

SOLUTION BRIEF

Most compliance evidence describes what was intended, not what happened.

An assessment is usually assembled from policies, diagrams, screenshots and interviews. Each of those describes the design of a control. None of them demonstrates that the control was operating on a Tuesday in March, which is the question an assessor is really asking and the one that is hardest to answer.

Network communications are different. They are a record of what actually occurred. If a boundary was crossed, the traffic crossed it. If a device used a weak certificate, the negotiation happened. WireTrace turns that record into control evidence, continuously, without anyone assembling it.

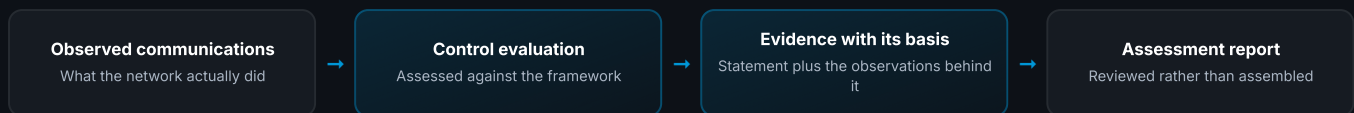
THE DIFFERENCE IN ONE COMPARISON

CONTROL AREA	CONVENTIONAL EVIDENCE	EVIDENCE FROM OBSERVATION
Asset inventory	A maintained register, accurate on the day it was last reviewed.	Every device that communicated during the assessment window, whether or not anyone recorded it.
Network segmentation	A design document and a firewall configuration export.	What actually crossed the boundary during the window, which is the test of whether the configuration achieved its purpose.
Secure communication	A policy requiring encryption in transit.	The protocols and certificate strength genuinely negotiated by systems in use.
Remote and vendor access	A signed procedure and an access request log.	The support sessions that actually took place, to which systems, over which protocols.
Change control	A change record system that reflects changes people remembered to raise.	New devices, relationships and behaviour appearing on the network, including those that bypassed the process.

SEVEN FRAMEWORKS, 415 CONTROLS

FRAMEWORK	CONTROLS	WHERE OBSERVATION CONTRIBUTES MOST
NIST CSF 2.0	106	Identify and Protect outcomes: what is connected, how it communicates, and whether the boundaries described actually hold.
ISO 27001	93	Asset inventory, network controls, cryptographic use in practice and supplier access, accumulated between surveillance visits.
HIPAA Security Rule	52	Connected device inventory, segmentation of clinical systems and transmission protection, without touching a device attached to a patient.
IEC 62443-3-3	51	Zone and conduit evidence and industrial asset inventory. The controls where documented design and operating reality most often diverge.
NERC CIP	44	Cyber system inventory, electronic security perimeter traffic and remote access into the perimeter, observed rather than attested.
NCA OTCC	35	Operational technology controls for organisations assessed under the Saudi national framework.
NCA ECC	34	Asset management, network security and access control evidence under the Saudi essential controls.

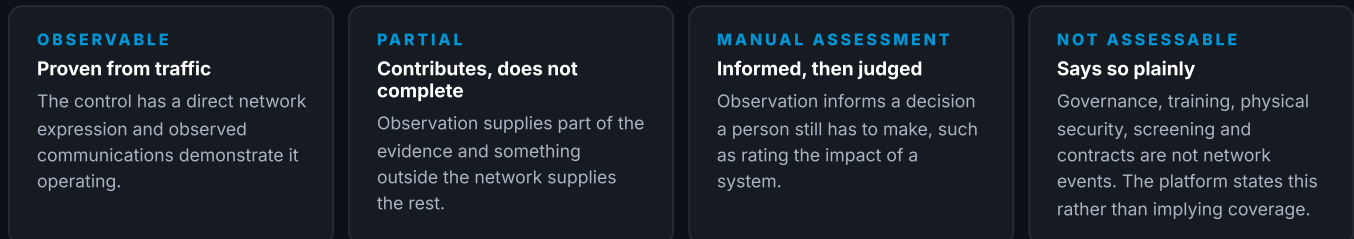
HOW THE EVIDENCE IS PRODUCED



Every statement is tied to the window it was observed in and to the observations that support it. That matters more than it sounds: an assessor's follow-up question is almost always **how do you know**, and a statement that cannot answer it is not evidence, it is an assertion.

EVERY CONTROL STATES WHAT WE CAN ACTUALLY PROVE

A platform that claims complete framework coverage is not credible, and any assessor will say so within a minute. So each of the 415 controls carries its own rating for how far network observation can go, and that rating is visible to you and to your auditor rather than buried.



Across the seven frameworks, the largest single category is **not assessable**, and we would rather you learned that here than discovered it during an audit. A framework is a whole management system; the part with a network expression is genuinely valuable and genuinely partial. Every control also carries the specific limitation that applies to it, in the platform, in writing.

The practical value is time and defensibility, in that order. Assessment preparation stops consuming skilled people for weeks. More importantly, the evidence stops being a snapshot assembled shortly before the assessment and becomes a continuous record, which is a materially harder position to challenge and a materially easier one to maintain.

WHO THIS HELPS



Test it against a control you find hard to evidence

Choose the control that costs you the most effort at each assessment, usually inventory completeness or segmentation. We will show you what observation produces for it, and tell you plainly if the answer is that observation is the wrong instrument for that control.

[Book a demo at wiretrace.io/request-demo](https://wiretrace.io/request-demo) · or email sales@wiretrace.io