

DeepShield: choose the protection model before making a production change

Understand the observation, response and operational-control options in a network that already has security tools.

Start with the existing environment

Most customers already operate firewalls, endpoint protection, logging and security monitoring. DeepShield is evaluated around the remaining operational question: can network events be recognized, investigated and handled consistently, with clear policy ownership and a useful audit trail? The first design session maps links, segments, critical assets and existing monitoring points. The objective is a controlled integration, rather than adding another unmanaged security console.

Separate observation from enforcement

In a first evaluation, observation and telemetry correlation can be assessed without modifying production packet flows. Any subsequent blocking or isolation belongs to a separately authorized change. The implementation plan identifies the control owner, approved action, exceptions, change window and tested return to the previous state. The architecture is selected according to the customer network, equipment and continuity requirements.

From event to decision

Consider a workstation repeatedly contacting an unusual destination. The evaluation follows the source event through asset identification, context enrichment, policy assessment, incident evidence and operational response. The same scenario is repeated with an authorized business exception, a loss of upstream connectivity and a false positive. The buyer can judge the workflow and the effect on real operations rather than a dashboard animation.

How an evaluation works

1. Define permitted visibility — Named sites, segments, telemetry sources and data minimization choices are recorded before collection.
2. Replay representative events — Compare the expected alert, analyst decision, evidence chain and false-positive handling with observed results.
3. Test safe operating boundaries — Review the authorized response, approval, operator override and restoration procedure.
4. Decide whether to expand — A written recommendation records fit, dependencies, gaps and next-stage acceptance conditions.

What your team receives

A bounded evaluation delivers a topology-and-integration note, the test and evidence register, a policy ownership matrix, a worked incident chronology and a decision on whether and how to proceed.

Send a procurement-ready request

I am evaluating DeepShield for [environment/sites]. Existing network controls: [tools]. Requested evaluation mode: observation / authorized enforcement. Critical assets and operating restrictions: [summary]. Please propose prerequisites, a technical evaluation scope, measurable tests and an itemized quotation.

sales.shield@deepinfosec.com