Good Security Architecture Begins With Better Questions

By: Jaiz Anuar

24 July 2026 · Cybersecurity · Security Architecture · 9 min read

Good security architecture begins by challenging the assumptions behind trust, access, data flows, controls and recovery.

Architecture diagrams often look convincing. They contain labelled systems, network zones, firewalls, cloud platforms, authentication flows and encrypted connections. But a diagram can be technically complete and still leave important risks unanswered.

A good review should not begin by asking only whether there is a firewall, MFA or encryption. It should challenge assumptions: what is being trusted, why is trust necessary, what crosses each boundary, can controls be bypassed, who notices when something fails and how does the business recover?

Connectivity Does Not Explain Trust

An arrow between systems shows communication exists. It does not explain whether communication should be allowed. Connections may be encrypted and boundaries protected, yet questions remain about initiation, data transferred, continuous access, production reachability and the consequences of compromise.

As discussed in Most Architecture Diagrams Show Connectivity. Few Show Trust and Controls, connectivity is not trust. A line should represent a deliberately approved relationship, not merely technical reachability.

What Are We Actually Protecting?

Security teams often begin with controls before understanding the asset. Before deciding on controls, architects should ask what information a system processes, how sensitive it is, where copies are stored, who can access it, how long it is retained and what happens if it is exposed or modified.

Security architecture becomes meaningful when it connects technology decisions to business consequences. This is why Security Architecture Protects the Business; Security Controls Protect the Technology.

Where Does Trust Begin and End?

Network location, an approved subscription or SSO authentication are not sufficient proof of trust. An authenticated user may have excessive access, a workload may be compromised and a valid session token may be stolen.

Better questions concern explicit authorisation, device compliance, MFA for sensitive activity, post-authentication authorisation, privileged identities, vendor access and governance of service

accounts. As explained in The New Security Perimeter Is No Longer the Network. It Is Identity, trust must be based on identity, device posture, permissions, context and continuous verification.

Can the Control Be Bypassed?

The presence of a control does not prove the architecture is protected. A WAF has limited value if another endpoint remains direct; MFA can be bypassed by local accounts; segmentation fails when broad rules permit unrestricted communication.

Every control should be challenged: can traffic bypass inspection, are exceptions permanently open, does it cover service identities, is it blocking or monitoring only, who reviews alerts and has it been tested against a realistic attack path?

Cybersecurity Best Practice Is a Baseline, Not a Blueprint. The objective is to understand risk and choose controls that genuinely reduce it in the actual environment.

What Happens When the Design Fails?

Architecture reviews often focus on normal operation. Attackers focus on failure: unavailable identity providers, failed cloud connections, compromised servers, stolen credentials and cross-environment movement.

Security architecture must consider failure paths, backup integrity, restoration testing, detection and containment. The Best Security Architects Know How Systems Break because defendable architecture is built by understanding how trust can fail.

Better Questions Do Not Block Modernisation

Challenging architecture does not mean rejecting it. It helps organisations modernise with confidence by making trust deliberate, access limited, data governed, controls difficult to bypass, suspicious activity detectable and recovery possible.

Final Thought

Architecture diagrams show how systems are expected to work. Security architecture must show what happens when identities are compromised, controls fail, connections are misused and trusted components behave unexpectedly.

The quality of architecture is measured by the quality of questions it can answer. Good security architecture begins with better questions.

Question assumptions. Share knowledge. Build trust.