kryptowire

About
KRYPTOWIRE

For more information visit us at **www.kryptowire.com** or contact us directly at **info@kryptowire.com**

“

The Mobile & IOT Security Compliance Technology of Choice Because Security Matters

ABOUT KRYPTOWIRE

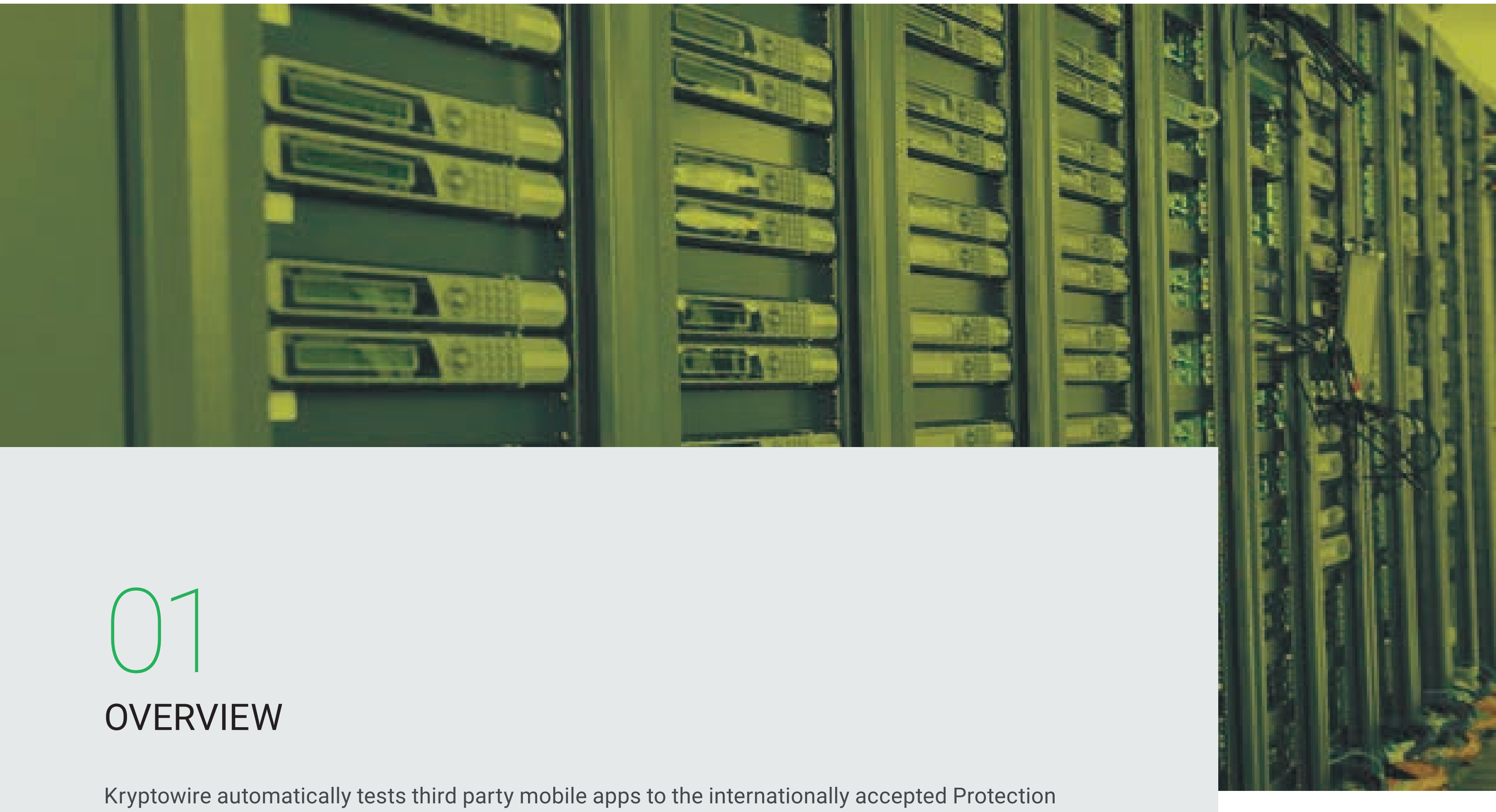
Protecting against mobile and IoT vulnerabilities can be arduous, error-prone, and costly when your employees’ devices have hundreds of third-party applications, libraries, and perform frequent unmanaged updates exposing the organization to software vulnerabilities and zero-day threats on a daily basis. A single insecure mobile device may result in irreparable data losses, compromised networks, and millions of dollars in damages to your enterprise.

Kryptowire is the preferred turnkey mobile security vetting technology of choice for government agencies. Kryptowire tests mobile & IoT devices against the highest internationally-recognized security standards used for classified and national security systems. This military-grade technology is now available to commercial enterprise users and integrated with major MDM enterprise mobility platforms.

KRYPTOWIRE KEY BENEFITS:

kryptowire

- Continuously assesses the security of all enterprise mobile and IoT devices against the highest internationally-recognized software assurance standards published by the National Institute of Standards and Technologies (NIST), National Information Assurance Partnership (NIAP), and the OWASP Top Mobile Security Risks.
- Tests the security of every mobile app, on every mobile device, for every enterprise employee, using the latest mobile threat intelligence.
- Provides Risk Assessments with pass/fail evidence down to the line of code to assure transparent and high-confidence results.
- Enables automated remediation that includes automated exporting of firewall rules, whitelisting or blacklisting applications, notifying the end user, or even removing non- compliant assets to protect enterprise resources and data.
- Enforces compliance with HIPAA, PCI, GDRP, and custom enterprise-wide privacy and security policies.
- Kryptowire offers both cloud-based (SaaS) and secure on-premise appliance solutions.
- Compliance Testing for General Data Protection Regulation (GDPR).



01

OVERVIEW

Kryptowire automatically tests third party mobile apps to the internationally accepted Protection NIAP Profile for Application Software. Kryptowire licenses the technology to allow both government and industry to test their mobile applications to the highest software assurance levels suitable for classified and national security systems. Kryptowire can analyze 3rd-party and in-house developed mobile apps without access to source code. Kryptowire's automated mobile app testing technology is available as a 24/7 cloud service and as an on-premise appliance.

02

WHAT IS THE COMMON CRITERIA?

The Common Criteria (CC) is an international set of guidelines and specifications developed for evaluating information security products, specifically to ensure they meet an agreed- upon security standard for government deployments. Common Criteria is more formally called "Common Criteria for Information Technology Security Evaluation." Common Criteria has two key components: Protection Profiles and Evaluation Assurance Levels. A Protection Profile (PPro) defines a standard set of security requirements for a specific type of product, such as a firewall, router, or mobile application. The Evaluation Assurance Level (EAL) defines how thoroughly the product is tested.

03

WHAT US THE NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP)?

The National Information Assurance Partnership (NIAP) is responsible for U.S. implementation of the Common Criteria, including management of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) validation body. NIAP manages a national program for developing Protection Profiles, evaluation methodologies, and policiesthatwillensureachievable,repeatable,andtestablerequirements. Inpartnership with NIST, NIAP also approves Common Criteria Testing Laboratories to conduct these security evaluations in private sector operations across the U.S. See https://www.niap-ccevs.org

04

WHICH PROTECTION PROFILE IS USED FOR MOBILE APPS?

Protection Profile for Application Software. The scope of this Protection Profile (PP) is to describe the security functionality of application software in terms of [CC] and to define functional and assurance requirements for such software. In recent years, software attacks have shifted from targeting operating systems to targeting applications. This has been the natural response to improvements in operating system security and development processes. As a result, it is paramount that the security of applications be improved to reduce the risk of compromise.

05

WHICH UNITED KINGDOM AGENCY IS A COMMON CRITERIA MEMBER?

The National Cyber Security Centre (NCSC) is the UK's authority on cyber security. The NCSC is part of GCHQ. The NCSC brings together and replaces CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI).

UK IT Security Evaluation and Certification Scheme
NCSC Certification Body NCSC, Room A2J Hubble Road Cheltenham Gloucestershire
GL51 0EX United Kingdom

Tel. 44 (0)1242 221491, Ext 30074
Fax. 44 (0)1242 709194
email: iacs@ncsc.gov.uk
Web URL: http://www.ncsc.gov.uk/

06

COMPLIANCE TESTING

Kryptowire perform compliance testing on mobile applications for internationally recognized standard for the banking, finance, and health care industries. Kryptowire performs compliance testing for GDPR, NIST, NIAP, OWASP, as well custom enterprise security and privacy policies.

07

PRICING

Kryptowire offers a tiered pricing model with volume discounts based on the number of mobile applications to be tested. Kryptowire automatically tests every new version of every new mobile application.

Item	Description	Term	Quantity	Price
KW-001-UK	Cloud-based Mobile App Security, Privacy, and Compliance Testing of up to 10 Android and iOS mobile apps	12 months	1	£20,000/ year
KW-002-UK	Cloud-based Mobile App Security, Privacy, and Compliance Testing of up to 25 Android and iOS mobile apps	12 months	1	£50,000/ year
KW-003-UK	Cloud-based Mobile App Security, Privacy, and Compliance Testing of up to 50 Android and iOS mobile apps	12 months	1	£80,000/ year
KW-004-UK	Cloud-based Mobile App Security, Privacy, and Compliance Testing of up to 100 Android and iOS mobile apps	12 months	1	£150,000/ year
KW-005-UK	Cloud-based Mobile App Security, Privacy, and Compliance Testing of up to 250 Android and iOS mobile apps	12 months	1	£200,000/ year
KW-006-UK	Cloud-based Mobile App Security, Privacy, and Compliance Testing of up to 500 Android and iOS mobile apps	12 months	1	£300,000/ year
KW-007-UK	On-premise Appliance Mobile App Security, Privacy, and Compliance Testing of up to 100 Android and iOS mobile apps	12 months	1	£200,000/ year
KW-008-UK	On-premise Appliance Mobile App Security, Privacy, and Compliance Testing of up to 250 Android and iOS mobile apps	12 months	1	£250,000/ year
KW-009-UK	On-premise Appliance Mobile App Security, Privacy, and Compliance Testing of up to 500 Android and iOS mobile apps	12 months	1	£300,000/ year
KW-010-UK	On-premise Appliance Mobile App Security, Privacy, and Compliance Testing of up to 1000 Android and iOS mobile apps	12 months	1	£350,000/ year