

Your security controls. Put to the test.

See how Reach finds gaps, fixes weaknesses, and strengthens your defenses.

Get hands-on with Reach in a dedicated tenant modeled to your tools, licensing, and priority security use cases.

Modeled to you

We shape the workshop around your tools and licensing.

Your use cases

Explore the scenarios and security stack your team actually cares about.

Nothing to connect

No integrations to stand up and no production data to hand over.

One to three hours

Run the workshop on site or online, whatever works best for your team.

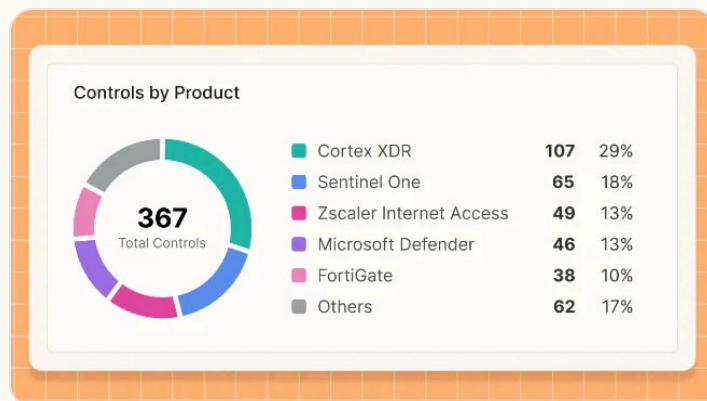
HOW IT WORKS

- 01 We start with a short scoping session to understand your security stack, priority use cases, and what you want to see from Reach.
- 02 Reach then creates a dedicated tenant modeled to those inputs and populated with synthetic data representative of the findings, drift, and security control scenarios teams encounter in production.
- 03 There is nothing to deploy or connect. Your team simply joins the session and starts exploring.

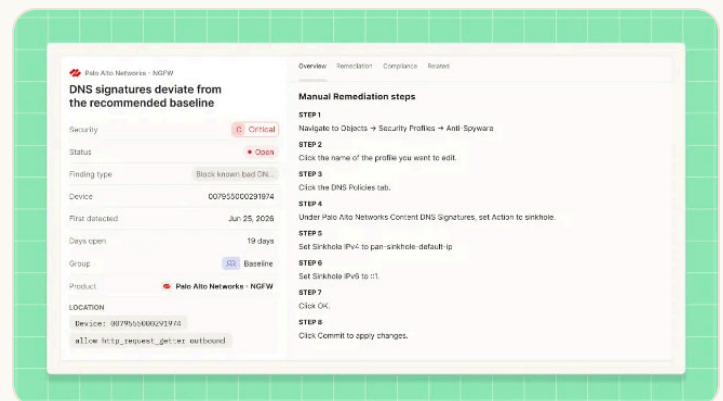
WHAT YOU GET

- 01 Understand how your security controls are protecting you and where weaknesses can emerge.
- 02 Identify, prioritize, and remediate control gaps before attackers can exploit them.
- 03 Detect configuration drift and continuously validate controls as your environment changes.
- 04 See Reach solve the security use cases that matter to your team in a hands-on environment.

INSIDE THE WORKSHOP



Reach shows all available security controls by product



Reach identifies a misconfiguration and recommends how to fix it

Put Reach to work on the security challenges that matter to you.

[Schedule a Reach Workshop](#)