automation API. It's a turnkey assessment tool enabling you to identify security gaps in IoT devices related to security, compliance, and labeling requirements. The system offers a comprehensive security assessment, encompassing firmware analysis to uncover vulnerabilities and weaknesses, SBOM generation for tracking software components, and protocol fuzzing to identify issues embedded in the supply chain. It can detect weak passwords, outdated encryption, and other security flaws, making it suitable for a wide range of use cases.

Use	Description
Firmware analysis and SBOM generation	Identifies vulnerabilities and weaknesses and ensures transparency by analyzing device firmware and generating a comprehensive inventory of software components
Protocol fuzzing	Provides industry leading fuzzing, which accelerates discovery of unknown flaws in protocol stacks and chipsets
Compliance testing	Evaluates target against specific requirements such as encryption, open ports, and certificate validation
Vulnerability assessment	Scans devices against a list of known threats and vulnerabilities

Table 1. Use cases

How does it work?

The Keysight IoT Security Assessment consists of static analysis using firmware analysis and a set of dynamic analysis audits. Static analysis doesn't require access to the device; having only the binary firmware file is sufficient. However, dynamic analysis requires access to the Device Under Test (DUT).

To perform static firmware analysis, the user only needs to define a new product and upload the corresponding firmware or firmware files (Figure 1). The system automatically conducts a comprehensive analysis, providing detailed results for review. Figure 2 illustrates the overview page of an analyzed firmware, showcasing the key insights.

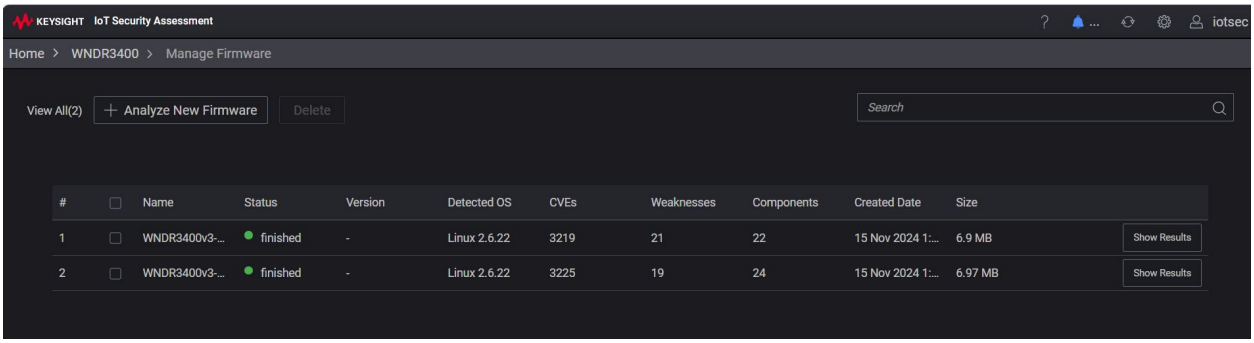

Figure 1. Firmware upload page

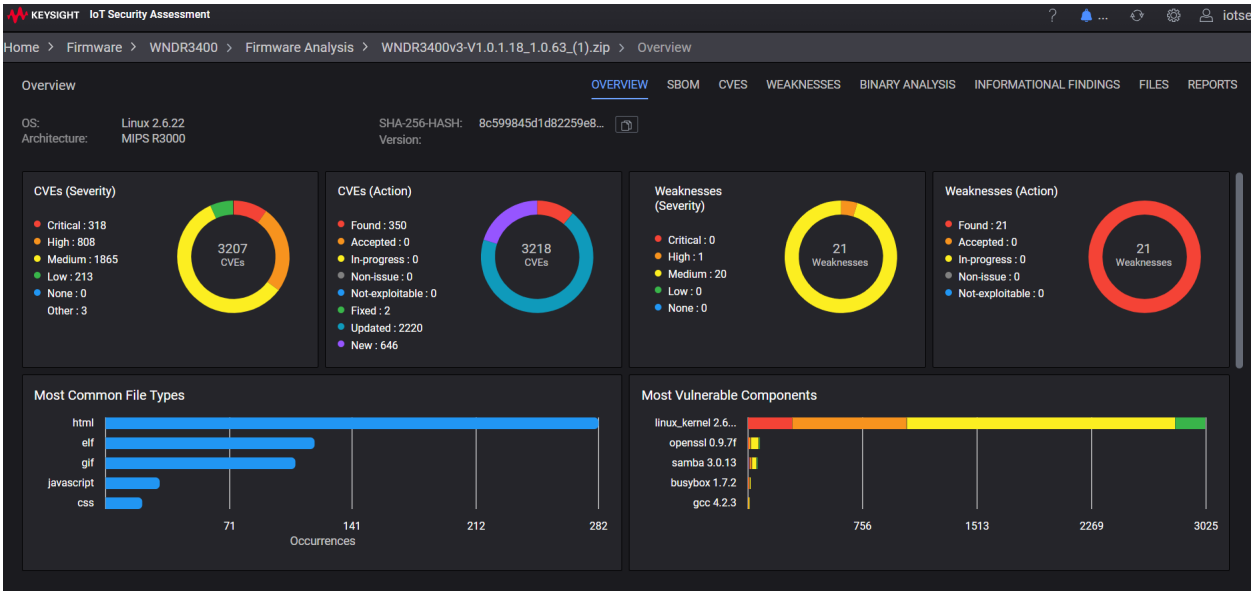

Figure 2. Firmware overview page

In Figure 3, you can see an example of the user interface and a short demo example of how dynamic audits work. It allows you to easily see recent IoT test scenarios, and with a simple press of a button, you can run automated tests and see the results as well as re-run the tests that fail. You can also use the product for automated IoT compliance testing. It allows you to determine whether your IoT device has any security vulnerabilities, assess the severity of these vulnerabilities, and evaluate whether you pass or fail compliance requirements. Additionally, it can assist with the certification process for your IoT devices.

https://www.keysight.com/zz/en/assets/3123-1478/demos/healthcare-demo.mp4

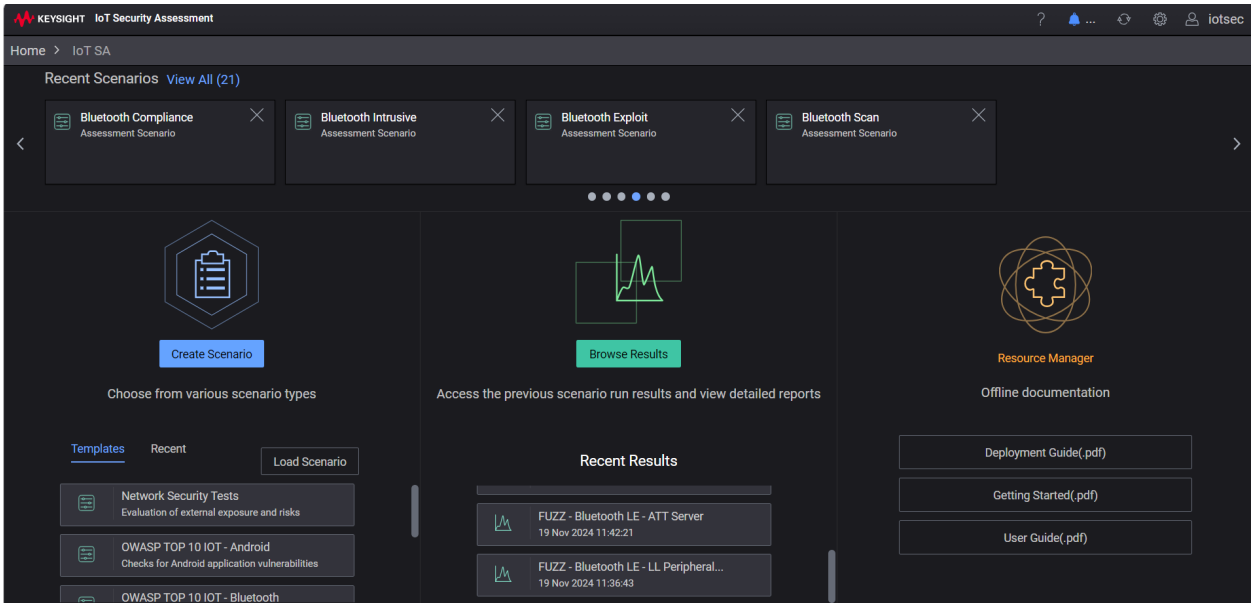

Figure 3. Dynamic audits main page

Key Features

Keysight IoT Security Assessment has been used in the discovery and validation of significant IoT devices' vulnerabilities in everything from industrial devices, connected cars and 5G O-RAN to medical devices. For example, the Keysight IoT Security Assessment helped researchers find previously unknown security flaws that could impact millions of connected devices, prompting the U.S. Food and Drug Administration (FDA) to issue an urgent safety communication.

The key features of the product include the following:

Feature	Benefit description
API driven	• Northbound API for complete control and reporting, we have an intuitive UI or complete REST API management. • Southbound API for easy integration of additional security testing modules such as existing in-house or third-party plugins.
Firmware analysis and powerful binary SBOM generation	Firmware analysis and powerful binary SBOM generation provide unparalleled visibility into device security by dissecting firmware to uncover hidden vulnerabilities, misconfigurations, and weaknesses while generating detailed SBOMs directly from binaries for comprehensive risk assessment and compliance.
Comprehensive assessments and tests	Full-spectrum security and resiliency testing, including Wi-Fi, O-RAN, CAN-bus, Bluetooth, Android, TLS/SSL, and web. Application-layer attacks such as password guessing and Android Debug Interface exploitation.
Industry leading Fuzzing	With our partnership, the Synopsys Defensics®, our fuzzing capabilities cover a wide range of networking transports, including Bluetooth®, Bluetooth LE, Wi-Fi, IPv4, and IPv6.
Easy to use UI with detailed reporting	• Results are presented with clear and complete data, allowing you to quickly find security flaws in connected devices and understand the severity. • Includes Risk and CVSS score and vector as well as explanation and solution.
Plug-and-play on-premises hardware appliance	A plug-and-play on-premises hardware appliance designed for seamless use while ensuring complete data privacy.

Table 2. Features

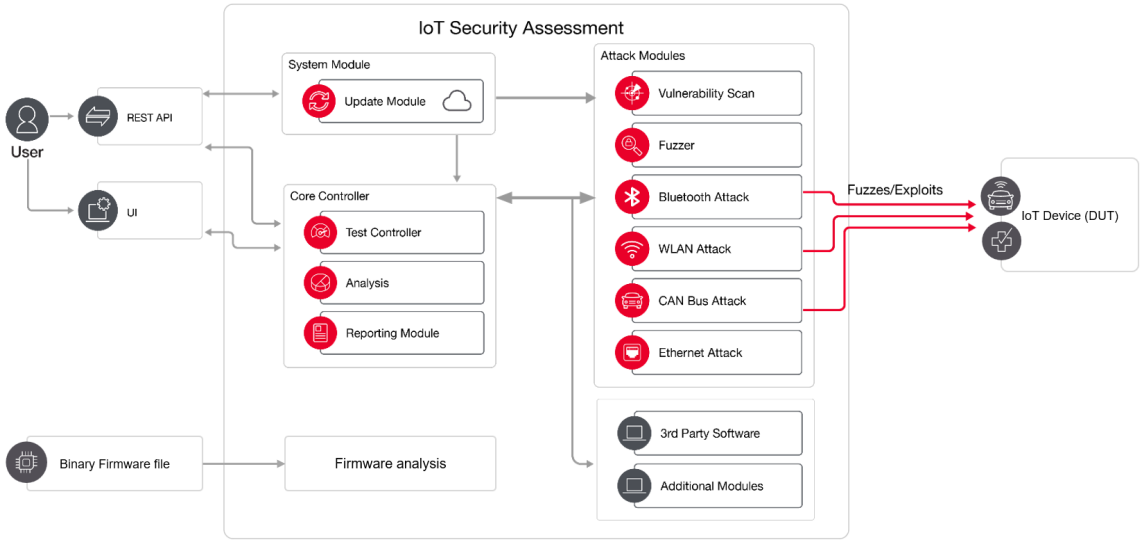

Figure 4. IoT Security Assessment architecture

The entire IoT Security Assessment package is API-driven, so it is easy to plug in existing and third-party modules. So, if you have already built your own test scripts and do not want to discard them, just plug them in and keep using them — all controlled by the same API as the rest of the IoT Security Assessments.

One of the main capabilities of the product is automated firmware analysis. It can identify vulnerabilities directly within the device's operating code, including everything from extracting the Software Bill of Materials (SBOM) to uncovering associated vulnerabilities, detecting hard-coded credentials that pose unauthorized access risks, pinpointing configuration flaws, identifying weak or expired cryptographic keys and certificates, and finding unknown vulnerabilities in binary components within the firmware. This allows for a more comprehensive and proactive security posture assessment, ensuring vulnerabilities are identified and mitigated before they can be exploited.

Another capability is fuzzing, an automated software testing method that injects invalid, malformed, or unexpected inputs into a device to reveal defects and vulnerabilities.

Keysight and Synopsys have partnered to provide IoT device makers with a comprehensive cybersecurity assessment solution. Under the partnership, the Synopsys Defensics® fuzzing tool has been embedded as an option into the Keysight IoT Security Assessment solution.

Hardware Information

Hardware appliance specifications

IoT Security Assessment is delivered as a plug-and-play hardware appliance, designed for seamless deployment and installation within user environments. Detailed hardware specifications are provided below. Figures 5 and 6 showcase the appliance's front and rear views, respectively.

- Intel® i9-13900 13th-Gen Alder Lake Core™
- 1 TB M.2 Gen 4x4 NVME
- 2x32GB SODIMM
- Rugged, -25°C to 70°C fanless operation
- 5x 2.5GbE and 1x GigE
- 2x SATA ports
- MezIO™ interface for easy function expansion
- 6xUSB 3.2 type-A, 2xUSB 2.0 type-A, 1x USB 3.2 type-C

Figure 5. Hardware appliance front view

Figure 6. Hardware appliance rear view

Hardware appliance regulatory specifications

Safety	• IEC 62368-1 • EN 62368-1 • UL 62368-1 / CSA C22.2 No. 62368-1
Emissions and immunity	• FCC Part 15B, Class A • CAN ICES-003(A)/NMB-003(A) • EN 55032, Class A/ EN 55035 / EN 61000-3-2 / EN 61000-3-3 • BS EN 55032, Class A/ BS EN 55035/ BS EN 61000-3-2/ BS EN 61000-3-3 • AS/NZS CISPR 32, Class A • KS C 9832, Class A/ KS C 9835 / KS C 9610-3-2 / KS C 9610-3-3 • VCCI – CISPR 32, Class A
Regulatory approvals	• UL, c-UL (USA, Canada) • CE (Europe) • UKCA (United Kingdom) • RCM (Australia) • KCC (Korea) • VCCI (Japan)
Environmental	• RoHS Directive 2011/65/EU; Annex II, Directive (EU) 2015/863 • WEEE Directive 2012/19/EU • China RoHS

Supported network interfaces

Network interface type	Vendor and model	Usage
WLAN / Wi-Fi	ALFA Network AWUS036AC	All Wi-Fi Keysight Legacy Fuzzing capability and Wi-Fi audits, excluding the Defensics Wi-Fi Fuzzing
	ALFA AC1900 TP Link Archer T9UH ASUS AC68	Defensics Wi-Fi Fuzzing
Bluetooth classic	Esprissif Systems ESP-WROVER-KIT	All BT Classic Keysight Legacy Fuzzing, exploits, and assessments
	TP Link UB400 V1 (V2 is NOT supported) Laird BT851	Bluetooth Classic Fuzzing using Defensics Fuzzing
Bluetooth low energy	Nrf52840 Dongle	BT LE Exploits, BT LE Defensics Fuzzing and Keysight Legacy BT LE Fuzzing
	Laird BL654	Bluetooth LE Fuzzing using Defensics Fuzzing
Bluetooth host controller interface	LM Technologies LM1010, TP Link UB400 V1 (V2 is NOT supported), or Asus BT500	All *Bluetooth* HCI audits
CAN bus	Intrepid ValueCAN 4	
IP (Layer 3-7)	Any supported Ubuntu IP interface	All IP, web, and application-layer assessments

Table 3. Supported network interfaces

Regulatory compliance disclaimer

This product, including its hardware appliance and any integrated or associated third-party RF transceivers used for Wi-Fi and Bluetooth fuzzing, may not have the required certifications for operation in all countries or regions.

It is the responsibility of the purchaser and/or end-user to verify and ensure compliance with all applicable local laws, regulations, and certification requirements before deploying this product or its components. This includes verifying the certification status of any RF transceivers integrated into or used with the product. Use of uncertified hardware in jurisdictions where certification is mandatory may result in legal or regulatory non-compliance.

No responsibility or liability is assumed for the deployment or use of uncertified hardware appliances or RF transceivers in violation of local laws or regulations. For further guidance on regulatory compliance in your region, consult your local regulatory authority or the relevant transceiver manufacturer.

Ordering Information

947-5990

Novus Mini Pro appliance for IoT Security Assessment, and IoT Security Controller Bundle (Perpetual)

Bundle including Novus Mini Pro IoT Security Assessment Hardware Appliance (941-1620), and IoT Security Base Controller Software (Perpetual) (983-1103).

983-1105

Keysight IoT Security, IPv4 Attack Module w/ ATI software (1-year subscription)

Enables TCP/IP Based Tools for Security Assessment (IPv4 Attack Module). Includes new tools based on ATI security research throughout the subscription period and tools for system/service discovery, vulnerability management, assessment against known weaknesses, and discovery of new weaknesses or vulnerabilities. The IPv4 Attack Module will work over any connectivity, wired or wireless, that supports Ethernet/IP. Requires IoT Security Base Controller License. Requires license term to be specified (must be purchased in a single or multiples of years, the list price is per unit per year).

983-1106

Keysight IoT Security, WLAN Attack Module w/ ATI software (1-year subscription)

Enables WLAN Based Tools for Security Assessment (WLAN Attack Module) Includes new tools based on ATI security research throughout subscription period and tools for Fuzzing radio stack, system/service discovery, Vulnerability Management, assessment against known weaknesses, and discovery of new weaknesses or vulnerabilities. Requires IoT Security Base Controller License. Requires license term to be specified (must be purchased in a single or multiples of years, the list price is per unit per year).

983-1107

Keysight IoT Security, Bluetooth Attack Module w/ ATI software (1-year subscription)

Enables WLAN Based Tools for Security Assessment (WLAN Attack Module) Includes new tools based on ATI security research throughout subscription period and tools for Fuzzing radio stack, system/service discovery, Vulnerability Management, assessment against known weaknesses, and discovery of new weaknesses or vulnerabilities. Requires IoT Security Base Controller License. Requires license term to be specified (must be purchased in a single or multiples of years, the list price is per unit per year).

983-1109

Keysight IoT Security, IPv6 Attack Module w/ ATI software (1-year subscription)

Enables TCP/IP Based Tools for Security Assessment (IPv6 Attack Module). Includes new tools based on ATI security research throughout the subscription period and tools for system/service discovery, vulnerability management, assessment against known weaknesses, and discovery of new weaknesses or vulnerabilities. The IPv6 Attack Module will work over any connectivity, wired or wireless, that supports Ethernet/IP. Requires IoT Security Base Controller License. Requires license term to be specified (must be purchased in a single or multiples of years, the list price is per unit per year).

983-1201

IoT Security, RichOS Firmware Analysis Module. (1-year subscription)

Enables RichOS firmware analysis for Linux and Android, SBOM (Software Bill of Materials) generation, CVE scan, identification of firmware weaknesses such as hard-coded credentials and configuration issues, and provides actionable insights. Includes automated analysis of binaries to detect potential vulnerabilities. Requires Novus Mini Pro appliance for IoT Security Assessment, and IoT Security Controller Bundle(947-5990) License. Requires license term to be specified (must be purchased in a single or multiples of years, the list price is per unit per year).

983-1202

IoT Security, Bare-metal (Microcontroller) firmware Analysis Module. (1-year subscription)

Enables bare-metal firmware analysis for microcontroller firmware. Includes static code analysis and targeted code emulation for vulnerability identification including SDK API usage, memory corruption issues, disabled SoC/MCU security features, and outdated vendor SDKs and RTOS. Requires Novus Mini Pro appliance for IoT Security Assessment, and IoT Security Controller Bundle (947-5990) License. Requires license term to be specified (must be purchased in a single or multiples of years, the list price is per unit per year).

983-1301

IoT Security MSSP Bluetooth bundle license (30-day subscription)

Covers Bluetooth fuzzing, including Bluetooth EDR/Classic and Bluetooth LE. The license cannot be sold in multiple 30-day term increments and is not for resale. At all times, the MSSP must retain title and license to, and be the sole user of, all IoT Security Assessment licenses it purchases.

983-1302

IoT Security MSSP WLAN Bundle License (30-day Subscription)

Includes WLAN fuzzing, including WLAN AP and WLAN Client. The license cannot be sold in multiple 30-day term increments and is not for resale. At all times, the MSSP must retain title and license to, and be the sole user of, all IoT Security Assessment licenses it purchases.

983-1303

IoT Security MSSP IPv4 License (30-day subscription)

Includes IPv4 fuzzing. The license cannot be sold in multiple 30-day term increments and is not for resale. At all times, the MSSP must retain title and license to, and be the sole user of, all IoT Security Assessment licenses it purchases.

983-1304

IoT Security MSSP IPv6 license (30-day subscription)

Includes IPv6 fuzzing. The license cannot be sold in multiple 30-day term increments and is not for resale. At all times, the MSSP must retain title and license to, and be the sole user of, all IoT Security Assessment licenses it purchases.

983-1015

Keysight IoT Security Bundle for O-RAN Security w/ ATI software (Perpetual)

All-inclusive IoT Security Bundle for O-RAN Security. Includes IoT Security Base Controller and IP Attack Module with 1 year of ATI updates.

Proposed Ordering Options

Device security assessment

For customers needing dynamic device security assessment:

947-5990: Novus Mini Pro appliance and IoT Security Controller Bundle (Perpetual)

983-1105: IPv4 Attack Module w/ ATI software (1-year subscription)

983-1106: WLAN Attack Module w/ ATI software (1-year subscription)

983-1107: Bluetooth Attack Module w/ ATI software (1-year subscription)

983-1109: IPv6 Attack Module w/ ATI software (1-year subscription)

Firmware analysis and SBOM generation

For customers needing static firmware analysis and SBOM generation capabilities:

947-5990: Novus Mini Pro appliance and IoT Security Controller Bundle (Perpetual)

983-1201: RichOS Firmware Analysis Module (1-year subscription)

983-1202: Bare-metal Firmware Analysis Module (1-year subscription)

Comprehensive security assessment — Full functionality

This configuration includes both dynamic device security assessment and static firmware analysis for a comprehensive IoT security assessment:

947-5990: Novus Mini Pro appliance and IoT Security Controller Bundle (Perpetual)

983-1201: RichOS Firmware Analysis Module (1-year subscription)

983-1202: Bare-metal Firmware Analysis Module (1-year subscription)

983-1105: IPv4 Attack Module w/ ATI software (1-year subscription)

983-1106: WLAN Attack Module w/ ATI software (1-year subscription)

983-1107: Bluetooth Attack Module w/ ATI software (1-year subscription)

983-1109: IPv6 Attack Module w/ ATI software (1-year subscription)