Timesys TRST Device Security Solutions

Bring products to market faster without compromising security, and maintain stronger security with over-the-air updates

The security of devices based on open source embedded systems has never been more critical. The vast majority of commercial products contain embedded Linux, Android, or other Open Source Software, a strategy that enables faster time-to-market. But these same pressures for bringing products to market faster can mean that device security is not adequately addressed in design or in planning for product maintenance after release.

At the same time, you face the daunting task of sifting through thousands of Common Vulnerabilities and Exposures (CVE) notifications every year to determine which ones apply to your devices in production and require patching to mitigate. And by not responding to known security issues affecting your software quickly and efficiently, you risk the chance of your product being compromised.

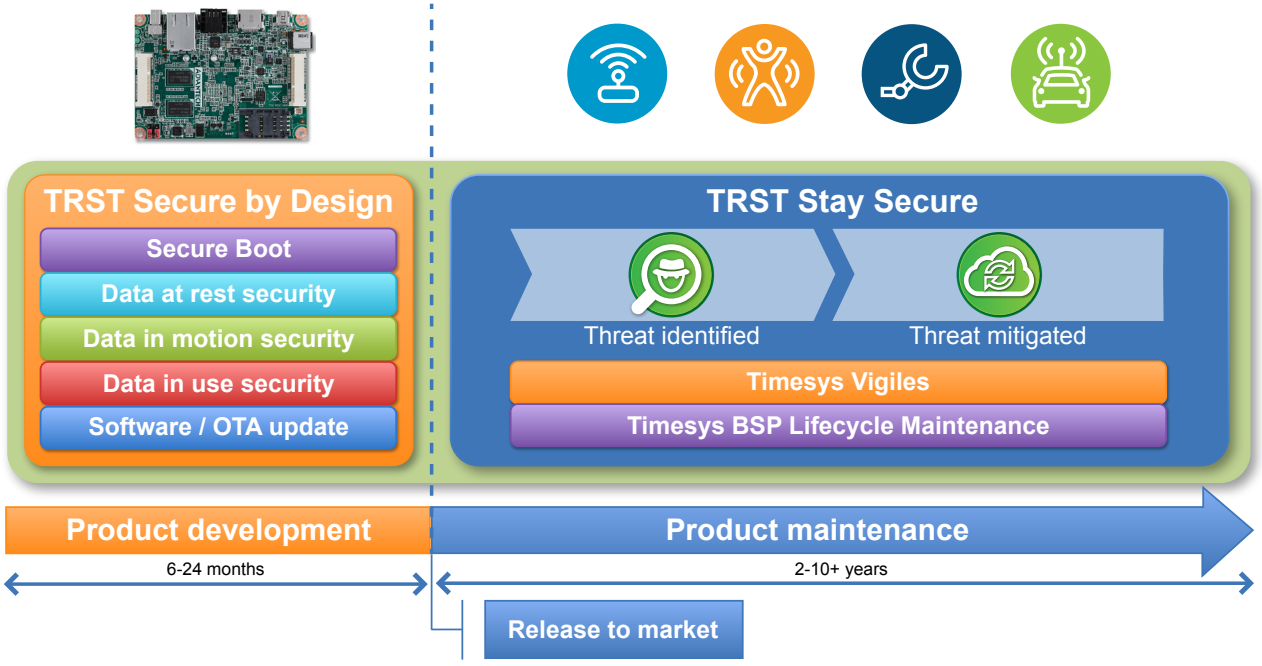
Developers around the world rely on Timesys to accelerate product time-to-market with our build environments including Yocto Project and Timesys Factory. Now you can access the industry's best practices for security of embedded open source systems with our TRST Device Security Solutions, enabling you to:

- **Secure by Design** — Implement security best practices in product design, including over-the-air (OTA) updates, secure boot, encrypting data, authenticating users and servers, and using trusted execution environments to keep confidential data and algorithms private.
- **Stay Secure** — Maintain the target security posture over time with vulnerability monitoring and patching services that focus on only the exploits that are relative to specific device configurations.

Timesys has 20+ years experience with embedded system development and lifecycle management. Timesys' broad portfolio of products and services and embedded expertise are used by 1000+ customers to develop leading products and applications across a variety of industries including medical, industrial, networking, aerospace, and consumer.

Timesys TRST Device Security Solutions:
TRST Secure by Design + TRST Stay Secure = Your best defense against security threats

Cradle-to-grave security for the entire device lifecycle



Timesys TRST Device Security Solutions offer a complete end-to-end device security solution that enables you to address security early in the design of your products and more efficiently manage and maintain your device's security posture.

No matter what stage your product development is in, you can rely on Timesys TRST Device Security Solutions to help you bring open source embedded products to market that are secure by design and stay secure throughout the product lifecycle.

- **Reduce time-to-market delays** — Through our TRST Secure by Design services, security is baked in at the outset of your development, enabling you to cut the time, rework, and cost overruns that often come with deploying security too late in design.
- **Minimize the chance of your software being compromised** — Our Timesys TRST Stay Secure offering helps you to cut through the vulnerability storm and identify, analyze and respond to known security issues in the quickest time possible.
- **Establish and maintain the strongest security posture for your embedded systems** — Our Timesys TRST Device Security Solutions offering is easily adaptable, so you can tailor a solution that best fits your unique security requirements.

TRST Timesys to help you with your product security

When you engage with Timesys, you can rely on our expertise to implement security into your product design. We've worked with hundreds of boards, on thousands of projects and with numerous build systems including: Yocto Project, Timesys Factory, Buildroot, PetaLinux, and LTIB. Our years of experience have enabled us to provide you with a solution that delivers security best practices in the most cost-efficient way possible. And with our products and tools, you can significantly reduce the time and costs associated with maintaining software security — by up to 60%.

Timesys TRST Device Security Solutions

TRST Secure by Design: Implement Device Security During Development

Secure Boot/Chain of Trust
Ensure your device is not running tampered software by verifying its authenticity before execution. Our secure boot/chain of trust service helps you establish software authenticity all the way from the bootloader to user applications.

Device Encryption and Secure Key Storage
You can protect IP and sensitive user information by encrypting data/software. Our services help you encrypt data/software and also protect the key used for encryption. Additionally, our services can help you set up a hardware/software-isolated environment for running software that handles confidential data.

OTA Software Updates
Our security services can help you determine how to update/deploy software securely and deny unauthorized software installs.

Security Audit
By performing a risk analysis, our audit services can help you determine what potential threats your system might encounter and what should be secured.

Hardening
Our hardening service focuses on system configurations needed to reduce your product's attack surface.

TRST Stay Secure: Manage Vulnerabilities

Timesys Vigiles — Real-time Monitoring for More Secure Products
Timesys Vigiles security monitoring and notification service eliminates the time spent monitoring CVEs and assessing their risks.

With Vigiles update management service, applying updates and security patches into your software is easy — and you remain in control of what gets updated.

Timesys BSP Lifecycle Maintenance
The Timesys BSP Lifecycle Maintenance and Timesys TRST teams have the expertise to maintain the security of your BSP, on your custom hardware, allowing your team to focus on improving products to expand your customer base.

To learn more about Timesys TRST Device Security Solutions for devices based on embedded OSS, email us at **sales@timesys.com** or call us at **1.866.392.4897** (toll-free) or **+1.412.232.3250** to schedule a complimentary, no-obligation consultation.

Disclaimer: *Security is an ongoing process and is not foolproof. Timesys' security offering provides assistance with minimizing known vulnerabilities based on known issues, but doesn't have any warranty.*

timesys®

Headquarters / North America Office:
1905 Boulevard of the Allies,
Pittsburgh, PA 15219 UNITED STATES
1.866.392.4897
sales@timesys.com

EMEA Office:
ul. Palmowa 1A,
62-081 Chyby POLAND
+48.53.733.8080
emea@timesys.com

APAC Office:
3rd Floor, Jaag Homes, Achyutha Square,
No. 3, MTH Road, Villivakkam,
Chennai, Tamil Nadu – 600 049 INDIA
+91.0124.4299897
apac@timesys.com