CREST. Accredited

certin Empanelled

5 Mistakes That Break Zero Trust Implementation

Zero Trust isn't a checkbox or software license; it's a living security philosophy.

Swipe to explore

sales@briskinfosec.com

1 Trusting Internal Traffic by Default

Mistake:

Assuming that anything inside the corporate network is “safe.”

Fix:

Apply micro-segmentation and identity verification even for east-west (internal) traffic. Use strong network policies and device identity for every request.

Example:

An attacker phishes an employee, gains VPN access, and moves laterally across internal servers because internal traffic isn’t authenticated again.

sales@briskinfosec.com

2 Inconsistent Identity & Access Policies

Mistake:

Different apps, clouds, or departments using separate IAM setups.

Fix:

Centralize identity with SSO and MFA across all environments. Implement conditional access such as blocking access from unknown devices or locations.

Example:

A company using Azure AD for corporate logins but local accounts for AWS leading to forgotten credentials and inconsistent MFA rules.

sales@briskinfosec.com

3 Ignoring Device Posture and Health

Mistake:

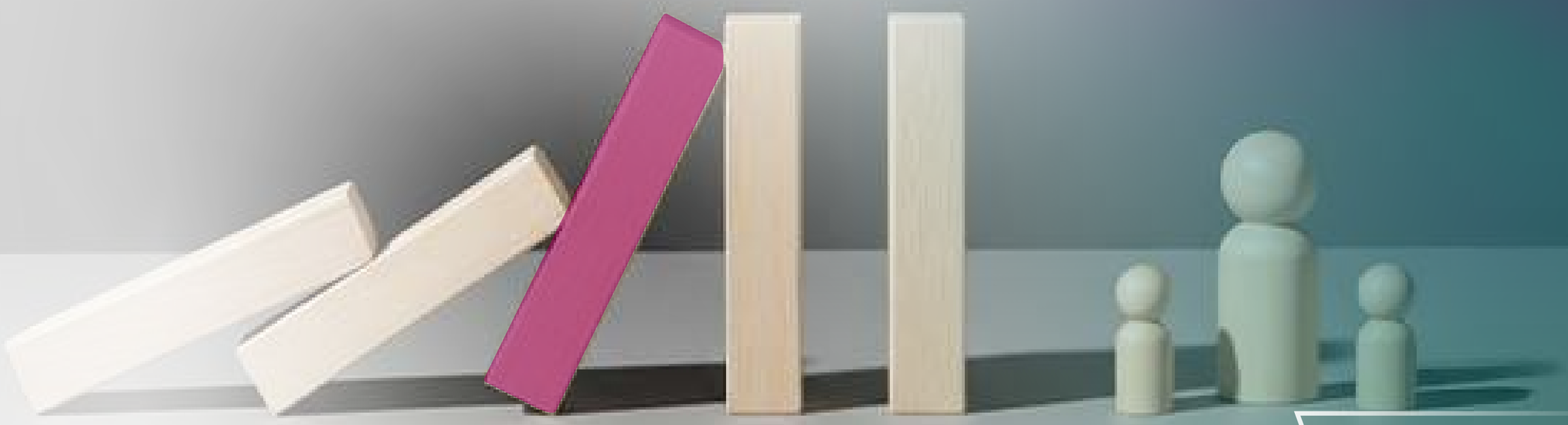
Only verifying who logs in, not what they log in from.

Fix:

Integrate MDM or endpoint posture checks. Allow access only from compliant devices with updated OS, encryption, and EDR protection.

Example:

An employee connects from a personal laptop infected with malware. Though credentials are valid, the device becomes a backdoor for attackers.



sales@briskinfosec.com

4 Skipping Continuous Monitoring & Adaptation

Mistake:

Treating Zero Trust as a “set and forget” configuration.

Fix:

Implement continuous anomaly detection, UEBA (User and Entity Behavior Analytics), and adaptive policy updates based on risk scores.

Example:

A user’s account suddenly downloads 5GB of data at 2 AM from a new location, but no alert triggers because monitoring is static.

sales@briskinfosec.com

5 Focusing Only on Technology, Not Culture

Mistake:

Deploying advanced tools but skipping user education.

Fix:

Conduct regular awareness sessions. Make Zero Trust principles part of employee KPIs and daily security hygiene.

Example:

Despite having Zero Trust controls, an employee shares access credentials via email to “speed up work.”

sales@briskinfosec.com

Is Your Zero Trust Model Truly Zero?

Let our experts assess your security posture and uncover trust gaps before attackers do.

BOOK A MEETING

BriskInfosec™

sales@briskinfosec.com