PRODUCT OVERVIEW -- EARLY ADOPTER EARLY ACCESS DENSEDEFENSE | FORTESTRIKE

ForteStrike

A passing scan says a control is configured. It does not say it holds. ForteStrike runs the attack path against the systems you own and reports the real result, then retests to prove what is closed. In active development -- this is an overview of what it is for, not an API reference.

- Early Adopter -- in active development
- Scoped & authorized -- nothing runs outside a loaded scope policy
- Retest-to-prove -- a fix counts only when the attack no longer works
- API reference published at general availability

What this document is

STATUS

ForteStrike is an **Early-Adopter** product, in active development. There is no shipping public REST API yet, so an API reference would be premature. This page is a product overview: what it is for and where it fits.

SCOPE OF CLAIMS

This overview describes *purpose and intent*. Any run figures it mentions are **clearly-labeled demonstration values** from runs against systems we control -- not a shipped-product benchmark and not a claim about your environment.

WHAT COMES NEXT

Full API documentation and the operator manual will be published at general availability. Until then, contact us for early access to help shape it before it ships.

CONTENTS

1 What ForteStrike is
2 What it is for
3 Proof, not paperwork
4 Where it fits in the suite
5 Status & what comes next

1 | What ForteStrike is

ForteStrike is the DenseDefense suite's offensive console. The compliance engine scans and remediates your fleet and proves each control is configured; ForteStrike asks the next question -- does that control actually *hold* against someone trying to get through it? It is being built to run the real attack path against systems you own and report what an attacker would actually find.

The point is the retest. A finding is not closed because a report says it was remediated; it is closed when the same attack, run again, no longer works. ForteStrike is designed around that loop: attack, fix, attack again, and only then call it closed.

> **Tip --** This is an overview of a product in active development. It describes what ForteStrike is *for*. It is not an API reference, and nothing here is a claim that the product performs any of these functions against your environment today.

2 | What it is for

A compliance scan and an attacker look at the same host and see different things. The scan asks "is this control configured?" The attacker asks "can I get through it anyway?" ForteStrike is aimed at that gap -- the difference between configured and proven.

The engagement it is being built around walks a scoped path:

STAGE	WHAT IT IS FOR
Authorize & scope	Nothing runs until a scope policy is loaded. Scope is a fail-safe deny allow-list; anything not listed is blocked and logged. You cannot test what you never authorized.
Recon & scan	Find the hosts inventory forgot, then name every open port and the CVEs behind it -- with public-exploit availability flagged.
Validate	A non-destructive check per finding -- never a fired payload -- so a confirmed-exploitable result is evidence, not a guess.
Retest & report	Re-run the engagement after a fix and the report shows what is new, fixed, and still open. The retest is the proof; the report writes itself each run.

Note -- Positioning only. Each row states an *intended* stage for a product in active development, not a shipped feature list. Names and behavior may change before general availability.

3 | Proof, not paperwork

ForteStrike is being built to hold the suite's line: **documented is not the same as closed.** The design intent is that every confirmed finding carries the raw check output as evidence, that a lockdown of a confirmed-exploitable service is reversible and audited, and that a re-scan -- not a checkbox -- is what proves the exposure is gone.

Where the product shows run figures -- a rescan lift, a finding count, a critical count -- those are **demonstration values from runs against systems we control**, shown to illustrate the loop. They are not a benchmark of your environment, and they are not a claim of shipped capability.

Tip -- The whole reason ForteStrike exists is to replace "we remediated it" with "we attacked it again and it held." That is the difference an assessor can trust.

4 | Where it fits in the suite

ForteStrike is one member of the DenseDefense suite, alongside the compliance engine that scans and remediates against CMMC Level 2 / NIST 800-171, the data-discovery and AI-posture capabilities, and the evidence-and-custody layer beneath them. ForteStrike adds the independent proof that the controls the compliance engine configured actually stop an attacker.

ForteLock is ForteStrike's active-protect mode -- the same engine holding the line between engagements, reversibly containing new exposure as it appears. It is a mode of ForteStrike, not a separate product to license.

> **Tip --** Assess (the compliance engine) -> **prove (ForteStrike)** -> contain (ForteLock) -> attest (the custody layer). ForteStrike is the "prove it" step.

5 | Status & what comes next

ForteStrike is an **Early-Adopter** product, in active development. There is no shipping public REST API today, which is why this is an overview and not an API reference -- publishing an interface reference for a console still being shaped would be a promise it is not yet ready to keep.

- **Available now:** the early-access program. Contact us for early access to see the console take shape and to help steer what it covers first.
- **At general availability: full API documentation and the operator manual will be published** -- every route and every engagement stage, in the same detailed form as the rest of the suite's products.

> **Note --** Everything in this overview describes purpose and direction for a product in active development. Treat any capability named here as *not available today* for planning purposes, and confirm current status against the build you are offered.