SECURE · WHAT IS CONNECTED, AND WHAT CAN REACH IT

What is on our network, and what can reach the systems that matter?

Before a maintenance window or an audit, managers need three answers: which devices are really connected, which have known weaknesses, and how an attacker could reach the systems that matter. Secure answers from what it hears on your own network.

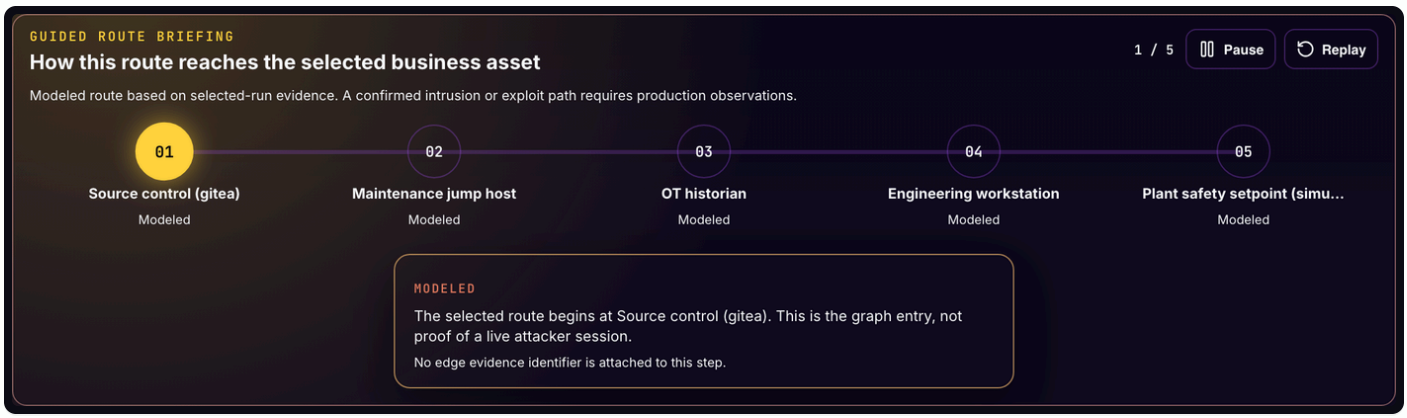
One company network, start to finish

Secure works by placing a small piece of listening software, called a collector, on a network you approve. It listens to the traffic and reports what it hears, and Secure turns that into a list of devices, each tied to the evidence behind it.

Secure comes with a practice company network built in, so you can watch it work before connecting it to anything real. There it found **29 devices**. 18 were already confirmed, and **11 were waiting** for a person to confirm them or send a technician to check, including one it could not name at all. It does not guess what software a device runs just because the device answers on the network.

It then compared those devices with public lists of known software flaws. Ten had possible matches, and two appear on the US government's list of flaws that attackers are already using, including a possible flaw in a security camera. Each stays **possible** until a person confirms that it really applies.

Finally, it drew how an attacker could move from one system to the next: in the practice company network, from the software team's code server through a maintenance computer and an operations records server to a safety control. Every step is marked as a model, not as something that happened.



The modeled route in the practice company network. Every step is marked “Modeled”.

Before your team makes a change, Secure can run it on a simulated copy of the network to show what else it would touch. It also helps plan for future quantum computers, which are expected to break some of today's encryption: you enter how long your data must stay secret, how long a changeover would take and when you expect the threat, and it shows which of your options leaves the fewest of those dates at risk.

It cannot prove it has found every device: it reports what its collector could hear. Your team makes every change.

Next: the manager guide tells the company's story in full, and the evaluation brief describes a four-week trial on your own network.