

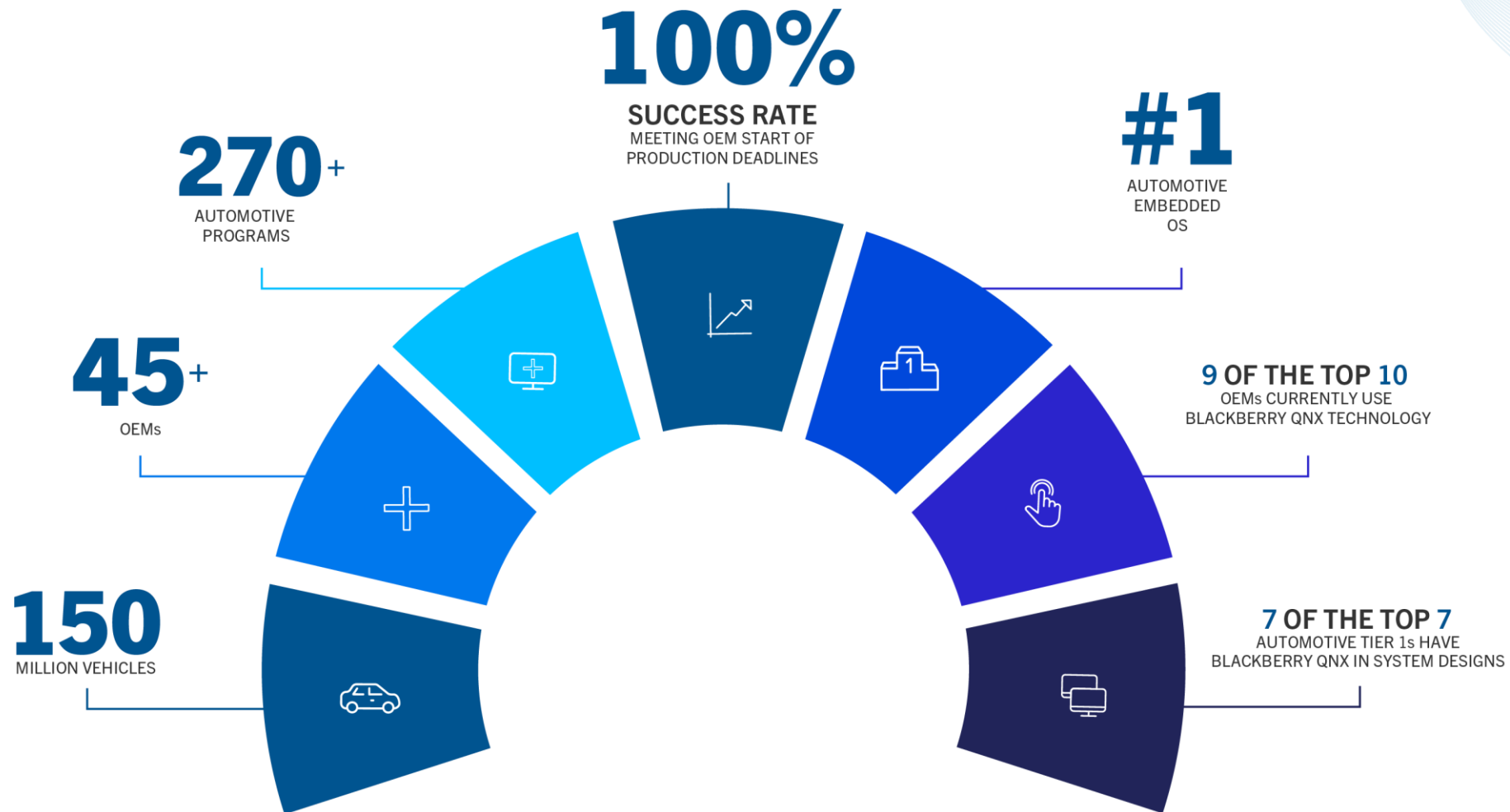


Secure Automotive SW Supply Chain









Nov. 2022

고정직 / Field Application Engineer

BlackBerry QNX: Proven Track Record

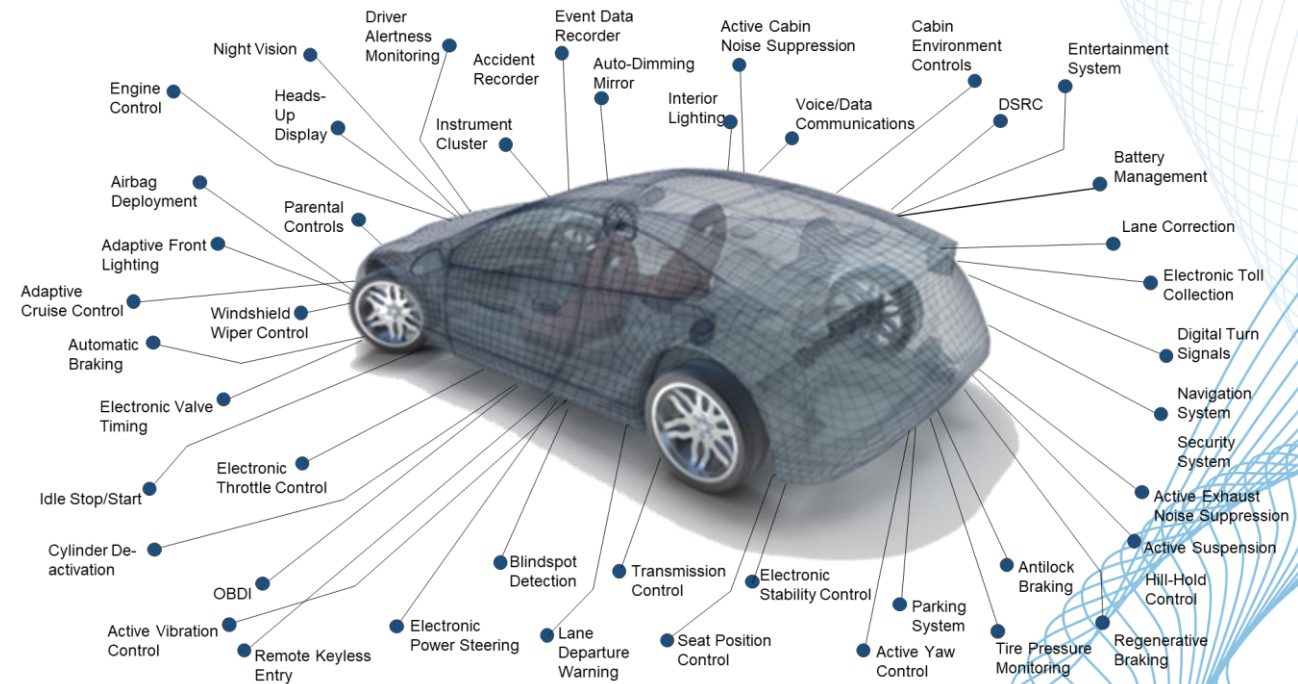
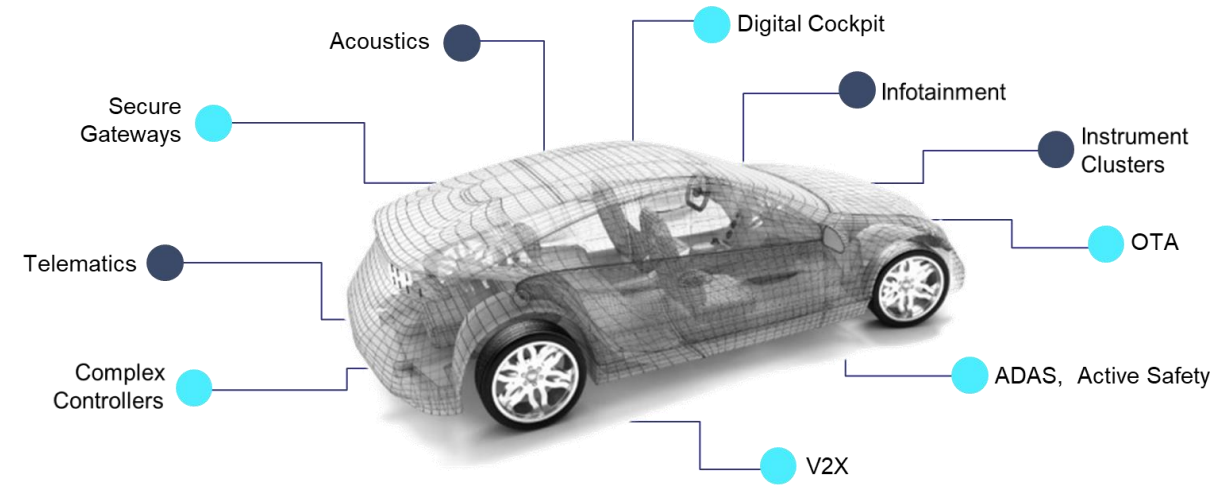


BlackBerry QNX Product Portfolio - Investment and Innovation

Platform Enablement	ADAS & Automated Drive	Instrument Cluster	Acoustics Management Platform	Infotainment	Secure Credential Management System for V2X	Digital Cockpit Platform	Over-The-Air Software Update	Secure Gateway	Provisioning and Key Management
Middleware	QNX Screen Graphics	Multimedia, Speech Framework, CarPlay, AA	SOME/IP ROS2.x	SDK for Bluetooth Connectivity	Wireless Framework	Embedded Browser	SDK for Crypto and Security	Sensor Framework	Secure Encrypted Filesystem
Certified Foundations	Certified OS for Safety	Certified OS for Industrial	Certified OS for Medical	Certified Hypervisor	Certified Black Channel Comms	Certified C++ and Math System Libraries	Certified OS for Rail*	Certified Filesystem*	Certified Graphics Monitor
Virtualization	Hypervisor	Advanced Virtualization Frameworks							
Operating System and Tools	QNX Operating System	QNX Momentics IDE & Tools	WITTENSTEIN SAFERTOS Integration	AUTOSAR Adaptive Stack	BlackBerry Jarvis Binary Scanning Tool				
									
Professional Services	Porting Assessment	Architecture Assessment	Functional Safety Training	Functional Safety Consulting	Open Source Software Assessment	Software Security Assessment	Penetration Testing	OS & Tools Training	Custom Support Plans

Trend – Electronic Control Units (ECU) and Software

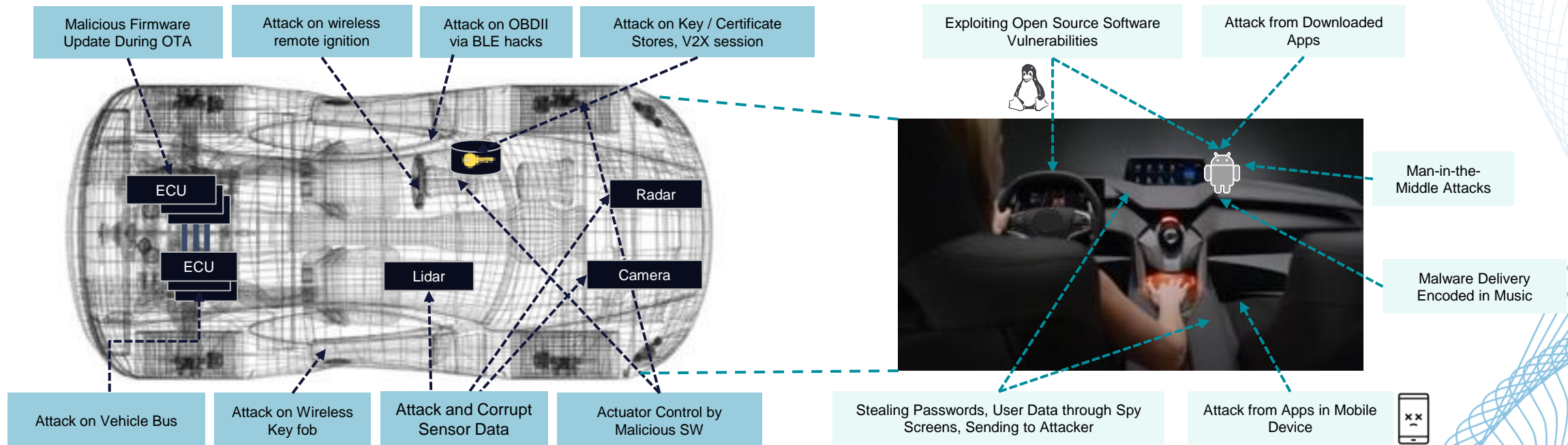
- Commoditization of hardware
- Emergence of software as a key differentiator, by 2030:
 - Electronics + Software = 50% of car BoM
 - Software = 30% of the overall car BoM
- Service-oriented business models will start taking shape
- Increased need for cybersecurity



Trend – Cybersecurity Risk Increasing with Connectivity/Complexity

Threat vectors throughout the vehicle

- Internet based attacks: 4G/5G
- Sensor attacks: GPS, Radar and other sensors
- Hardware attacks: OBDII port, USB, ECUs, etc.
- Nearfield wireless attacks: Bluetooth, key fobs, TPM, etc.



Trend – Winds of Changes – Security Standards and Regulations

- Several industries are leading security regulations, including automotive, aerospace and defense, medical and rail
- For the auto industry, in June 2020, UNECE's World Forum for Harmonization of Vehicle Regulations adopted two new regulations for cybersecurity. Compliance with the regulation will be required to achieve Type Approval before vehicles can be sold in the market
- Governments are taking an active role in demanding security from their suppliers



Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS



Jeep hackers at it again, this time taking control of steering and braking systems

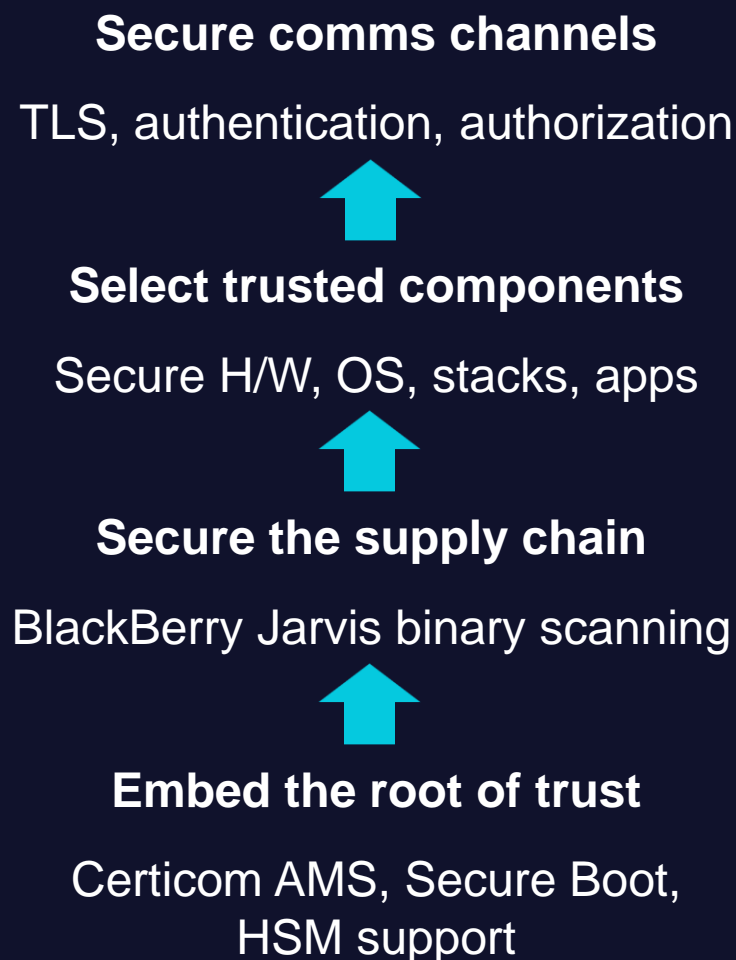
Source: *The Verge*, Aug 2, 2016



America Has to Make High-Tech Medicine Hack-Proof | Opinion

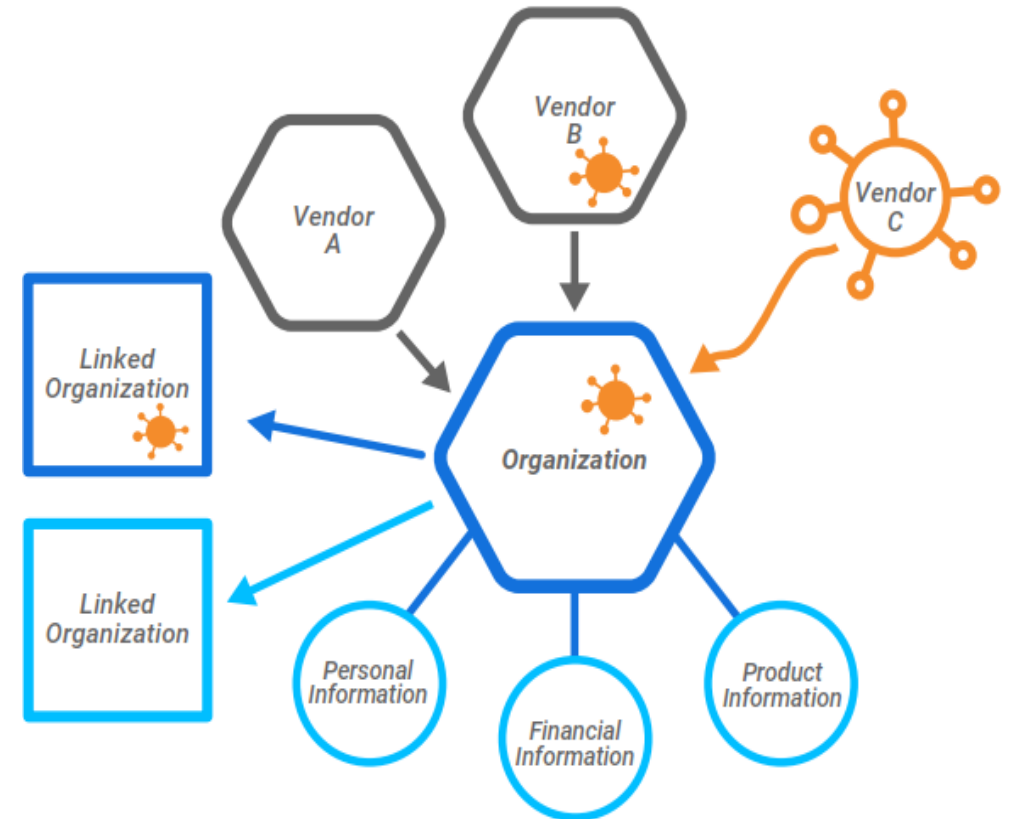
Source: *Newsweek*, May 26, 2021

The Complete Embedded Security Story



Supply Chain – What is Supply Chain

- A software supply chain is composed of the components, libraries, tools, and processes used to develop, build, and publish a software artifact.
- Auto industry has 3-5 levels in the supply chain
- The software supply chain has been increasingly used as an attack vector in recent years. Why?
 - a. Extensive attack surface by complex SW supply chain level
 - b. Once attackers are inside, all in SW supply chain they can access may be exploited



Topological view of a supply chain attack

Supply Chain – Recent SW Supply Chain Attacks

- Common techniques to execute software supply chain attacks^[1]
 - a. Hijacking updates
 - b. Undermining code signing
 - c. Compromising open-source code
- Some examples of historical software supply chain
 - a. **The NotPetya ransomware attacks in 2017.** Attackers compromised the Ukrainian tax software MEDoc and caused billions in damages to pharmaceutical giants.
 - b. **The SolarWinds breach in 2020.** The Orion IT Management and monitoring software was compromised and pushed out to a number of high-profile entities
 - c. **Kaseya in 2021.** A zero-day exploit allowed attackers to deploy an update to every customer running their Virtual System/Server Administration (VSA) software. The update was pure ransomware, and it encrypted a large portion of Kaseya's VSA customer base

[1] Reference: https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

Supply Chain – Recent SW Supply Chain Attacks(Cont.)

- The European Union Agency for Cybersecurity recently published a report studying 24 supply chain attacks from January 2020 to July 2021. The report revealed some stark statistics:
 - a. Suppliers either did not know or did not report how they were compromised in 66% of supply chain attacks
 - b. Advanced persistent threat (APT) groups were credited with carrying out 50% of supply chain attacks
 - c. Exploiting trust in the supplier accounted for nearly 62% of attacks on customers
 - A trusted supplier or vendor is assumed to maintain rigorous security standard

Supply Chain – Recommendations to reduce SW supply chain security risks

-
- Many security issues can be addressed through taking a holistic approach to security and adopting the principles of Zero Trust
- Third-party applications needs to be investigated more thoroughly
- An organization's product security incident response team (PSIRT) is a key component of improving its security posture
- **Looks for known weaknesses/vulnerabilities** in their source code and **compiled code**, and demonstrates the degree of rigor they apply. This may include requiring a specified level of developer **testing and evaluation** (e.g., static code analysis, threat modeling and vulnerability analysis, third-party verification of processes, manual code review, penetration testing, dynamic code analysis, etc.)
- Require **a software component inventory (e.g., software bill of materials)** that articulates the components and other attributes of delivered software developed by the vendor and third parties.
- Actively identifies and discloses vulnerabilities
- Maintains a product vulnerability response program
-

Why Run Binary Static Analysis in your SDLC?

- Software security relies on many factors, including effective tooling
- Security analysis tools can help detect and protect vulnerable software
- Source code analysis is most widely used but comes with limitations
- Binary analysis can help harden your software assets, both as a part of the SDLC and as a powerful tool to secure the supply chain



Assess the actual
deployed software
product



Ensure the quality
of deliverables from
your supply chain

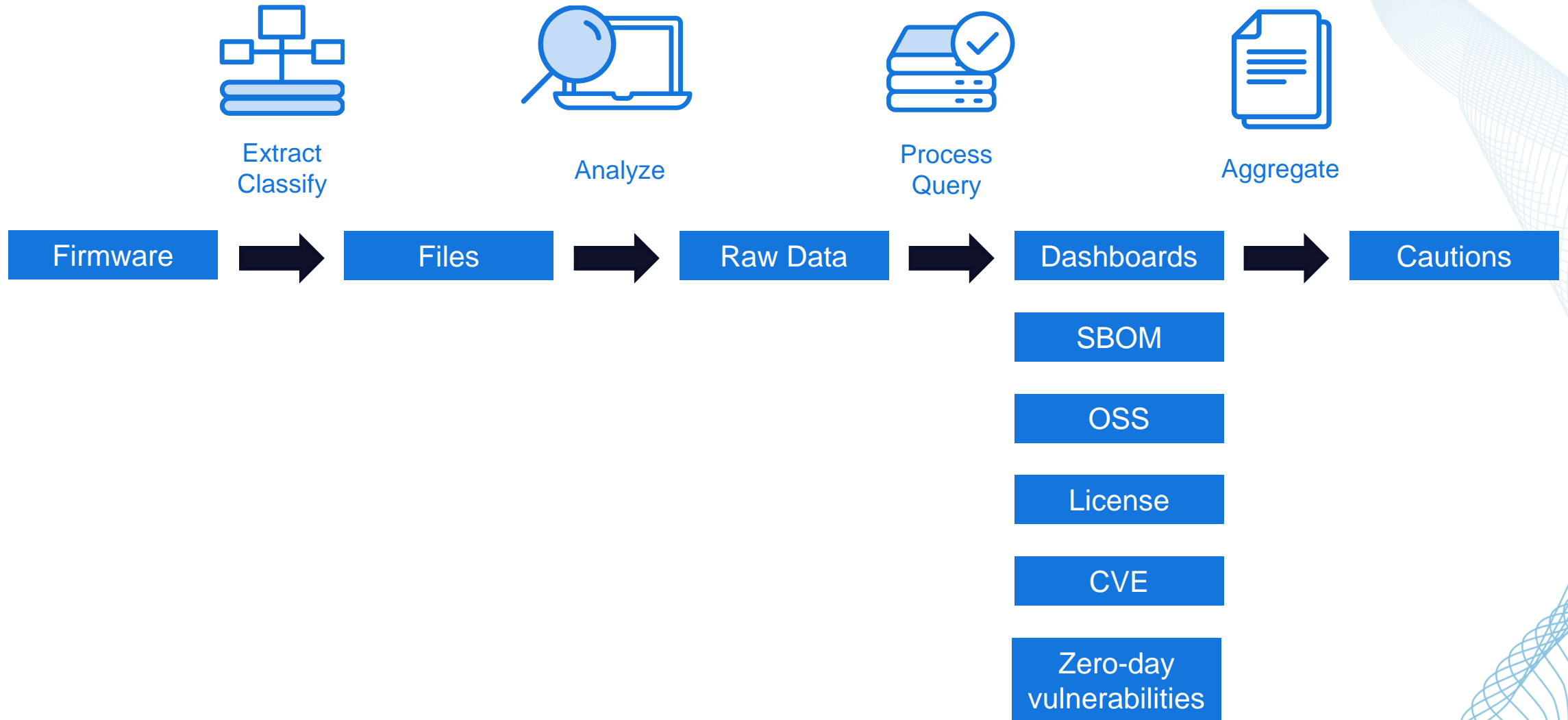


Understand the integrity
of your build process



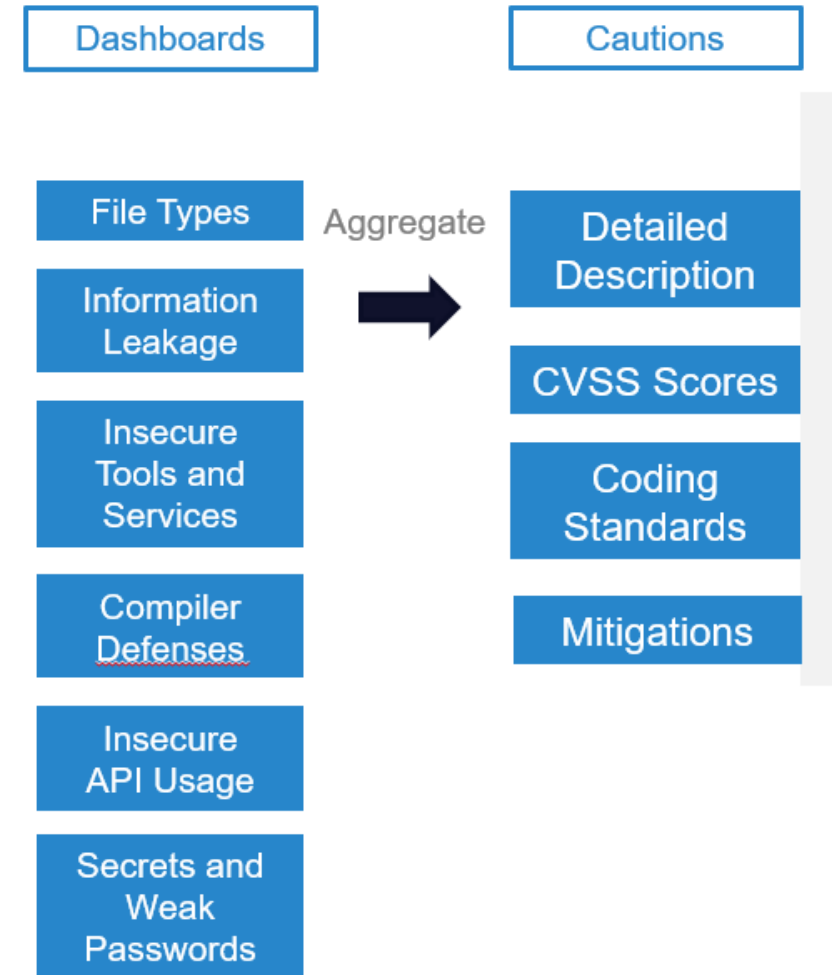
Understand the artifacts
introduced by source
code compilers

Binary Static Analysis – Workflow



Binary Static Analysis – Defense in Depth

- Helps you build defense in depth through “cautions”, security warnings built on top of best practices, Zero-day vulnerabilities and standards, which operate on the disassembled code
 - a. Detects the effective implementation of compiler defensive techniques such as stack cookies and offers remediation options
 - b. Identifies the presence of insecure API’s and recommends the secure version
 - c. Provides access to best practices and published standards, including CWE, CERT-C, MISRA, and ISO26262
 - d. Secure craftsmanship: cyclomatic complexity



Binary Static Analysis – Software Bill of Materials

- **What is it?**
 - Detail of list of items in a product
 - Files, types, sizes, versions, licenses
- **Why is it important?**
 - An SBOM provides those who produce, purchase, and operate software with information that enhances their understanding of the supply chain
 - May 12th 2021 - Executive Order 14028
 - UNECE WP.29 Regulation 155
 - Medical Industry and FDA regulation
- **What can you do with it?**
 - Independent verification
 - Custom device configuration / deployments
- **The practicalities of SBOM**
 - Perspectives in Software Composition Analysis
 - Code, **binary**, or on device requests
 - Software craftsmanship
 - Formats (SPDX, CycloneDX, SWID)

Nutrition Facts	
8 servings per container	
Serving size	2/3 cup (55g)
Amount per serving	
Calories	230
% Daily Value*	
Total Fat 8g	10%
Saturated Fat 1g	5%
Trans Fat 0g	
Cholesterol 0mg	0%
Sodium 160mg	7%
Total Carbohydrate 37g	13%
Dietary Fiber 4g	14%
Total Sugars 12g	
Includes 10g Added Sugars	20%
Protein 3g	
Vitamin D 2mcg	10%
Calcium 260mg	20%
Iron 8mg	45%
Potassium 235mg	6%
<small>* The % Daily Value (DV) tells you how much a nutrient in a serving of food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.</small>	



Q&A



Thank you!

koreasales@blackberry.com