



Rethinking Data Loss Prevention

A Simple Introduction to Proofpoint Information Protection

Andrew Chisholm – Proofpoint Principal Information Protection Specialist APAC



Why are we here?

Voice of the CISO

The top targets....

1. Healthcare (**89%**),
2. Media/entertainment (**88%**)
3. Financial services (**83%**) and
4. Transport (**80%**)

95 %

of CISOs have lost data with an employee leaving their organisation.

Can we quantify the cost?

Cost of a breach outstrips the cost of protections

- **Costs of AUD \$46.4m in year 1**

- comprised \$22 million of administration expenses,
- \$15.6 million in employee benefits expenses,
- \$7.5 million in extra tech, and \$1.2 million in marketing

- **Increased by AUD \$35m+ the following year**

- further IT security uplift, legal costs, regulatory investigations and litigation

- Roughly **\$20k per person** affected = **AUD \$9.7m**

medibank

The October 2022 breach occurred when attackers obtained the credentials of a third-party contractor, resulting in the leaking of customer data.



Operating Traditional DLP

33% detection rate of data loss incidents

50% more alerts to manage

2.5x longer time to triage incidents

....Why does content based DLP
struggle to show value?

Legacy DLP Problems

Classification Focused

High False positives

High Analyst workload – limited results

Agent performance problems

No Human Risk Insight

Why is human Risk Insight Important

Data doesn't lose itself...People Lose it

82 %

of breaches involved a human element*

44 %

of insider incidents involved malicious and compromised users**

74 %

of CISOs consider human error to be their organization's biggest cyber vulnerability***

* Verizon. "2022 Data Breach Investigations Report."

** Ponemon. "2022 Cost of Insider Threats Report"

*** Proofpoint "2024 Voice of the CISO"



Negligent users may make an honest mistake or try to take a shortcut to do their jobs.



Compromised users may have their accounts taken over and misused by an outside cyber attacker.



Malicious users can intentionally exfiltrate data for personal gain.

You can't protect if you don't know!

Data loss prevention

Reinvent your data loss prevention program for the digital workplace



Email



Cloud



Endpoint

Insider threat management

Secure your organization from within



Anomaly Detection



Behavioural Context

CONTENT

INTENT

CHANNELS

WHAT?

WHY?

HOW?

How does Human Behavioural DLP change things?

#1 Data Loss Profile: John is leaving the company



Leaver "John"



Looking for work



Downloads files to work laptop



Renames File



Copies sensitive files to USB



Installs or Runs encryption App



Gives notice. Added to Leaver policy



John works his notice period and moves to his new job

Data-Centric Information Protection



Web Searches (blind spot)



Cloud Download



Rename (blind spot)



USB Copy



Application Usage (blind spot)



ML/AI Triage (Blind Spot)

No real Insight. Likely to be missed altogether OR Retrospective investigation

Behavioural Based DLP



Web Searches



Cloud Download



Rename



USB Copy



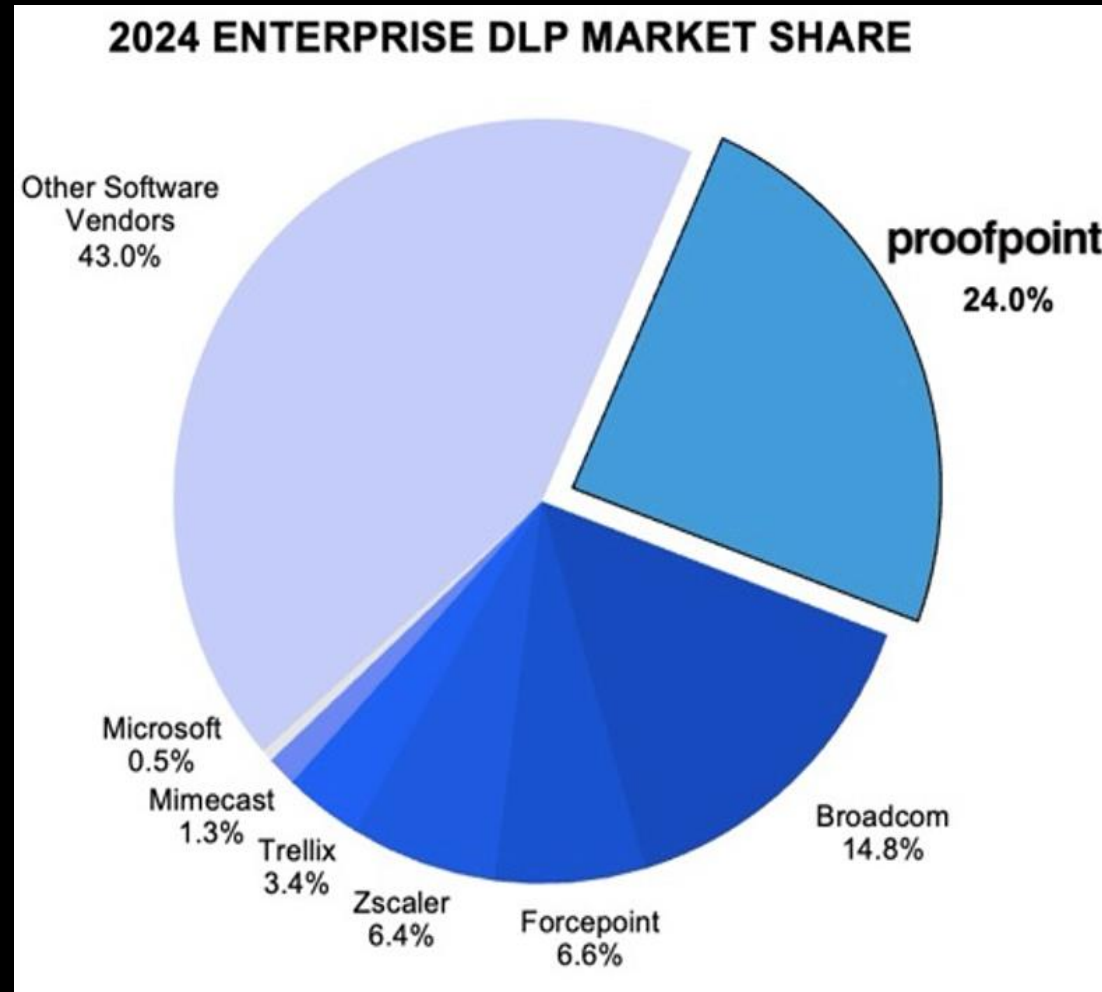
Application Usage



Anomaly Correlation

Proactive insider threat & DLP visibility before & after John gives notice

DLP Ranked #1 in Market Share



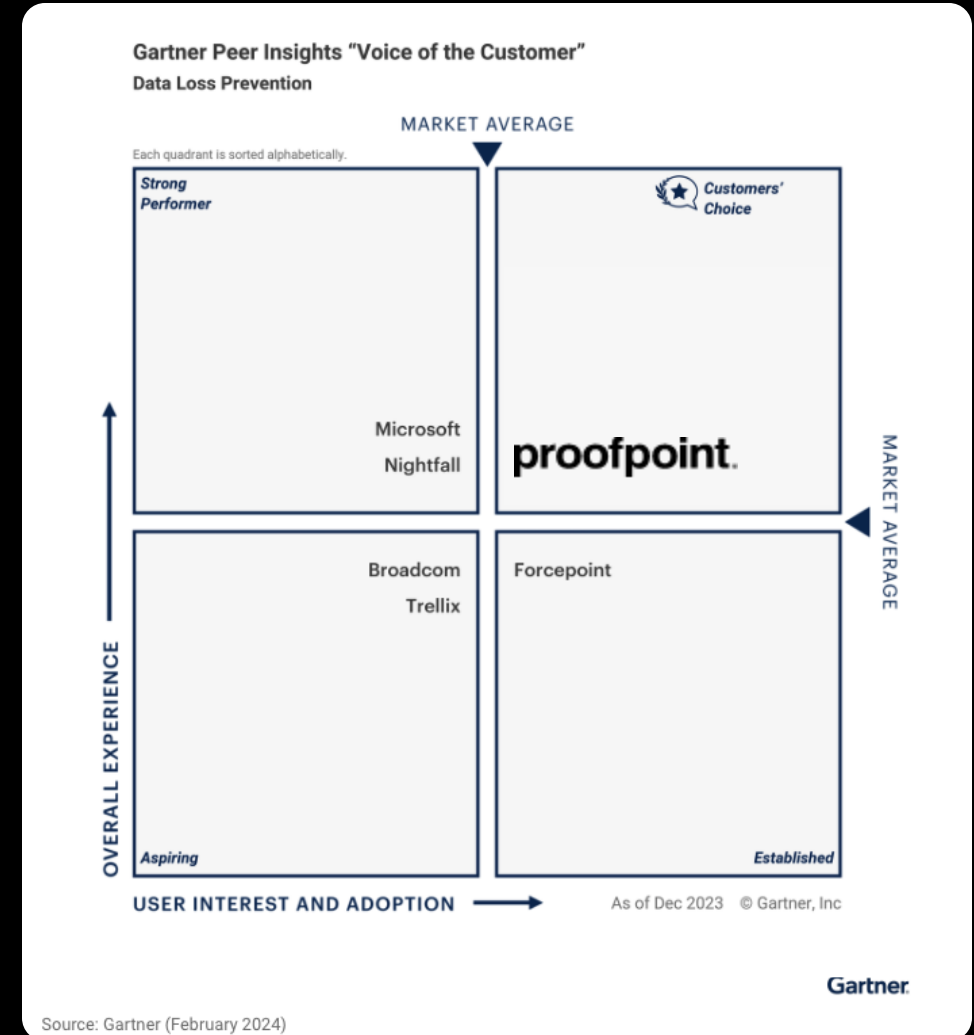
Graphic created by Proofpoint based on Gartner: [Market Share: Enterprise Software, Worldwide, 2024](#) | Varsha Mehta, Nicholas Carter, and 37 more | 17 April 2025. Total Worldwide Software Revenue for Enterprise Software Markets and Regions, Software Cloud Revenue Market Share, Security Software, Enterprise Data Loss Prevention, 2023 - 2024 (Millions of U.S. Dollars). Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

DLP Ranked #1 in Customer Choice



The only company named as
a Customers' Choice in the
2024 Gartner® Peer Insights™
Voice of the Customer Data
Loss Prevention

Source: Gartner | [Voice of the Customer for Data Loss Prevention](#) | February 2024 | Peer Contributors.
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and PEER INSIGHTS is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.



Source: Gartner (February 2024)

Proofpoint

Adaptive Information Protection



Dynamic policy based on ever-changing user behavior and risk



Adjust level of monitoring



Enforce varying levels of data controls



Acme Organization

Active Sources:

Endpoint DLP

Email DLP

Cloud DLP

Insider Threat

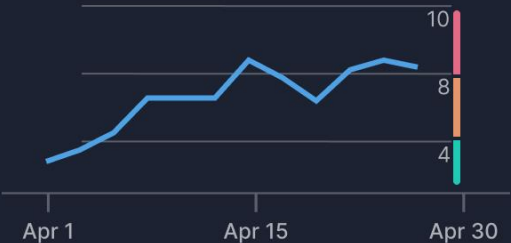
Account Take-Over

Identity & App Posture

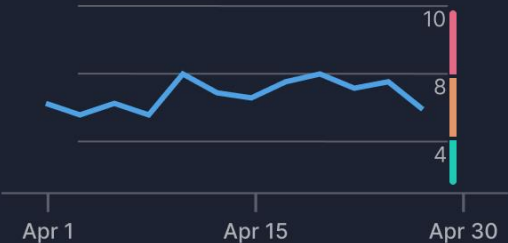
Overall Risk



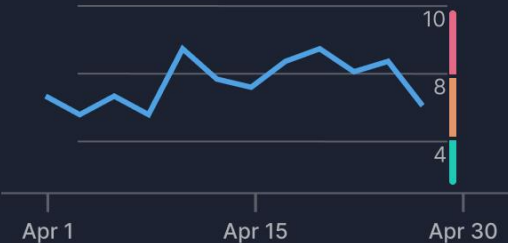
Data



Awareness



Threat



Top Risky Users

9.1 Darrell Stewardt
Finance Manager

8.7 Bobby Lyte
Sr Finance Analyst

8.5 Marvin McKinney
Account Assistant

7.7 Clement Mori
Finance Analyst

7.5 Jacob Smith
Finance Analyst

7.2 Linda Corsi
Finance Analyst

Top Risk Profiles

Risky Behavior

Users
32
3.5%

3 Controls

Sensitive Data Users

Users
28
5.2%

3 Controls

VAPs

Users
25
4.7%

3 Controls



8.7

Bobby Lyte

Sr. Finance Analyst

agargia@acme.com

Boston, US

Manager: Jaime Quesada, IT Manager

More Information

- Overview
- Data Insights
- Data Activities
- Awareness Insights

7.9

Data

Insider

Exfiltration

Exposure

8.1

Awareness

Insider

Exfiltration

6.5

Threat

Privileged

Attacked

Vulnerability

Risk Indicators

3

Risky Behavior

Exfiltration

Simulation

3

Exposure

Training

Privileged

2

Attacked

Vulnerability

Top Risk Profiles

Sensitive Data Users

Protect sensitive information from accidental or deliberate leakage by users of sensitive data.

3 Controls

Risky Users

Users with risky behavior can result in data theft / loss.

3 Controls

VAPs

VAPs are targets for social engineering and other forms of attack, that result in account take over and data loss.

3 Controls

Mitigation Recommendations

Enable ITM Adaptive Controls

Sensitive Data Users

Risky Users

Enable

Move users to elevated DLP rules in Endpoint

Risky Users

Enable

Activate Insider Threat Pathway in ZenGuide

VAPs

Risky Users

Sensitive Data Users

Enabled

Mitigation Recommendations

 Enable ITM Adaptive Controls

Sensitive Data Users

Risky Users

Enable

 Move users to elevated DLP rules in Endpoint

Risky Users

Enable

 Activate Insider Threat Pathway in ZenGuide Enabled

VAPs

Risky Users

Sensitive Data Users

Behavioural Anomalies & Pattern Detection

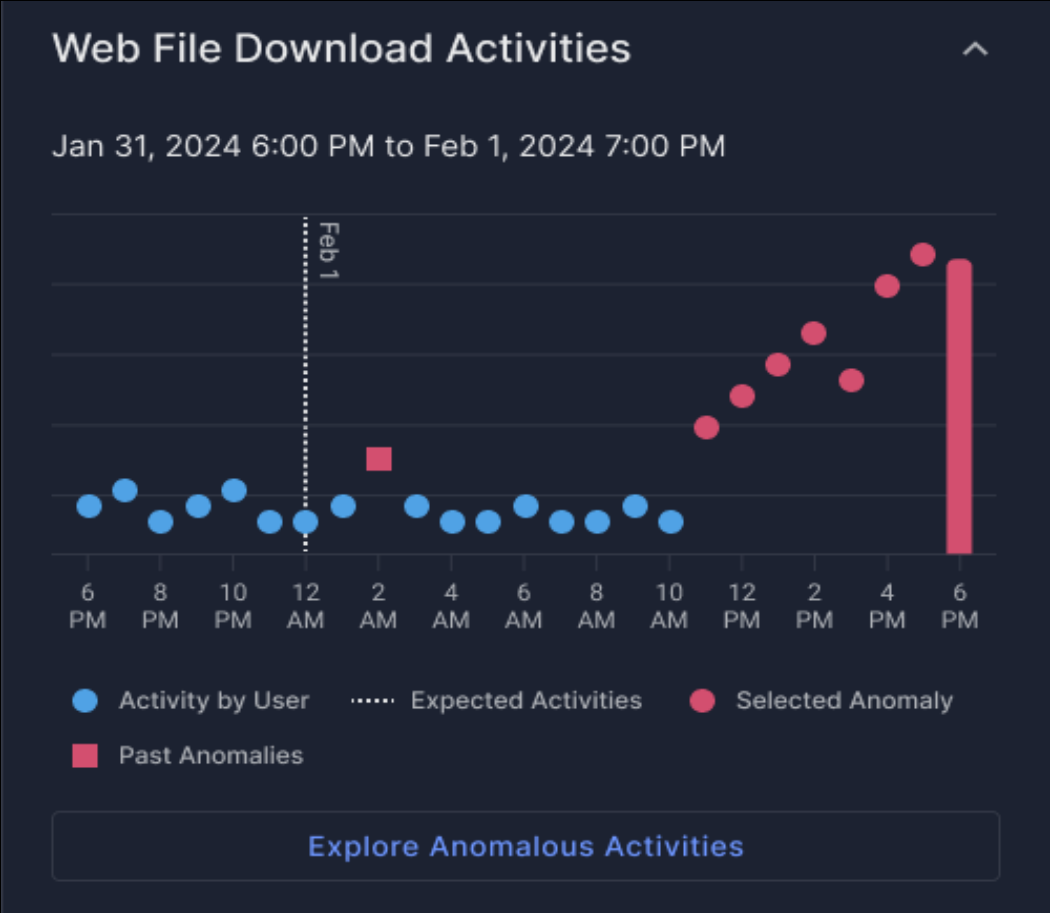
Behaviour Anomaly Detection

Alert on uncommon activity volumes

Description

Web File Download activity volume exceeds user's expected maximum for the same time of day.

There was an unusual number of **Web File Download** activities between 6pm - 7pm February 1, 2024, while the total expected volume is **1**.



Adaptive Risk Protection

High Risk Activities



Risky User
Behaviour



High Risk
Users/Group



User with
High Risk Score



Dial Up / Down Policies



Step up monitoring
with ITM context



Elevate policy w/
visual evidence




Step up Data
Protection Controls

Sep 11, 2024
10:51:33 AM



File Print: "Q2_Financials.xls"

 Blocked

Sep 13, 2024
08:48:01 AM



File Download: "Customers.xls" [Salesforce]

Sep 13, 2024
08:48:15 AM



Policy Change due to Risk [Medium → High]

Policy	From	DLP
	To	Insider Threat Management [Extended Metadata]

Sep 18, 2024
1:03:19 PM



Application Install: WhatsApp

8.7

Andy Chisholm

Sr. Finance Analyst

agargia@acme.com

Boston, US

Manager: Jaime Quesada, IT Manager

More Information

Overview

Data Insights

Data Activities

Awareness Insights

- Sep 10, 2024
10:51:33 AM

File Upload: "Q2_Financials.xls" [google.drive.com]

Blocked
- Sep 11, 2024
10:51:33 AM

File Print: "Q2_Financials.xls"

Blocked
- Sep 13, 2024
08:48:01 AM

File Download: "Customers.xls" [Salesforce]
- Sep 13, 2024
08:48:15 AM

Policy Change due to Risk [Medium → High]

Policy

From

DLP

To

Insider Threat Management [Extended Metadata]
- Sep 18, 2024
1:03:19 PM

Application Install: WhatsApp
- Sep 18, 2024
1:03:50 PM

Policy Change due to User Action

Policy

From

Insider Threat Management [Extended Metadata]

To

Insider Threat Management [Screenshots]
- Sep 19, 2024
08:15:34 AM

Web Browsing: drive.google.com

JUL 12, 2024 at 10:51:33 AM PDT

Web Browsing: drive.google.com

Alert ID: 427de7a7-b3ac-5daf-a8d9-8420ec0e904e:74698916-a9a7-477a-9cfa-04

Drive

Search in Drive

×

≡

+ New

Home

My Drive

Computers

Shared with me

Recent

Starred

Spam

Trash

Storage

761.03 GB of 2.2 TB used

Get more storage

My Drive > Fortress Data Corp

×

1 selected

Files

ChiaAcciones.pdf

ChiaDiciembre.pdf

ExtractoAhorrosNov

FiducuentaExtractoNo...

GiovanniDiciembre.pdf

JennyCasa.pdf

JennyCasa2.pdf

LuzMarinaDiciembre.p...

RecaudosNov.csv

Summary

Details

History

Comments

Origin

ALIASES

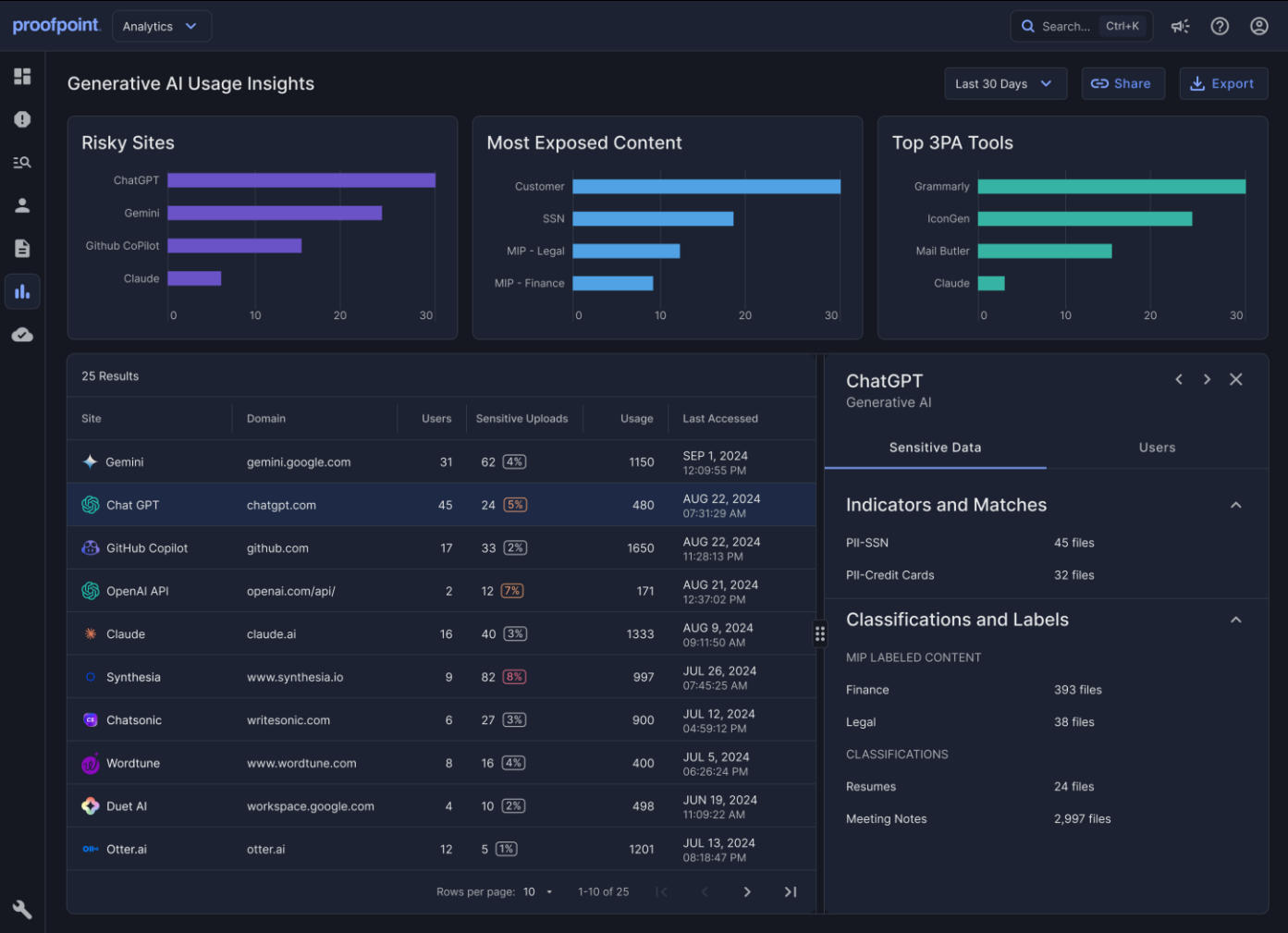
User

Bobby Lyte

bobby.lyte@fortressdatacorp.com, bobby.lyte

GenAI Visibility

LATEST & GREATEST RELEASE - AVAILABLE NOW



Managed GenAI Services

- Who is using each service
- Sensitive data is being accessed

Unmanaged GenAI Services

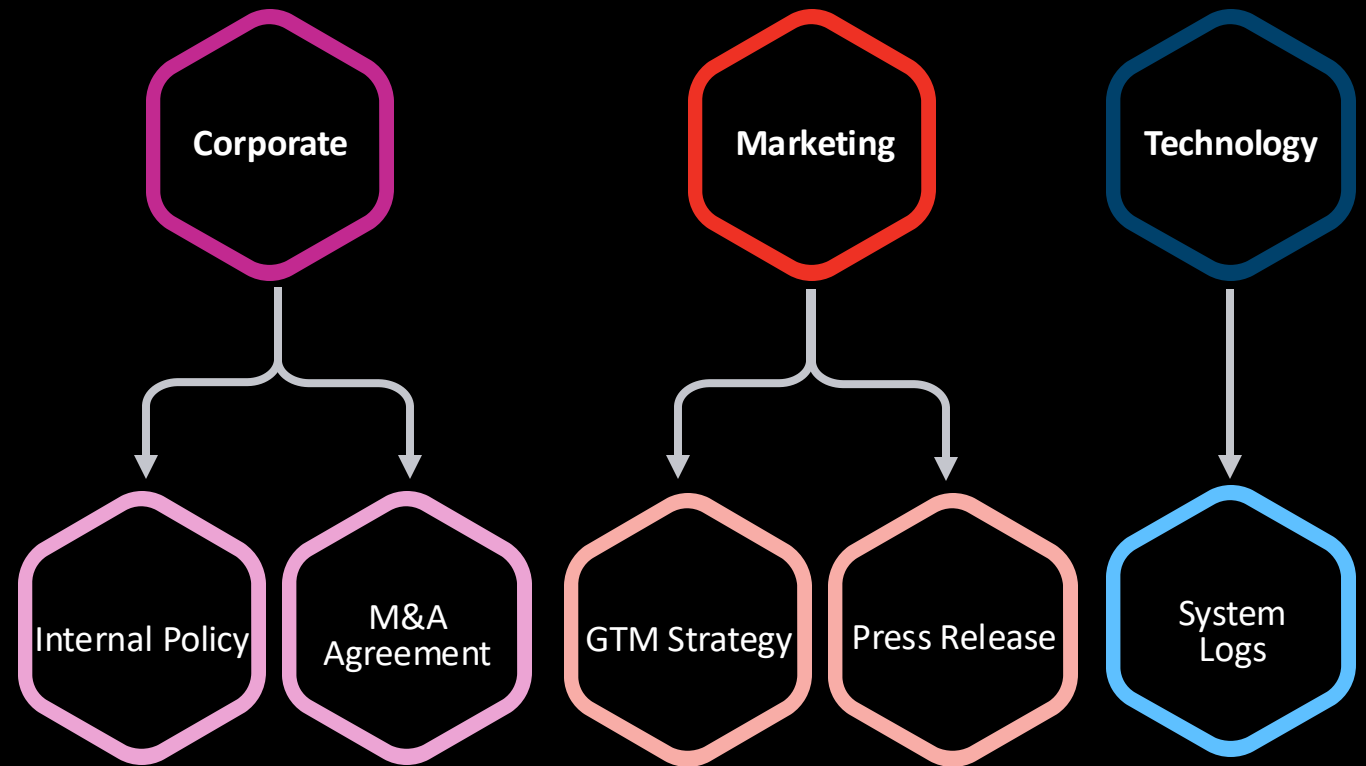
- Who is using each service
- Sensitive data being submitted
- Goal (intent) of requests

Simplify the identification of data Assets

Pre-trained LLM classification during DLP Scan



Doc Categories
LLM-based
Classification



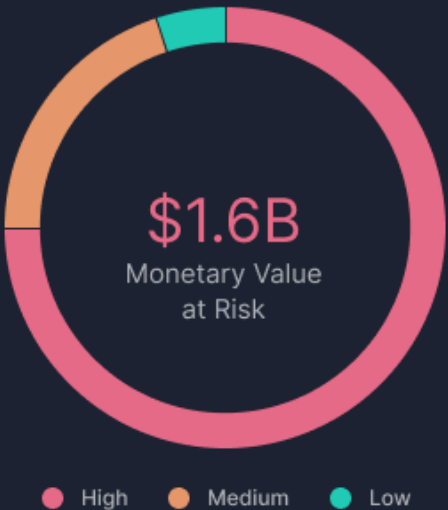


Dashboard

Last 7 Days

Export Data

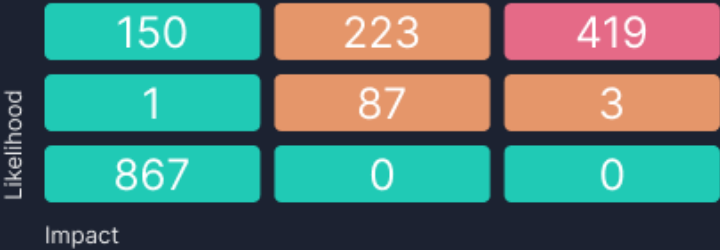
Monetary Value of Scanned Data ⓘ



Sensitive Data Stored by Type ⓘ



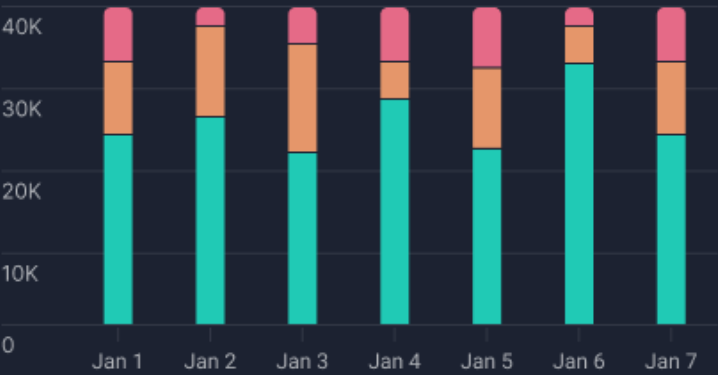
Data Stores Needing Attention ⓘ



Access to Sensitive Data ⓘ



Risk Trends ⓘ



Data Stored by Location ⓘ



Risks by Exposure ⓘ

View All

Storage	Exposure	Risks
Azure	Not encrypted with managed k...	24K
Azure	VM publicly exposed via public...	11K
AWS	Accessible by an external princi...	963
GCP	Accessible by users without MFA	528
AWS	Accessible by external or guest...	312
SaaS	EC2 instance with public acces...	105

Q3 Innovation – AI LLM Auto classification

Data Landscape (1.2 TB Classified | 300 TB Discovered)

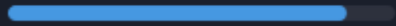
By Accounts

By Data Store

By Volume



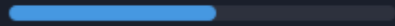
72% Classified



300/412



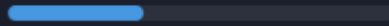
50% Classified



325/630



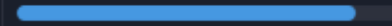
30% Classified



136/408



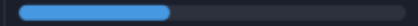
72% Classified



280/300



36% Classified



45/122

Auto-Learned Data Classes

Sensitive Data

[Auto-Learned Classifiers](#)



Human Resources

Employee Records

Payroll & Benefits

Talent Acquisition

HR Policies

Legal and Compliance

Contracts & Agreements

Contracts

Finance and Accounting

Tax Documents

Bank Statements

Operations

Supply Chain Management

IT & Data Management

Infrastructure

Marketing

Branding & Creative

Customer Feedback

Data Distribution

By Providers

By Location



OneDrive
\$2410.00 M



AWS
\$2100.45 M



Databricks
\$850 M



GCP
\$750 M



Snowflake
\$640.21 M

Proofpoint Information Protection Platform

Data Security Posture Management

Gain greater context of your data wherever it is

Discover

Classify

Prioritise

Remediate

Data Loss Prevention

Prevent data loss across digital workplace



Email



Cloud



Endpoint

Insider Threat Management

Contain insider threats proactively



Anomaly Detection



Behavioural Context

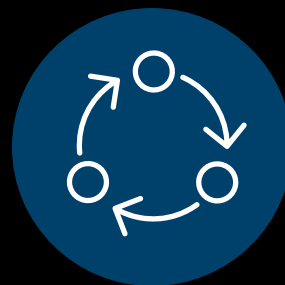
Specialist Information Protection Managed Services

Maturing an Information Protection Program Is Difficult



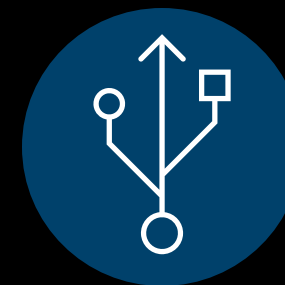
People

right people
right skillset



Process

no single,
definitive playbook



Technology

leading-edge platform
optimizing your ROI

What People does DLP require?



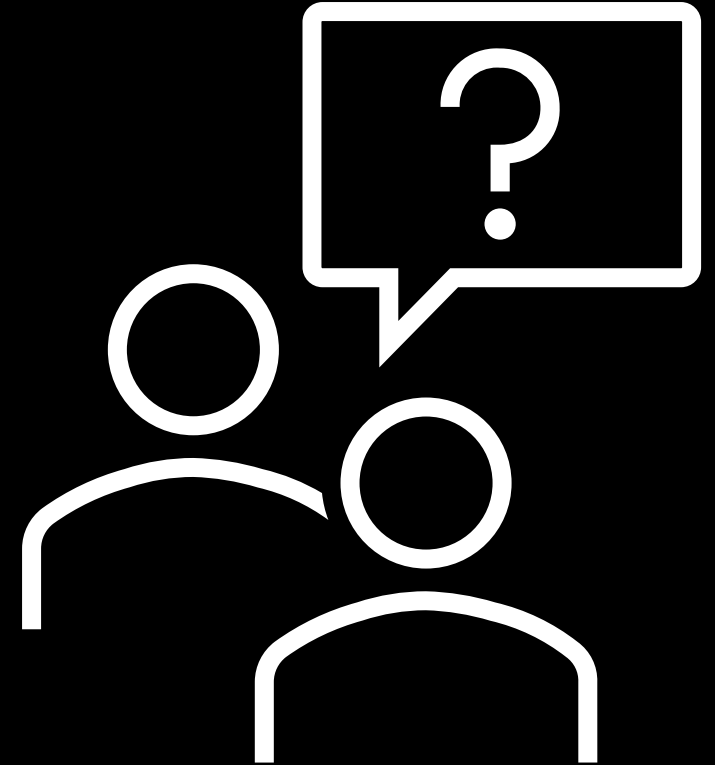
How many **active policies** do you have?

How many **alerts** do they generate?

Are you able to find **signal** in the “noise”?

Using how many **staff**?

Can you **prove the value** of your current efforts to your board?



Finding Talent Remains a Challenge



470K
Cybersecurity job openings
in the U.S. alone*

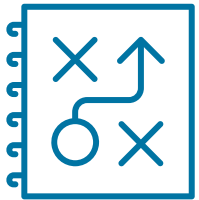
85%
SUPPLY/DEMAND RATIO
In the U.S. only enough
cybersecurity workers to fill
**85% of employer
demand***

4.8M
2024 global cybersecurity
workforce gap, a
19% YoY increase†

* Source: Cyberseek.org, September 2024

† Source: 2024 ISC2 Cybersecurity Workforce Study

How We Deliver Outcomes



**Program Strategy Manager
(PSM)**



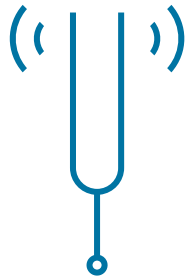
**Data Protection Analyst
(DPA)**



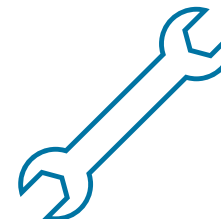
Triage Analyst (TA)



**Compliance Consultant
(CC)**



Program Analyst (PA)



**Security Solutions
Engineer (SSE)**

How do we do that?



Proactive Expertise



We see the world's attempts at exfiltration.

We know what to look for, per industry, based on threats and regulatory risk.

We tune out the noise and give you actionable signals—active threats to your data protection.

Staff Continuity



We have an ever-ready team of experts for you.

We won't abandon you in a time of need.

We're constantly available and informing your team of your security posture, at a fixed annual cost.

Executive Insights



We give you proof of value.

We can show you data that's relative to your industry peers, the proactive steps you've taken, and relevant trends.

We provide weekly and monthly updates, executive-level metrics, and proof of a clean bill of health.