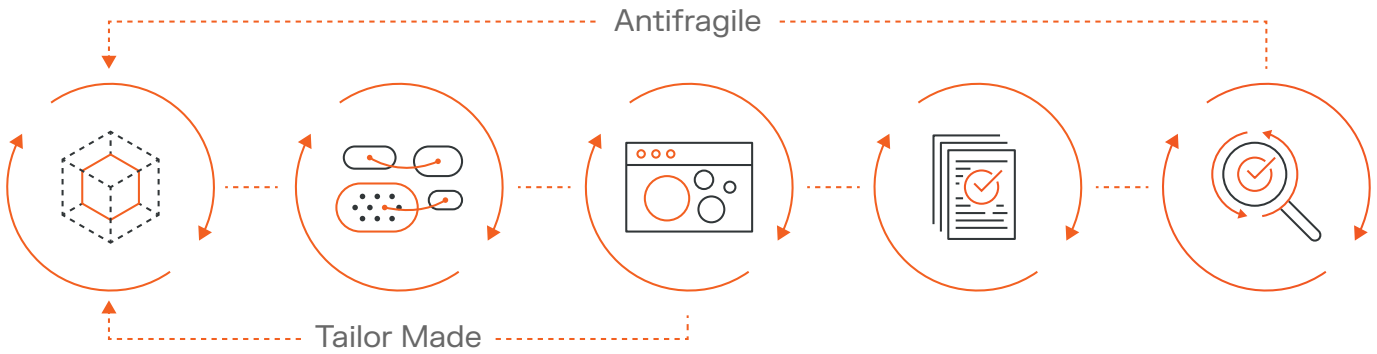
Five Steps to Deploying Zero Trust

illumio

A practical roadmap to modern cybersecurity

Few ideas redefine an entire industry. Zero Trust is one of them. Since John Kindervag introduced it in 2010, the once-radical notion has become the benchmark for modern security strategies and a cornerstone of national and international policy. It has transformed boardroom priorities, giving organizations a clear framework to reduce complexity and strengthen defenses where it matters most.

To make Zero Trust actionable, Kindervag developed this clear five-step model, built on years of experience, turning the vision into a repeatable practice.



	Define the Protect Surface	Map the Transaction Flows	Build a Zero Trust Architecture	Create Your Zero Trust Policy	Monitor and Maintain the Network
Goal	Decide what absolutely must be defended — The DAAS elements: data, applications, assets, and services.	Understand how the Protect Surface interacts with the rest of the environment.	Design a Zero Trust architecture tailored to each Protect Surface.	Establish least-privilege access for the Protect Surface.	Continuously strengthen the Zero Trust architecture.
Action	Identify and prioritize a single DAAS element and define it as a Protect Surface. Start small; don't try to protect everything at once. The output is a concise, prioritized list of Protect Surfaces.	Map the transaction flows to and from the Protect Surface, documenting source, destination, ports, protocols, direction, and business purpose. This creates a living map that ensures Zero Trust controls support (not disrupt) operations.	Use the mapped flows to place controls as close to the Protect Surface as possible. This could include micro-perimeters, segmentation boundaries, identity integrations, and inspection points. Treat every Protect Surface as bespoke architecture.	Write Zero Trust policies using the Kipling Method, answering the 5Ws (who, what,when, where, why/how). Define exactly which person or non-person entities may access the Protect Surface and under what conditions. Enforce these as allow/deny rules; deny everything not explicitly permitted.	Inspect logs, telemetry, and enforcement results to confirm the policy is working as intended. Treat every incident or near-miss as an input to refine the Protect Surface and steps 1-4. Done right, Zero Trust accelerates from resilience to antifragility.
Benefit	Shrinks the problem from infinite attack surface to finite Protect Surface.	Provides clarity, visibility, and context so that controls support the business instead of disrupting it.	Reduces lateral movement and limits the blast radius of any breach.	Ensures all access is authorized, verified, necessary, and appropriate.	Creates a measurable defense that adapts to change and gets stronger with every iteration.

Zero Trust is no longer optional; it's the industry standard. John Kindervag's five-step model gives you the map to build it in your own environment. Start small, build momentum, and watch your defenses get stronger with every step.