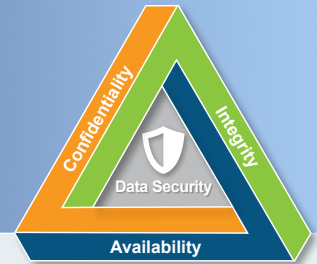







Timesys Device Security Solutions

No matter where you are in your security journey, Timesys can help.

Whether you're new to cybersecurity or you already have your list of security requirements and standards, we offer a complete, end-to-end Linux & RTOS (FreeRTOS, Zephyr, and more) security solution to get your product to market faster and with stronger security.








Timesys Customizable Security Solutions: How It Works

-  Build and refine your security requirement list
-  Train your team on security best practices (optional)
-  Select best-suited technology options for your requirements
-  Implement solution based on your budget and your timeline
-  Assist with integration of the security solution into your manufacturing process



Already know your exact requirements, and just need someone to take the security and/or maintenance work off your plate? Jump right to our **30-minute security consultation**, where we'll go through your requirements and create your custom security roadmap.

With more than 20 years of experience in embedded systems and 1000+ projects completed, Timesys is an industry leader in open source software and security. Timesys offers complete end-to-end device security solutions including:

VigiShield 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.

Stay Secure: Maintain Product While In the Field

-  **Timesys Vigiles — Vulnerability Monitoring and Remediation**
The industry's first CVE monitoring, notification, and remediation tool optimized for embedded Linux. Vigiles continuously scans thousands of vulnerabilities curated by Timesys, filters CVEs based on your actual product configurations, and monitors fixes across all of your product branches. Get 85% fewer CVEs to analyze and 95% fewer false positives.
-  **Timesys Linux OS and BSP Maintenance — Long-term Security Updates & Maintenance for Embedded Systems**
Get up-to-date software with security fixes for the full product lifecycle. Includes routine updates on your schedule (minor Kernel version upgrade; security patches/updates/backports); vulnerability alerts, monitoring, and management; and an emergency release if needed; all for 50%+ cost reduction vs DIY.

Sign up for a free 30-minute security consultation to create your custom security plan at www.timesys.com/solutions/schedule-consultation/

Timesys OS technologies help you meet security standards

Every industry has a slew of compliance requirements and security standards: medical companies follow FDA Premarket and Postmarket Security Guidance, IEC 62304, and NEMA Requirements; automotive companies follow ISO/SAE 21434 and European WP.29 Compliance; IoT companies follow ETSI EN 303 645 – Cyber Security for Consumer Internet of Things and NIST 8259; connected device companies follow UL 2900-1; industrial companies follow IEC 62443 and ISA99; and the list goes on.

Timesys Security Solutions simplify meeting these requirements across industries:

VIGISHIELD SECURE BY DESIGN		
Software integrity, authenticity	⇒	Secure boot, chain of trust
Data confidentiality	⇒	Encrypted storage
Software update	⇒	Secure OTA
Secure communication	⇒	Secure protocols & ciphers
Securely store sensitive security parameters	⇒	Trusted OS (OP-TEE)
Minimize attack surface, Secure Interfaces	⇒	Hardening - Hardware ports locked - Kernel protection features - Disable unwanted services
Software integrity	⇒	Manufacturing Protection
Prevent unauthorized use Resilient to outages Detect cybersecurity events Contain cybersecurity event Contain cybersecurity event	⇒ ⇒ ⇒ ⇒ ⇒	Runtime Protection - Access control - Firewall - Audit logs - Key revocation - Tamper protect
VIGILES VULNERABILITY MONITORING AND REMEDIATION		
CVE monitoring, triage, and remediation for 3rd party software	⇒	Vigiles vulnerability monitoring
LINUX OS AND BSP MAINTENANCE		
Up to date software with security fixes	⇒	Linux OS and BSP Maintenance

“We chose to partner with Timesys in the development of our new portfolio of medical devices to ensure that they stay secure throughout their life-cycle. Our customers globally face strict information security requirements combined with a heightened threat environment when deploying these devices within their enterprise. Our secure design methodology, partnership with Timesys, and operational policies allow our customers to be confident in choosing and deploying these devices in their healthcare practice.”

– Roshy J. Francis, Chief Technology Officer of Life Care Solutions for GE Healthcare

Learn more at www.timesys.com/industries/.

Generate an accurate Software Bill of Materials (SBOM) with Vigiles

An SBOM is essential to understanding what you’re shipping, and to maintaining the security of your device. Vigiles supports all major Linux build system integrations including Yocto, Buildroot, PetaLinux, Wind River Linux, PTXdist, OpenWrt, and Timesys Factory for more accurate SBOM generation.

Try out Vigiles Prime free for 30 days to generate your SBOM, and see your vulnerability report:
www.timesys.com/register-prime/



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