GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

D

Data Exfiltration: Methods, Detection, Prevention, and Response

Data exfiltration is an unauthorized transfer of data to a location or party outside the owner’s control. It may involve an external attacker, insider, malware, or stolen account.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	3 min

Data exfiltration is the unauthorized transfer of data to a location, system, account, or person outside the owner's control. An external attacker, malicious insider, compromised account, malware, or abused application can perform it.

Data leakage may be accidental, such as an incorrectly shared cloud folder. A **data breach** is the broader security incident in which protected data is accessed, disclosed, altered, or lost. Exfiltration is one possible breach action; not every breach includes a confirmed transfer.

How exfiltration may develop

1. **Access:** an attacker compromises an identity, endpoint, application, cloud resource, or trusted partner.

2. **Discovery and collection:** data stores, permissions, backups, messages, secrets, and high-value records are located.
3. **Staging:** files may be queried, copied, archived, compressed, split, encoded, or encrypted.
4. **Transfer:** data leaves through a direct connection, legitimate service, removable media, messaging, email, API, or covert channel.
5. **Concealment or impact:** logs may be altered, staging files deleted, or the theft combined with ransomware and extortion.

Common transfer channels

- HTTPS uploads, cloud storage, code repositories, collaboration tools, and personal webmail;
- stolen SaaS sessions, OAuth applications, API keys, database exports, and backup access;
- DNS tunneling, remote-access tools, command-and-control channels, and encrypted archives;
- USB storage, phones, printing, screenshots, cameras, and copied paper;
- mailbox forwarding, messaging bots, automated reports, and misconfigured public shares.

Encryption makes content inspection harder but is normal for legitimate traffic. Detection needs identity, endpoint, data, application, and network context rather than volume alone.

Evidence and detection ideas

- bulk reads, searches, exports, or archive creation unusual for the identity and role;
- large, repeated, or low-and-slow outbound transfer to a new destination;
- new OAuth grants, API tokens, mail rules, shared links, repositories, or cloud synchronization;
- sensitive files copied to removable media or accessed from an unmanaged device;

- DNS query length or frequency, egress protocol, or destination inconsistent with normal service;
- staging followed by deletion, log gaps, endpoint tampering, or account privilege changes.

A large upload can be a backup, software release, video call, or approved migration. Confirm who initiated it, what data was accessible, the destination owner, business approval, and the original records.

Response workflow

1. Preserve endpoint, identity, data-access, cloud, proxy, DNS, network-flow, email, DLP, and application evidence.
2. Contain the narrow transfer path: revoke affected sessions and keys, isolate a host, suspend a malicious share, or block a verified destination.
3. Identify the source account or process, initial access, staging location, time range, and related systems.
4. Determine which specific records were accessed and what evidence supports actual transfer. Do not equate access permission with confirmed theft.
5. Remove persistence, rotate exposed secrets, close the entry path, and monitor for another channel.
6. Engage privacy, legal, regulators, insurers, customers, and law enforcement according to applicable requirements and verified facts.

Prevention and preparation

- classify sensitive data, minimize retention, and restrict access by role and device;
- use phishing-resistant MFA, access reviews, strong offboarding, and managed service identities;
- control exports, removable media, external sharing, OAuth consent, API tokens, and unmanaged synchronization;

- apply DLP, endpoint, cloud, email, egress, and behavior monitoring to defined high-risk use cases;
- protect logs and test runbooks for insider, cloud, endpoint, and ransomware scenarios.

Reference: Canadian Centre for Cyber Security: Defending against data exfiltration.

Data exfiltration FAQ

Does encryption at rest stop exfiltration?

It protects storage media, but an authorized or compromised application may decrypt data during normal access. Control identities and exports too.

Does a failed upload mean no data left?

Not necessarily. Review retries, alternate channels, partial transfer, destination records, and prior activity.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com