



BlackBerry QNX Security Services

Helping you build secure embedded systems with
our specialized technology and expertise

With the increasing connectivity and growing complexity of embedded system software, designing secure systems has become more complex and more challenging than ever. Embedded developers need to consider security at every stage of the development lifecycle to mitigate risks associated with vulnerabilities and protect against attacks. BlackBerry® QNX® has developed a set of security services designed to provide you everything you need to ensure uncompromising security in your embedded systems.

We offer flexible delivery options to meet your unique need in these three service categories:

- **Predefined security packages**, services that are pre-packaged to address common security challenges in developing embedded systems
- **Service solutions** in areas such as threat modelling and risk assessments in which we can provide frameworks and guidance as well as hands on support.
- **Custom services** that can be tailored to your unique needs and organization.

The BlackBerry QNX Advantage

Our Expertise

Our security services are built on our deep embedded systems expertise and BlackBerry's long history of proven security experience. We have helped thousands of clients across automotive, medical, aerospace and defense and more. We have specialized embedded system and security knowledge and are members of the Consortium for Information and Software Quality's (CISQ) SBOM Standards Working Group. By leveraging our expertise along with the power of our proprietary binary scanning technology, we have helped many organizations assess the security of their code, both in development and in the field. Let our team of experts help you thwart cyberattacks, take advantage of emerging opportunities and overcome the technical limitations that are unique to embedded systems.

Our Technology

Many of our security service offerings rely on BlackBerry® Jarvis™, our proprietary binary code scanning and software composition analysis tool. BlackBerry Jarvis has been specifically tailored for embedded and safety critical systems such as those in the automotive, medical and defense sectors, and has automated capabilities for enumerating both software and hardware bills of materials. It provides insights into software composition, and helps you manage risk by tracking changes in software quality over time. Through cutting-edge system exploration technology and expert security services, you can scan a complete software product for security vulnerabilities and software craftsmanship. Since BlackBerry Jarvis extracts the characteristics and attributes from compiled binaries, access to source code is not required to gain insights into the final product.

Through cutting-edge system exploration technology and expert security services, you can scan a complete software product for security vulnerabilities and software craftsmanship.

Predefined Service Packages





With BlackBerry QNX as your partner, you have the assurance of working with the experts in delivering software solutions for critical embedded systems. We offer these predefined security service packages to address some of the most common security requirements experienced by embedded systems developers today:

- Penetration Testing
- Open Source Software (OSS) Assessment
- Software Security Assessment

Penetration Testing

Using BlackBerry Jarvis and our deep security expertise, we will run a thorough assessment of the vulnerabilities of your embedded system. The BlackBerry QNX team will assess the security of your system hardware and software by attempting to reach high value assets or specific targets using similar tools and techniques to those employed by a potential adversary. We will tailor our specific techniques to the system being assessed. The overall strategy is to understand weaknesses in the software's security design, then define and test exploits. We may also need to define threat models such as misuse cases, attacker profiles and provide a threat testing plan to address challenges with more complex systems.

The penetration testing service package will cover:

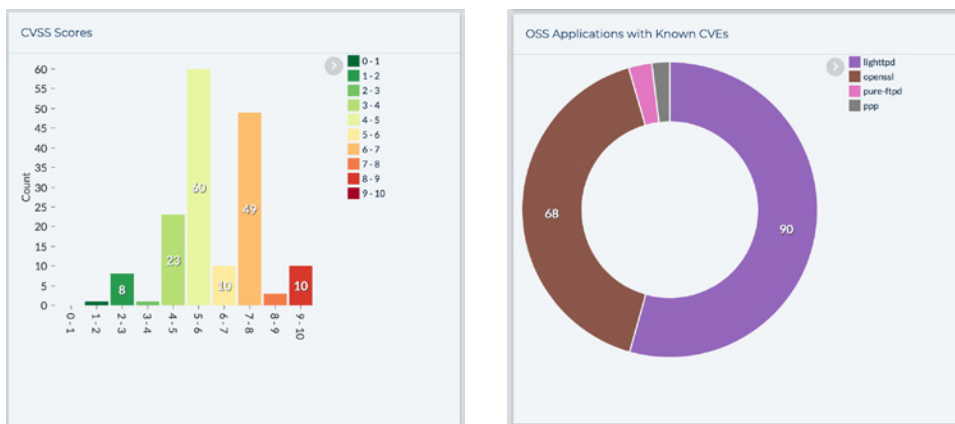
Planning and Discovery	Exploitation
 <ul style="list-style-type: none">• Scoping• Definition of rules of engagement• Hardware analysis• Software composition file type recognition• Static firmware analysis and vulnerability identification• Interface and access assessment (MITM, CAN, BT, WiFi, Ethernet, etc.)	 <ul style="list-style-type: none">• Attack identified hardware interfaces• Reverse engineering on the extracted firmware• Software vulnerability exploitation• Software security controls testing including secure boot, code protection, key handling and protection
Reporting	Threat Modeling
 <ul style="list-style-type: none">• Detailed exploitable vulnerabilities found and reproduction steps• Vulnerabilities report by likelihood, impact and criticality• Mitigation recommendations	 <ul style="list-style-type: none">• Attacker profiling• Risk and threat analysis• Misuse case analysis

Open Source Software (OSS) Assessment

Many OEMs are faced with the challenge of dealing with the risks inherent when using open source software coming from their suppliers. BlackBerry Jarvis lets us inspect binary files in a device's software image to uncover any vulnerabilities that may be present in third party or open source software components. Through this service engagement we will identify the open source software bill of materials (OSS BOM) for a given software image including each OSS component, version, copyright notice and license. Because BlackBerry Jarvis does not require source code access, this service is useful in assessing software from third parties or to validate stated compliance, risk profile and licensing restrictions.

The BlackBerry QNX Professional Services team will make use of BlackBerry Jarvis to:

- Document the open source software bill of materials including library, license, and version detection
- Detect dynamic public vulnerability (CVE) and linkage
- Supply a report detailing the open source software findings.



Sample BlackBerry Jarvis report showing open source software vulnerability findings, as part of an OSS assessment

Software Security Assessment

The security of your embedded system is only as good as its least secure hardware and software components. This is why it's important to fully understand security across the supply chain and entire software development lifecycle (SDLC). Applying a combination of our cybersecurity expertise and binary code scanning technology, we will assess the security of hardware and software within an embedded system.

We will tailor the specific techniques to the system being assessed. This approach will help us understand weaknesses in the software's security design by inspecting the binary, support and operating system files. We will provide a walkthrough of detailed dashboards showing statistics on software craftsmanship, code quality and vulnerability.

Our team of security specialists will:

- Perform an automated composition analysis of binary images, support files with full identification of system components
- Conduct a static firmware analysis with a focus on application specific vulnerabilities (e.g., use of insecure system calls, memory handling, processing of uncontrolled user input) as well as logic flaws in the applications
- Map the software bill of materials, open source software and identify target materials
- Review the operating system for applications running on QNX, Android and Linux varieties

Service Solutions

For more than 35 years, BlackBerry has been synonymous with security. Let our team of embedded security experts help you identify vulnerabilities and recommend specific remediation actions. From regulatory readiness assessments to a holistic appraisal of your company's security posture, our professional services team can assess and address security issues with your processes or products at every stage of your SDLC.

How It Works

We deliver each of our service solutions using our proven methodology that enables you to gain critical insights into your risks. We can then provide expert recommendations on what actions you need to take to remediate those risks. While approaches may differ depending on the focus of your project, most engagements involve a three-phase approach over a four- to six-week period. The phases can include workshops with key stakeholders, binary scanning and analysis, or a deep dive into your policies and procedures. The output of the engagement is a detailed report and where appropriate, presentation of our findings to the decision makers.

What You Get

Depending on the area of focus for your project, deliverables can vary. But most often, each engagement results in a documented analysis of your current situation and plan for remediation. Your report presents an assessment of your readiness to address the challenge in question and provides an analysis of areas of weakness, risks, recommendations, along with a remediation roadmap.

Service Solutions

We offer service solutions based on these capabilities:

- Cyber Risk Assessment
- WP.29 Readiness Assessment
- Control Maturity Assessment
- Policy / Documentation Review
- Threat Modelling

Highlights

- Pre-packaged and custom services to address your specific embedded system security challenges
- Proven expertise with BlackBerry's more than 35 years in security
- Built on deep embedded system expertise and knowledge across a range of industries
- Helps you understand software composition and uncover software vulnerabilities with BlackBerry Jarvis

- Threat Intelligence
- Product IoT Cybersecurity / Safety Strategy and Governance
- Insider Threat Management
- Third-Party Security Risk Management

Cyber Risk Assessment

Cyber risk assessments should be a continual assessment of risks to your information systems and conducted at least once a year or when significant changes occur to your business, your IT estate, or your legal / regulatory environment. These assessments may also be part of cybersecurity assessment associated with insurance obligations. Risk assessments are used to identify, estimate, and prioritize risk. Your cyber risk assessment will help inform decisionmakers across your organization, support proper risk responses, and improve your spending efficiency and cyber resilience.

WP.29 Readiness Assessment

The upcoming WP.29 regulation places an obligation on OEMs to be certified in order to release vehicles into markets covered by the United Nations Economic Commission for Europe (UNECE). BlackBerry QNX has developed a readiness assessment service to help you with compliance to the WP.29 regulation. The service will facilitate a better understanding of their conformity levels with the regulation, your overall cybersecurity posture, and the risks you may face. It will result in a report and pragmatic plan for your compliance journey.

Security Control Maturity Assessment

This maturity assessment will help you develop or continue your governance strategy by identifying security and governance control maturity levels and pinpointing weaknesses or areas in which your organization needs improvement. By understanding the maturity, the environment, your threats and risks you can more effectively prioritize remediation, manage resources, allocate spending, accelerate projects and pragmatically build out a cybersecurity roadmap.

A BlackBerry QNX subject matter expert will perform a three-staged assessment to clarify where there are areas of good practice (e.g., the overarching cybersecurity strategy), areas of weakness (e.g., the controls are present, but not embedded in the organization) and identify risks. Our proprietary maturity assessment is linked to industry standards such as ISO 27001, NIST, and Cobit.

Policy or Documentation Review

Policies are the backbone of ensuring businesses have a systematic approach to comply with security expectations, laws and regulations. This review will help inform your team about their duties by clearly outlining procedures for collecting, storing and processing data. As part of the review, our experts will perform a policy and procedure assessment to explore your security, privacy, data protection policies, standards and procedures you use to secure your embedded systems and comply with regulatory requirements. We will assist you in creating net new policies, updating current policies or recommend more efficient frameworks and compliance processes.

From regulatory readiness assessments to a holistic appraisal of your company's security posture, our professional services team can assess and address security issues with your processes or products at every stage of your SDLC.

Threat Modelling

With an increased focus on “security by design” and an increase in connectivity in the IoT and embedded space, you need to understand how to adopt security practices within your development team. Our threat modelling solution provides a clear view of cyberthreats, enables measurement of security initiatives, displays trends and provides pragmatic evidence of the vulnerabilities and required mitigations.

This service engagement will result in a threat modelling report that consists of:

- Threat/weakness/vulnerability/risk analysis section;
- Attack modelling and simulation scenarios section;
- Attack testing/simulation results section

Product IoT Cybersecurity Strategy and Governance

The threat landscape and attack surface of embedded systems is constantly evolving, and new risks are constantly emerging. You need to ensure your cybersecurity plans are aligned with wider business objectives, all while keeping your organization, partners, customers and supply chain secure. We will review your documentation, then hold a workshop(s) to understand your vision, resources, unique characteristics, security / data protection by design approach. The engagement results in the presentation of a roadmap, strategy and steps to reach your goals.

Insider Threat Management

Insider cyberattacks continue to be a leading risk for organizations. And the threat of malicious actors is not the only risk. The growing complexity of IoT and embedded networks can introduce the possibility of accidental threats by well-meaning insiders. BlackBerry QNX will assess your vulnerability to insider threats by analyzing your:

- Asset inventory
- Configuration and compliance monitoring
- Automated policy remediation
- Identity and access security
- Anomaly detection
- Network traffic
- Account compromise, insider threat detection and monitoring mechanisms
- Users behaviour analysis
- Privileged activity monitoring mechanisms

Third-Party Security Risk Management

Large organizations often lack a clear picture of their extended enterprise, including secondary or tertiary-level parties. In 2018, third-party attacks or incidents caused 21 percent of confirmed security breaches. Third-party security risk management helps you assess and control financial, operational, regulatory or cyber risks resulting from doing business with third-party vendors. Our third-party vendor management solution investigates the quality of software that is inherited by your products from third party and open source, and helps you:

- Identify the right people to gain an understanding of your extended enterprise
- Formulate a process for interfacing with vendors

With an increased focus on “security by design” and an increase in connectivity in the IoT and embedded space, you need to understand how to adopt security practices within your development team.

- Identify and leverage the technologies to manage your processes
- Determine metrics for internal and external compliance purposes
- Document due diligence processes for vendors
- Document data processor contract processes
- Update third-party contracts

Hardware/Software Reverse Engineering

We often provide reverse engineering (hardware/software) activities as a part of a penetration testing project or as a standalone project. Reverse engineering involves dissecting a device to examine and test your firmware for security vulnerabilities. This service can help you understand how a device is built, its connections and how to manipulate the hardware / software for additional access and control. We work with the OEMs rather than against them for better efficiency.

Standard reverse engineering engagements include:

- Identification of the system's components and their interrelationships
- Creation of system representations in another form or a higher level of abstraction
- Creating the physical representation of a system

Custom Services

The BlackBerry QNX Professional Services team has deep expertise and experience to help you understand emerging threats and protect your products. Traditional security consultants test to find holes, and then go home just as the real work begins. We will support your organization from product design to ongoing incident response.

We understand the unique challenges of securing embedded systems throughout the development lifecycle and can advise you on secure architecture design, development, deployment, and supply chain management. Whether you are looking to build a secure platform, harden a product, or deploy a secure and effective IoT capability, we're here to help.

To engage an expert today, contact qnx-security@blackberry.com.

About BlackBerry® QNX®

BlackBerry QNX is a leading supplier of safe, secure, and trusted operating systems, middleware, development tools, and engineering services for mission-critical embedded systems. BlackBerry QNX helps customers develop and deliver complex and connected next generation systems on time. Their technology is trusted in over 175 million vehicles and more than a hundred million embedded systems in medical, industrial automation, energy, and defense and aerospace markets. Founded in 1980, BlackBerry QNX is headquartered in Ottawa, Canada and was acquired by BlackBerry in 2010.

For more information, visit blackberry.qnx.com and follow [@QNX_News](https://twitter.com/QNX_News).

© 2020 BlackBerry Limited. All rights reserved. QNX, Momentics, Neutrino, Jarvis are trademarks of BlackBerry Limited, which are registered and/or used in certain jurisdictions, and used under license by BlackBerry. All other trademarks belong to their respective owners.

