Data Exfiltration: What it is, warning signs, and how to stop data from leaving your network

Gridinsoft Help Center

What it is

Data exfiltration is the unauthorized transfer of your data out of your device or network-quietly slipping customer records, passwords, designs, or finances to an attacker. It’s the punchline of many breaches: get in, get data out, cash in.

Why it matters

Stolen data fuels identity theft, fraud, and extortion (including "double-extortion" ransomware). Even small leaks can trigger fines, lost customers, and public trust damage.

How attackers pull it off

- Malware & ransomware: plant stealers, then zip and send files out.
- Phishing & social engineering: trick users into uploading or sharing.
- Abused access: compromised accounts, API tokens, or misconfigured cloud storage.
- Covert channels: HTTPS to look legit, DNS/HTTP beacons, cloud drives, or personal email.

Signs to watch

- Repeated outbound connections to odd domains/IPs, especially at night
- Sudden spikes in upload traffic or big archives leaving the network
- New mail forwarding rules, unknown OAuth app connections
- Security tools disabled, or logs conveniently missing

If you suspect a leak

- Isolate affected systems; preserve logs and memory-don’t wipe yet.
- Block destinations (domains/IPs/accounts) and kill suspicious sessions/tokens.
- From a clean device, rotate credentials and keys (admins, APIs, cloud).
- Start scope & impact: what data, whose data, how much, and when.
- Engage IR/Sec and notify stakeholders; follow legal/regulatory steps.

Prevent it

- MFA everywhere; least-privilege access and regular access reviews.
- Patch fast on internet-facing apps; monitor endpoints with EDR.
- Encrypt sensitive data at rest and in transit; disable public buckets/shares.

- Egress controls: DNS filtering, proxy allowlists, DLP rules for uploads and email.
- Detect early: alerts for large downloads, mass file access, new forwarders/OAuth apps.
- Train people: verify unusual data requests out of band; beware of urgent "executive" asks.