TECHNICAL EXPLAINER · 2026 · FDA-DEFENSIBLE TESTING

Why ELTON uses a digital twin

The blueprint that makes test cases, exploitability calls, and CVSS ratings defensible in FDA review.

KEY TAKEAWAYS

- Blind pentesting is no longer compliant. FDA expects the full set of test cases, and the reason each case was chosen has to correspond to the threats and components of the product.
- The digital twin is a blueprint of the product: components, interfaces, data flows, and assets, built from documentation your quality system already produced.
- The twin does three jobs: it enumerates the test cases for a defensible test plan, it identifies the attack surface a threat actor would actually start from, and it drives path analysis for CVSSv3 and CVSSv4 ratings.
- Exploitability is classified from the twin: directly exploitable, conditionally exploitable, or a weakness, mitigated or unmitigated, based on external attack surface, preconditions, and postconditions.
- Ratings reflect the product as designed: privileges, trust levels, and the confidentiality, integrity, and availability impact of a finding’s postconditions, not a database worst case.
- Depth in, defensibility out. The more the twin knows, the more defensible the test plan and the lower the ratings tend to land, because the model shows the walls a thin blueprint hides.

> **"A blueprint with two boxes looks easy to break into. The full blueprint shows the interior walls."**

Blind pentesting stopped being compliant

For years a penetration test was a scope, a window, and a report of what the tester happened to find. FDA review does not accept that shape anymore. Reviewers ask for the whole test: every test case that ran, and a reason each case exists that traces to a specific threat and a specific component of the product. A finding list without that mapping reads as an opinion about coverage, and deficiency letters now say so.

You cannot produce that mapping by pointing tools at a target. You need a model of the product to map against. That model is the digital twin.

The twin is a blueprint

ELTON builds a working blueprint of each product release: the key components, the interfaces they expose, the data flows between them, and the assets worth protecting. The twin is assembled from documentation your quality system has already produced, reviewed, and in most cases submitted. Architecture views define what the device is and where it sits. The SBOM binds every component and version to a real location in the model. Interface and protocol documentation becomes the list of doors. Documented countermeasures become claims the testing will verify.

It is not a binary inventory rebuilt from firmware. It is the security architecture of the product, at the level where exploitability questions are actually decided.

Three jobs the twin does

JOB	WHAT THE TWIN PROVIDES
1 · Enumerate the test plan	Test cases are generated from the twin's components, interfaces, and data flows, so the plan covers the product rather than the tester's instincts. Every case traces to the scope element and threat it exercises, which is the traceability FDA asks to see.
2 · Classify exploitability	The twin identifies the key attack surface where a threat actor would initiate an attack. A finding reachable from that surface on its own is directly exploitable. A finding that requires another condition first is conditionally exploitable. A finding with no path is a weakness, tracked as mitigated or unmitigated by the controls the twin records.
3 · Rate by path analysis	Path analysis from the key attack surface produces CVSSv3 and CVSSv4 metrics that are defensible to FDA because they consider the architecture and security design of the product: the privileges required along the path, the trust levels crossed, and the confidentiality, integrity, and availability impact of the postconditions the vulnerability actually yields.

The three jobs compound. A defensible test plan of test cases mapped to scope elements, defensible CVSS ratings, and a defensible exploitability determination, direct versus conditional versus not exploitable at all, all rest on the same foundation, and all of it is driven by external attack surface, preconditions, and postconditions the twin makes explicit.

Two blueprints of the same house

Imagine a blueprint with two boxes. Every wall is exterior, every direction looks like a way in, and an assessor has no grounds to argue otherwise. Now imagine the full blueprint: every interior wall, every locked door, every hallway an intruder has to cross. The house did not change. The evidence did, and most break-in theories now die at a wall the thin drawing never showed.

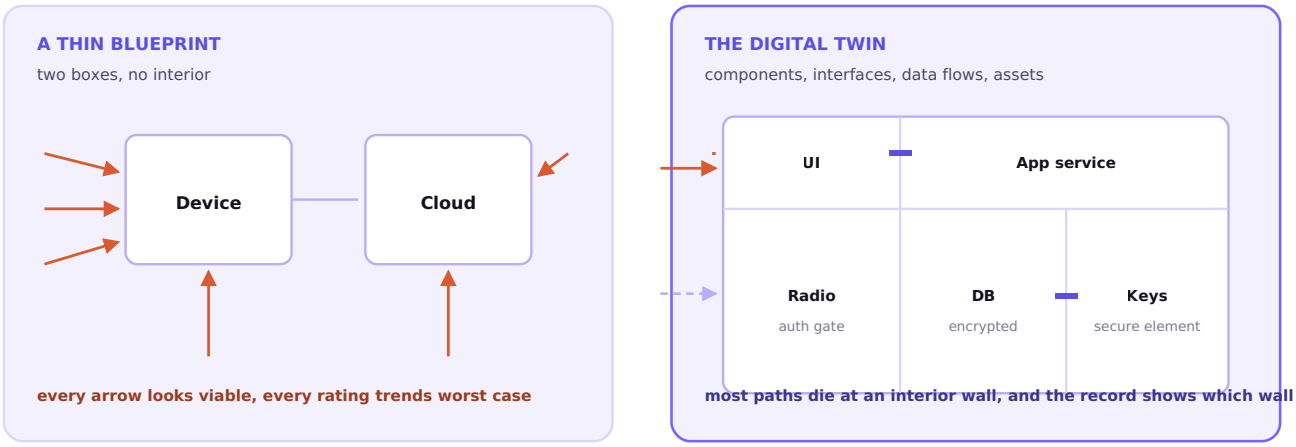

Figure 1. The same product, modeled thin and modeled fully. Depth in the twin turns worst-case assumptions into rated, evidenced paths.

Ratings work the same way. The more ELTON knows, the better the twin. The better the twin, the more defensible the test cases, and the lower the severity of the ratings, because paths that a bare CVE score assumes are open are shown to end at an authentication gate, a trust boundary, or a control that was documented and then verified.

What builds the twin

Depth is the input. The documentation below is what we commonly request before testing and for ongoing vulnerability management. No single item is mandatory, and the twin improves with every one provided.

DEVICE DESIGN & DEVELOPMENT

- System Requirements Specification (SyRS)
- Software Requirements Specification (SRS)
- System/Software Architecture Description (SAD)
- Software Design Description / Design Specification (SDD/SDS)
- User and service manuals
- Detailed / low-level design documents
- Product requirements & functional specifications
- Intended use / use environment / user needs
- Hardware design docs: block diagrams, board schematics, hardware BOM
- State / sequence / behavioral diagrams

ARCHITECTURE, DATA FLOW & INTERFACES

- Architecture views / system block diagrams
- Data Flow Diagrams (DFDs)
- Network & deployment / topology diagrams
- Interface Control Documents (ICDs) / interface requirements
- API documentation (Swagger/OpenAPI)
- Communication protocol specs (DICOM, HL7/ FHIR, MQTT, BLE, proprietary)
- Cloud architecture diagrams plus serverless/ function docs
- Ports, protocols & services list

SOFTWARE COMPOSITION & BUILD

- Software Bill of Materials (SBOM), CycloneDX/ SPDX
- Third-party / OSS dependency list & versions
- Build / configuration and deployment specifications
- Source code access (repo or secure file share)

CYBERSECURITY & RISK

- Threat model(s)
- Security risk assessment / security risk management file (ISO 14971 plus AAMI TIR57)
- Security architecture & trust-boundary views
- Security requirements / controls list
- Cryptography & key management documentation
- Secure boot / firmware update mechanism docs
- List of security features, changes, or fixes for the release

PRIOR TESTING & ASSESSMENT HISTORY

- Previous penetration test reports
- Vulnerability scan results (SAST / DAST / SCA)
- Prior vulnerability assessments & CVSS ratings
- Known / open findings and remediation status

The foundation, plainly

The twin is the underlying foundation that lets ELTON meet FDA expectations: a defensible test plan of test cases mapped to scope elements, defensible CVSSv3 and CVSSv4 ratings, and a defensible determination of exploitability driven by external attack surface, preconditions, and postconditions. Everything downstream, the verdicts, the dispositions, the VEX, the submission language, inherits its defensibility from that model. Testing without one is guessing with tools. We built ELTON so nobody has to defend a guess in front of a reviewer.

About ELTON. ELTON is an AI-native, integrated cybersecurity testing and management service for medical devices. ELTON builds a digital twin of each device, runs testing across the full stack on every release, and proves which findings are exploitable, with every verdict evidenced for regulatory review. ELTON meets FDA premarket (524B) and postmarket cybersecurity testing and management requirements. Talk to us at **eltoncyber.com**.