

Wind River Linux Secure

Companies charged with creating complex, connected, secure, and mission-critical solutions are looking to open source and open standards software to leverage rapid growth in the ecosystem and provide the functionality, flexibility, and total cost of ownership advantages these solutions deliver. To address this need, Wind River has created a commercial-off-the-shelf (COTS) embedded Linux platform designed for highly connected solutions based on open standards.

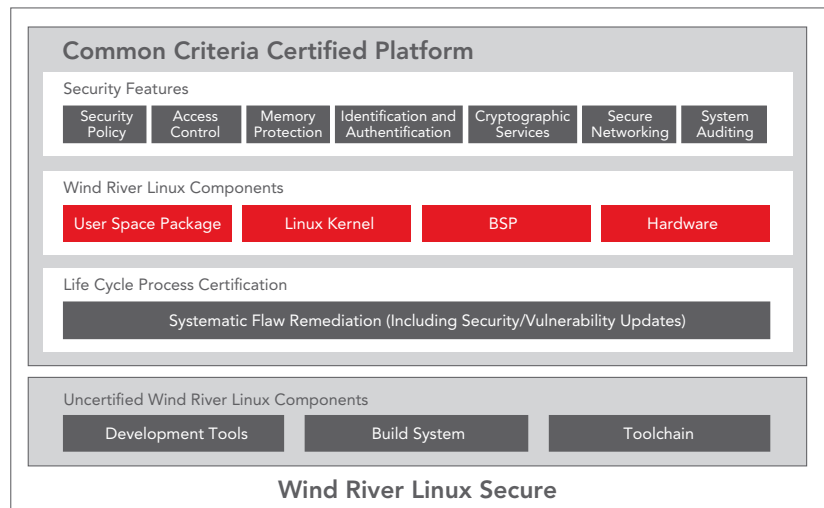
Wind River Linux Secure is a Common Criteria security-certified, commercial-grade embedded Linux development and run-time platform for use where assured security is a project requirement. Wind River Linux Secure is built on Wind River's industry-leading embedded Linux platform and provides a flexible development environment that enables companies to develop, test, and support both COTS and highly customized devices quickly and cost effectively.

Wind River Linux Secure is based on the stable Linux 2.627 kernel and GCC 4.3.2 compiler and is certified to Common Criteria Evaluation Assurance Level 4+ (EAL4+) and Federal Information Processing Standard (FIPS) 140-2 certification. This certified platform also includes support for multiple hardware architectures, including ARM, Freescale, and Intel, enabling Linux system designers to deploy on the platform that best balances power and performance.

Wind River Linux Secure is the first commercial embedded Linux platform to achieve Common Criteria EAL4+ certification using the new and more rigorous General Purpose Operating System Protection Profile (GP-OSPP). The FIPS 140-2 certified cryptography includes a comprehensive set of cryptographic algorithms to assure information security and integrity in connected settings. The platform also provides a pre-configured system profile that meets Common Criteria-certified requirements to fast-track your development and security evaluation process. By identifying, assembling, and integrating hundreds of commonly used packages, Wind River Linux Secure saves you weeks of specialized labor, so resources can be focused on creating highly optimized devices.

Wind River Linux Secure contains the following security features:

- **Security policy:** Wind River Linux Secure uses the National Security Agency (NSA)-developed Security Enhanced Linux (SELinux) technology and an independent reference policy as the basis for security policy definition and enforcement. The foundation for the security policy is achieved by type enforcement and role-based access control, which ensure robust data integrity and confidentiality of user applications.



Wind River Linux Secure features, conforming to the specification of the General Purpose Operating System Protection Profile (GP-OSPP)

The security policy is further enhanced by controlling all network communications and applying multilevel security (MLS) and multi-category security (MCS) capabilities in the system.

- **Access control:** Both Discretionary Access Control (DAC) and Mandatory Access Control (MAC) security mechanisms are supported, which provides the ability to configure and optimize access privileges for user applications and system objects (files, directories, and sockets). MAC enforces MLS based on the Bell-LaPadula Model.
- **Memory protection:** The compile-time stack protection and run-time write-or-execute memory segmentation eliminate common security issues associated with memory leaks and programming errors, improving buffer management and making applications more secure. grsecurity enables role-based access control (RBAC) capabilities that can generate least-privilege policies for your entire system. PaX is also included and provides address space layout randomization (ASLR), enhanced stack protection, isolation of untrusted applications, and prevention of many types of security vulnerabilities, including buffer overflows.
- **Identification and authentication:** Password-based authentication is enforced for any access to Wind River Linux Secure. The identification and authentication mechanism is based on the Linux Pluggable Authentication Module, which is configured to enforce proper password quality and ensure a locking of accounts in case of failed login attempts.

- **Cryptographic services:** FIPS 140-certified Network Security Services (NSS) provides a set of libraries designed to support cross-platform development of security-enabled client and server applications. Validated algorithms include Triple DES, AES, DSA, ECDSA, SHS, RSA, DRBG, and HMAC. NSS is offered to users via the Wind River Cryptographic Framework, which provides separation between userspace and the crypto layer, protecting the NSS libraries while facilitating user access to initialized cipher mechanisms.
- **Secure networking:** Wind River Linux Secure offers remote access via OpenSSH to protect network communication against wiretapping or eavesdropping. It also includes labeled networking through the security policy. IPsec technologies such as Kerberos, racoon, OpenSSL, and GNU Transport Layer Security (TLS) are all integrated, validated Linux Secure components available to system developer.
- **System auditing:** Wind River Linux Secure provides reliable and effective system-level auditing of all security-related events and actions based on the Linux Audit Framework. It also includes a variety of additional tools to help both the system administrator and users to monitor the system and their own applications. A fine-grained configuration of the audit framework allows users to choose the system calls or events they want to log, streamlining data management and helping to optimize system performance.
- **Systematic flaw remediation:** Wind River Linux Secure is certified for its security response methodology as an additional requirement. Systematic flaw remediation levels 1–3 establish increasingly rigorous processes for identifying, documenting, communicating, and correcting system security flaws in a target of evaluation (TOE), up to and including the assignment of dedicated support engineering resources to ensure timely responses.

Multi-architecture Platform Support

Wind River Linux Secure is certified on selected platforms of Intel Architecture, PowerPC, and ARM. Wind River Linux Secure can be deployed securely on COTS and custom hardware from multiple vendors including Freescale, Intel, and Texas Instruments, reducing the overall cost of development and certification. Our flexible design makes it possible to enable new boards and facilitate incremental certifications to minimize the total cost of ownership.

Open Source Code

Wind River Linux Secure is built on thoroughly tested and fully supported open source code that includes complete traceability from binaries to source code. This enables the exact definition of the lineage of your product from its open source origins through any modifications from the addition of patches, packages, or proprietary code. This traceability is a key requirement when developing secure systems based on open source software.

Optimized Build System

From easy installation and modification of the kernel and root file system to the cross-compiling unique to embedded development, our open, intuitive build system provides a methodology for saving time, achieving clarity, and managing, storing, and sharing parts of the development system among developers or teams.

Based on the concept of “layers,” the Wind River Linux Distribution Assembly Tool (LDAT) simplifies every step of the Linux development process, from reviewing and reversing changes to quickly addressing performance issues, bugs, or defects.

Tools

Wind River Linux Secure comes with Wind River Workbench, an Eclipse-based development suite. Workbench provides deep capability across the entire development life cycle and hosts a number of powerful plug-ins for analysis and on-chip debugging. For developers who prefer command-line programming, Wind River Linux provides a rich set of command-line tools.

Carrier Grade Linux

Wind River Linux Secure supports Carrier Grade Linux (CGL) standards for high availability networking applications. Wind River Linux Secure is open source and open standards compliant and comes with extensive license documentation to help ensure license compliance for your shipped device software. Wind River Linux Secure meets U.S. government export regulations.

License Management

Wind River performs thorough legal reviews of the compilation and documentation of the General Public License (GPL) and other licenses that control each major release of Wind River Linux Secure. Combining human legal expertise and proprietary automated tools, Wind River examines each open source package that comes into the product to identify and resolve potential IP issues before the product is released. Customers receive prodigious documentation to assist them in the protection and control of their intellectual property.

Reduced Risk

Wind River’s extensively tested and validated embedded development platform significantly reduces the risks commonly associated with open source software. Wind River’s global support and services teams stand behind your device throughout its life cycle. Choosing to develop on an already certified platform mitigates both the risks and expenses of developing these devices from scratch.