RESOURCE CENTER

What is data exfiltration?

Get the full interactive view at
https://bitwarden.com/nl-nl/resources/what-is-data-exfiltration/

bitwarden

Understanding data exfiltration: A guide for tech leaders

Data exfiltration can cause major financial, legal, and reputational damage, from leaked customer information to stolen trade secrets. This guide helps technology leaders understand what data exfiltration is, why it matters, and how to prevent it with practical, real-world strategies like continuous monitoring, employee training, and access control.

What is data exfiltration?

At its core, data exfiltration refers to the unauthorized transfer of data from your network. Often, the person stealing the data does so quietly and with malicious intent, like selling, exploiting, or using the information to cause further damage.

This type of breach can involve:

- Personal customer information
- Internal business documents
- Intellectual property, such as product designs or code

Not all data exfiltration is malicious. In some cases, unintentional exfiltration occurs when employees send sensitive data to personal email accounts or upload files to unsanctioned cloud services. Negligent exfiltration can result from misconfigured permissions, overly broad access rights, or poor security habits, leading to accidental exposure or unauthorized downloads. Regardless of intent, the result is the same: sensitive information leaving the organization and increasing its exposure risks.

Data can be exfiltrated in many ways, including through email, cloud storage platforms, or removable devices. In other words, it's a digital break-in. The goal isn't just to gain entry, but to take something valuable on the way out. That's why it's critical to monitor how data moves across systems. When organizations understand how attackers operate and where vulnerabilities exist, they're better prepared to implement safeguards and protect sensitive assets.

Preventing data exfiltration starts with a well-rounded strategy. This includes deploying data loss prevention (DLP) tools, performing regular security audits, and training employees to handle sensitive information responsibly. Since threats can come from multiple sources — including insider actions, human error, or technical gaps — strong access controls and layered security practices are essential to reducing risk.

Why it matters

When data is exfiltrated, it puts an entire business at risk. Enterprise data breaches frequently involve some form of exfiltration. Whether discovered quickly or after months of dwell time, the consequences are real: lost trust, financial penalties, and operational disruptions.

For regulated industries, the stakes can be even higher. Noncompliance with privacy laws or security frameworks (like GDPR, HIPAA, or PCI DSS) can result in fines, investigations, or reputational fallout.

As a tech leader, staying ahead of these threats helps protect company data and the people who rely on it, including customers, partners, and employees.

Exfiltration vs. infiltration

Infiltration is when a bad actor gets inside a system, like a hacker breaking into a computer or exploiting a network vulnerability. Exfiltration is what happens after: they take the data and get out.

Think of it as the difference between sneaking into a building and stealing a file from a locked cabinet once you're inside.

What kind of data gets targeted?

Cybercriminals don't just want "data," they want data with value. That often includes:

- **Intellectual property** – Product designs, source code, formulas, or engineering blueprints. Losing this kind of data can adversely impact revenue, R&D investments, and marketing positioning.
- **Customer information** – Names, addresses, Social Security numbers, or credit card details can be sold or used for fraud, identity theft, or phishing. When this kind of data is exposed, privacy violations and regulatory consequences often follow.
- **Trade secrets** – Internal strategies, product roadmaps, supplier agreements, and confidential communications can reveal competitive advantages or weaken negotiating power.

Techniques used by attackers

Cybercriminals continue to evolve their techniques. Some exfiltration methods are straightforward, like emailing a file or uploading it to cloud storage. Others are more covert. For example:

- Embedding data within images using steganography
- Using custom malware to exfiltrate data in small, unnoticed packets
- Leveraging legitimate tools like remote desktop software

Regardless of methodology, the goal is the same: to remove sensitive data without detection.

Preventing data exfiltration

Prevention starts with:

- Limiting who can access what data based on roles and responsibilities
- Monitoring systems and endpoints for unusual behavior or access patterns
- Training employees to recognize phishing attempts and other suspicious activity
- Using tools like Data Loss Prevention (DLP) systems, Endpoint Detection and Response (EDR), and CAST (Cloud Access Security Broker) solutions
- Encrypting data at rest and in transit

Building multiple layers of defense ensures that even if one control fails, others remain in place to stop or slow exfiltration attempts.

Meeting legal and compliance expectations

Regulations like GDPR, HIPAA, and PCI DSS are designed to protect sensitive data, and organizations are expected to meet their requirements. Preventing data exfiltration is critical to staying compliant and avoiding legal exposure.

Following security standards such as NIST, ISO 27001, or CIS Controls enables a strong foundation for compliance and risk mitigation. Aligning with these frameworks also gives technology leaders confidence when collaboratingrisk with legal, executive, or regulatory teams.

Bitwarden: A trusted ally in data protection

Understanding data exfiltration is the first step in defending against it. The next step is putting the right tools in place.

Bitwarden helps organizations take control of who has access to what. By securely managing passwords, enforcing multi-factor authentication, and simplifying access controls, Bitwarden reduces the risk of stolen credentials — a common starting point for exfiltration.

Bitwarden supports a strong security posture, whether you're protecting a global business or helping a startup scale securely. It's a vital part of keeping sensitive data exactly where it belongs: safe and in your hands.