

EXECUTIVE ADVISORY

Threat Modeling & Architecture Blueprints

Design Security Into the Architecture Before Risk Becomes a Backlog

Security architecture should be a blueprint, not a backlog. The most effective controls are designed around the threats that matter before systems are deployed.

01 — THE CHALLENGE

Many organizations add security after systems are built. Engineering moves quickly, architecture evolves, and security teams are left managing vulnerabilities and compensating controls that could have been addressed through better design decisions.

The result is technical debt, fragmented controls, and architectures that are difficult to explain, defend, or scale.

02 — WHY ARCTIQ

Arctiq brings security into the design conversation before code ships and before technology decisions become difficult to reverse.

Our Threat Modeling and Architecture Blueprint engagements model threats against applications, platforms, and business processes, then translate those threats into clear control requirements. We create engineering-consumable artifacts including data flow diagrams, trust boundary maps, and threat-to-control mappings.

For broader architecture initiatives, Arctiq develops target-state security blueprints aligned to the client's cloud, platform, identity, data, and operational environment. The goal is not attestation. The goal is better design.

03 — ADVISORY CAPABILITIES

-  Application, platform, and business process threat modeling
-  Data flow diagrams and trust boundary mapping
-  Threat-to-control mapping
-  Zero trust and conditional access patterns
-  PAM and workload identity architecture
-  Microsegmentation, SASE, and ZTNA design
-  Data classification, DLP, encryption, and tokenization patterns
-  SIEM, EDR, identity, and cloud telemetry architecture
-  Backup immutability and isolated recovery architecture
-  NIST CSF 2.0 and client reference architecture alignment

PATTERNS & FRAMEWORKS

NIST CSF 2.0

Zero Trust

SASE

ZTNA

PAM

DLP

Microsegmentation

04 — BUSINESS OUTCOMES

 Organizations gain:

- ✓ Security requirements defined earlier in the development lifecycle
- ✓ Build-ready architecture specifications
- ✓ Reduced reliance on compensating controls
- ✓ Clearer security boundaries and trust relationships
- ✓ Stronger alignment between security and engineering
- ✓ Architecture that security teams can defend and engineering teams can build

05 — WHY IT MATTERS

Security decisions become more expensive and disruptive when they are made after deployment. Arctiq helps organizations design controls into the architecture from the beginning, reducing risk and creating a more defensible technology foundation.

[Book an architecture workshop →](#) www.arctiq.com