Killware - What it is, how it causes real-world harm, and how to prevent it

Gridinsoft Help Center

What it is

Killware is a cyberattack designed to cause real-world harm. Instead of only stealing data or money, attackers aim to disrupt systems people rely on - power, water, hospitals, transport - so failures can lead to injuries or loss of life.

Why it matters

Modern infrastructure is deeply connected. A successful digital hit on operational tech can shut down care, delay responders, or taint supplies, turning a keyboard attack into a physical emergency.

How it works - quick tour

- Ransomware or wipers cripple critical systems to force downtime
- Access to OT/ICS through flat networks or weak remote access
- Supply chain compromises push malicious updates into trusted systems
- Data tampering alters sensor readings or alarms so operators act on lies

What to watch for

- Simultaneous outages across dependent systems
- Sudden loss of visibility into sensors or alarms
- Unexplained configuration changes on PLCs, HMIs, or gateways

If you suspect it - first moves

- Protect people first - fail safe to manual procedures.
- Isolate affected networks and switch to known-good backups.
- Engage incident response and regulators - preserve logs and images.
- Segment and verify before bringing systems back online.

Prevent it

- Separate IT and OT networks with strict segmentation and one-way gateways where possible
- Enforce MFA, least privilege, and monitored remote access
- Patch internet-facing assets fast and harden vendor connections
- Continuously monitor OT with anomaly detection and tested runbooks

- Run regular drills that include safety, clinicians, and operators