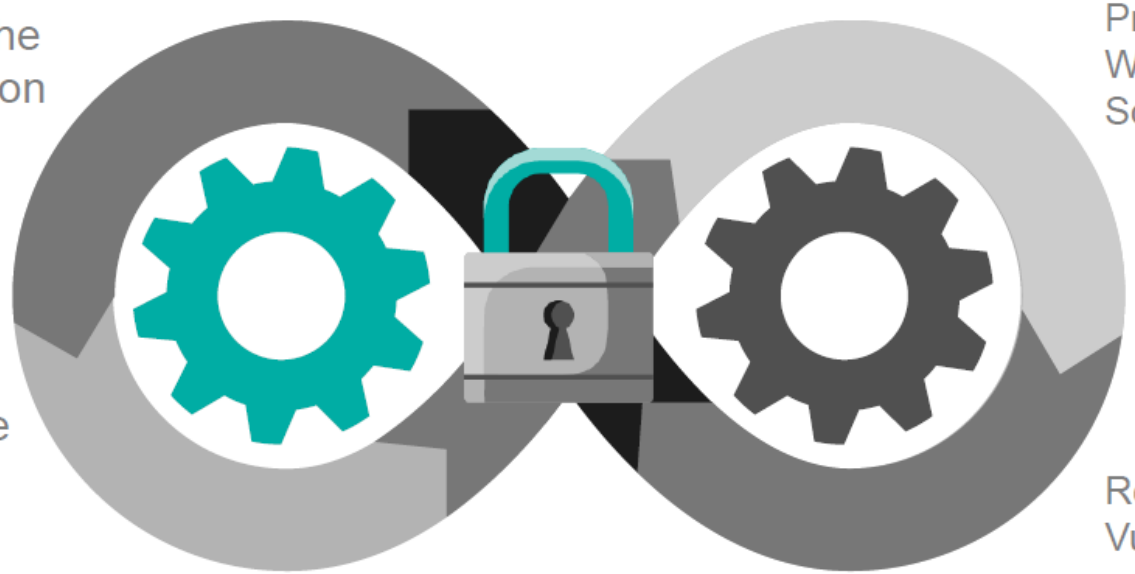
WNDRVR

박 주동 (Judong.park@windriver.com, 010-9530-3022)

SECURE DEVELOPMENT LIFECYCLE

SECURITY-CENTRIC DEVELOPMENT IS NOW A FOUNDATIONAL IMPERATIVE



Source Develop Deploy Service End-Of-Life

Executive Order 14028 on "Improving the Nation's Cybersecurity"

NIST SP 800-218 "Secure Software Development Framework (SSDF)"

CISA "Secure Software Development Attestation Form"

REQUIRED NOW FOR USG AGENCY PROCUREMENT!

WNDRVR

SECURITY STANDARDS

Industry & Regulation

- SSLC, DSS
- CIS-16
- 14028
- CRA Act
- And More…
- 62443
- 21434
- 24089
- Security
- 81001

Empowering

Foundation

- Secure Enterprise: 27001/2
- Secure Products: SP 800-53
- Secure Development: SP 800-218

Product Compliance

WNDRVR

INCREASED CONCERNS WITH SECURITY OF DEVICES AND DATA

CHALLENGES

- Stronger regulatory landscape covering organizations, processes, production, and operation

WIND RIVER'S APPROACH

- ISO 27001: Information Security Management
- NIST 800-218: Secure Software Development Framework
- NIST 800-171: Protecting CUI in Nonfederal Systems and Orgs
- ISO/IEC 30111: Vulnerability Handling Processes
- ISO/IEC 29147: Vulnerability Disclosure
- SBOM and active CVE for all products in the portfolio
- Wind River is a CVE Numbering Authority (CNA)

Wind River Secure Development Lifecycle

Wind River supports a secure development lifecycle (SDL) across our products that is enforced by policy and implemented with standards, processes, and procedures. The SDL is aligned directly with the NIST 800-218 Standard and its principles: prepare the organization, protect the software, produce well-secured software, and respond to vulnerabilities.

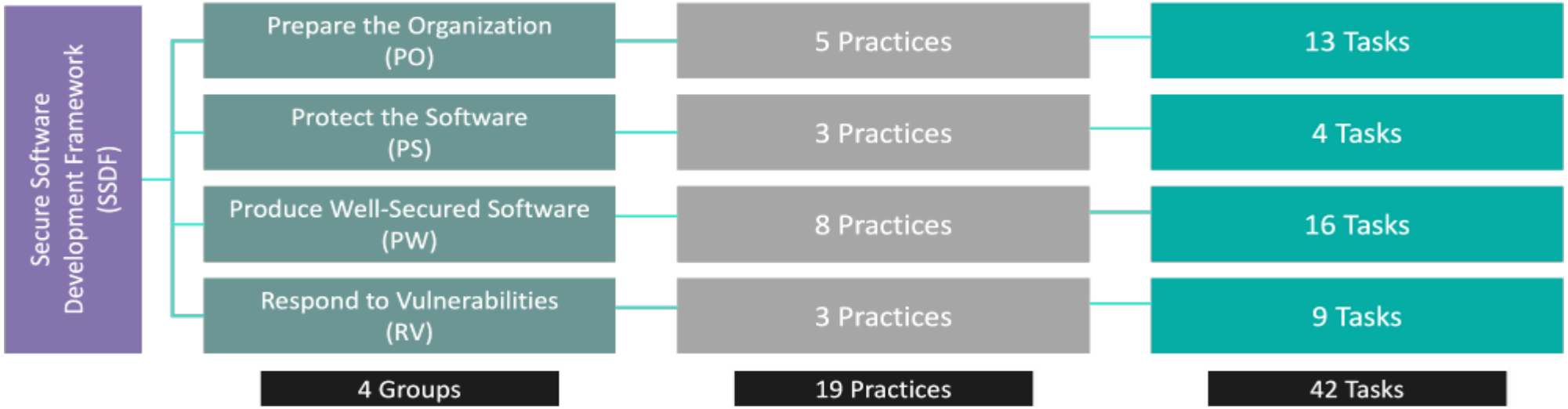
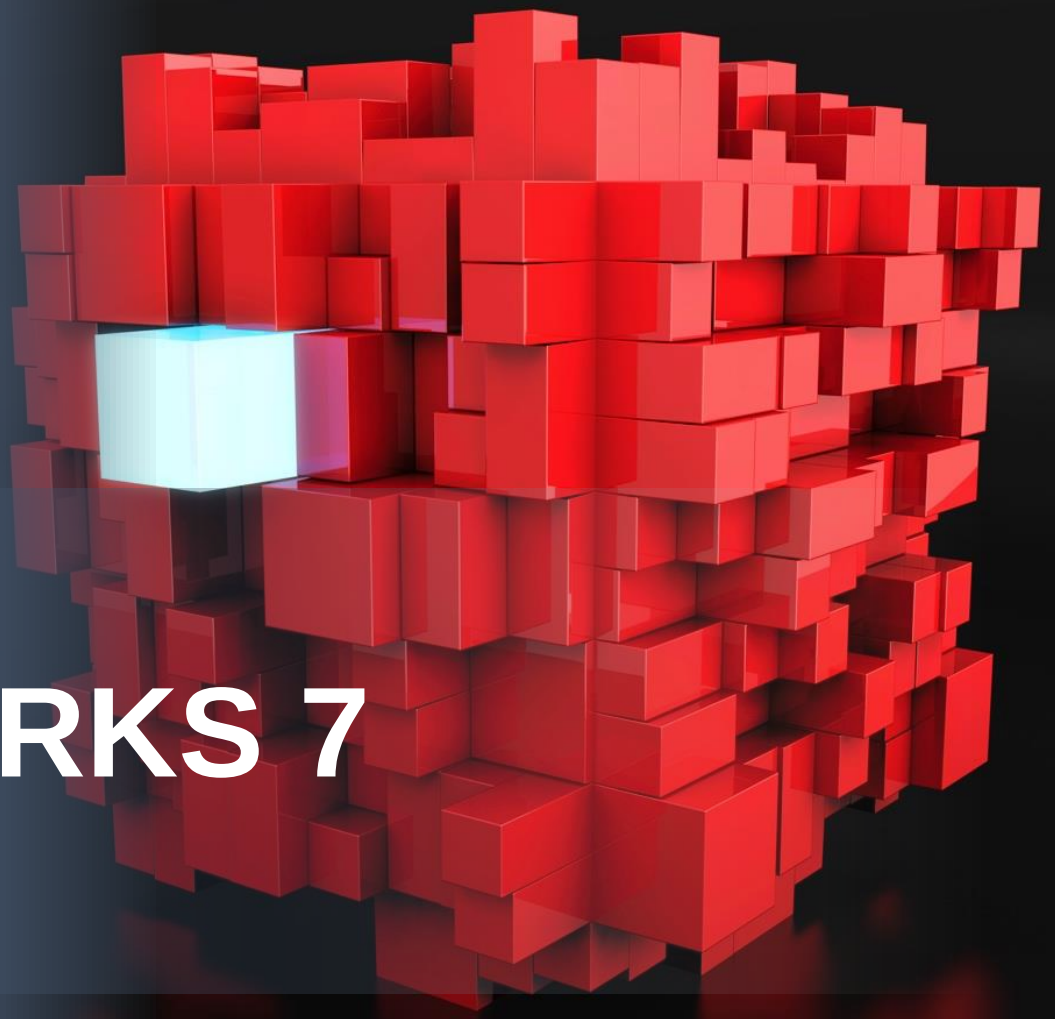


Figure 1. The Secure Software Development Framework (SSDF)

The SDL is tightly integrated with our product development lifecycle (PDLC), and it is deployed across our enterprise and assessed regularly for conformance and assurance to customers of our trusted products.

https://www.windriver.com/security/secure-development-lifecycle

SECURITY IN VXWORKS 7



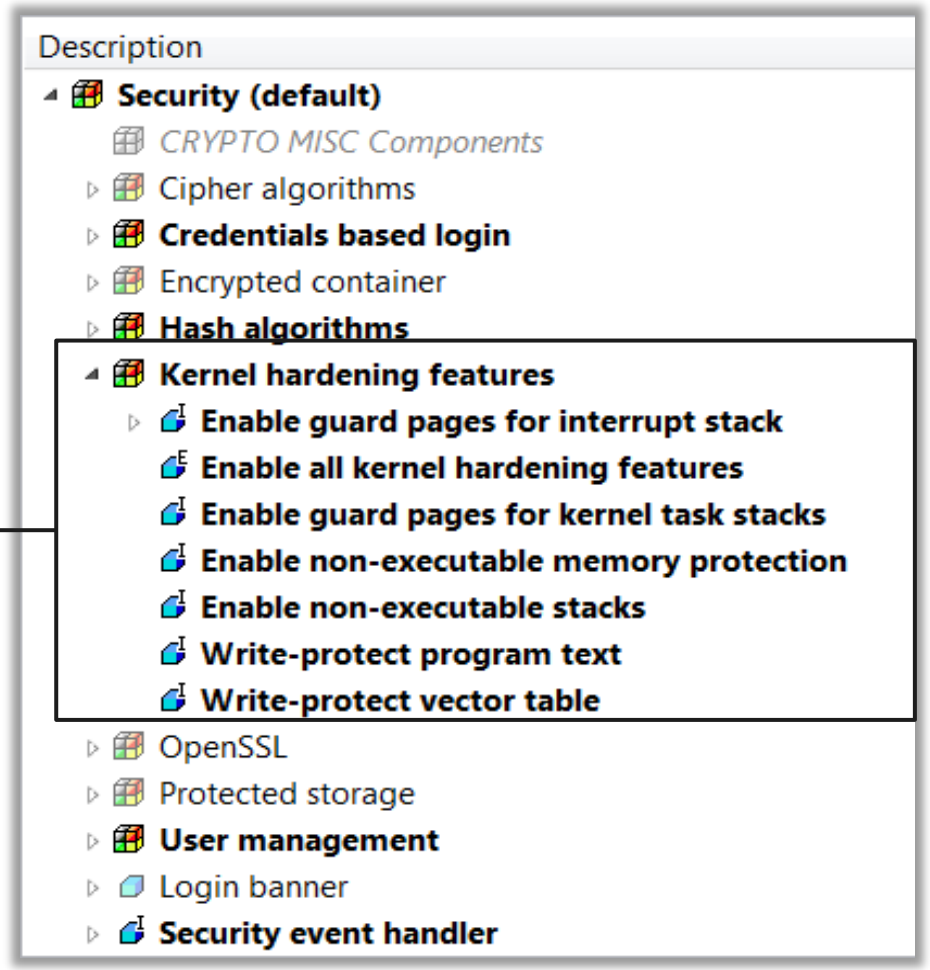
SECURITY IN DEVELOPMENT

- All code submitted must be reviewed
  - Reviews tracked with Code Collaborator
  - git enables full visibility of who does what
- All code scanned with Coverity
  - No warnings allowed
  - Common Weakness Enumeration (CWE)
  - CERT secure coding standard
  - SAMATE test suite
- Testing: CVE checker, Nessus, fuzz and Achilles

VXWORKS 7 SECURITY

HIGH LEVEL FUNCTIONALITY (CONT'D)

- Kernel hardening
  - Pages guards
- Access control
  - System calls
  - Kernel objects
  - Kernel resources
- Time partitioning
  - DoS protection



VXWORKS 7 SECURITY

HIGH LEVEL FUNCTIONALITY (CONT'D)

- Secure boot
- Secure Loader
- Digitally signed binaries
- Advanced user management
- Encrypted containers and disks
  (AES256, VeraCrypt compatible container
  XEX-AES256)
- TPM support
- ARM TrustZone (OP-TEE)
- Security events handler
- Achilles Level 2 certification
- Support for AD/LDAP
- Non-eXecutable pages
- SSH Client
- Extensions to IKE (SCEP and GDOI)
- …

VXWORKS 7 SECURITY

HIGH LEVEL FUNCTIONALITY

- Cryptography libraries
- Flexible application whitelisting
- Secure Sockets Layer (SSL)
- Secure Shell (SSH) server
- Internet Protocol Security (IPSec) and Internet and Key Exchange (IKE)
- Firewall
- RADIUS and Diameter

CYBERSECURITY STANDARDS WIND RIVER SUPPORT

ISA/IEC62443 **Industrial Automation & Control Systems (IACS) Cybersecurity**

- Defines requirements and processes for implementing and maintaining electronically secure systems.
- Sets best practices for security and a way to assess security performance.
- Sets cybersecurity benchmarks in IACS sectors, including **automation, medical devices, transportation,** and **aerospace/defense**.

- Achilles Certification is recognized as the industry standard for both verifying network robustness and validating security best practices.
- Achilles Level 2 certification verifies the security, reliability and robustness of a device's implementation of OSI layers 2-4 (data link, network, transport), via detailed tests, including denial of service tests at high link rates and numerous pass/fail requirements.

VxWorks Edition is GE Digital® Achilles Level II–certified for compliance with IEC 62443 part 4-2.

WNDRVR

EDGE to CLOUD (CI/CD – DevSecOps, Container)

Studio

DEVELOPER

Fast and secure development and testing of software in the cloud

Wind River Studio Gallery
A gallery that allows developers to select their preferred 3P tools for development

Wind River Studio Pipelines
Development pipeline customizable for development teams

Wind River Studio Test Automation
Framework to automate testing during software development in Studio

Wind River Studio Virtual Lab
Tool to simulate hardware and provide cloud-access to physical test hardware

Wind River Studio Digital Feedback Loop
Data pipeline to send edge device data (hardware and software) to the cloud

Wind River Studio Over-the-Air Updates
Open and flexible, over-the-air software update tools

OPERATOR

Edge software orchestrated on the cloud and edge data sent to the cloud for analytics

Wind River Studio Cloud Platform
Integrated platform for deployment and management of edge software

Wind River Studio Conductor
Monitors and orchestrates containers across edge devices

Wind River Studio Analytics
Platform to conduct analytics on collected edge device data

Edge

EDGE SOFTWARE

Seamless and secure deployment of cloud-native software architecture on the edge

VxWorks
A real-time operating system that ensures applications run within critically defined time constraints; VxWorks is the only RTOS that supports containers

Wind River Helix Virtualization Platform
A safety certifiable, multi-core, multi-OS virtualization platform (hypervisor) that supports mixed levels of criticality

Wind River Linux
Leading embedded Linux as the largest commercial contributor to Yocto Project

SERVICES

Custom Development | Managed Services | Safety and Certification | Lifecycle Management | Education | Customer Support

WNDRVR

EDGE to CLOUD (CI/CD – DevSecOps, Container)

VXWORKS

Industry-leading real-time operating system (RTOS) for modern high-performance, reliable, secure, robust, safety-certified mission-critical systems.

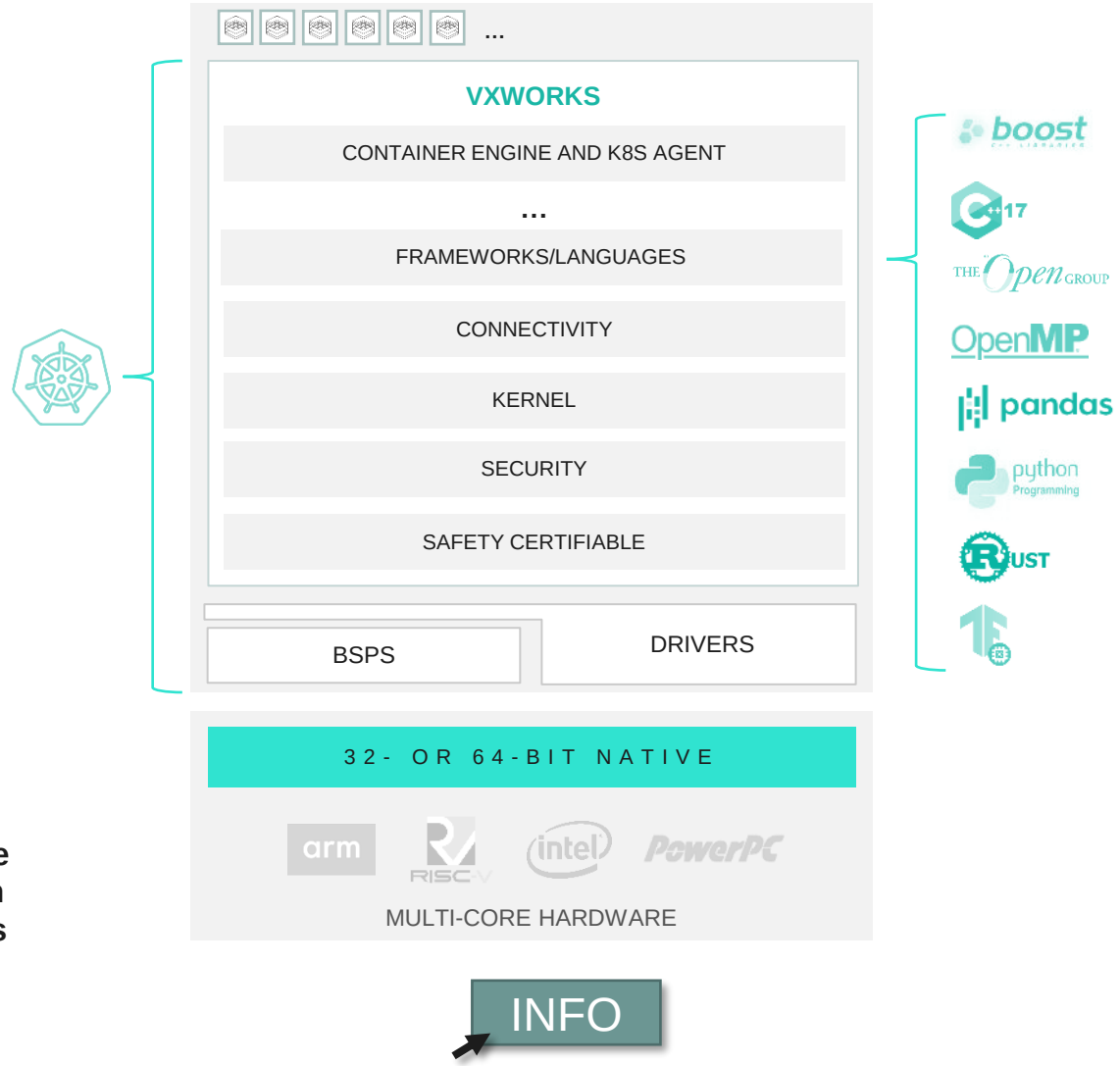
- Only RTOS with OCI container and orchestration support
- Ideal for high-performance AI/ML at the edge

RTOS of choice for automotive, industrial, medical and aerospace

Supports major processors, modern software frameworks

Available RTOS certification evidence to reduce cert costs

Used in more than 2 billion edge devices



WNDRVR

KEVLAR Linux
EMBEDDED SECURITY

A SECURITY TRANSFORMATION IS UNDERWAY

MANUFACTURERS MUST TAKE OWNERSHIP OF SECURITY OUTCOMES FOR CUSTOMERS

Paramount to this transformation is the shift in responsibility for security; device manufacturers will no longer be able to avoid integrating security solutions.

SECURITY SHOULD NOT BE A PAID ADD-ON

Paying more for security is an expiring paradigm; customers should be able to have confidence the baseline product they purchase is secure.

SECURE DEVELOPMENT PRACTICES AND INFRUSTRUCTURES ARE CRITICAL

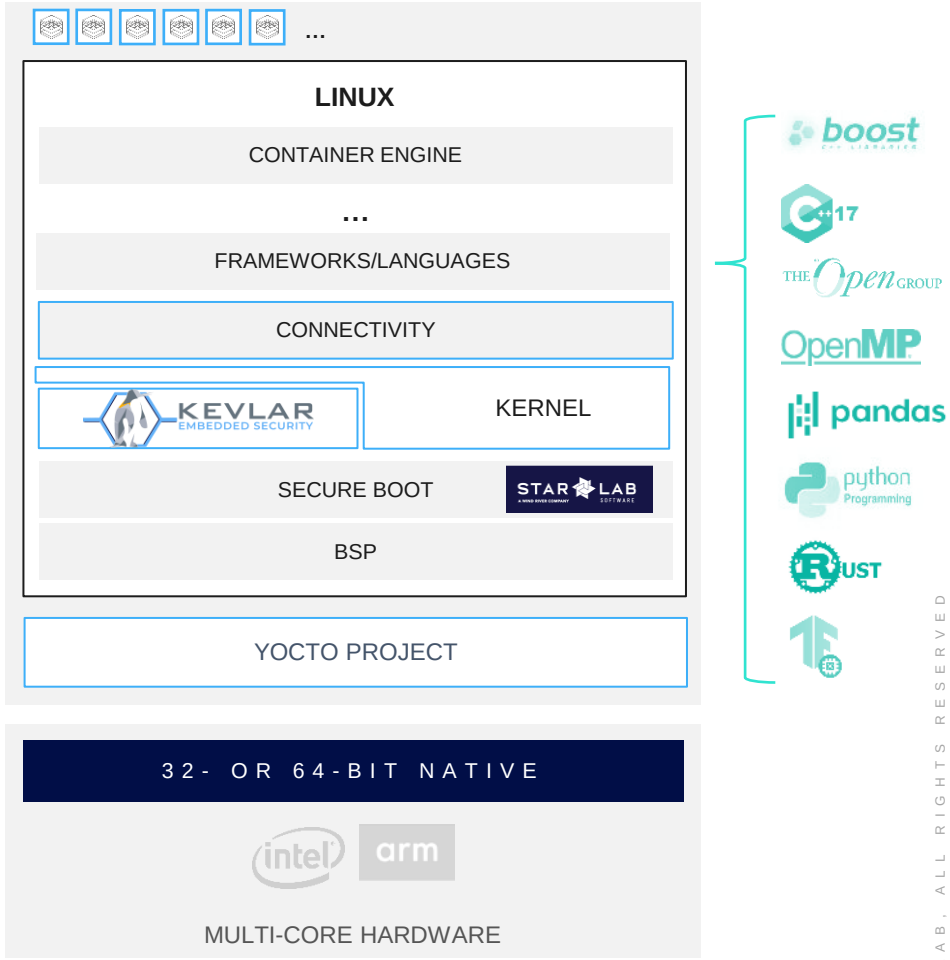
Many vulnerabilities can be discovered and corrected before deployment using secure development lifecycle practices; these same practices can identify insider threat activity as well.

PROGRAMMING LANGUAGES MATTER

Programming languages have evolved to address poor or careless development practices—they should be used!

KEVLAR EMBEDDED SECURITY

- **Kevlar Embedded Security** is a set of Yocto layers for embedded Linux that protect critical data and executables, both at rest and during runtime
- Addresses three important areas:
  - **Cyber Resiliency** capabilities used to build a defense in depth strategy tailored to specific threat models and performance requirements
  - **Data Protections** defeat efforts to access or capture critical data
  - **DevOps Integrations** makes building in security frictionless, simple, correct, and testable



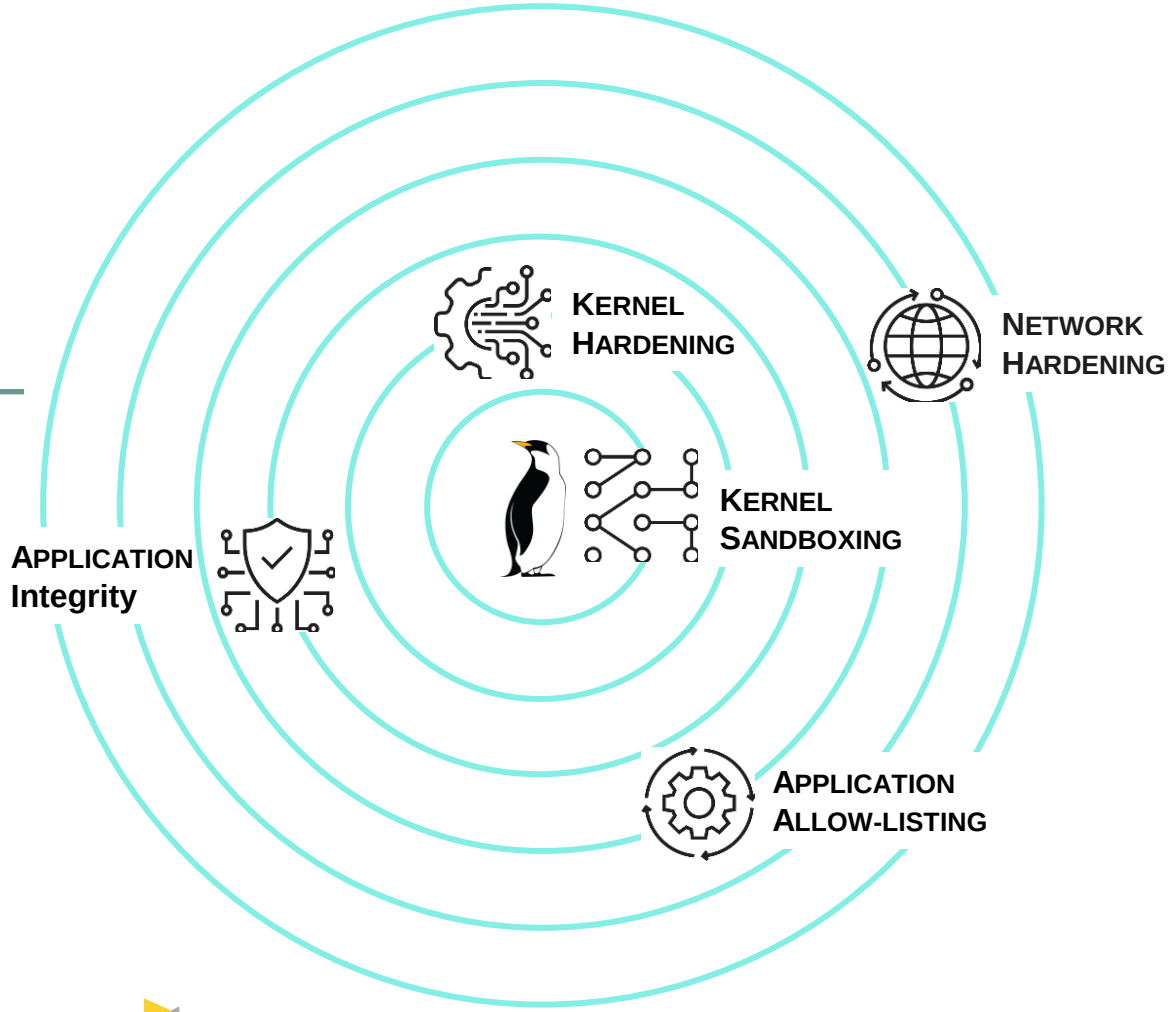
Exportable commercial product for Cyber Resilience and Data Protection

STAR LAB
A WIND RIVER COMPANY
SOFTWARE

ASSUME AN ATTACKER GAINS ACCESS

Cyber Resiliency

Kevlar Embedded Security consists of individual security capabilities that can be used to build a defense in depth strategy



Using a layered approach improves resiliency when an attacker does gain access

Improving your security posture even slightly will cause many attackers to move to easier targets

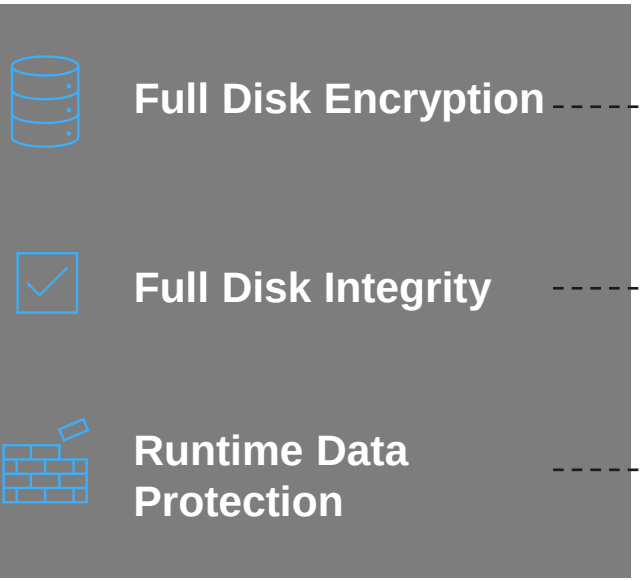
STAR LAB SOFTWARE
A WIND RIVER COMPANY

DATA PROTECTION FOR THE EDGE

A SOUND SECURITY APPROACH REQUIRES PROTECTING DATA FROM TAMPER AND THEFT

STAR LAB DATA PROTECTIONS HAVE SIGNIFICANT ADVANTAGES OVER OTHER SOLUTIONS

BUILD-IN SECURITY

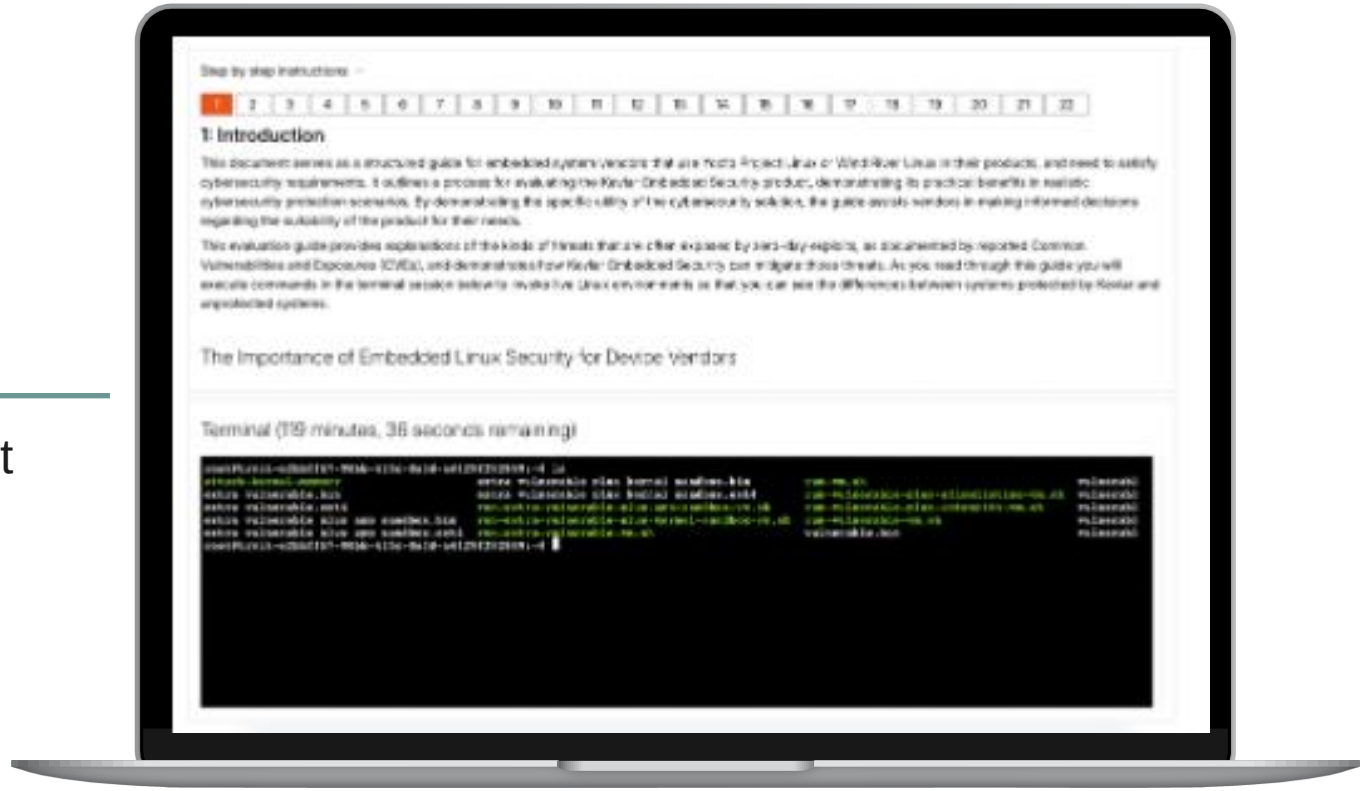


	IMPORTANCE	ADVANTAGES
Full Disk Encryption	Ensure the confidentiality of critical or important applications and data when a device is powered off	Self-encrypting - Automates the generation of a unique per-device key and enrolls the data with a TPM or Arm TrustZone
Full Disk Integrity	Detect unauthorized modifications to data, configurations, or applications	Built-in integrity – Combines integrity verification and FDE into one easy to integrate solution
Runtime Data Protection	Frustrate unauthorized efforts to access, read, or capture critical or proprietary data during runtime	Container-ready – Configures a barrier around critical containers limiting what can inspect the contents of containers

STAR LAB SOFTWARE
A WIND RIVER COMPANY

CLOUD-NATIVE EVALUATION

- Customers interact with evaluation environment hosted in the cloud
- Includes documentation for users to follow that provides step-by-step instructions
- Evals have a time limit in minutes



STAR LAB SOFTWARE
A WIND RIVER COMPANY

WNDRVR