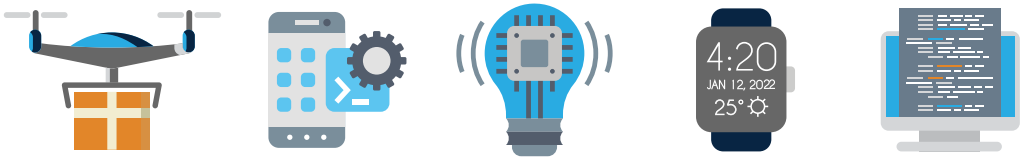
PRODUCT SECURITY TESTING AND ASSESSMENT

Find Critical Vulnerabilities in Your Connected Devices

By 2025 there will be 55.7 billion connected devices worldwide, according to IDC. Can technology companies secure all these objects from threats? As the proliferation of interconnected products and devices grows, the need for securing devices, applications, data and communication increases.

With Internet of Things (IoT) devices, Operational Technology (OT) devices, smart devices and cloud applications becoming more ubiquitous in all environments, **finding vulnerabilities in software and hardware is a requirement** no manufacturer should overlook.

CAN MY PRODUCT BE **HACKED?**



Internet of Things | Mobile Apps | Operational Tech | Smart Devices | SaaS Apps

Ethical hackers from Tangible Security determine what harm can be done when cyber threats target your new or existing product. Using a range of unique penetration testing tools for testing connected devices, Tangible's product security testing mimics real-world hacking tactics and techniques that uncover hidden vulnerabilities in your device or application and provide realistic insights and practical results. Tangible Security literally wrote the book on ethical hacking.

Tangible Security has honed this ethical hacker approach employing a full range of specialists and engineers who can work with and test different aspects of a product in parallel, minimizing impacts, and expediting time-to-market. Typical engagements include:

- **Product Architecture Assessments**
  Assessment to understand the architecture of the system and identify potential risks.
- **Vulnerability Assessments**
  Provides a broad picture of the vulnerabilities affecting one or more systems and determine the scale of known security problems for prioritizing fixes.
- **Penetration Testing**
  Testing with attack simulations where security scenarios are identified and defenses are tested.

Quick Glance:

WHO: Product leaders and developers

WHAT: Assess the efficacy of your product's security

WHY: Find vulnerabilites and security risks in your product in the face of increasing threats

By 2025, there will be
55.7B
connected devices
IDC 2020

Vulnerabilities and their exploitation by attackers of all skill levels and motivations, are driving the threat landscape.

- Gartner

Email: info@TangibleSecurity.com
Phone: 720-375-1551 | www.tangiblesecurity.com

Tangible Security
7048 Knightdale Blvd -Ste 220B, Knightdale, NC 275454

PRODUCT SECURITY TESTING AND ASSESSMENT

After initially defining the scope and nature of your project, Tangible Security engineers either perform a Black Box assessment or review your product documentation and/or meet with your developers in more of a Gray Box or White Box approach.

The better we understand the intent, function, and ecosystem of the product, the more thoroughly we can search for security gaps and vulnerabilities. Our findings reports are prioritized, structured, and detailed. We will assist your engineers with recreating and remediating the findings.

FREQUENT SECURITY FINDINGS

- Spoofable software updates
- Identity and privilege flaws
- Accessible, unencrypted binaries
- Hidden tools hackers can run
- Concealed physical ports with root access
- Logging unnecessarily capturing sensitive data
- Missing data input validation
- Unpatched libraries and components
- Unnecessary services running

Contact: info@TangibleSecurity.com | Phone: 757-525-1863 | www.tangiblesecurity.com