Is data leaking out on your watch?

What you need to know about data exfiltration

We asked **522** IT security professionals from around the world about their experience with data loss.[1]

Security pros have faced an average of

6 BREACHES

over the course of their careers.

2/3 Two-thirds of those required **public disclosure**.

WHO WANTS THE DATA?

Breaches are initiated by:

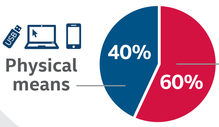
Internal actors 1/2 are **intentional**, 1/2 are **accidental**.

External actors

WHAT DATA DO THIEVES WANT?

1. Customer information
2. Employee information
3. Intellectual property
4. Credit card information

HOW ARE THIEVES GETTING DATA OUT?



Physical means

Electronic means

WHAT TACTICS ARE THIEVES USING?

Top ways to disguise theft:

32%	Encryption
22%	Compression
15%	Obfuscation
15%	Chunking

Favorite file types to steal:

1. Microsoft Office
2. .txt/.csv
3. .pdf

WHERE IS DATA BEING TAKEN FROM?

2/3 of breaches occur on traditional networks.

1/3 occur in cloud infrastructures.

DLP: STOP BREACHES BEFORE THEY HAPPEN.

Almost **70%** of surveyed security pros felt that data loss prevention (DLP) technology could have prevented previous data exfiltration events.

Don't lose data on your watch.

Learn more about McAfee® Total Protection for Data Loss Prevention: **www.mcafee.com/dlp**

See the complete survey results in the data exfiltration report: **www.mcafee.com/dataexfiltration**

[1] Intel Security survey of 522 IT security professionals. Only respondents who experienced a data breach were included in the survey.

Intel and the Intel and McAfee logos are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. Copyright © 2015 McAfee, Inc. www.intelsecurity.com 62109info_dlp-exfiltration_1015

intel Security

McAfee is part of Intel Security.