What is data exfiltration?

Data exfiltration is the unauthorised copying or transfer of data out of your environment to a place an attacker controls. It is the goal of most targeted attacks and usually the final stage, after an intruder has gained access and found what is worth taking. It can be fast and loud or slow and stealthy, and it is defended by controlling where data lives, who can reach it, and what is allowed to leave your network.

HOW IT WORKS

01 The channels attackers use

Data leaves by whatever path is open and least watched:

- Web traffic (HTTPS) to a server the attacker controls, blending in with normal browsing.
- DNS tunnelling, encoding data into DNS lookups that firewalls rarely inspect.
- Cloud storage and personal accounts, uploading to a personal drive or a bucket the attacker owns.
- Email, forwarding or attaching sensitive files to an outside address.
- Removable media, copying to a USB drive, which is common for insiders.
- Legitimate tools, using the same file-transfer and admin utilities your team uses, so nothing looks out of place.

02 Why it is hard to catch

Modern exfiltration is built to hide. The traffic is usually encrypted, so its contents cannot be read in flight. It often goes out slowly, in small chunks over days, to stay under volume alarms. And it rides normal channels, so it looks like the HTTPS, DNS, and cloud uploads your business does all day.

This is why simply having a firewall is not enough. Catching exfiltration takes knowing your normal baseline, watching the paths data leaves by, and alerting on the anomalies rather than the payload.

> ENCRYPTION IS NOT A DEFENSE HERE
>
> *Encrypting data at rest protects a lost laptop or a stolen backup. It does nothing against an attacker who has valid access and can read the data before copying it out.*

HOW TO DEFEND

- Know where your sensitive data lives and cut down how many places hold it. Less spread is less to steal.
- Enforce least privilege so a single compromised account can reach only a slice of the data.
- Control egress: restrict outbound traffic and destinations, and watch DNS.
- Deploy data-loss prevention (DLP) on the paths data actually leaves by (email, file sharing, endpoints).
- Monitor and baseline so an unusual transfer raises an alert while it is happening.

SOURCES

[1] Exfiltration (Tactic TA0010)

[2] Cyber Threats and Advisories

[3] Data Breach Investigations Report

03 Exfiltration by insiders

Not all exfiltration is an outside intruder. A departing employee emailing customer lists to a personal account, or copying source code to a USB drive, is exfiltration too, using access they were legitimately given.

Insider exfiltration is harder to spot because the access is expected. The signals are behavioural: someone touching data they do not usually touch, large downloads before a resignation, or transfers to personal accounts. Least privilege, access reviews, and monitoring of sensitive data are the practical defenses.

Find out whether an attacker could reach, and remove, your data.

securelayer7.net/learn/threats/data-exfiltration

Open online