PROTENUS

# Mini-Summit 5:  The Privacy Threat Spectrum

Understanding and preventing the full scope privacy threats the patient data

Nick Culbertson
CEO, Protenus

Teresa Burns
Privacy Officer, Protenus

Protenus is a healthcare compliance analytics company that helps health systems leverage A.I. and automation to predict and prevent various types of privacy and security threats.

KLAS CATEGORY LEADER
PATIENT PRIVACY MONITORING
2019

ONC Certified HIT
2015 EDITION
HEALTH IT MODULE

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports ®

# Today's Speakers and Disclaimers

Teresa Burns

Former Deputy Privacy Officer

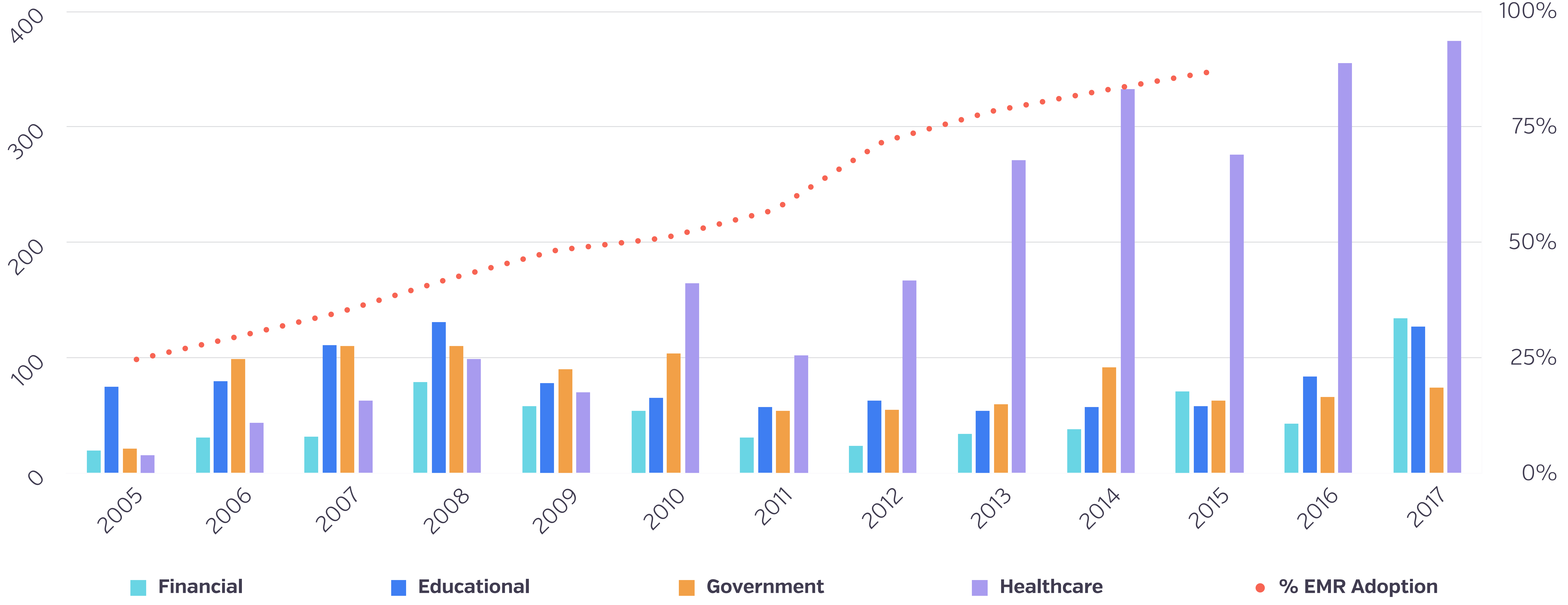
JOHNS HOPKINS MEDICINE

Nick Culbertson

Former Green Beret

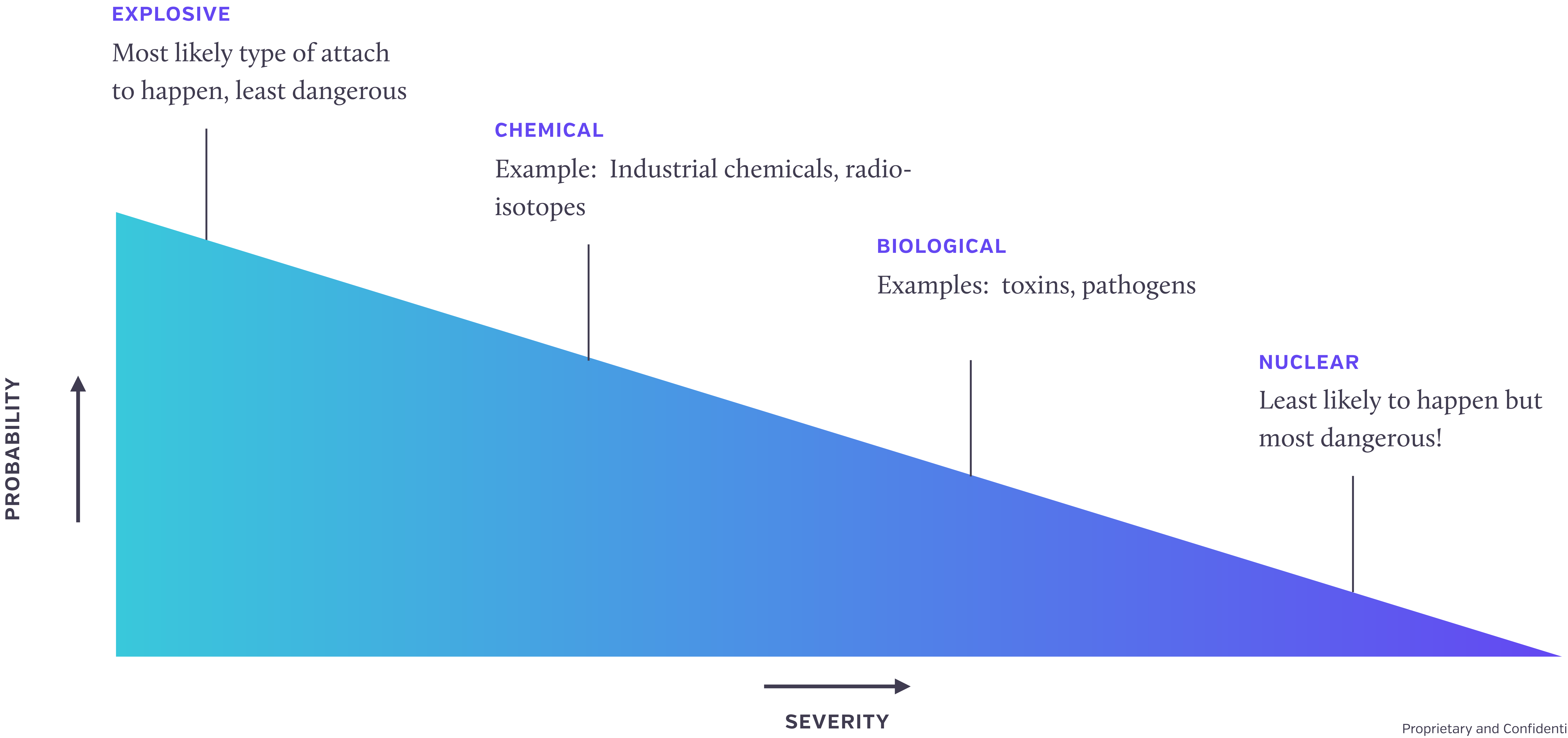
JOHNS HOPKINS UNIVERSITY

# Inappropriate access to PHI is on the rise and not slowing down



Sortie
Exit

# CBRNE Threat Spectrum



**EXPLOSIVE**

Most likely type of attach to happen, least dangerous

**CHEMICAL**

Example: Industrial chemicals, radio-isotopes

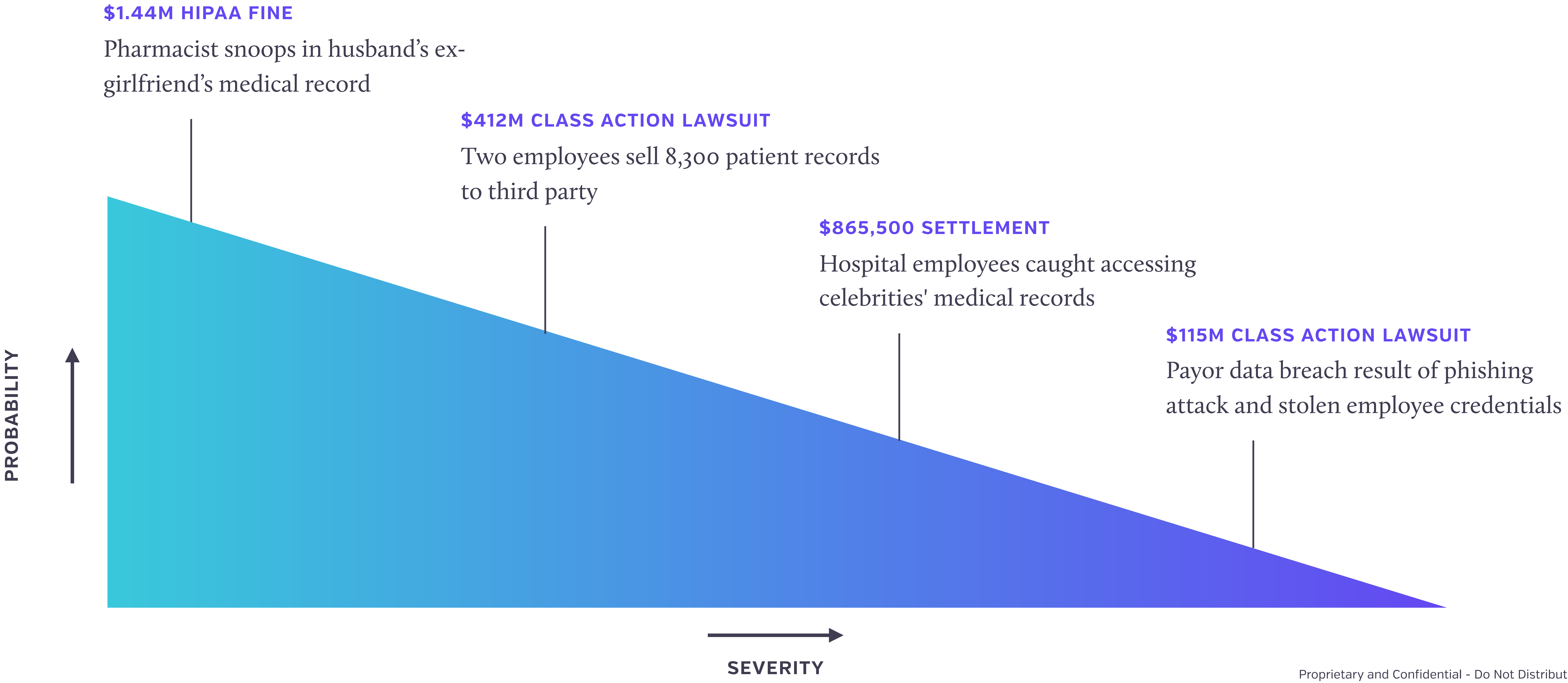
**BIOLOGICAL**

Examples: toxins, pathogens

**NUCLEAR**

Least likely to happen but most dangerous!

# Privacy/Security Threat Spectrum



**$1.44M HIPAA FINE**

Pharmacist snoops in husband's ex-girlfriend's medical record

**$412M CLASS ACTION LAWSUIT**

Two employees sell 8,300 patient records to third party

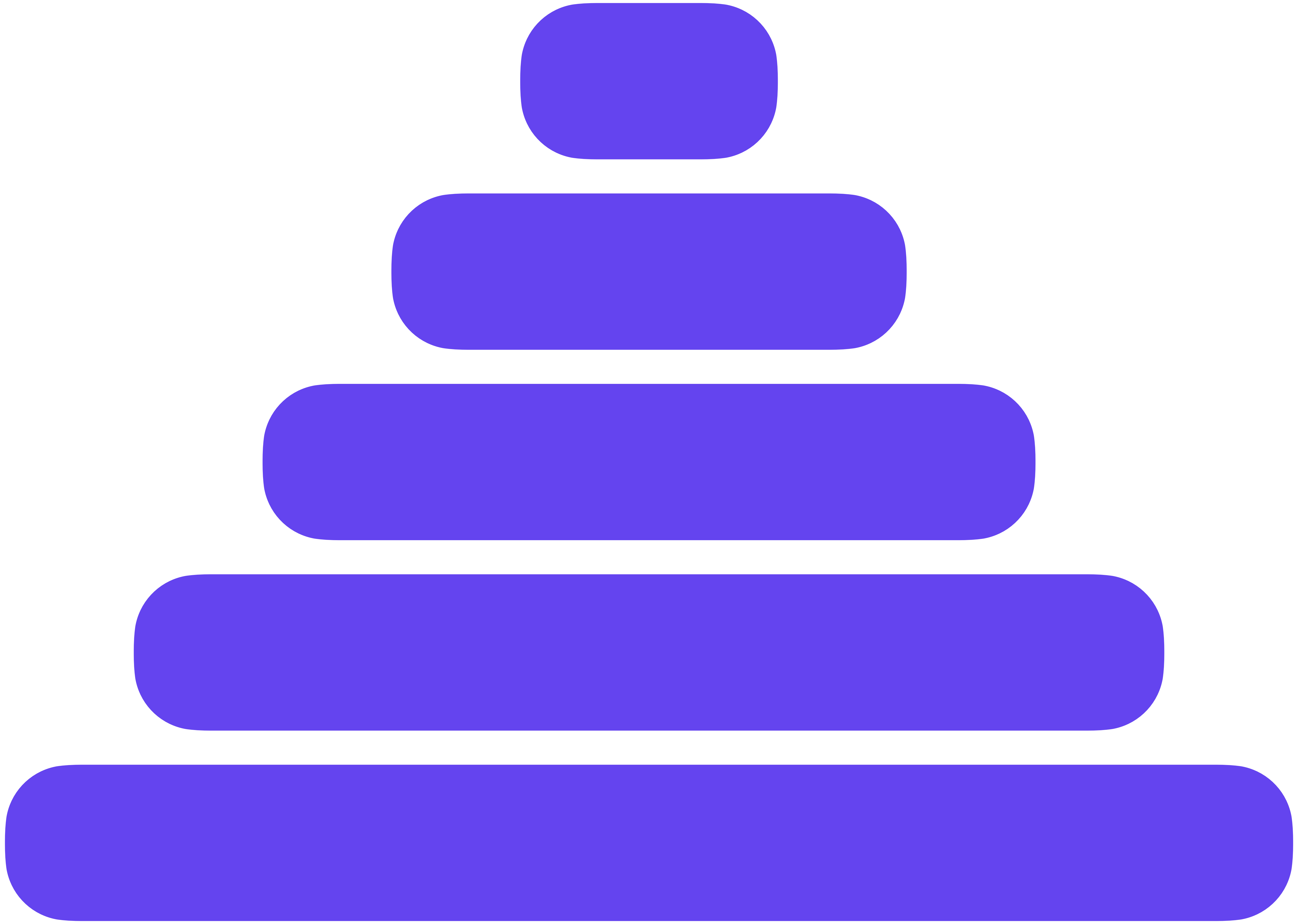
**$865,500 SETTLEMENT**

Hospital employees caught accessing celebrities' medical records

**$115M CLASS ACTION LAWSUIT**

Payor data breach result of phishing attack and stolen employee credentials

Effective privacy monitoring means that we're addressing the high-volume, low-risk threats as well as the low-volume, high-risk threats.

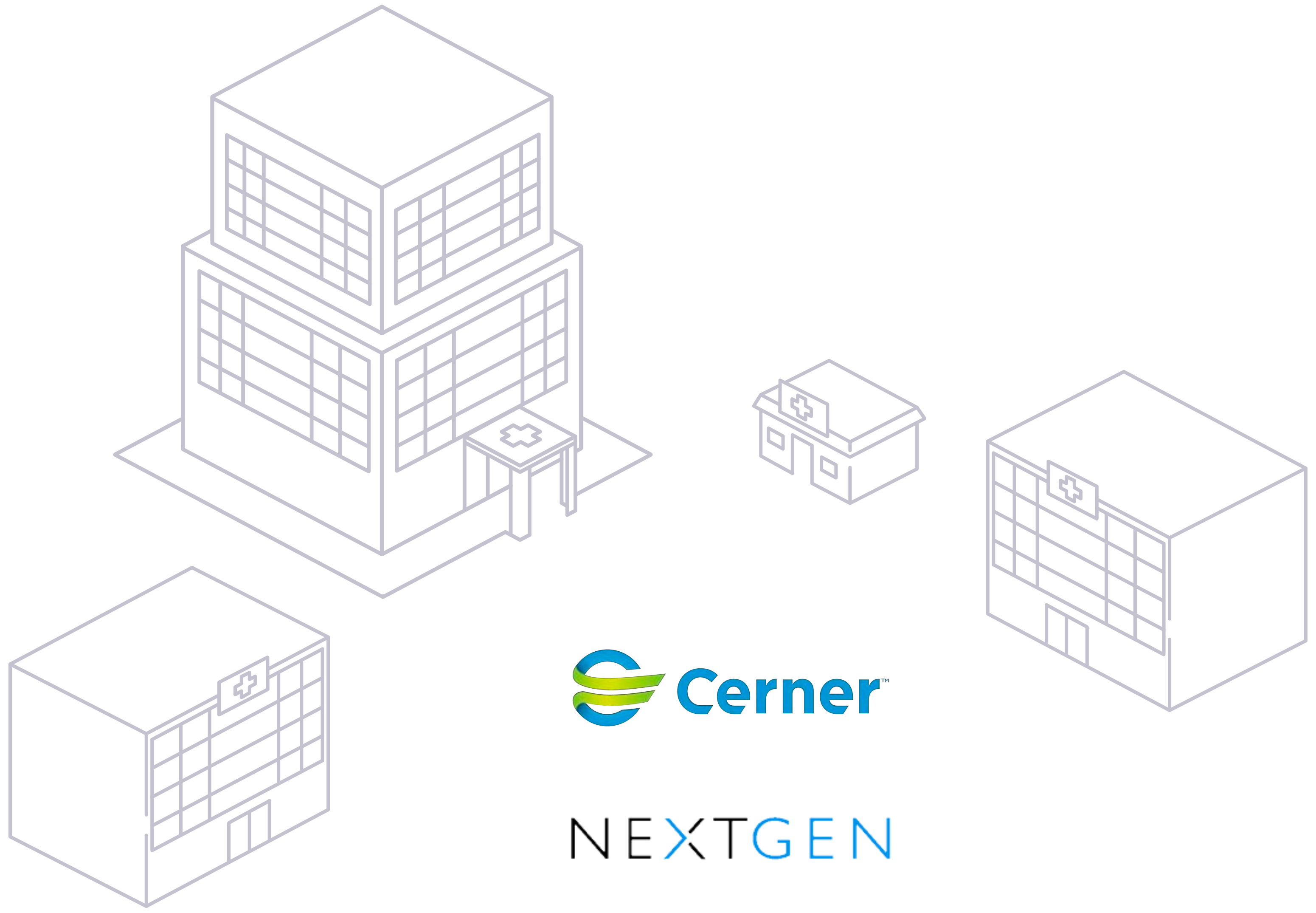


# Building effective monitoring from the ground up

Each layer of you privacy monitoring program holds opportunity to improve efficiency and efficacy.

# Best Practice Layer 1: Centralized Audit Log Data

Bring disparate audit log data from across the enterprise together under a “single pane of glass” in order to prevent data scrounging.



Cerner

NEXTGEN

Allscripts

Omnicell

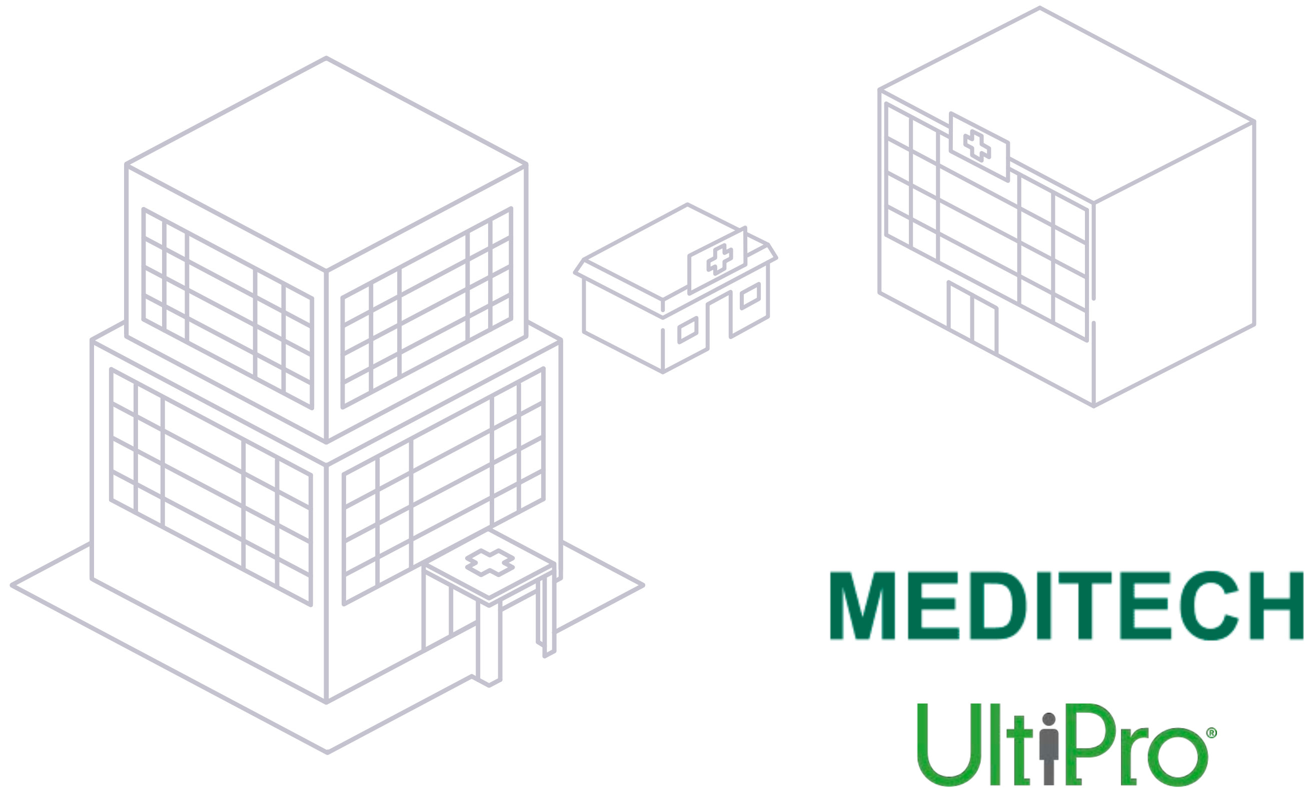
ORACLE
PEOPLESOFT

Epic

LAWSON

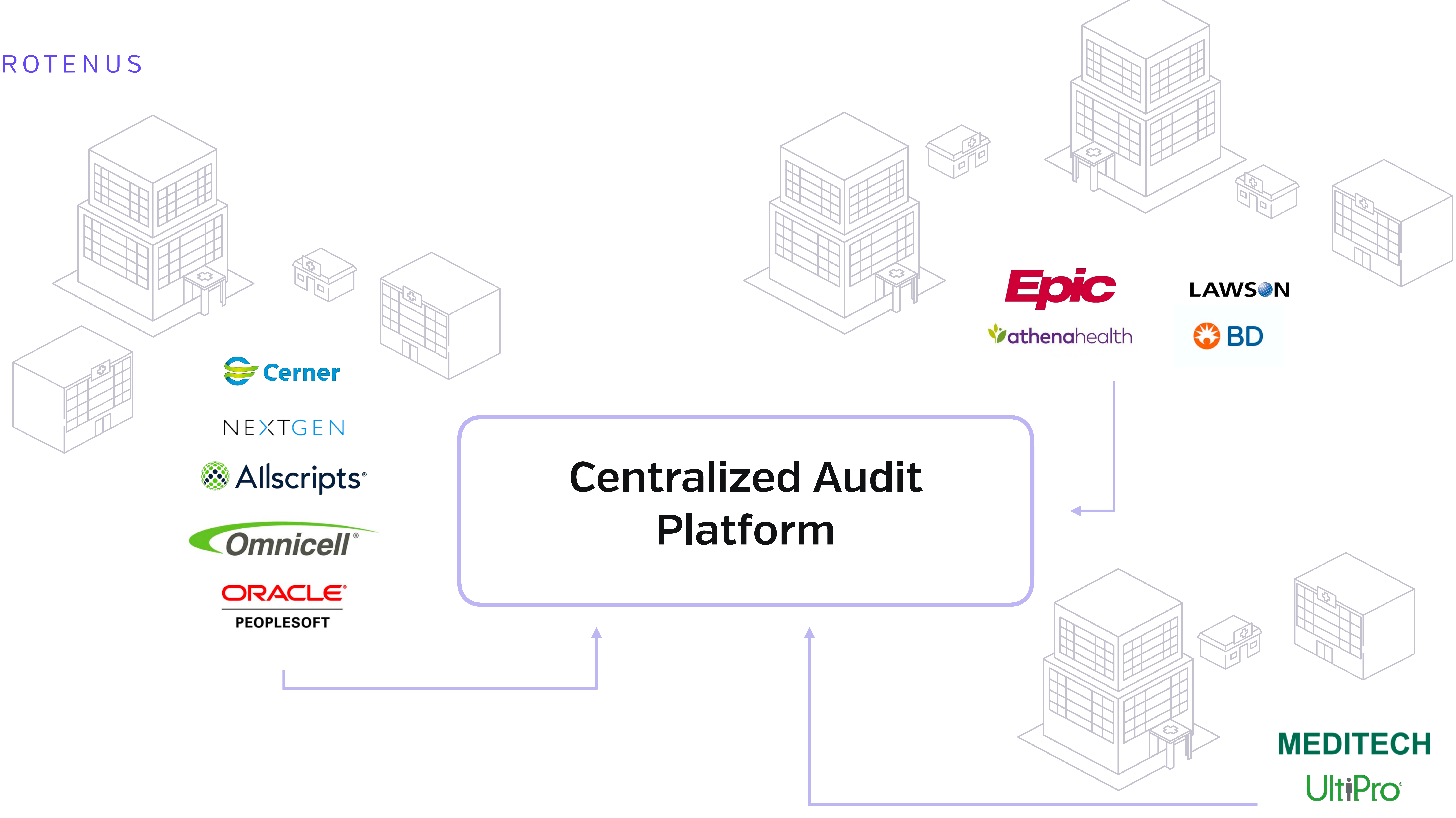
athenahealth

BD



MEDITECH

UltiPro



Centralized Audit Platform

# Benefits of a Centralized Audit Platform

- Less time spent gathering or requesting data from disparate sources
- Faster ad-hoc investigations
- Highly indexed data means that critical context isn’t missed
- Cost of storage is drastically dropping with modern cloud architectures

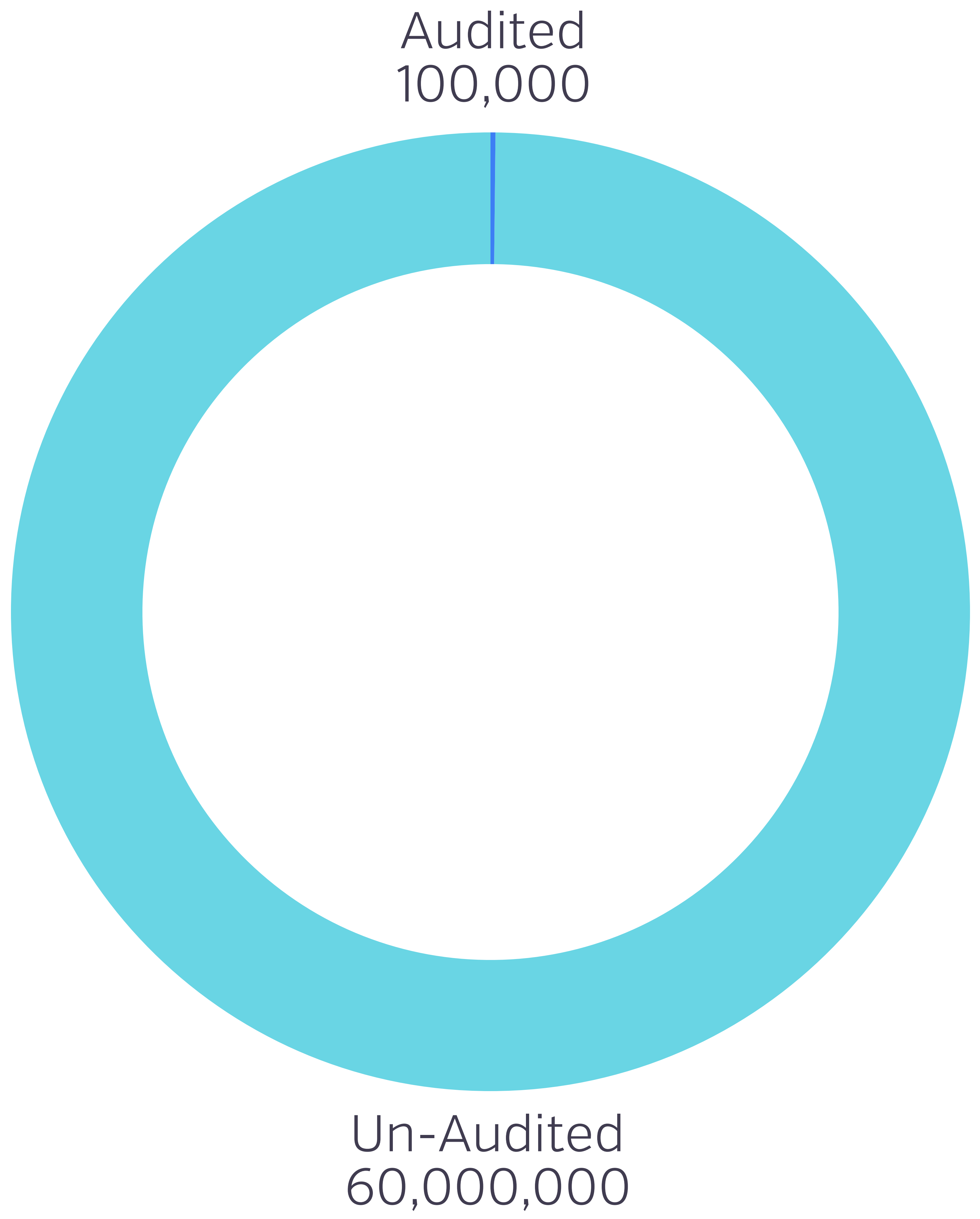
## Best Practice Layer 2: Leverage A.I. to Audit Every Access

A significant portion of auditing requires basic, repetitive data exploration - the kind of work that is ideal for artificial intelligence.

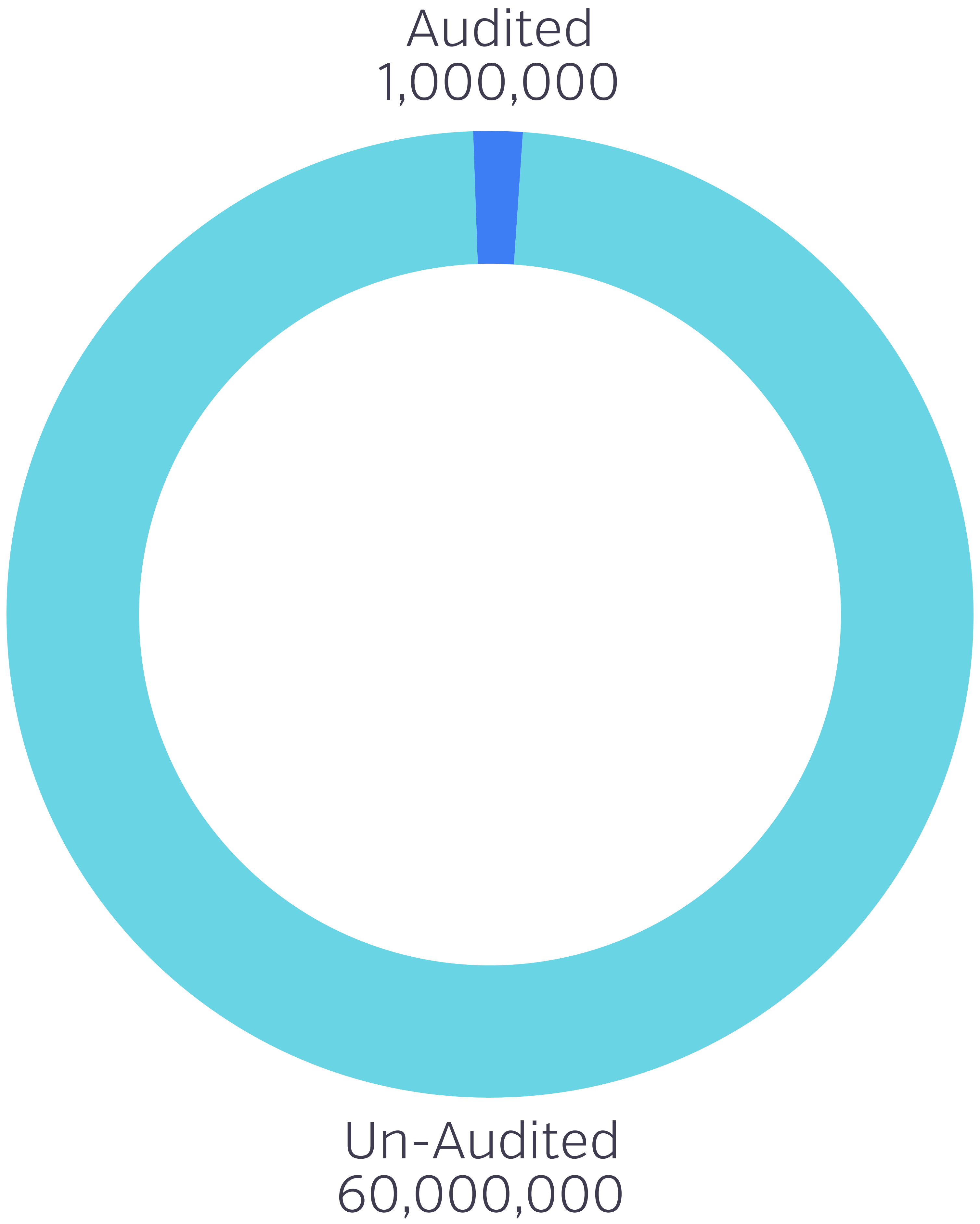
# The average hospital manually audits 1 in 60,000 thousand access log events per month

Audited
1,000
Un-Audited
60,000,000

# A 100x increase in auditing is still only scratching the surface



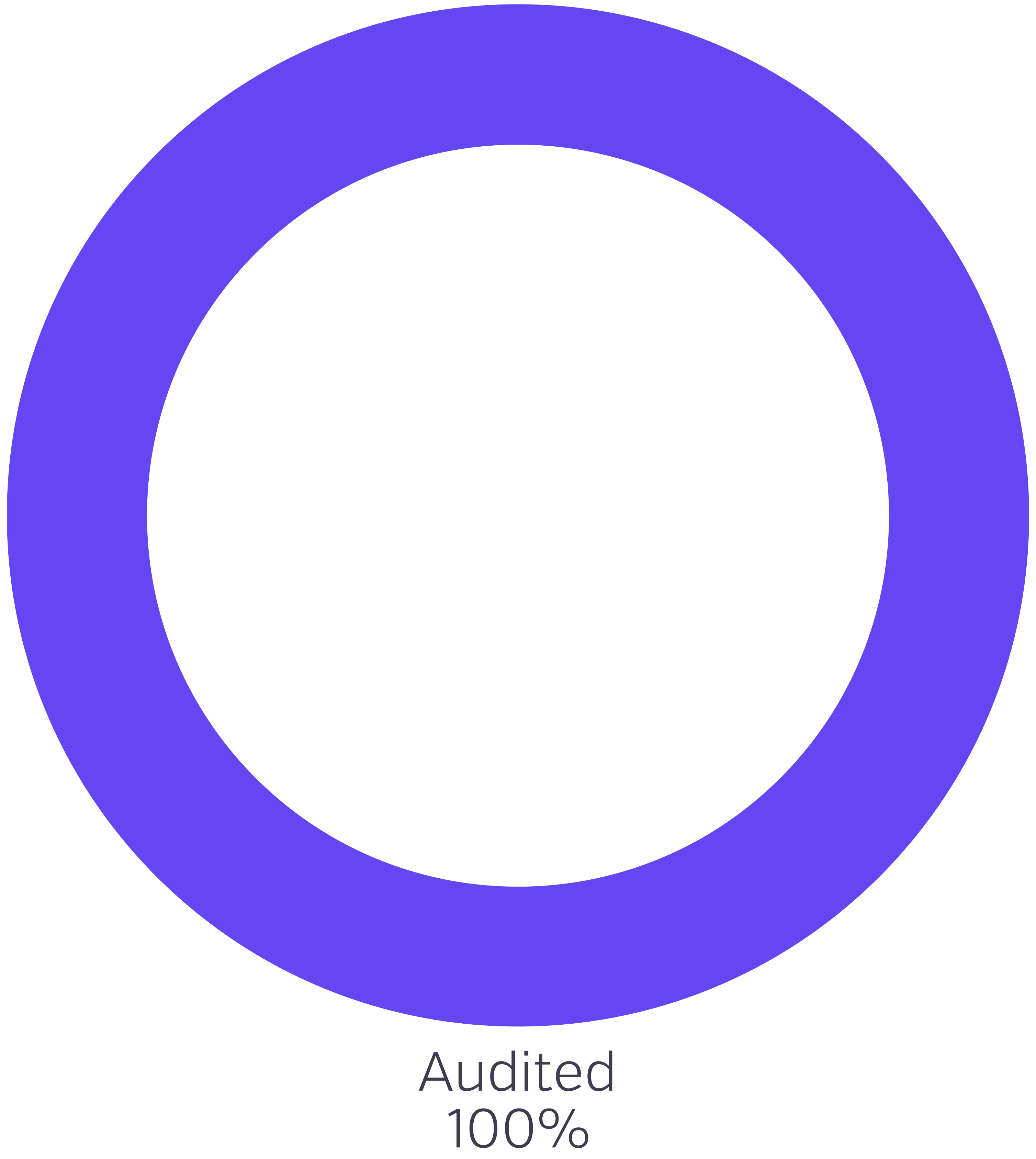
# Even if you manually reviewed 1M access log events, it's still only a fraction of activity



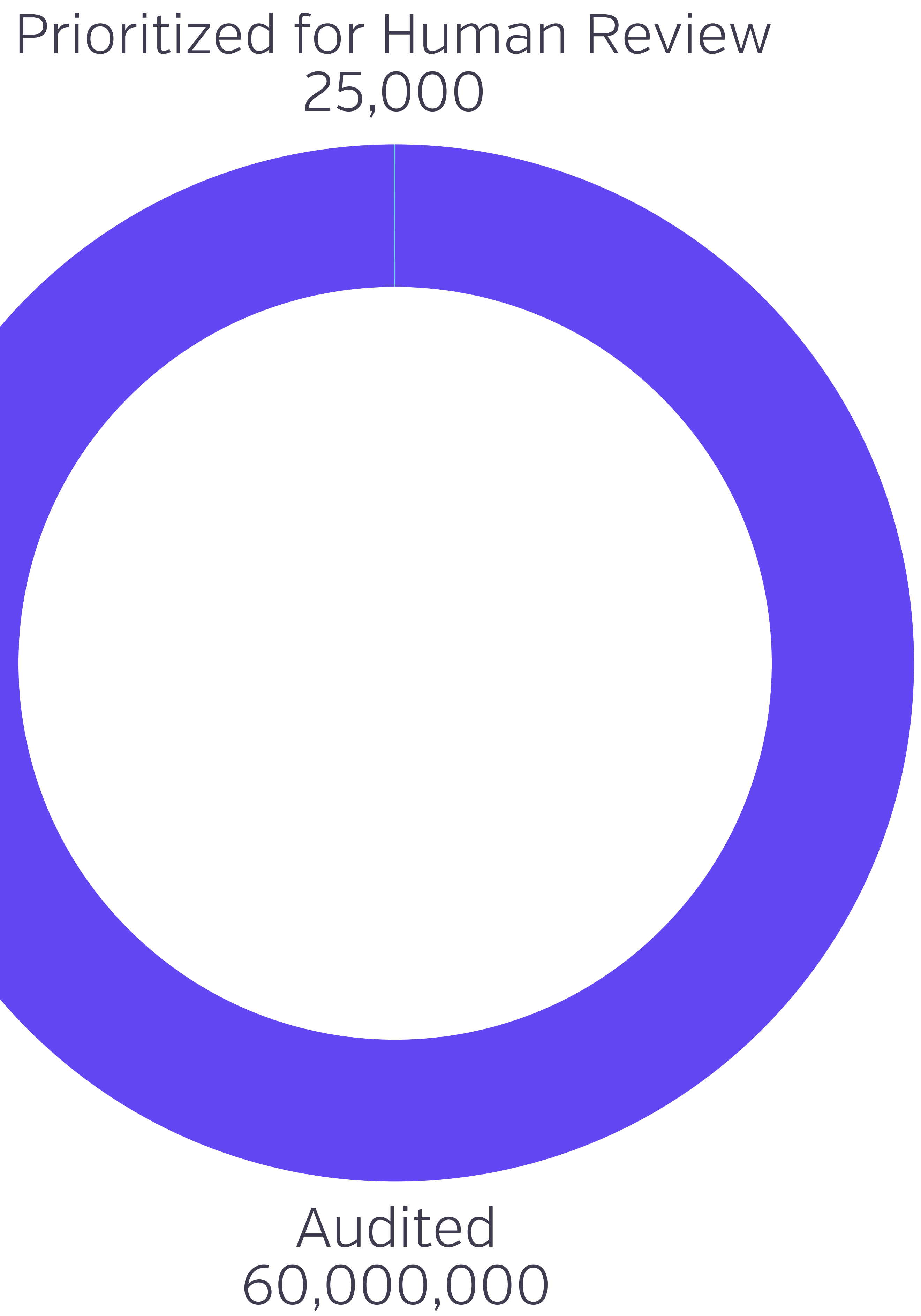
What if you could ask hundreds of questions about every access to every record, every day?

Then, based on how those questions are answered, what if you could prioritize questionable accesses that are the most suspicious and carry the most risk?

# Artificial intelligence allows privacy and security officers to to audit every access…



# Prioritize the Cases that Matter the Most



# But wait, isn't artificial intelligence a bad and scary thing?

Artificial Intelligence s the best solution for automating highly repetitive tasks that are objective in nature and require no human judgment.

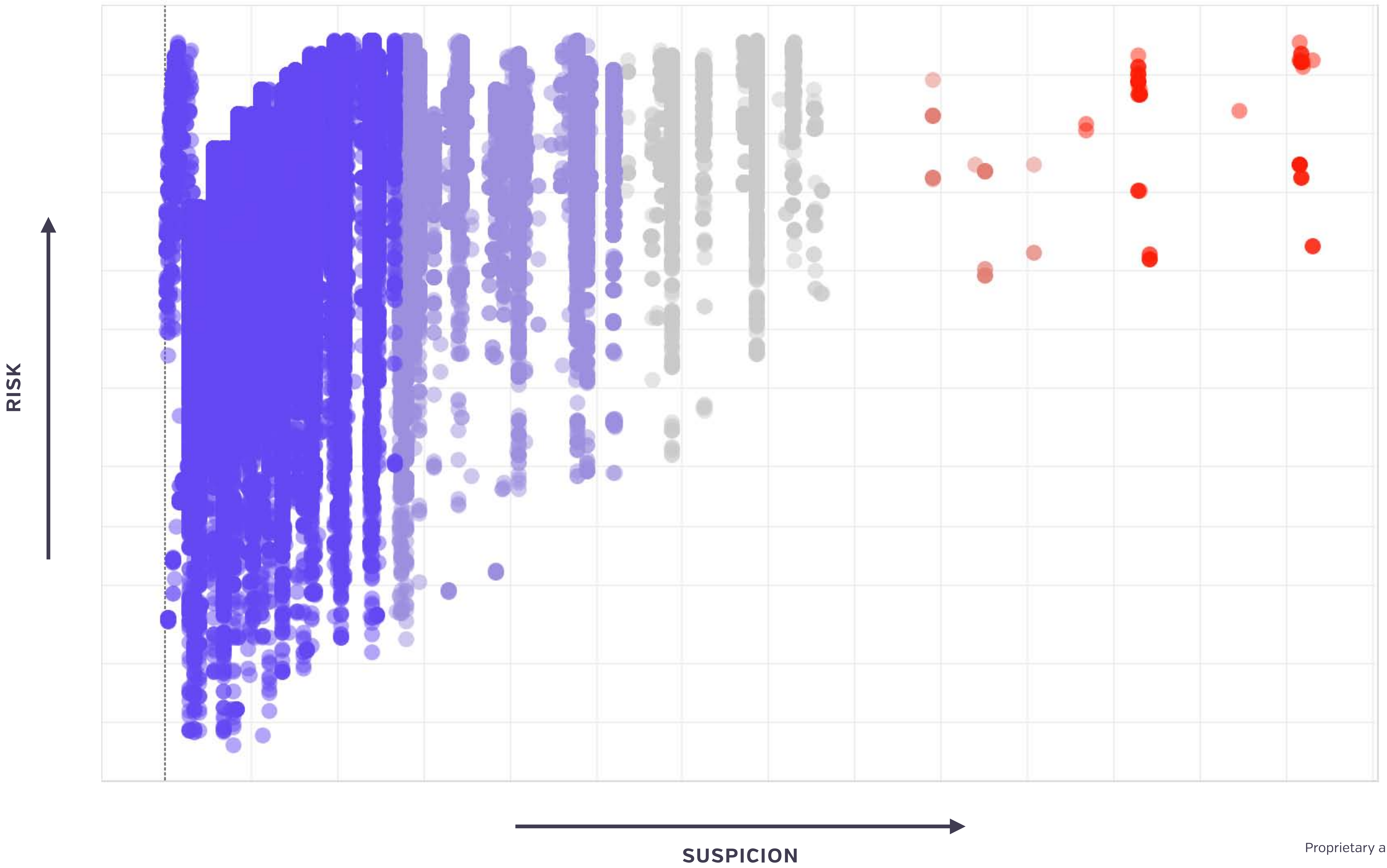
Features original art & gameplay
The Classic Mystery Face Game
GUESS WHO?
Does your person have blue eyes?
Is your person wearing a hat?
Hasbro Gaming
WARNING:
CHOKING HAZARD Small parts
Not for children under 3 years
Family
6+
Bill
Richard
Eric
George
Maria
Bernard

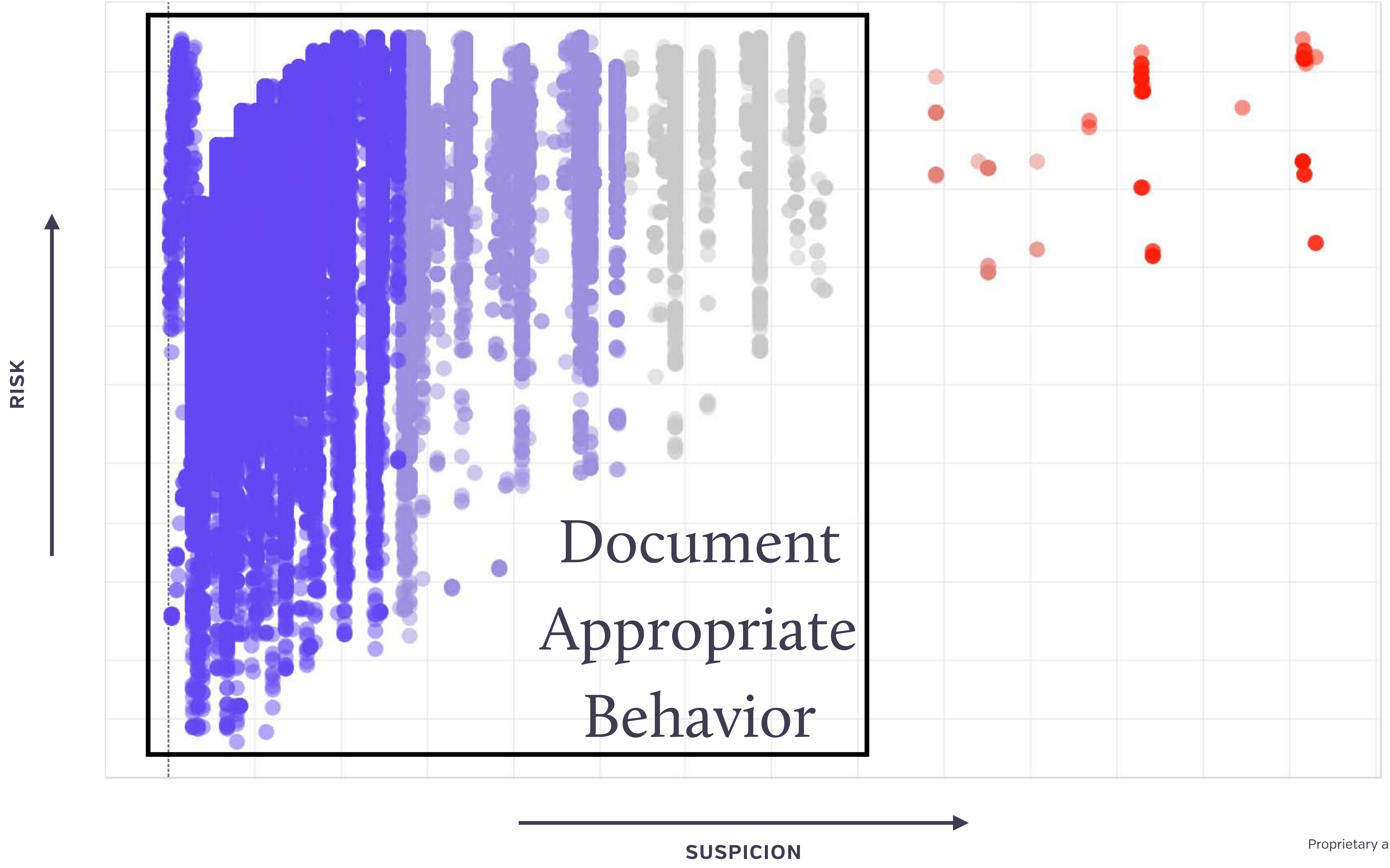
# An A.I. Approach to Guess Who

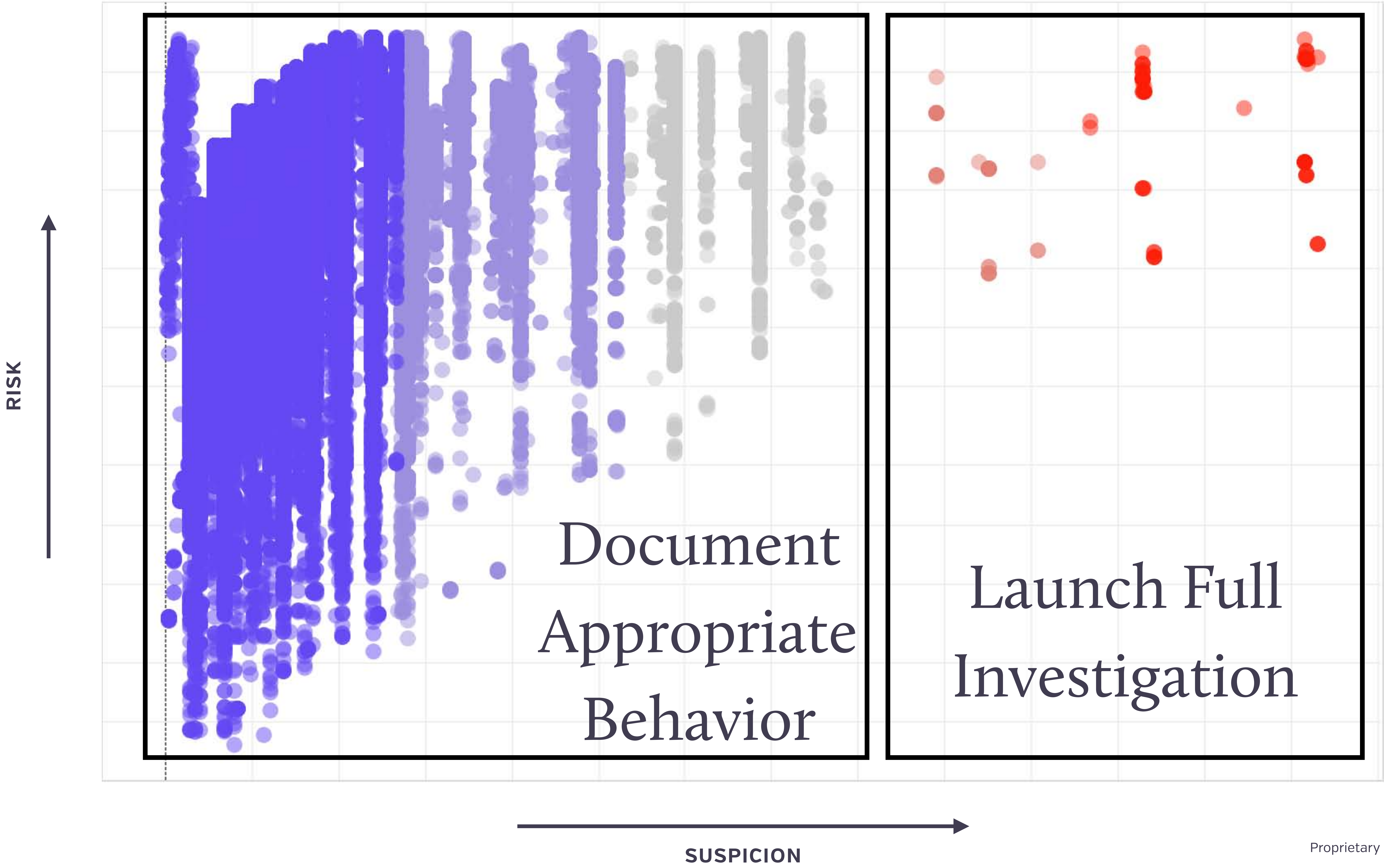
| Feature | Anne | Bob | Max | Anita | Sam | ... |
|---|---|---|---|---|---|---|
| Grey Hair? | | | | | | |
| Glasses? | | | | | | |
| Male? | | | | | | |
| Beard? | | | | | | |
| Blue Eyes? | | | | | | |
| ... | | | | | | |

# An A.I. Approach to Guess Who

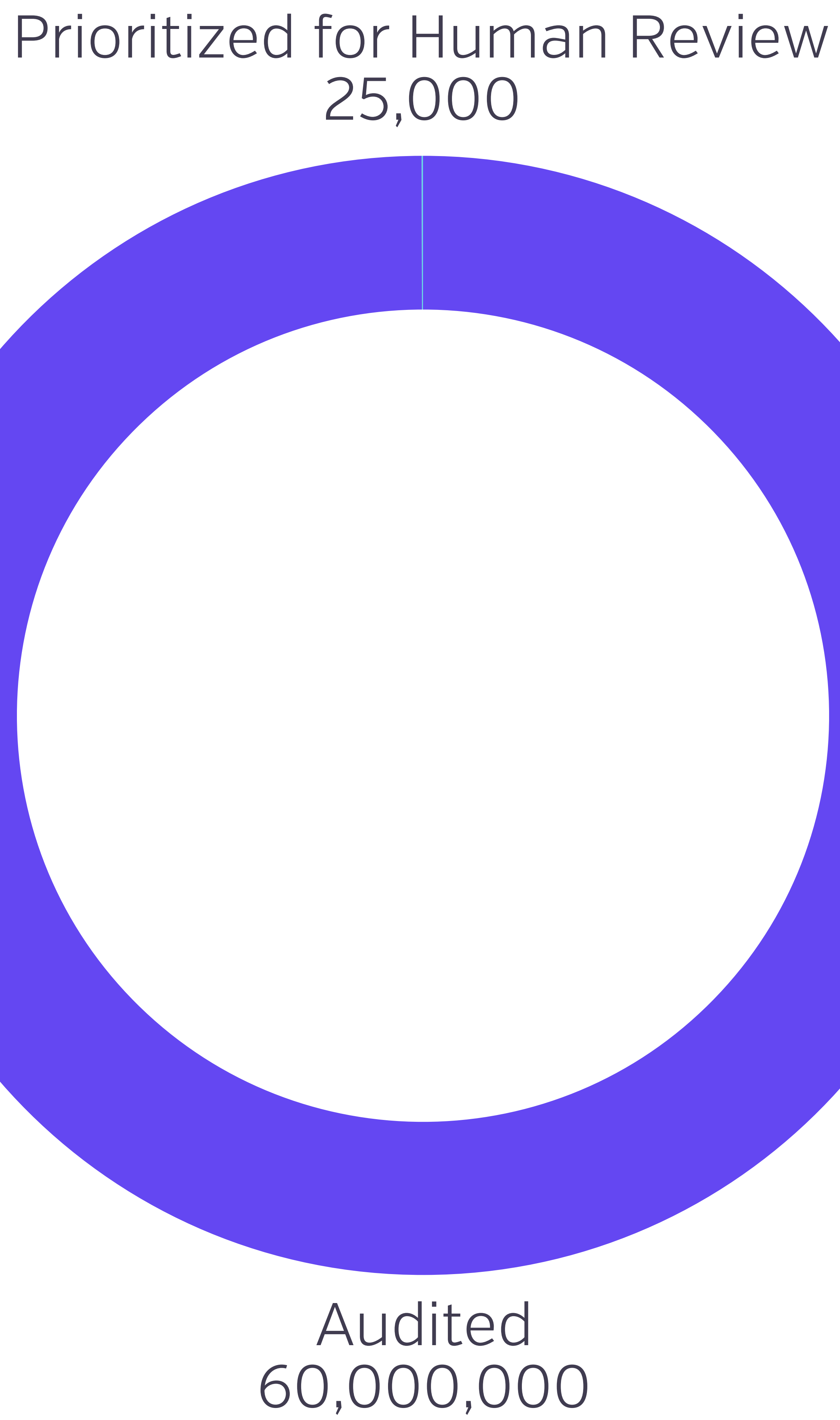
| Feature | Anne | Bob | Max | Anita | Sam | ... |
|---|---|---|---|---|---|---|
| Grey Hair? | No | No | **Yes** | No | Yes | No |
| Glasses? | No | No | **Yes** | No | Yes | No |
| Male? | No | Yes | **Yes** | No | No | Yes |
| Beard? | No | No | **Yes** | No | No | No |
| Blue Eyes? | Yes | Yes | **Yes** | Yes | Yes | Yes |
| ... | No | No | **Yes** | No | Yes | No |
| Match: | 14% | 29% | **100%** | 14% | 57% | 29% |

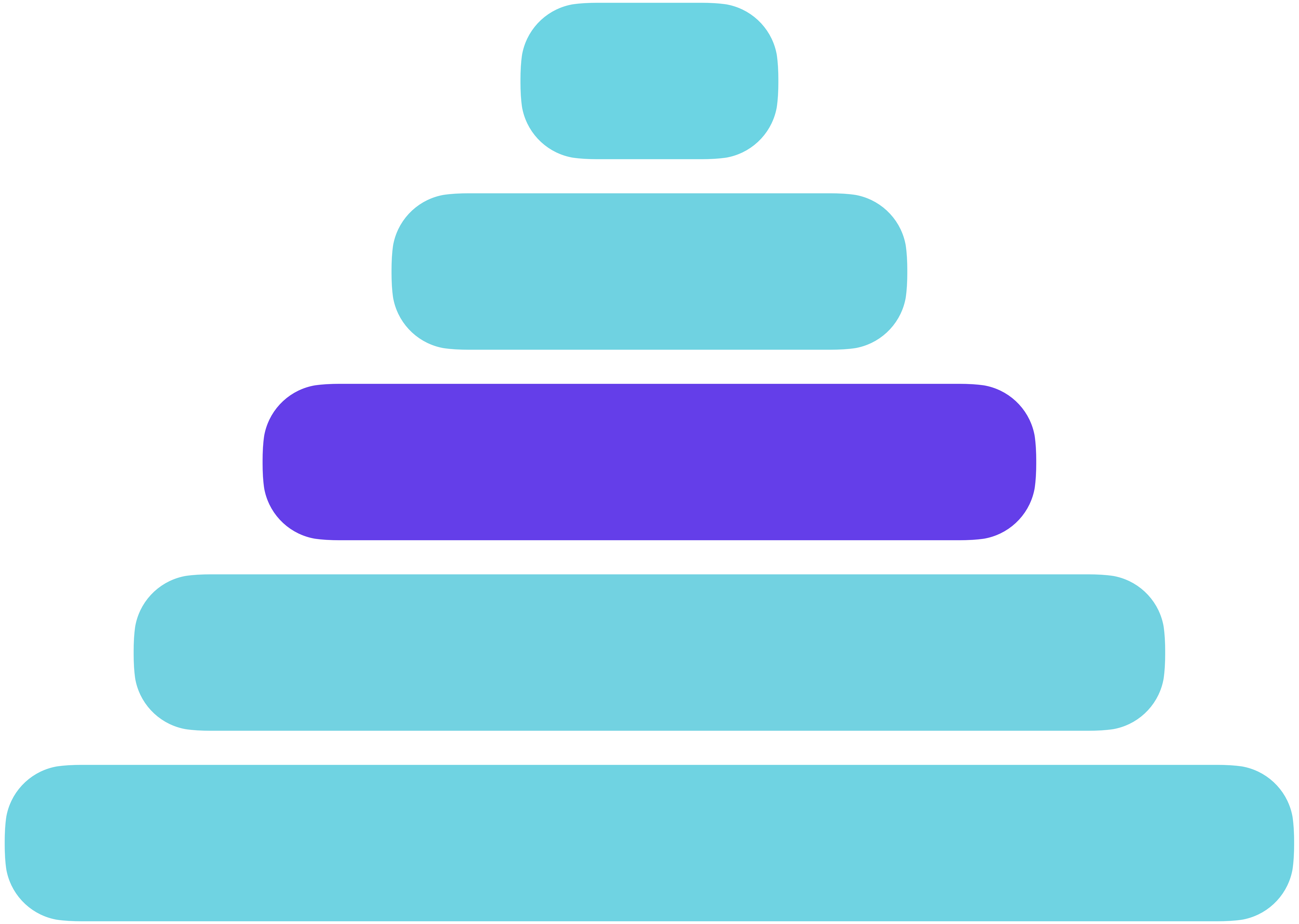

RISK
SUSPICION


RISK
Document
Appropriate
Behavior
SUSPICION


RISK
Document Appropriate Behavior
Launch Full Investigation
SUSPICION

# Prioritize the Cases that Matter the Most

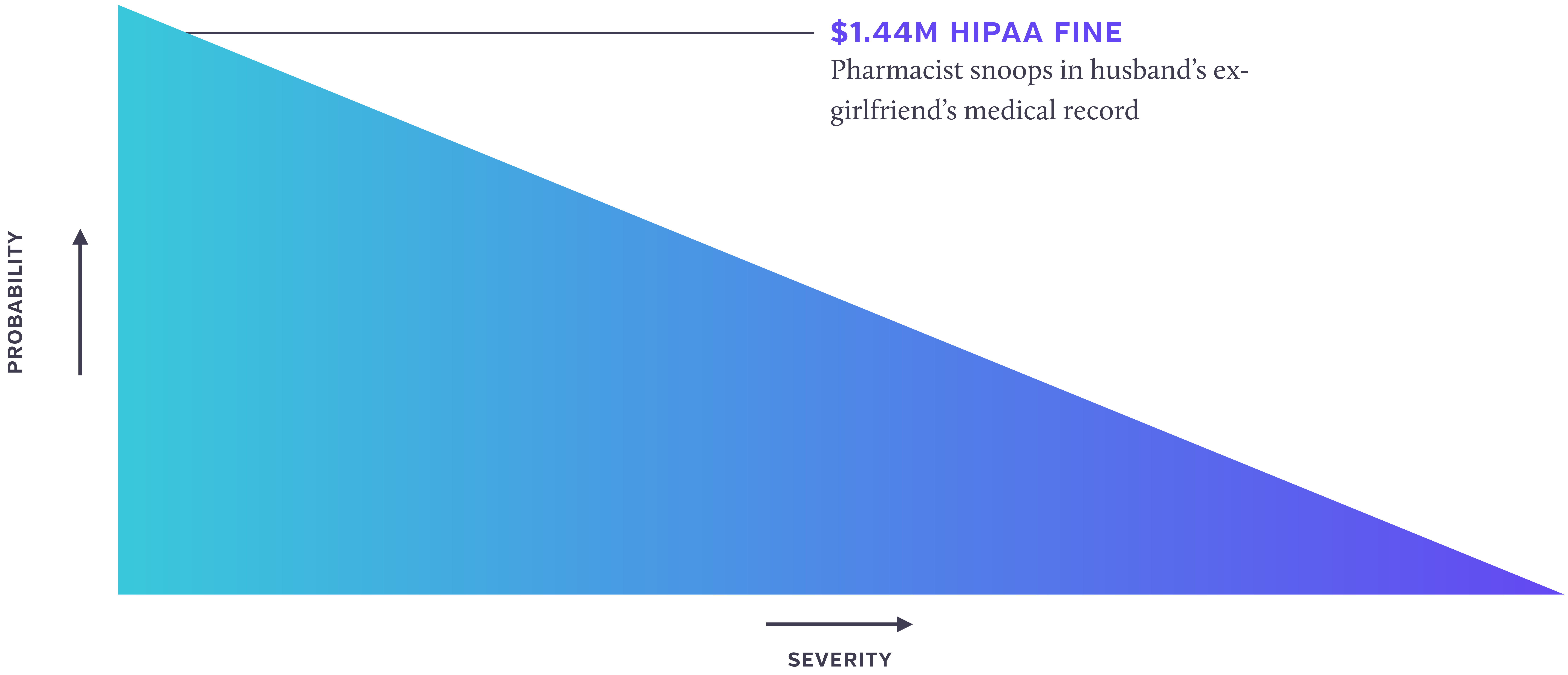




# Best Practice Layer 3: Put Privacy Operations on Autopilot

Align processes with policy in order to automate investigation procedures.  Enforce policies at scale and prevent violations before they happen.

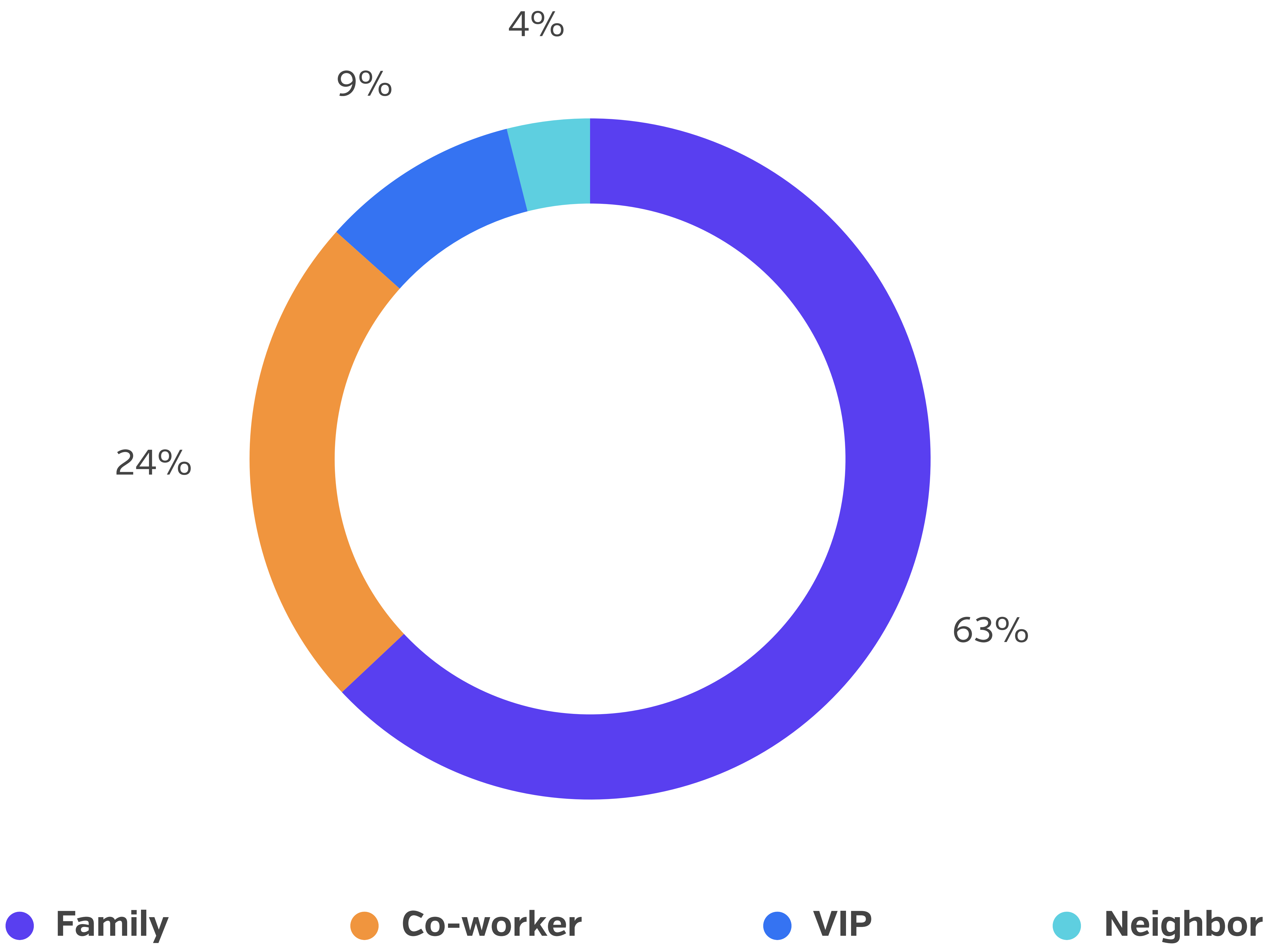
If investigatory procedures are well aligned with organizational policies, then automation can help education workforce and prevent high-volume, low-risk snooping.



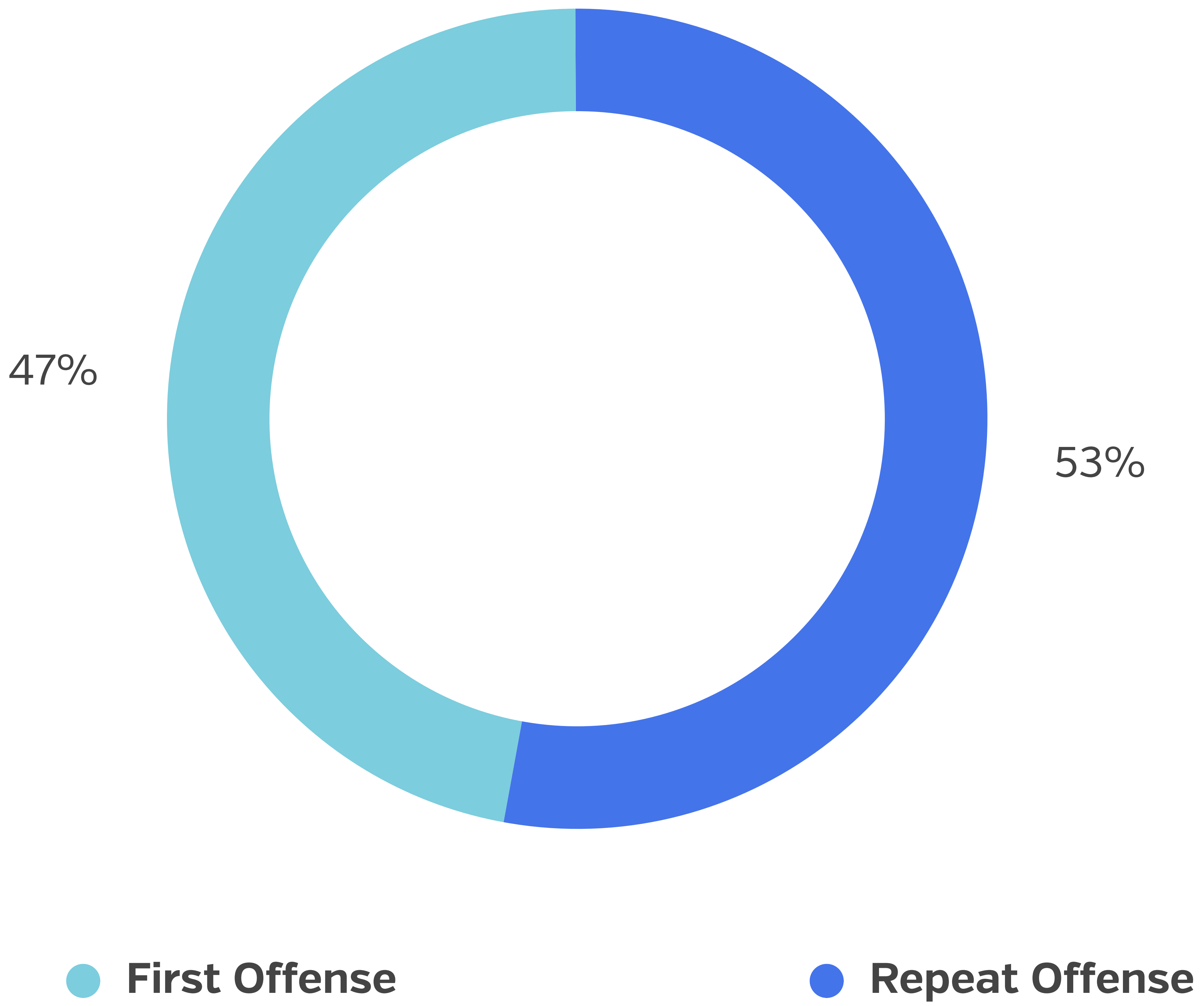
**$1.44M HIPAA FINE**

Pharmacist snoops in husband's ex-girlfriend's medical record

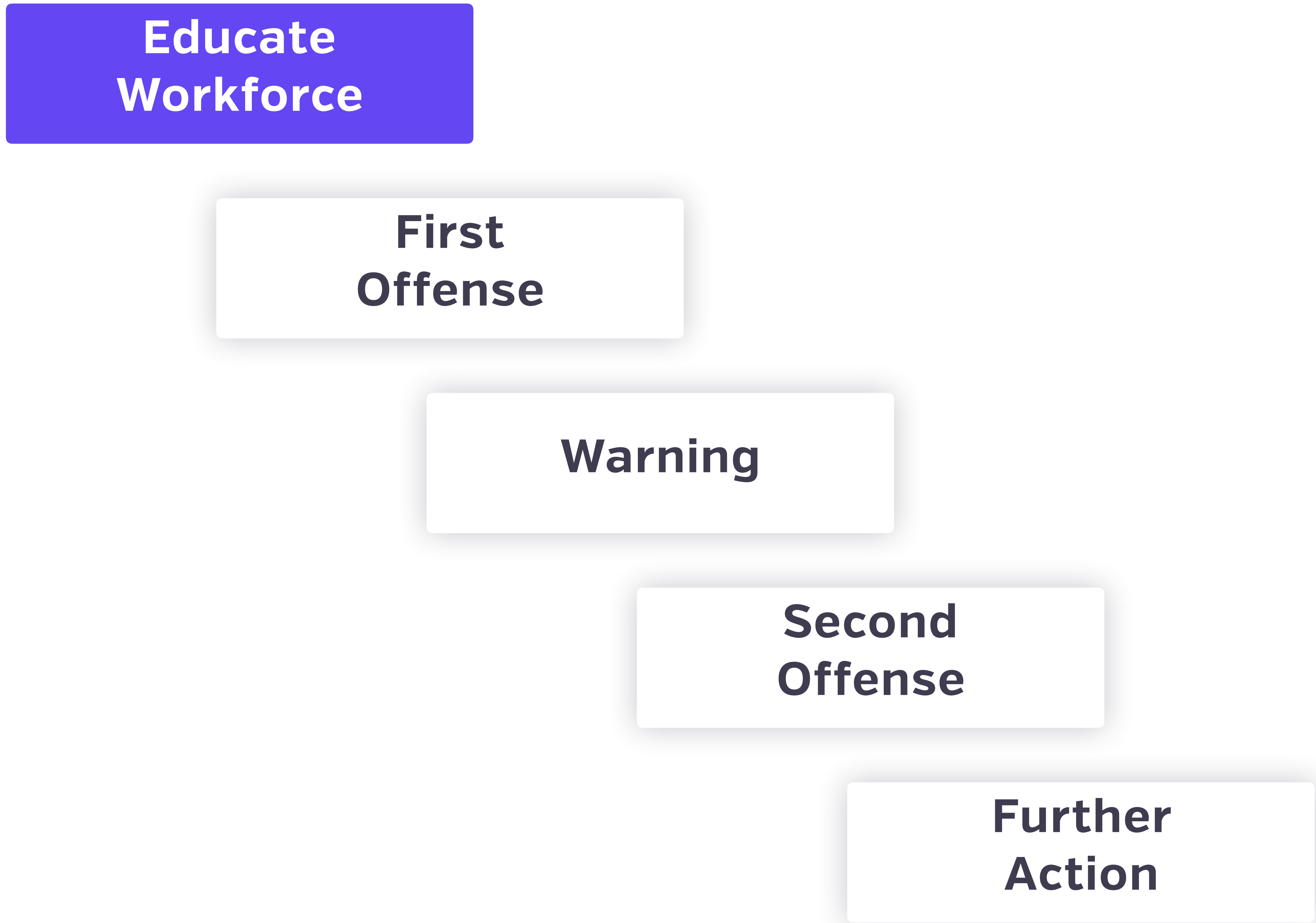
# Snooping Incidents



# Most Violators are Repeat Offenders



# Procedure - Family Member Snooping



Educate Workforce

First Offense

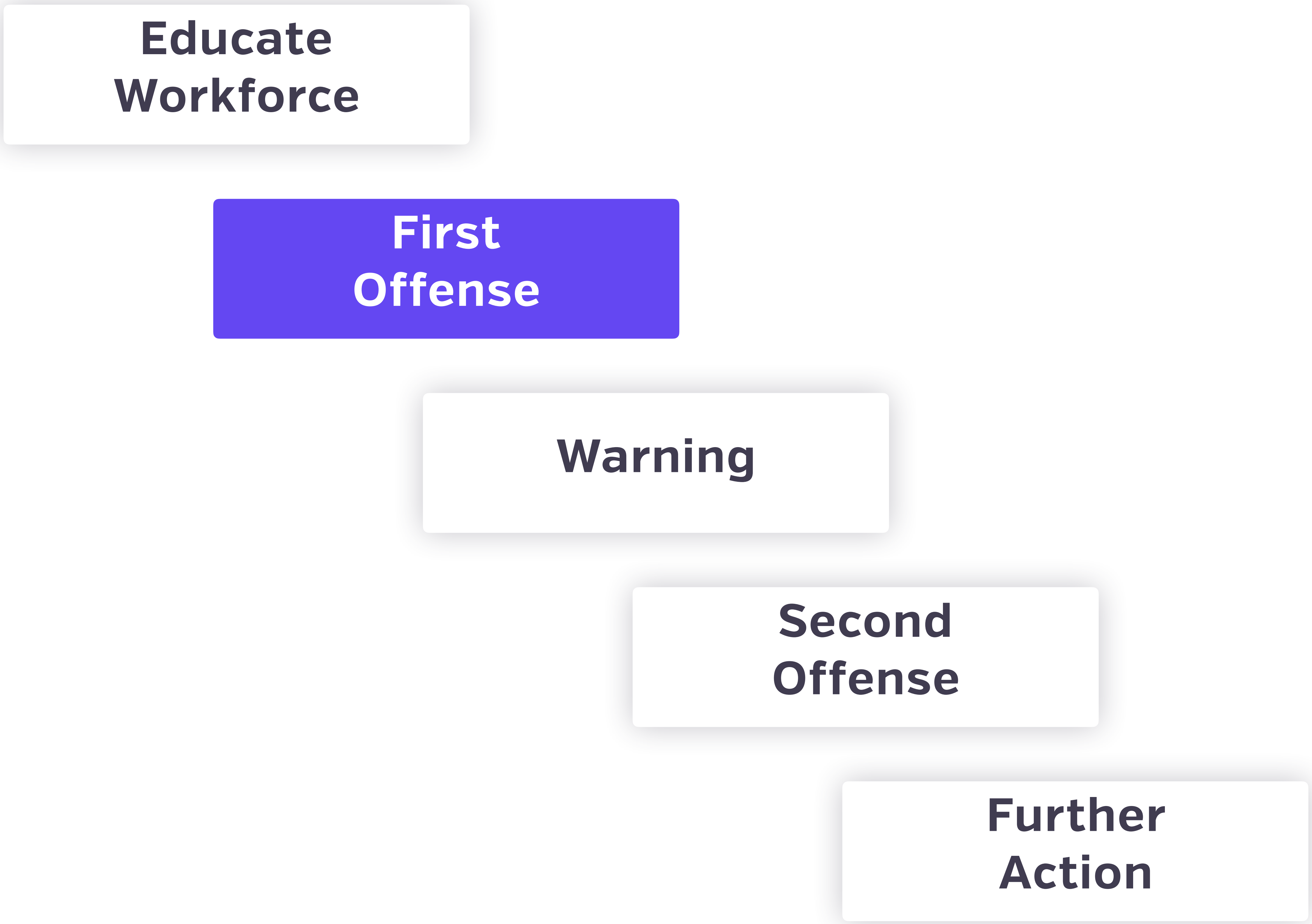
Warning

Second Offense

Further Action

- New employee orientation
- Annual online training
- Periodic privacy campaigns
- Bi-annual broadcast message
- On the spot education

# Procedure - Family Member Snooping



Educate Workforce

First Offense

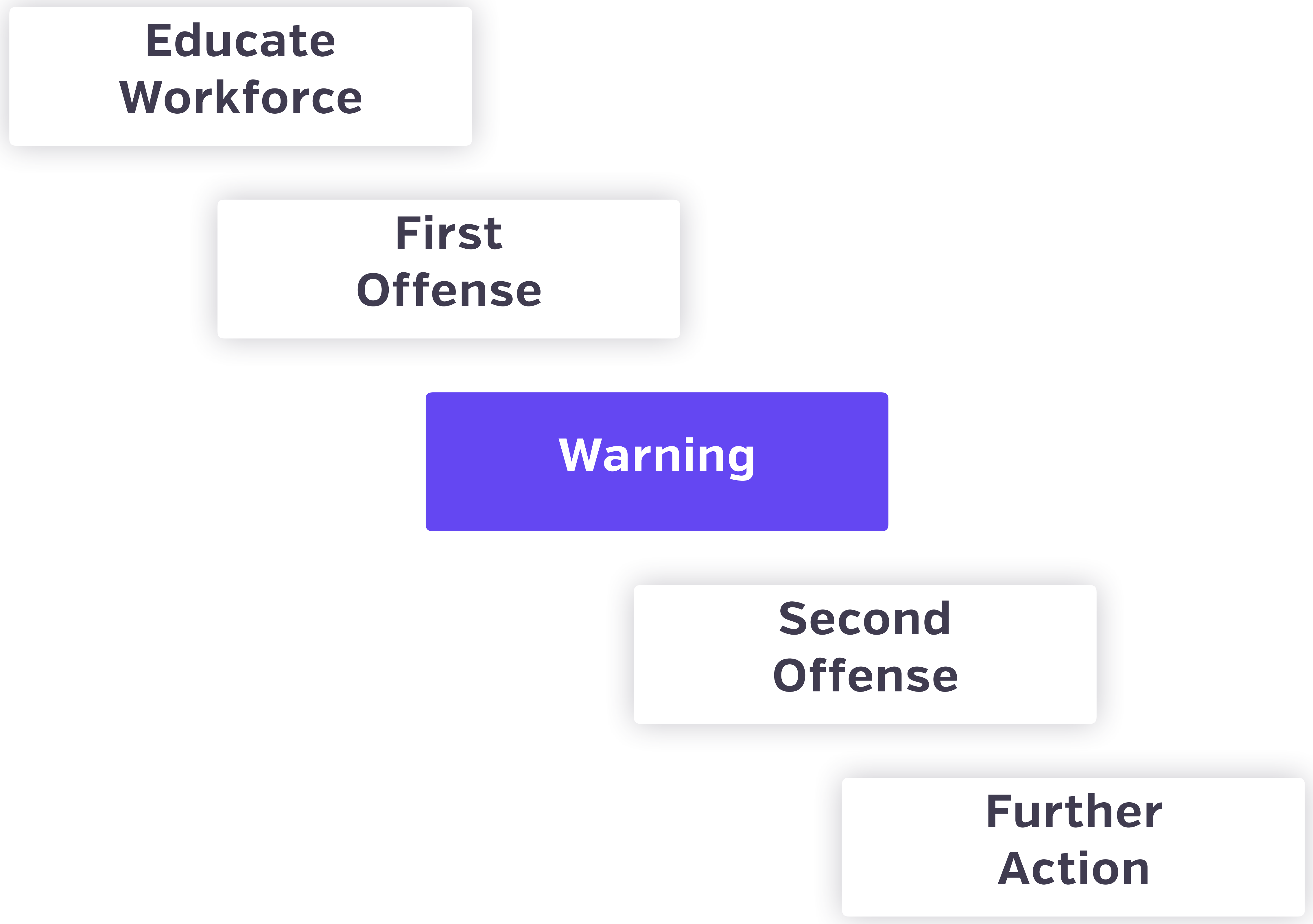
Warning

Second Offense

Further Action

- High-volume, low-risk
- Too many cases to address
- Typical response is just a warning

# Procedure - Family Member Snooping



Educate Workforce

First Offense

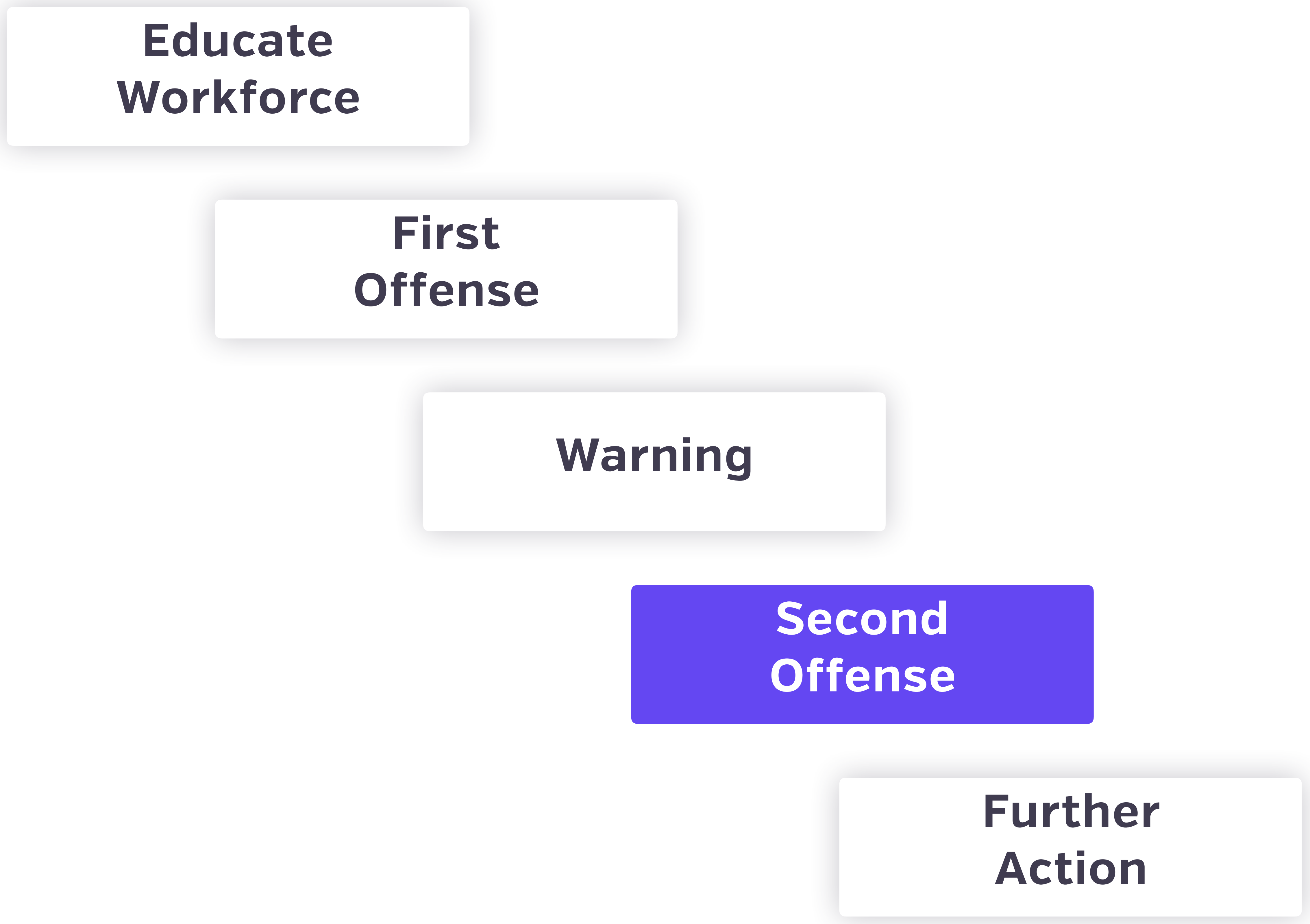
Warning

Second Offense

Further Action

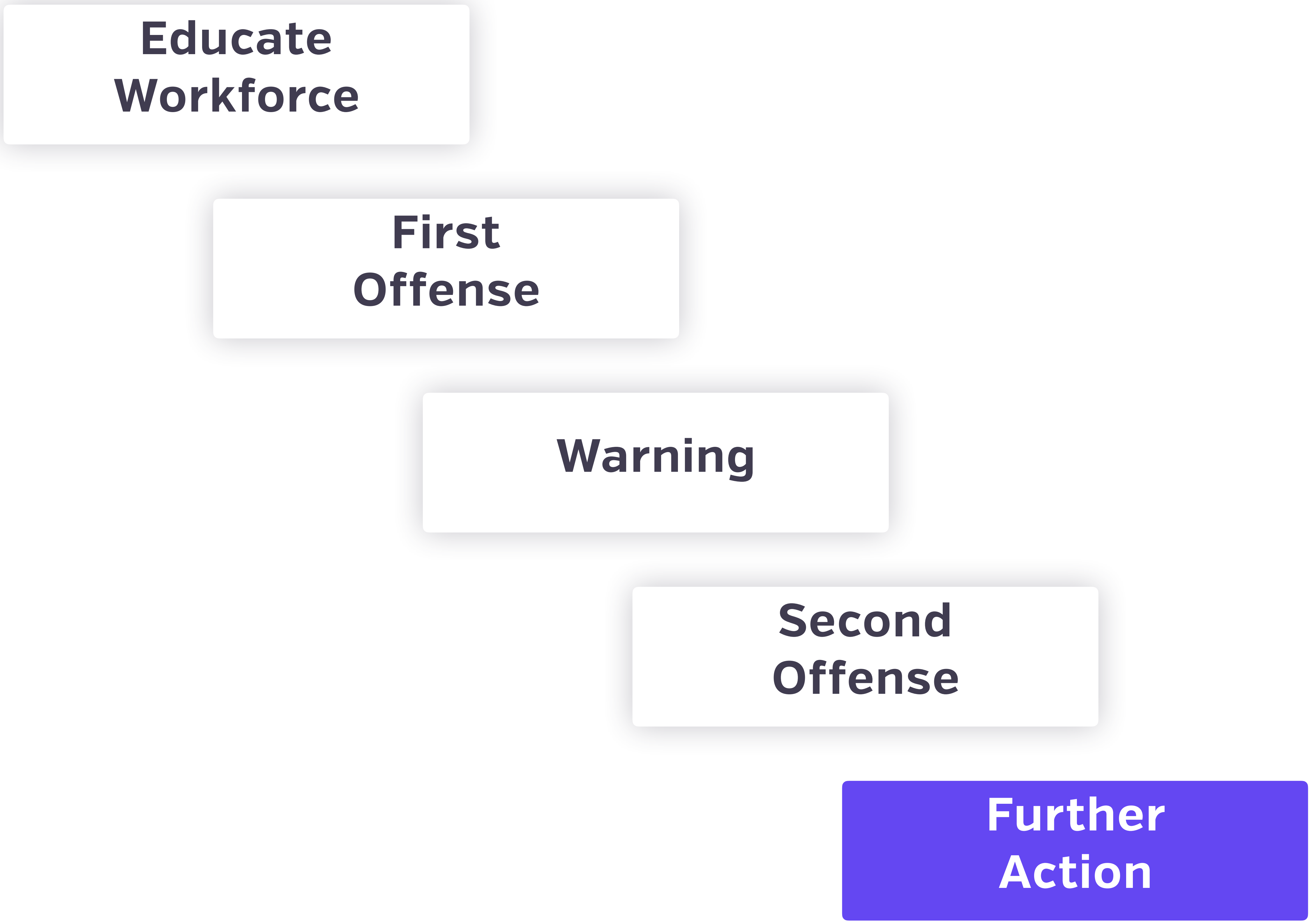
- Automate e-mail notice
- On-the-spot education
- Provide link to the policy
- Request follow up from the workforce member

# Procedure - Family Member Snooping



- Prioritize for human review
- Documented track record of first offense, warning, response (or lack of response), and second offense

# Procedure - Family Member Snooping



Educate Workforce

First Offense

Warning

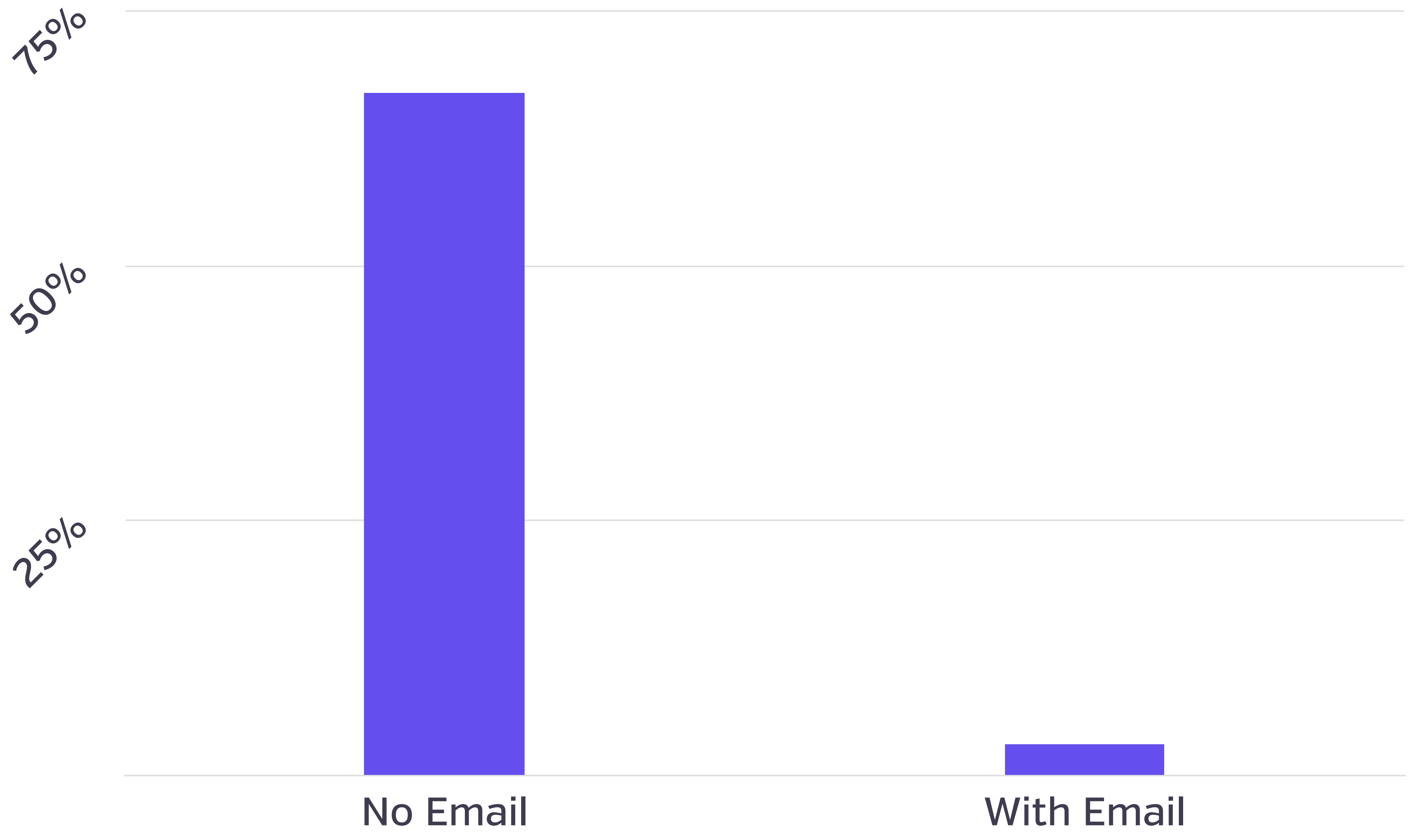
Second Offense

Further Action

- Assist in bringing workforce member into compliance with policy (if applicable)
- Sanctions or termination (if applicable)
- Address breach notification requirements (if applicable/appropriate)

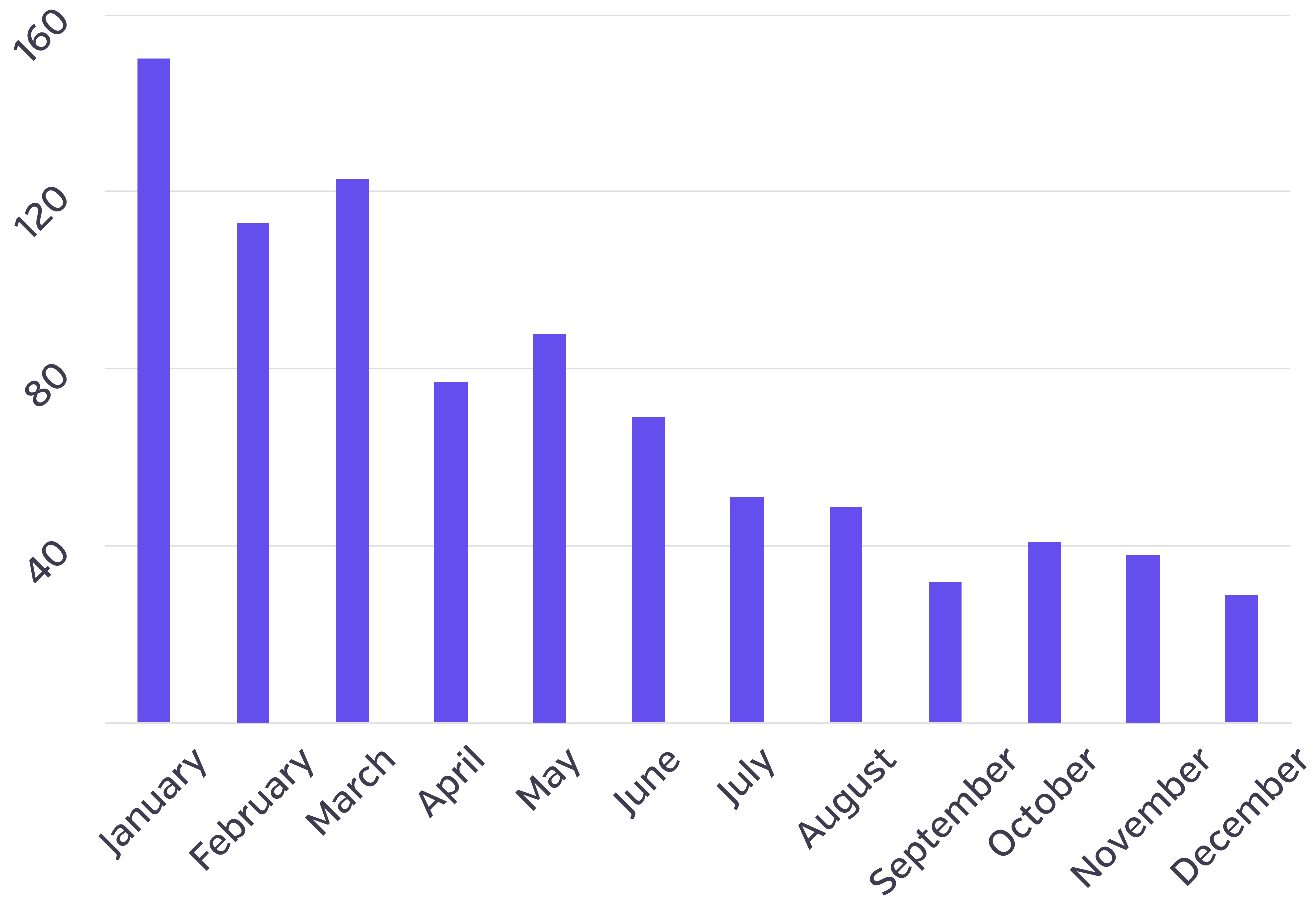
# Controlled Study: On-the-Spot Email Education

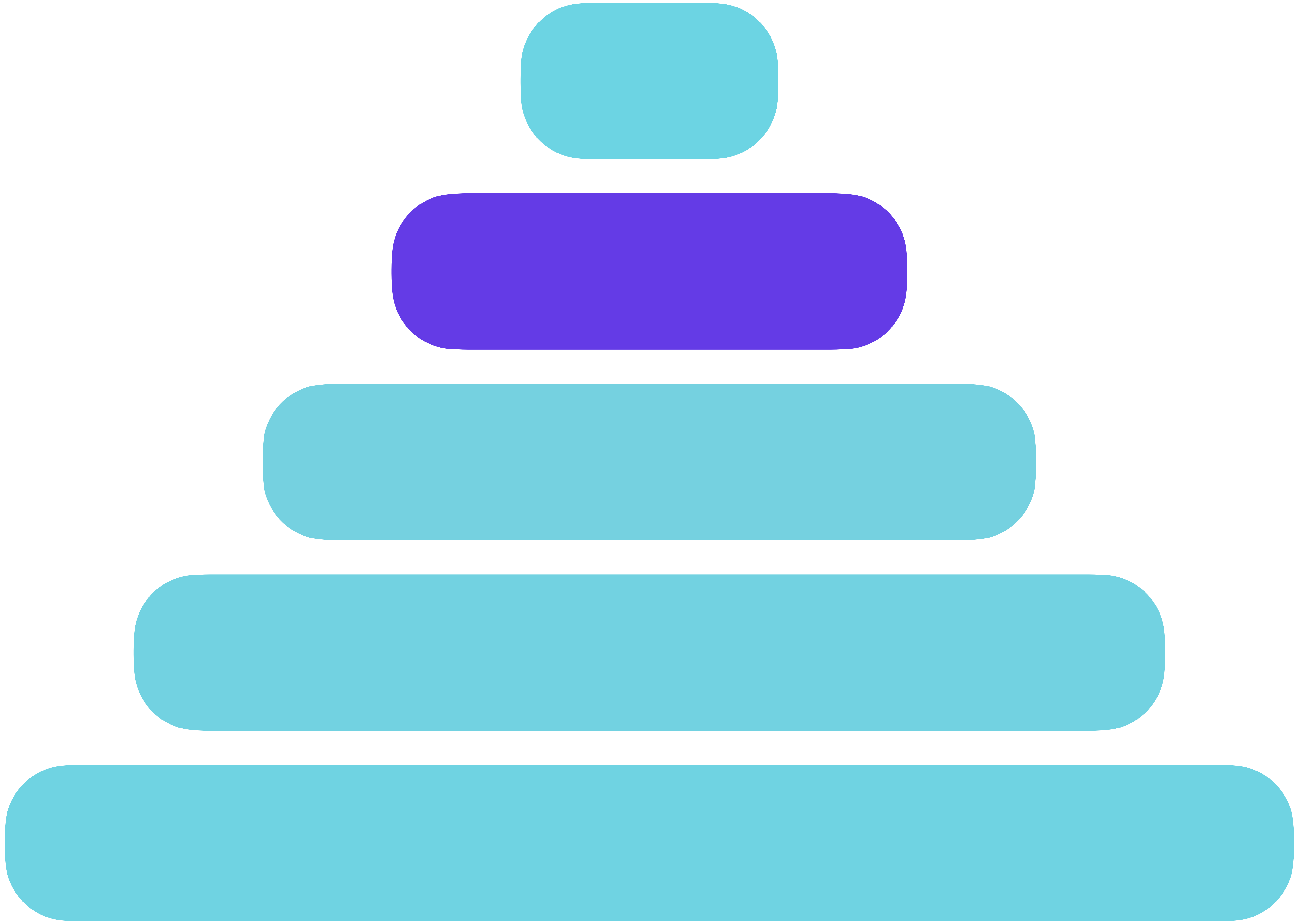
- With no email education, there was a **60-70%** chance of a repeat offense.
- With email education, there was a **2-3%** chance of a repeat offense.



# Controlled Study: Family Snooping Over Time

- With these types of processes, we've seen a decline in privacy violations over time.
- On-the-spot education has a significant impact on the reduction of risk over time.

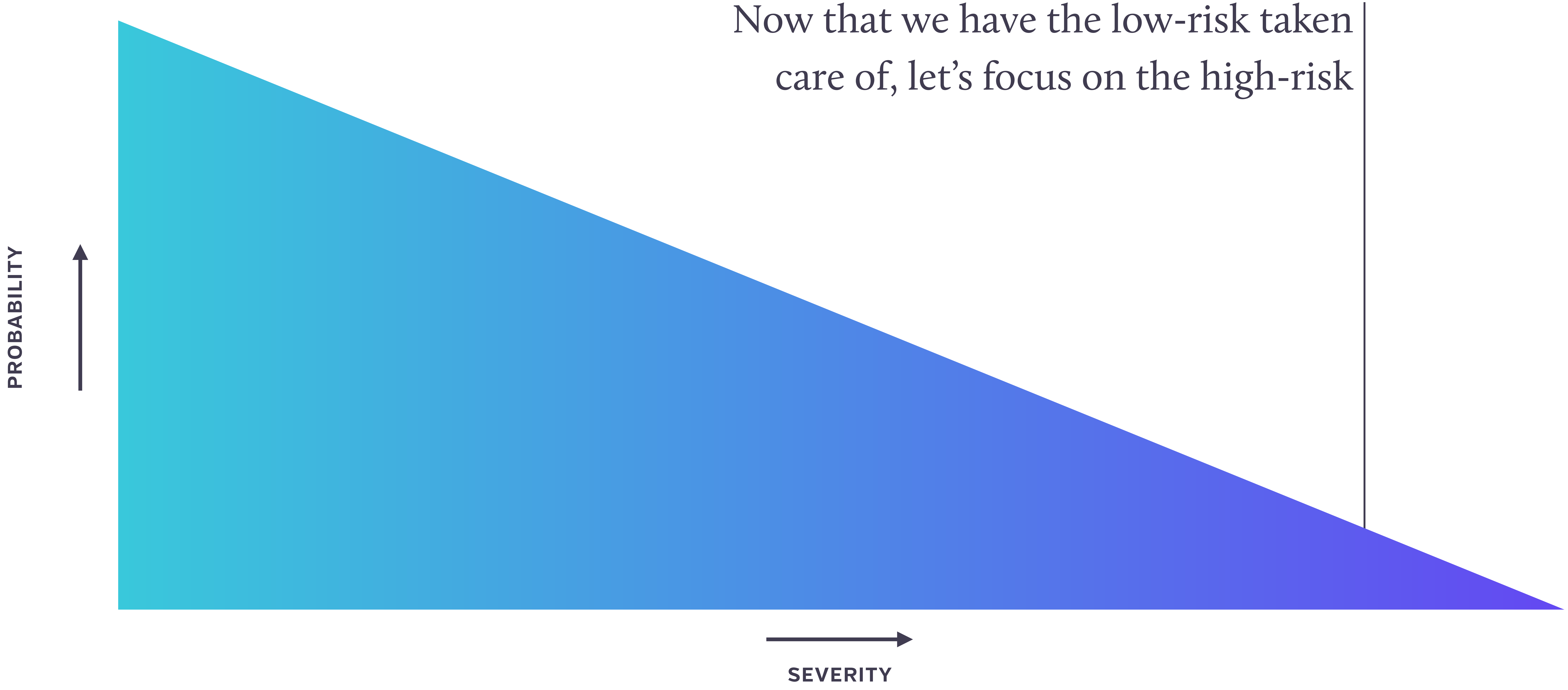


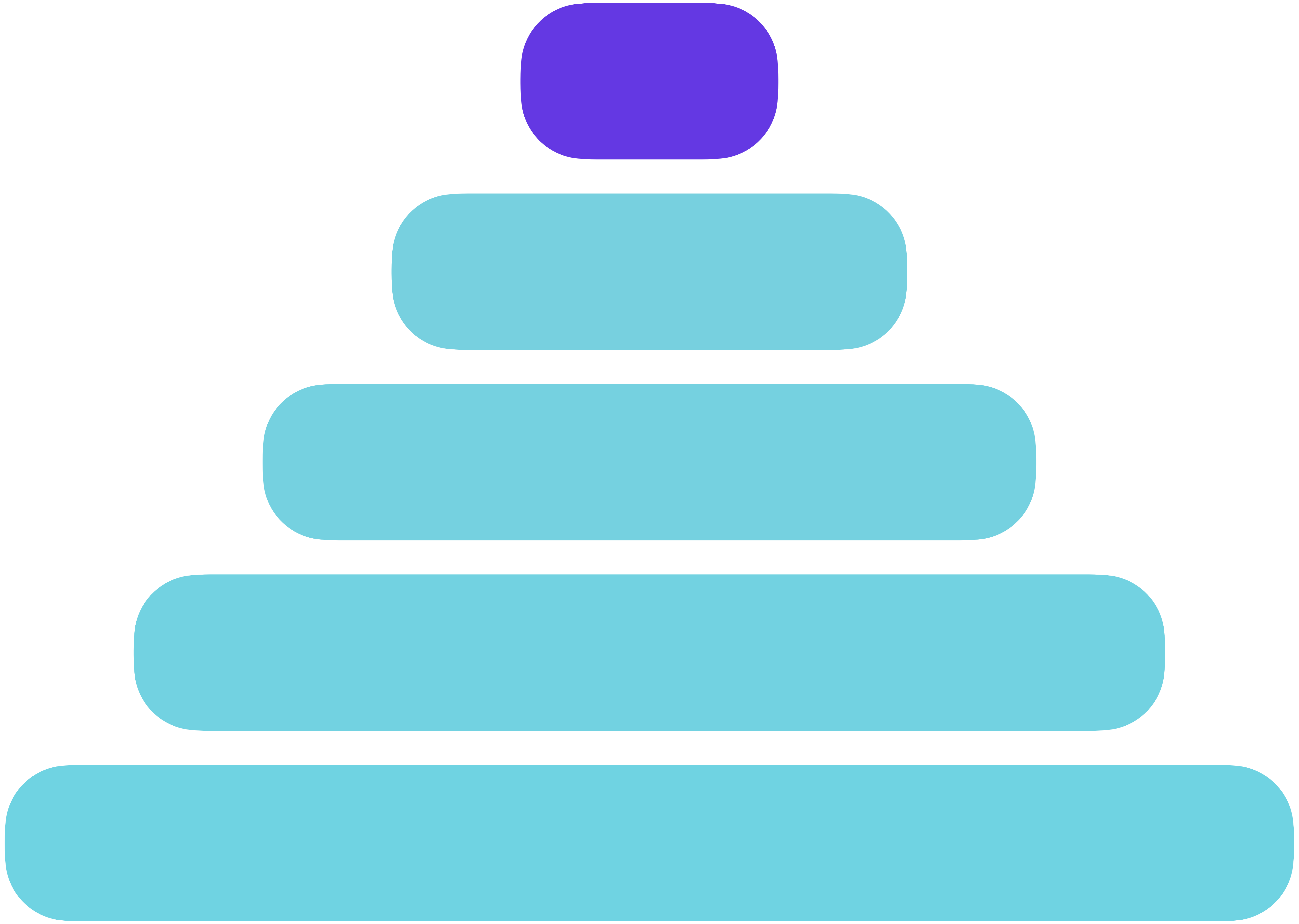


# Best Practice Layer 4: Proactively Identify VIPs and Patients in Media

Leverage publicly available resources to proactively identify and protect VIP records and patients mentioned in the news and social media.

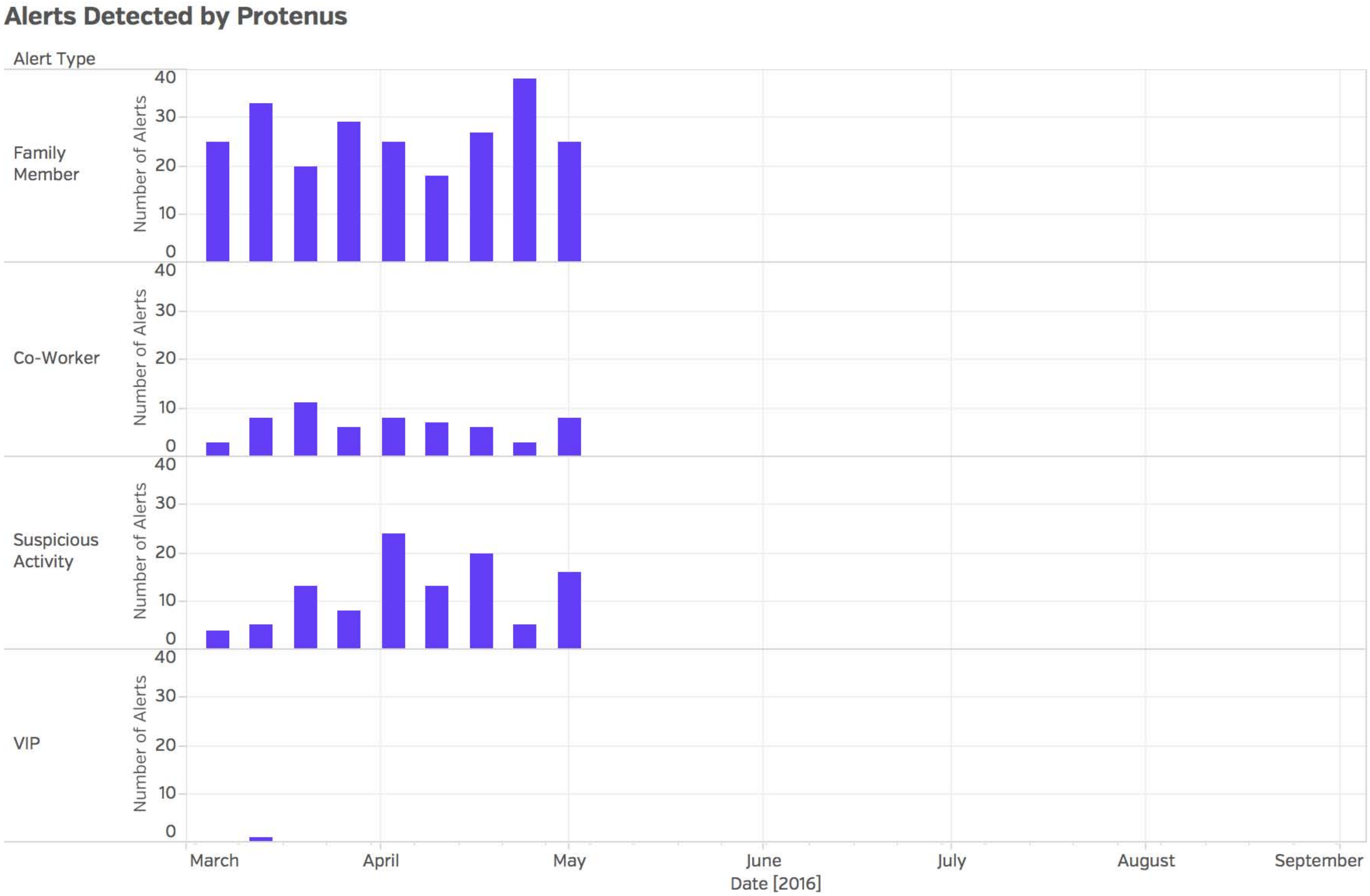
Now that we have the low-risk taken care of, let's focus on the high-risk

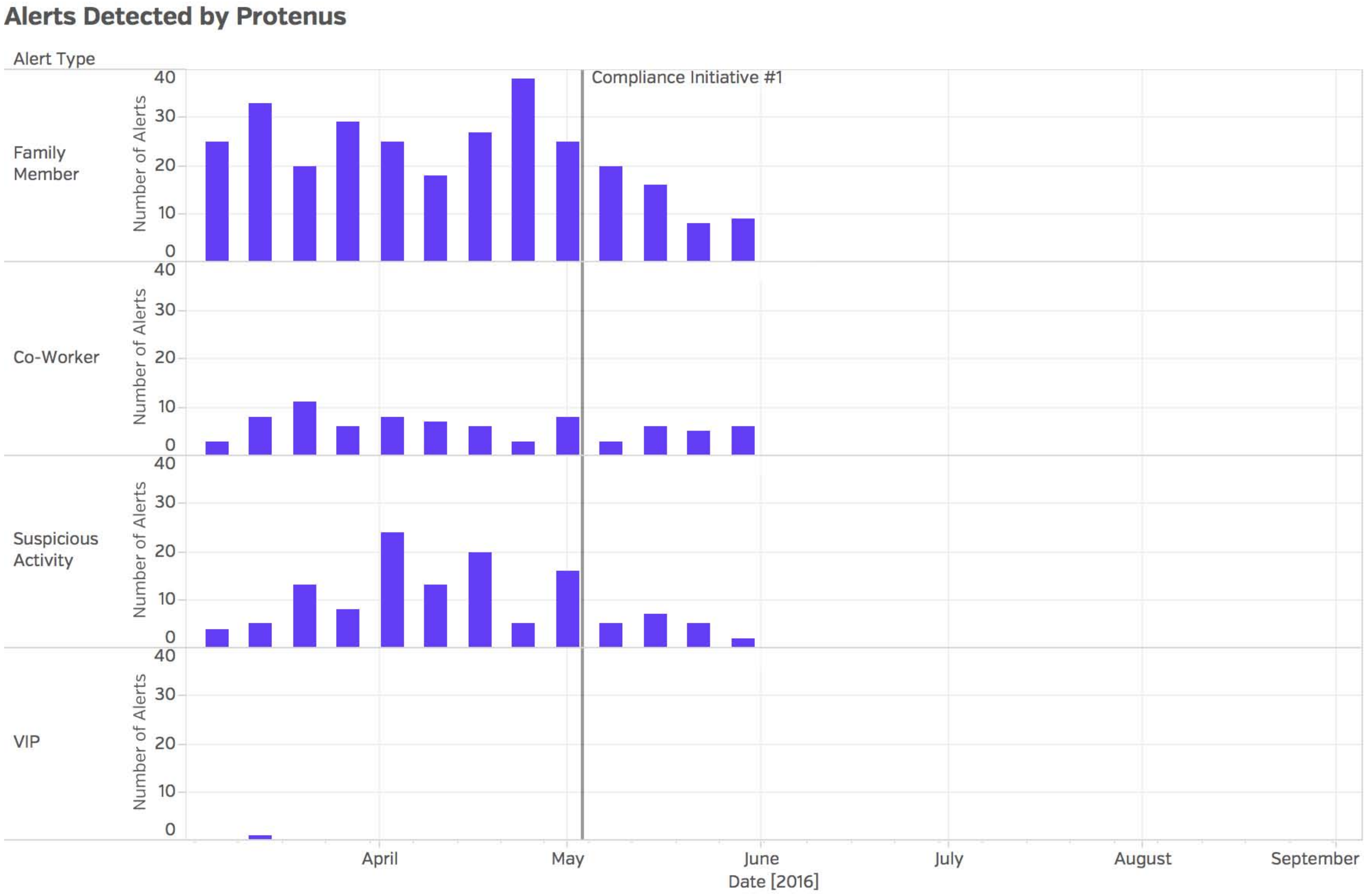




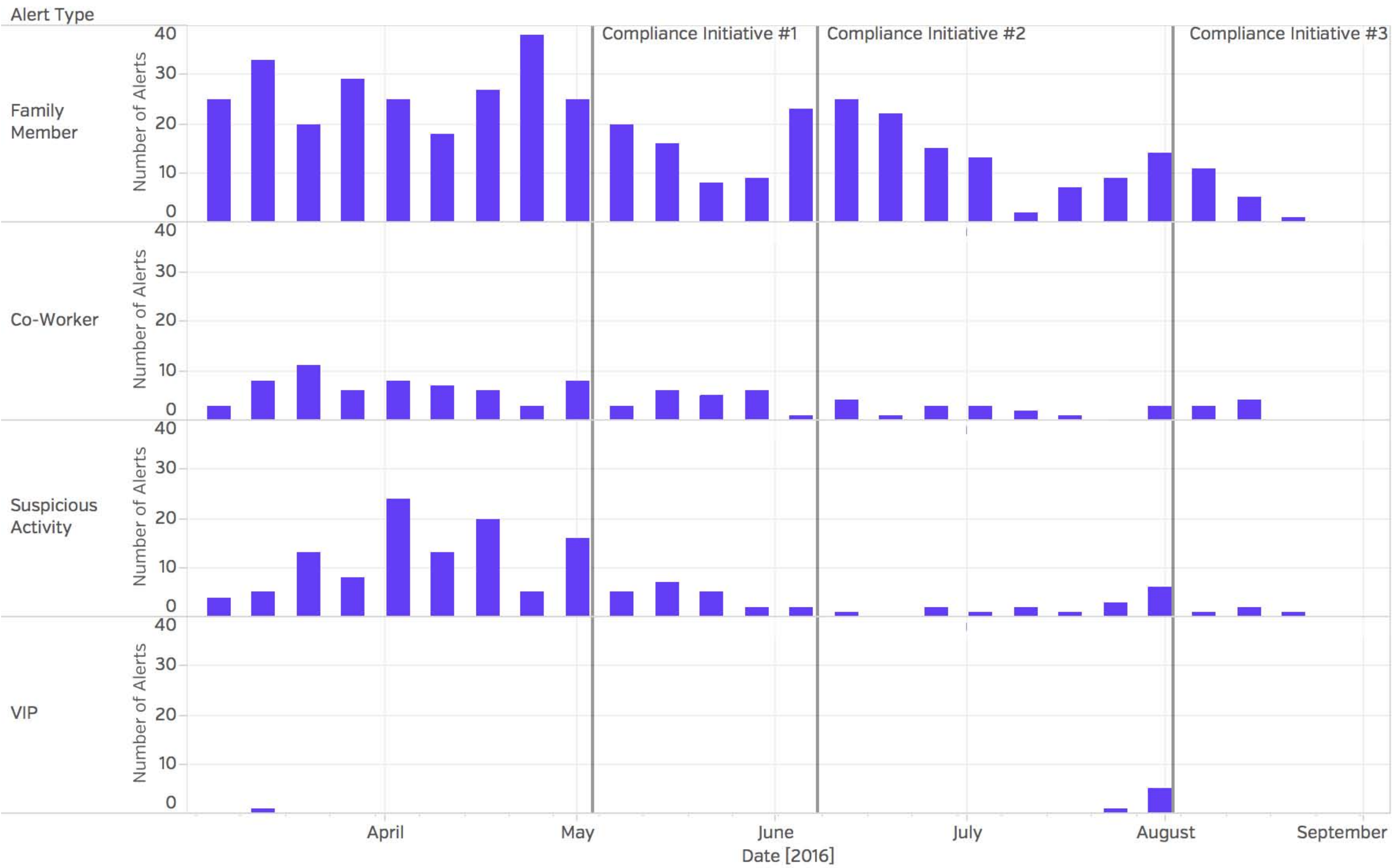
## Best Practice Layer 5: Use results to drive change

By proactively auditing every access to every record, you can measure the efficacy of your privacy program and fine tune policies, education, and workflows.


Alerts Detected by Protenus
Alert Type
Family Member
Co-Worker
Suspicious Activity
VIP
Number of Alerts
0
10
20
30
40
March
April
May
June
July
August
September
Date [2016]

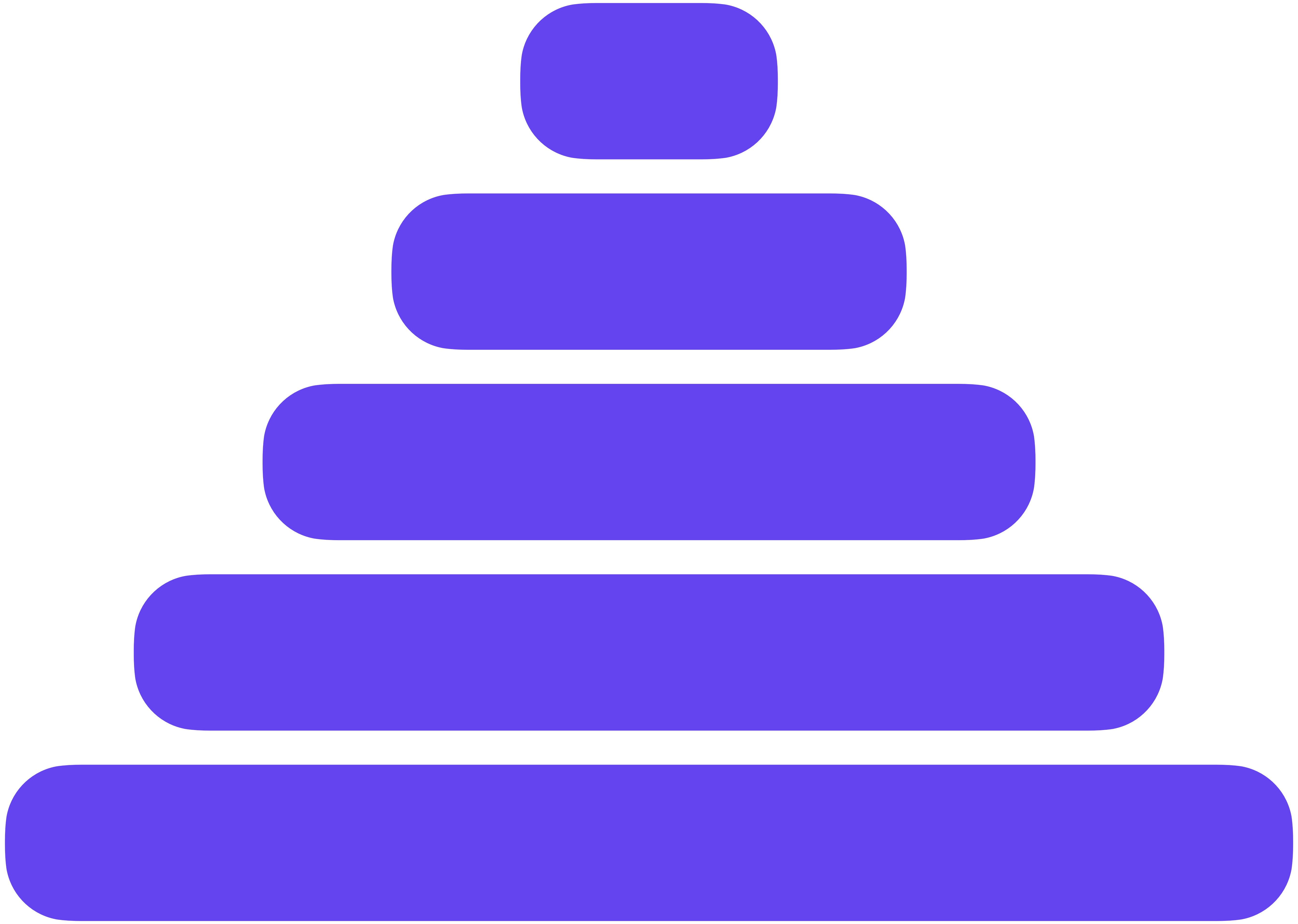

Alerts Detected by Protenus
Alert Type
Family Member
Co-Worker
Suspicious Activity
VIP
Number of Alerts
0
10
20
30
40
Compliance Initiative #1
April
May
June
July
August
September
Date [2016]

## Alerts Detected by Protenus



18% of healthcare employees said they would be willing to sell confidential data to unauthorized parties for was little as $500, according to a survey from Accenture.

# Let’s Review!



# Building effective monitoring from the ground up

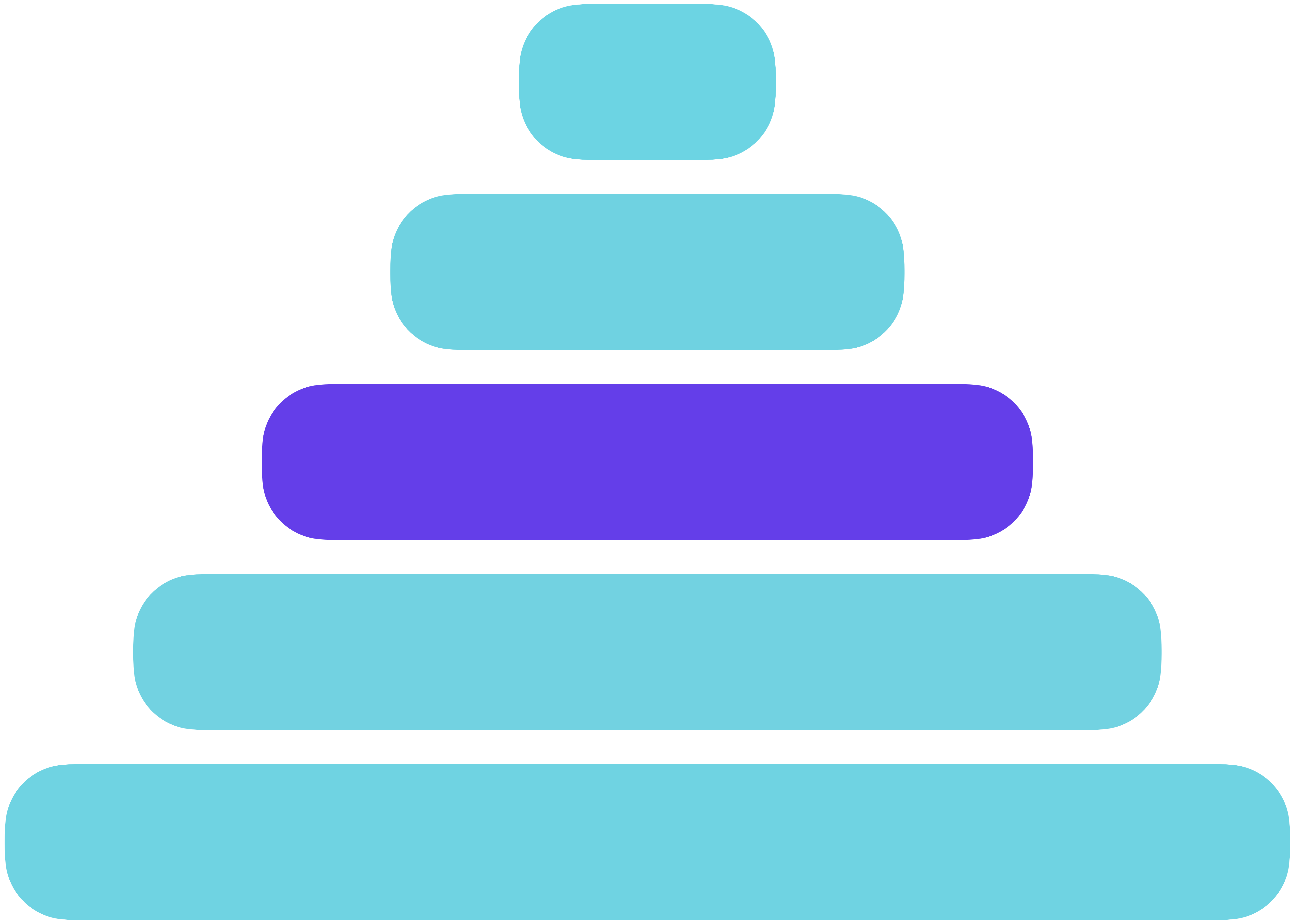
Each layer of you privacy monitoring program holds opportunity to improve efficiency and efficacy.

# Best Practice Layer 1: Centralized Audit Log Data

Bring disparate audit log data from across the enterprise together under a “single pane of glass” in order to prevent data scrounging;

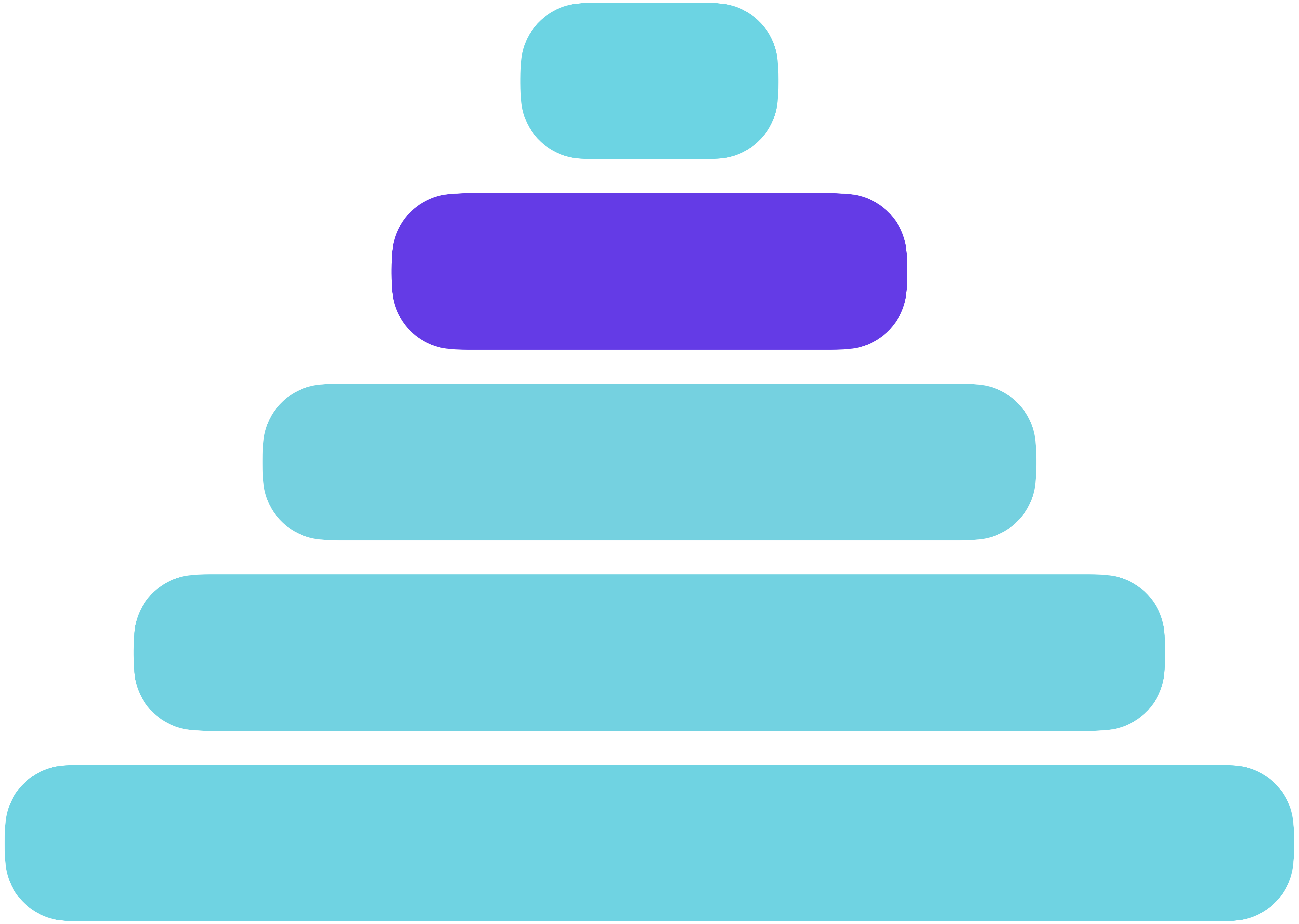
# Best Practice Layer 2: Leverage A.I. to Audit Every Access

A significant portion of auditing requires basic, repetitive data exploration - the kind of work that is ideal for artificial intelligence.



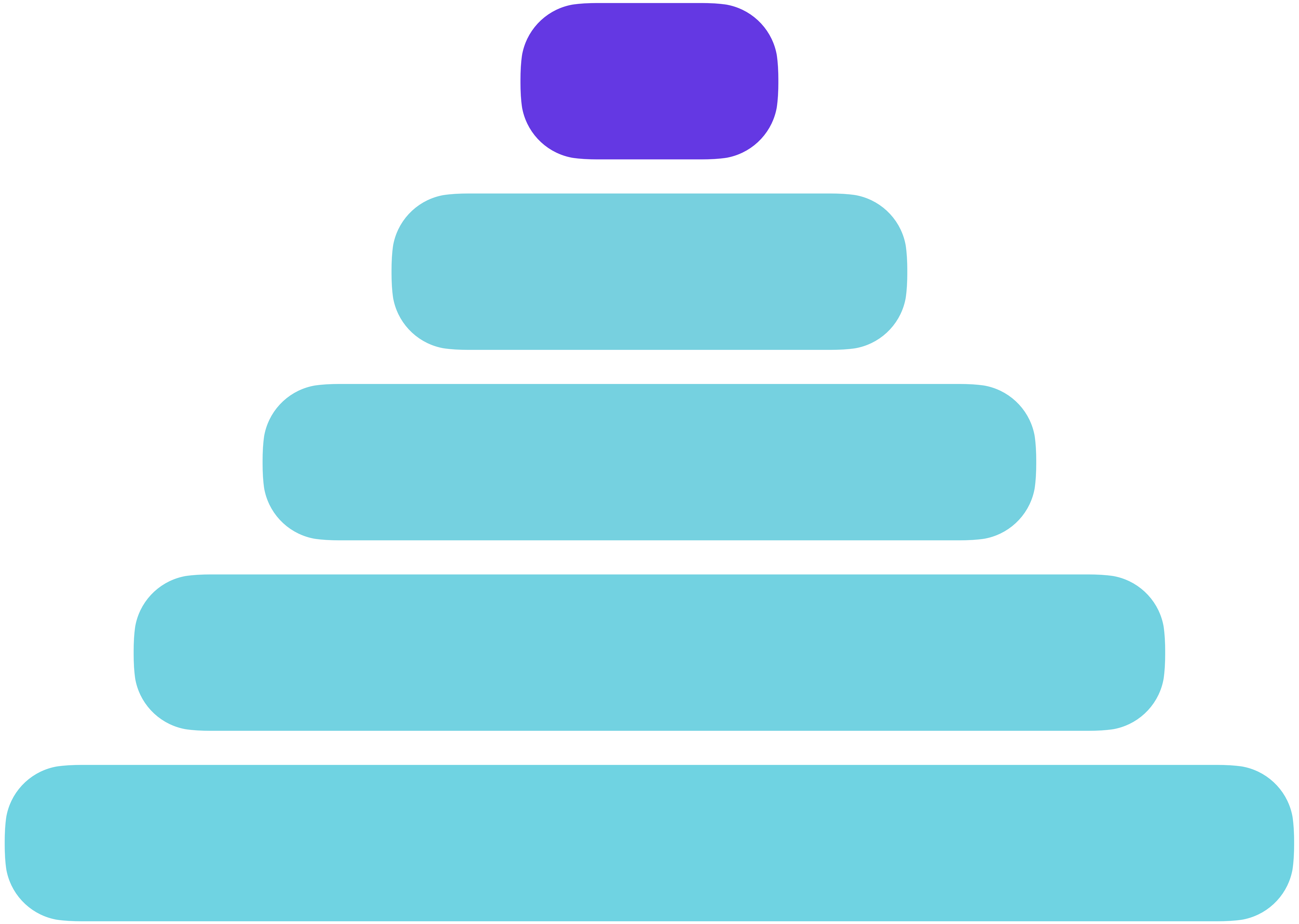
## Best Practice Layer 3: Put Privacy Operations on Autopilot

Align processes with policy in order to automate investigation procedures.  Enforce policies at scale and prevent violations before they happen.



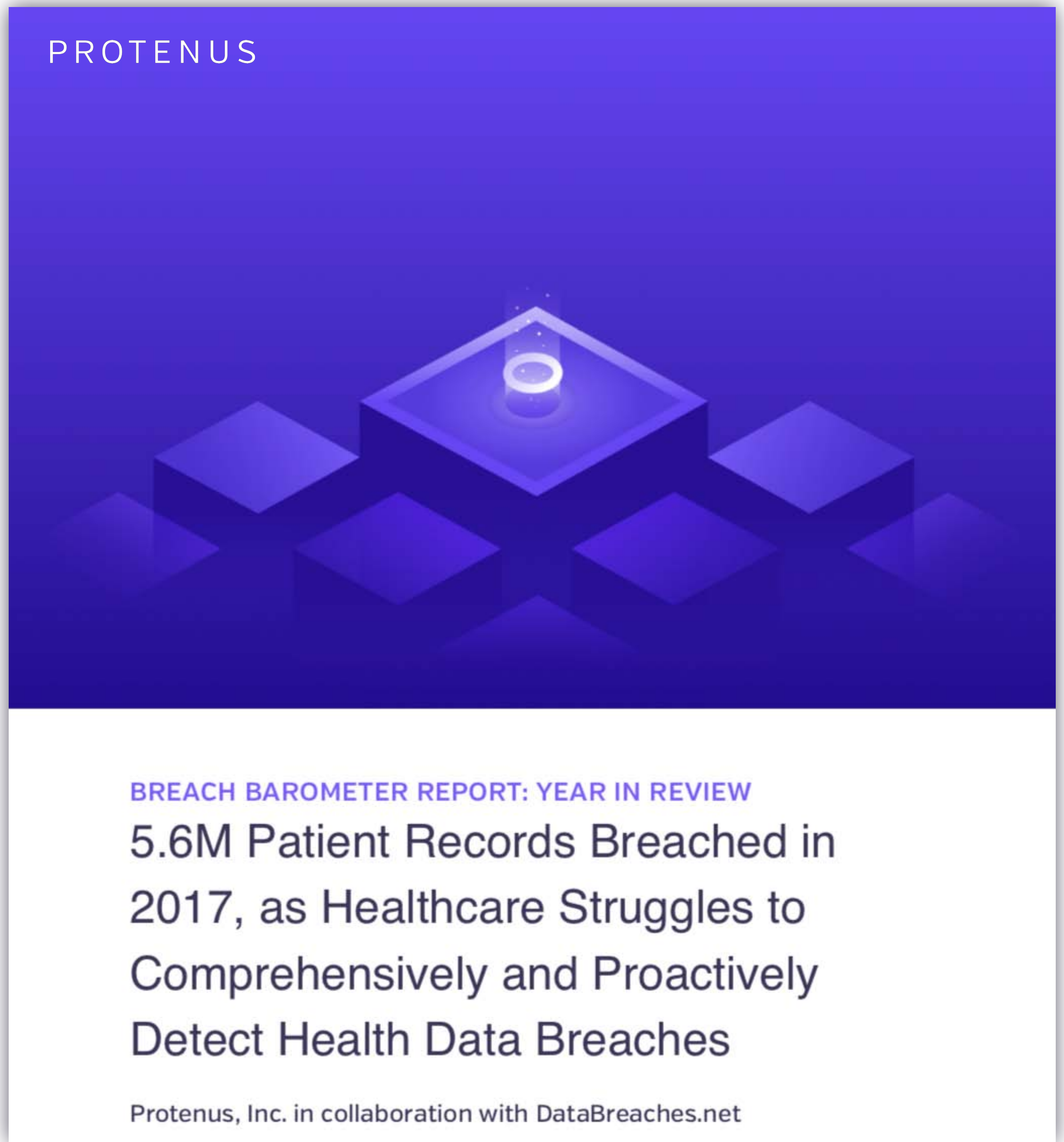
# Best Practice Layer 4: Proactively Identify VIPs and Patients in Media

Leverage publicly available resources to proactively identify and protect VIP records and patients mentioned in the news and social media.



# Best Practice Layer 5: Use results to drive change

By proactively auditing every access to every record, you can measure the efficacy of your privacy program and fine tune policies, education, and workflows.



PROTENUS

BREACH BAROMETER REPORT: YEAR IN REVIEW

5.6M Patient Records Breached in 2017, as Healthcare Struggles to Comprehensively and Proactively Detect Health Data Breaches

Protenus, Inc. in collaboration with DataBreaches.net

For more statistics, take a look at the Breach Barometer™, a full picture and analysis of reported or disclosed breaches impacting the health care industry.

www.protenus.com/breach-barometer-report

Learn more about what we're learning at info@protenus.com or follow us on Twitter @Protenus