Zero Trust - what it is, why it helps, and simple steps to start verifying every access

Gridinsoft Help Center

What it is

Zero Trust is a security approach that treats every request as untrusted until it is verified. It checks the user, the device, and the request each time - even inside your own network - instead of assuming "inside = safe." Quick explainer and examples: https://gridinsoft.com/zero-trust

Why it matters

Phishing, stolen passwords, and infected devices can slip past old perimeter rules. By verifying every step, Zero Trust limits what an attacker can do if they get in.

How it works

- Verify identity: strong sign-in with MFA or passkeys every time it matters.
- Check the device: only allow access from healthy, updated devices.
- Least privilege: give just the access needed, for just as long as needed.
- Segment: keep apps and data in small zones so one breach does not spread.
- Watch and react: log activity, spot odd behavior, and block fast.

Red flags

- One password opens many critical apps without extra checks.
- Old laptops or phones with no updates still have full access.
- Shared admin accounts or always-on VPNs with broad reach.
- No logs or alerts to show who accessed what and when.

Do it right

- Turn on MFA for email, cloud storage, banking, and admin tools.
- Use device health rules: updated OS, disk encryption, screen lock.
- Give people the minimum access they need and review it often.
- Split networks and apps into smaller zones.
- Monitor sign-ins and unusual downloads, then tighten policies based on what you see.