Zero Trust Is Not About Trust. It Is About Reducing the Cost of Being Wrong.

By: Jaiz Anuar

4 July 2026 · Cybersecurity · Zero Trust · Digital Trust · 8 min read

Few ideas in cybersecurity are as widely adopted—and as widely misunderstood—as Zero Trust. Ironically, the misunderstanding begins with its name.

When people hear the words Zero Trust, they often imagine an organisation that trusts nobody. Employees assume it means management distrusts them. Executives believe it requires buying another security platform. Technical teams reduce it to implementing multi-factor authentication or deploying a Zero Trust Network Access (ZTNA) solution.

None of these interpretations capture the real purpose of Zero Trust.

Zero Trust is not an architecture built on distrust. It is an architecture built on humility.

It begins with a simple acknowledgement: every trust decision, regardless of how confident we are, carries the possibility of being wrong.

The Problem Is Not Trust

Trust is essential for every organisation. Businesses cannot function without trusting employees, customers, suppliers, partners, cloud providers, software vendors, and increasingly, artificial intelligence.

The real problem is not that trust exists. The problem is assuming trust will always remain valid.

An employee can become the victim of phishing. An administrator can make a mistake. A trusted supplier can be compromised. A laptop can become infected. A software update can introduce malicious code. An AI agent can be manipulated into performing actions beyond its intended purpose.

None of these situations necessarily involve malicious insiders. They simply demonstrate that today's trusted identity may become tomorrow's attack path.

Zero Trust acknowledges this reality.

Every Trust Decision Is A Risk Decision

Every time a system grants access, it makes a judgement. Every firewall rule, every privileged role, every API token, every VPN session, every service account, and every authentication request represents a decision to trust.

Most organisations focus on making better trust decisions. Zero Trust asks a different question.

What happens when the decision is wrong?

This subtle shift changes everything.

Instead of trying to build perfect confidence in every decision, Zero Trust focuses on limiting the consequences when confidence turns out to be misplaced.

Reducing The Cost Of Being Wrong

Imagine an employee successfully authenticates using multi-factor authentication. Most organisations would consider the authentication successful and proceed to grant access.

But authentication answers only one question.

Who are you?

Zero Trust continues asking questions.

Is the device healthy? Is the session behaving normally? Does this user still require this level of privilege? Is this request consistent with previous behaviour? Has anything changed since access was first granted?

The objective is not to eliminate trust. The objective is to minimise the damage when trust becomes invalid.

Least privilege limits unnecessary access. Micro-segmentation limits lateral movement. Continuous verification reduces the lifetime of incorrect assumptions. Just-in-time access limits unnecessary standing privileges. Behaviour analytics identifies when trusted identities begin behaving differently.

Every one of these controls serves the same purpose. Reduce the cost of being wrong.

The Biggest Mistake About Zero Trust

Perhaps the biggest misconception is believing Zero Trust begins with technology.

Many organisations proudly announce their Zero Trust journey after deploying a new ZTNA solution or modern identity platform. Those technologies are valuable. But they are not Zero Trust.

Replacing a VPN with ZTNA does not automatically eliminate excessive privileges. Implementing MFA does not prevent credential theft. Deploying identity governance does not stop poor security architecture.

Technology enables Zero Trust. It does not define it.

Zero Trust is first a way of thinking. Architecture comes afterwards.

Zero Trust Is No Longer Only About People

For years, cybersecurity focused primarily on human identities. Today, organisations manage APIs, workloads, service accounts, bots, machine identities, and AI agents that often possess privileges exceeding those of human users.

Should these identities be trusted simply because they belong to the organisation?

The answer remains the same. Trust should never become permanent simply because it was once justified.

Machine identities deserve the same continuous verification as human identities. Perhaps even more.

Questions Worth Asking

Are we continuously verifying trust, or only authenticating once?

How much access do users retain after their business need has changed?

If an administrator's account were compromised today, how much damage could it cause before detection?

How many service accounts possess privileges that nobody has reviewed in years?

Have we reduced risk, or merely changed the technology performing the authentication?

Does our Zero Trust strategy include APIs, workloads, and AI agents—or only employees?

Final Thought

The phrase "Never Trust, Always Verify" has become the unofficial slogan of Zero Trust. It is memorable. But it is also incomplete.

Perhaps the better description is this:

Trust when necessary. Verify continuously. Assume every trust decision can eventually become wrong.

That is not paranoia. It is engineering.

Cybersecurity is not about eliminating trust. It is about designing systems that continue to protect the organisation when trust inevitably fails.

Because in cybersecurity, the most expensive mistake is rarely trusting someone. The most expensive mistake is assuming that trust can never be wrong.