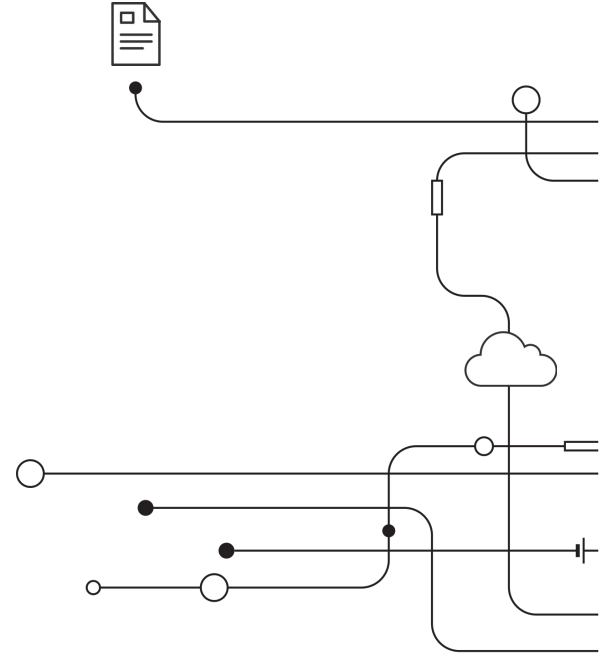


Safeguarding Product Designs and IP in Manufacturing



CYBERHAVEN

Agenda

- + Scope of the problem
- + Tips for protecting IP
- + Why IP protection is hard
- + IP protection technology



trade **INTELLECTUAL** **PROPERTY** **SECRETS**
industrial **PATENTS** exclusive **RIGHTS** **LAW**
INNOVATION formulas **designs** **COPYRIGHT** process
protection assets **INFRINGEMENT**



Poll Question 1



Manufacturing IP

- + Engineering Designs
- + Schematics
- + Source Code
- + Formulas
- + Bill of Materials
- + Supply chain pricing
- + Trade Secrets
- + Test Results
- + Product Roadmaps
- + Engineering Change Notifications
- + Patents

2020 Data Breach Investigations Report

<https://enterprise.verizon.com/resources/reports/dbir/2020/introduction>

Manufacturing NAICS 31-33

While the majority of attacks are financially motivated, there was a respectable showing of Cyber-Espionage-motivated attacks in this industry as well. Internal employees misusing their access to abscond with data also remains a concern for this vertical.

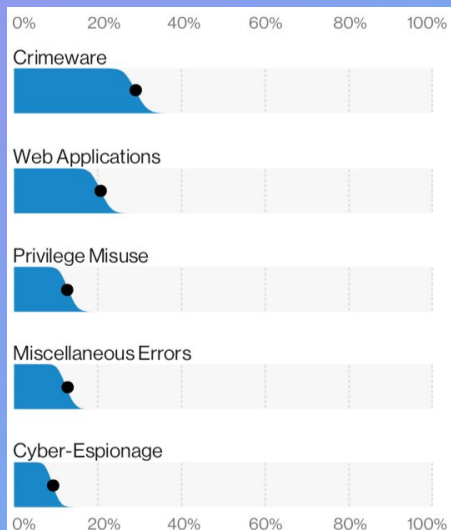
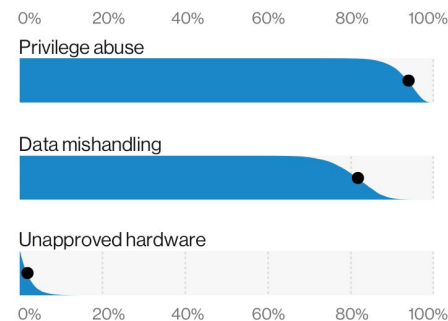


Figure 75. Patterns in Manufacturing industry breaches

The **Manufacturing vertical** is very well **represented** this year with regard to both incidents and breaches.

NAICS 31-33 has long been a much-coveted target of cybercrime and this year is no exception. Whether it is a nation-state trying to determine what its adversary is doing (and then replicate it) or just a member of a startup who wants to get a leg up on the competition, there is a great deal of valuable data for attackers to steal in this industry. And steal it they do.

Figure 77. Misuse varieties in Manufacturing industry breaches



By the Numbers

\$600B

Annual Cost
of IP Theft
to US

<https://tinyurl.com/y5ojcesu>

\$1.5T

Cybercrime
Illicit Profits

<https://tinyurl.com/y53w2j7x>

\$1.9B

Single IP
Theft
Incident

<https://tinyurl.com/y58he6g2>

Tesla is suing Alex Khatilov, alleging that he stole files related to their Warp Drive software and moved them to his personal Dropbox.

The American Genius

the pulse of today's entrepreneur

Tesla continues to deal with former employees and potential IP theft

(BUSINESS NEWS) Tesla has found itself at the center of numerous lawsuits against former employees and the theft of intellectual property, potentially jeopardizing their industry leadership position.



Published on February 1, 2021
By Robert Snodgrass, Staff Writer

Featured Article

Anthony Levandowski sentenced to 18 months in prison as new \$4B lawsuit against Uber is filed

Maverick self-driving car engineer will not need to report until threat of COVID-19 pandemic has passed

Kirsten Korosec, Mark Harris / 4:57 PM MDT • August 4, 2020



U.S. District Attorney charged Levandowski alone with 33 counts of theft and attempted theft of trade secrets

The magnitude of intellectual property theft over the past decade has been staggering, into the billions, probably the trillions

DARKReading

 SIGN UP FOR OUR NEWSLETTERS

2/1/2021
12:40 PM

US Needs Comprehensive Policy to Combat China on IP Theft



Robert Lemos
News

The United States cannot lose sight of Chinese cyber operations that target intellectual property, a panel of experts says.

The United States needs a more systematic approach to engage with China on cybersecurity and intellectual property issues, and to address the ongoing theft of industrial and defensive technologies via cyberattacks, a panel of policy and technology experts stated last week.

 0 COMMENTS



HOME NEWS COVID-19

5 signs there could be IP theft in your supply chain

From patent and copyright infringement to compromise of trade secrets and blueprints, intellectual property theft is a growing problem worldwide.

By Craig Guillot
31 January 2021

Employees, contractors, and third parties are responsible for 54% of all IP data theft experienced by organisations

Real World Example 1



The Billion-Dollar Secret

- + Scientist resigns
- + Downloaded IP to USB
- + Guilty plea + 24 months

“If you got your hands on this information, you would be decades ahead...”

Real World Example 2

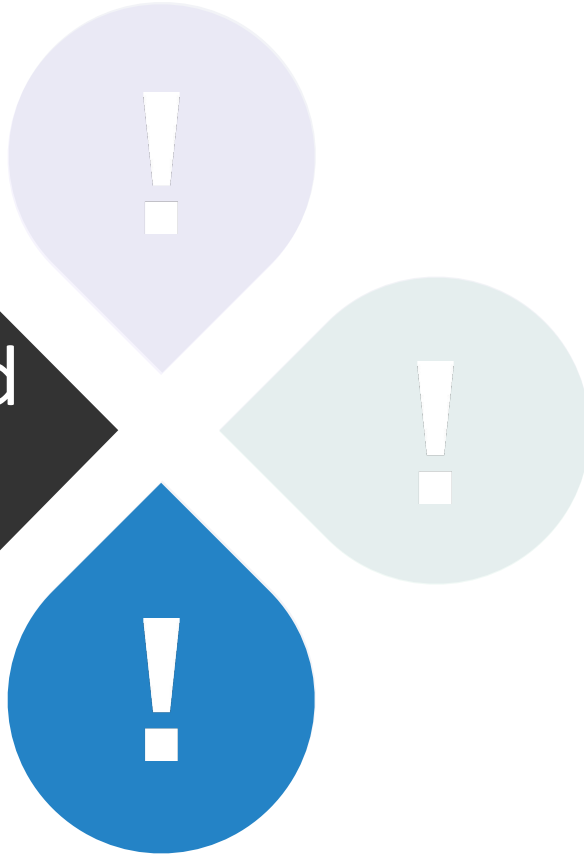


A Super Happy New Year

- + Dec 31 departing employee
- + Thousands of design files
- + Police alerted, loss averted

**“This was a big win for us and
absolutely proved the value.”**

Real World Example 3



So Long, Farewell...

- + Smartphone innovation
- + Tech couldn't stop it – or identify the culprit
- + 120 minute reveal

**“Finally had the evidence to
terminate the employee.”**

Tips for IP Protection

1. Make protection a priority
2. Understand your IP
3. Monitor data use
4. Use data protection tech
5. Train employees



Poll Question 2

- Why is protecting IP so dang hard?

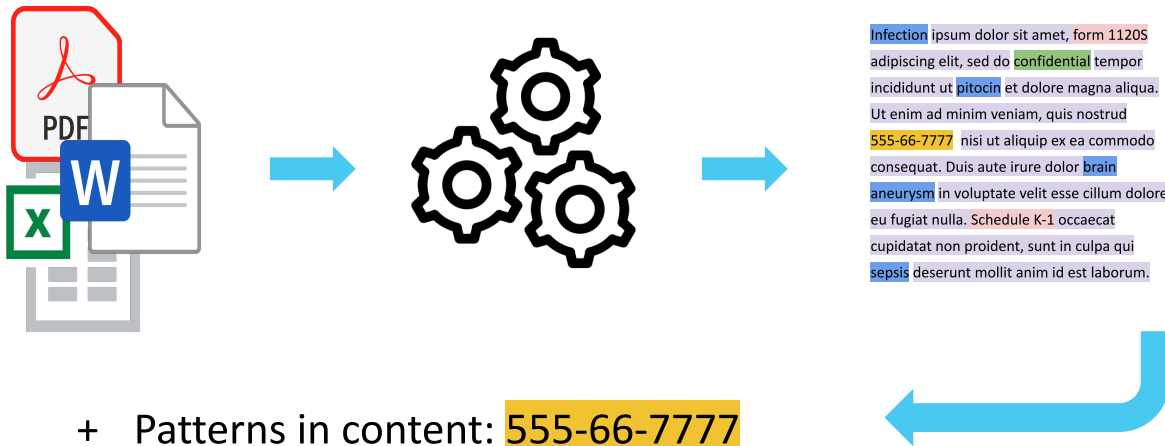


Accurate detection
is the **KEY**

Detection Methods

- + Content inspection 1
- + Content inspection 2
- + Content inspection 3
- + Content inspection 4
- + Content inspection 5

Content Inspection



- + Patterns in content: 555-66-7777
- + Keywords in content: confidential
- + Statistical analysis of content: 5x healthcare, 2x financial
- + Machine learning of content: feed samples of sensitive vs non-sensitive
- + Exact/partial content match

Other Challenges

Limited **visibility**

Requires known **policies**

Only logs policy **violations**



Dynamic Data Tracing technology is a transformative approach to preventing intellectual property theft and other insider threats.

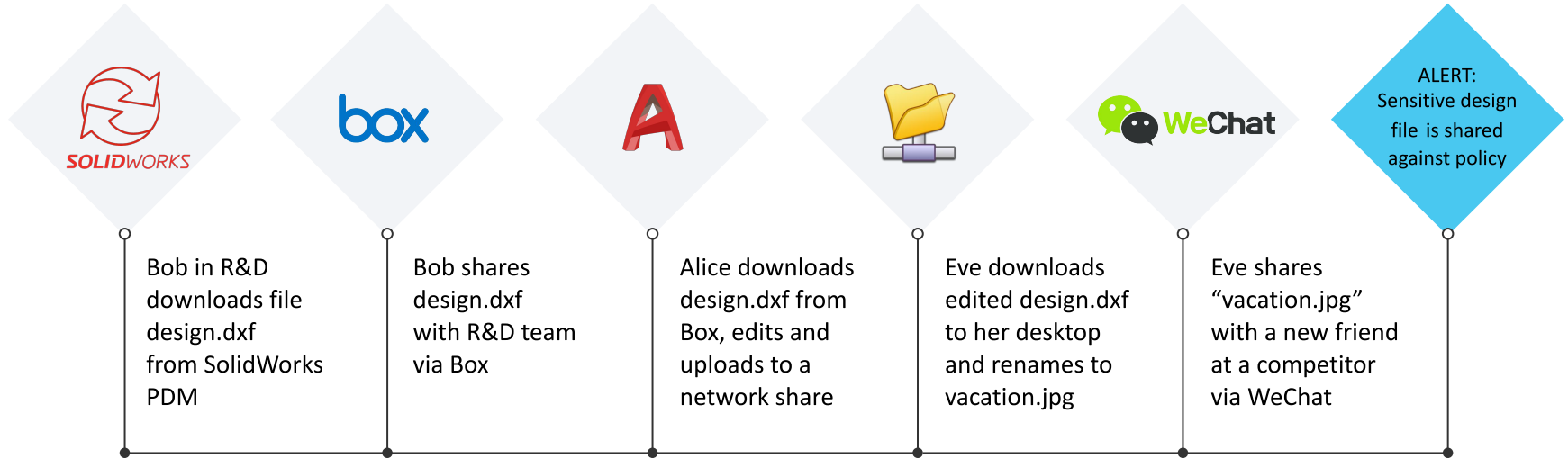
- Every piece of data tells a story

01010
11011
01100

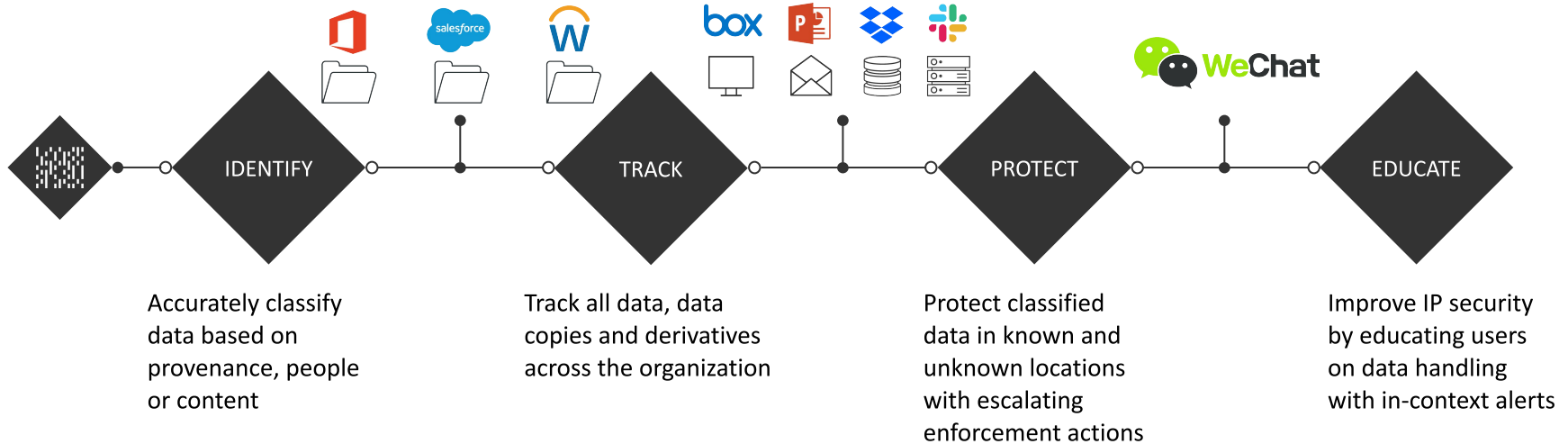


You need the **WHOLE** story to effectively protect IP

Tracing data lineage inside the modern enterprise



Using data lineage for data protection



Visibility Averages/Mo – 1000 Users

1.5M

Individual
Files in Use

5.6M

User
Actions with
Those Files

950/
44

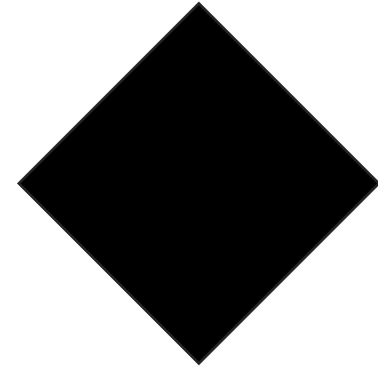
950 Files at
Risk/44 Actual
Incidents

IP Identification

- + Provenance
- + Data location
- + User/group interaction with data
- + Application interaction with data
- + Data attributes



Poll Question 3



New Search

MAP

LIST

INSIGHTS

Time range: 2020-11-18 - 2020-12-22

DATAFLOWS

LOCATIONS

USERS

ATTRIBUTES

LAST ACTIVITY

Project notes.dwg

Internal

2

External

1

donna.scott

2020-12-17, 02:19

Cyberhaven started tracking flow → office_365

2020-11-18, 03:54

donna.scott download file Project notes.dwg → to DONNA-SCOTT-PC

2020-11-18, 03:54

donna.scott moved file Project notes.dwg → on DONNA-SCOTT-PC as Project notes.dwg

2020-11-23, 15:04

donna.scott moved file Project notes.dwg → on DONNA-SCOTT-PC as Project notes.dwg

2020-11-28, 04:39

donna.scott copied file Project notes.dwg → on DONNA-SCOTT-PC as Copy of Project notes.dwg

2020-12-05, 08:04

donna.scott moved file Copy of Project notes.dwg → on DONNA-SCOTT-PC as Copy of Project notes.dwg

2020-12-11, 13:05

donna.scott moved file Copy of Project notes.dwg → on DONNA-SCOTT-PC as Copy of Project notes.dwg

2020-12-14, 14:41

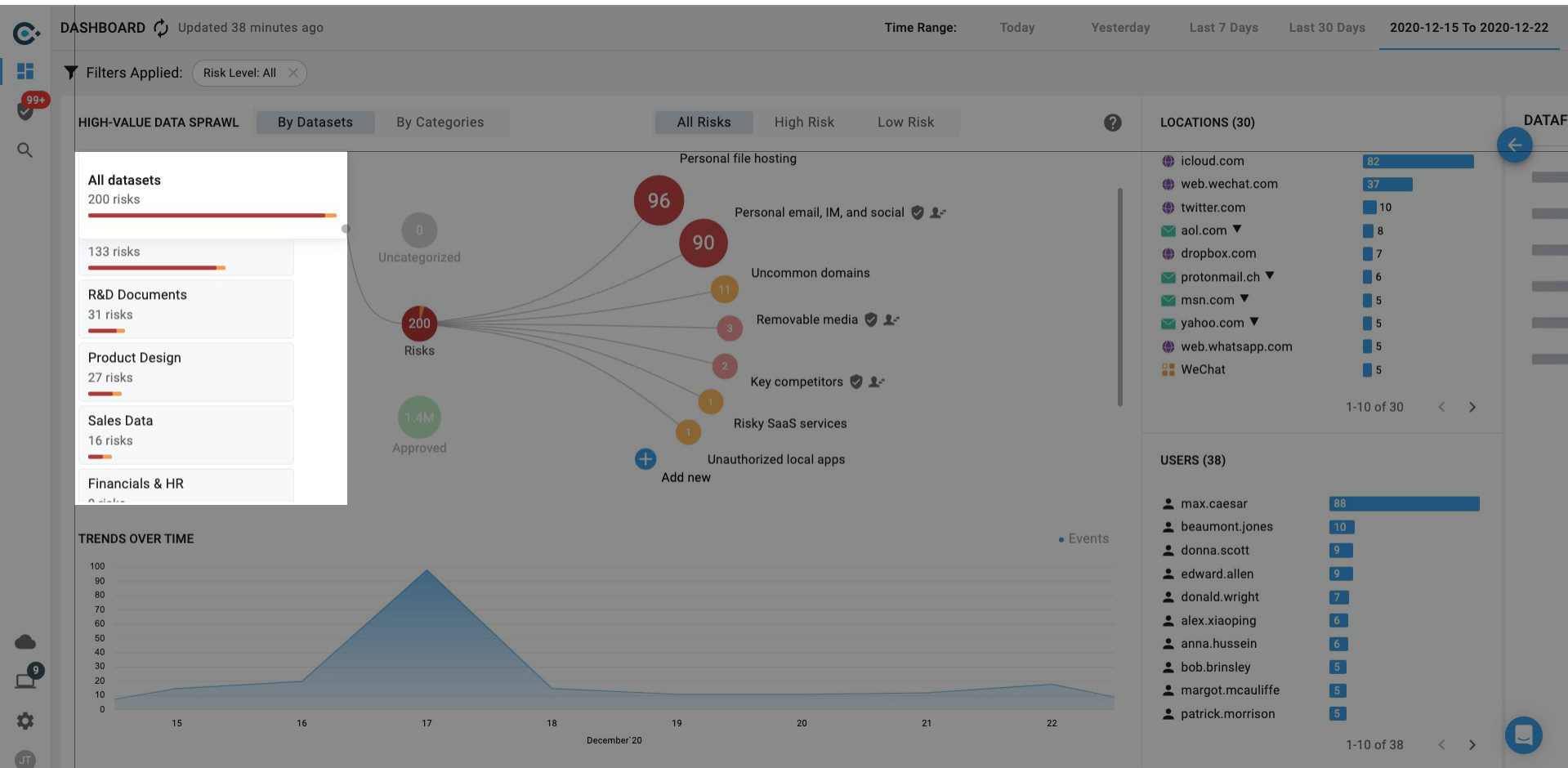
donna.scott uploaded file Copy of Project notes.dwg → to mega.co.nz as Copy of Project notes.dwg

2020-12-17, 02:19

EXPORT 1

1-1 of 1





Filters Applied: Datasets: Product Design Risk Level: Approved Clear All

HIGH-VALUE DATA SPRAWL

By Datasets

By Categories

All datasets

200 risks

Source Code

133 risks

R&D Documents

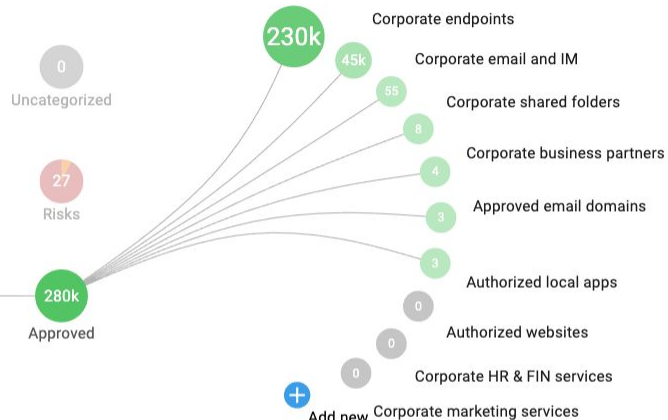
31 risks

Product Design

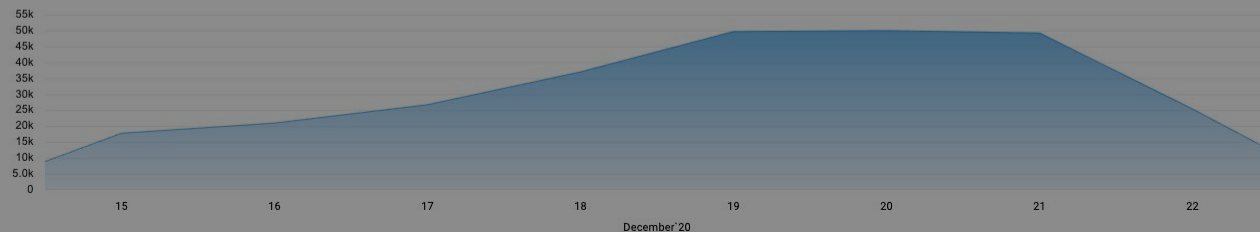
27 risks

Sales Data

16 risks



TRENDS OVER TIME



LOCATIONS (1000+)

acme.atlassian.com	190183
github.com	42942
acme.com	53
EDMUND-ZEDONG-PC	21
ANTHONY-WARHOL-PC	19
CHRISTOPHER-GONZAL...	19
DONALD-WRIGHT-PC	19
EDWARD-HERNANDEZ-...	19
ISRAEL-BROWN-PC	19
CLINT-HULL-PC	18

1-10 of 1000+ < >

USERS (1000+)

max.caesar	90
christopher.scott	75
jay.ellison	73
steven.carter	72
israel.brown	71
sam.mallet	71
kenneth.hall	70
michael.wilson	70
hans.gary	69
bruce.more	68

1-10 of 1000+ < >

Filters Applied: Risk Level: All Datasets: Product Design Clear All

HIGH-VALUE DATA SPRAWL

By Datasets

By Categories

All Risks

High Risk

Low Risk

All datasets

200 risks

Source Code

133 risks

R&D Documents

31 risks

Product Design

27 risks

Sales Data

16 risks

Uncategorized

27

Risks

280k

Approved

Personal email, IM, and social

16

Personal file hosting

5

Uncommon domains

4

Removable media

3

Key competitors

1

Risky SaaS services

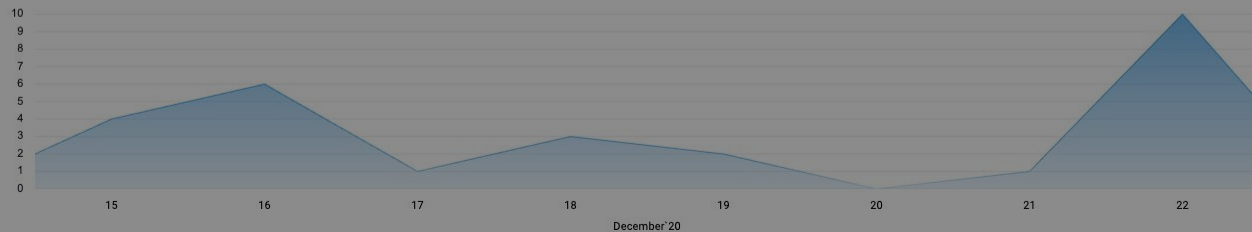
0

Unauthorized local apps

0

Add new

TRENDS OVER TIME



LOCATIONS (12)

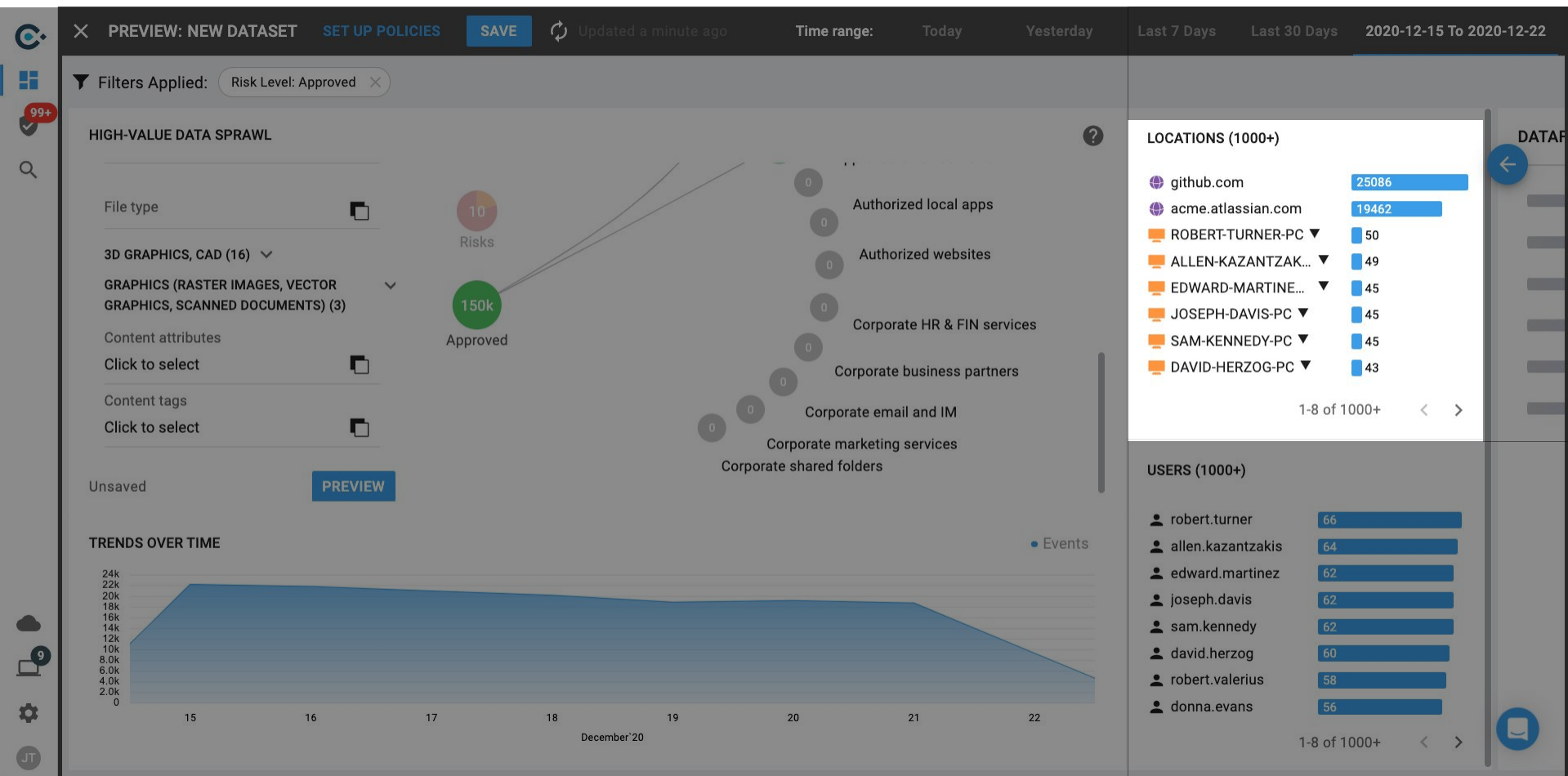
twitter.com	10
dropbox.com	3
gmail.com	2
protonmail.ch	2
yahoo.com	2
mega.co.nz	2
aol.com	1
bartoletti.com	1
web.whatsapp.com	1
BULLET (8866f816)	1

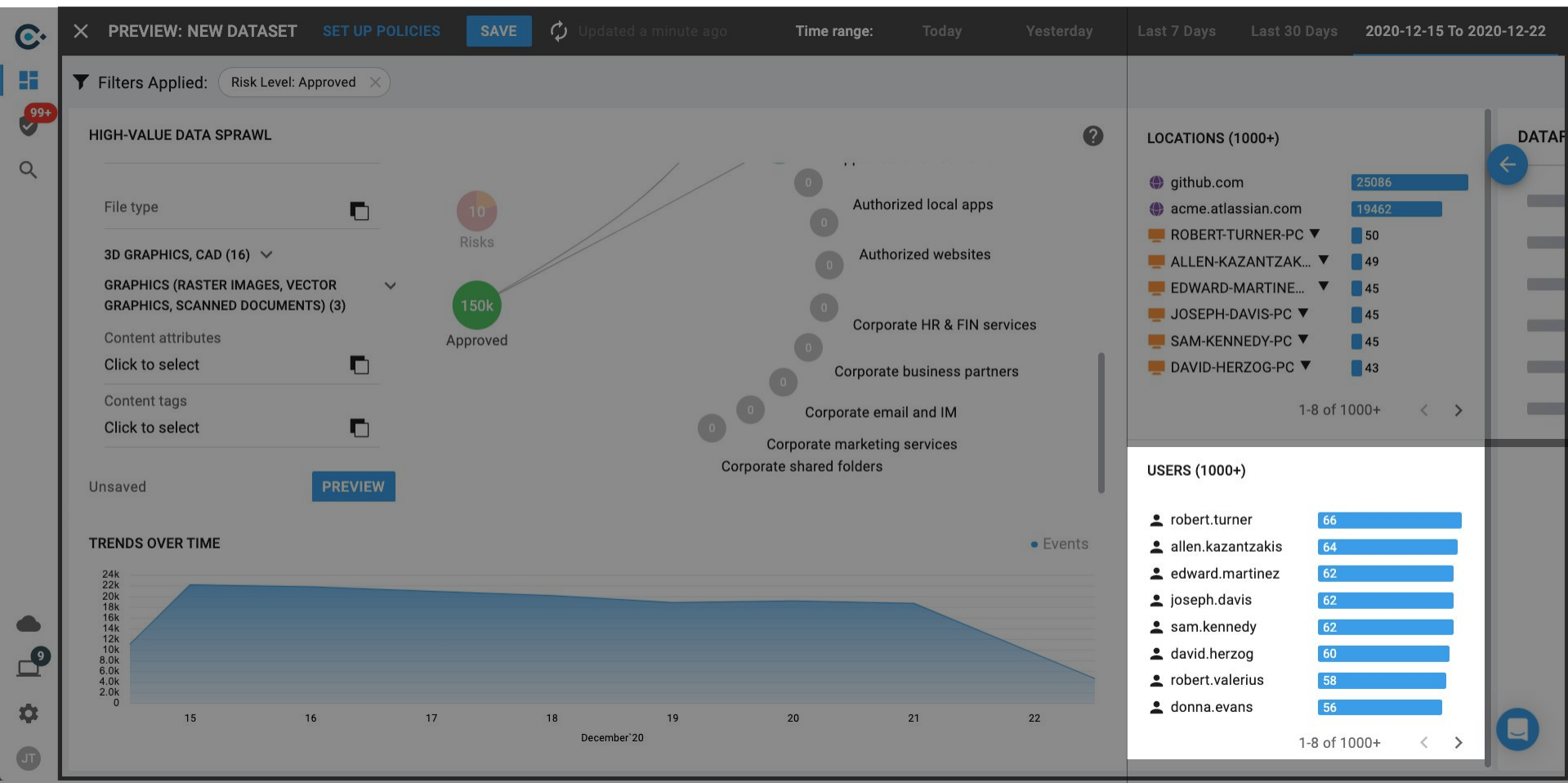
1-10 of 12

USERS (10)

beaumont.jones	10
donald.wright	6
edward.allen	4
deborah.gonzalez	1
donna.scott	1
emile	1
john	1
max	1
maximus	1
samo	1

1-10 of 10





PREVIEW: NEW DATASET SET UP POLICIES SAVE Updated 8 minutes ago Time range: Today Yesterday Last 7 Days Last 30 Days 2020-12-15 To 2020-12-22

Filters Applied: Risk Level

HIGH-VALUE DATA SPRAWL

Type of location

All

Keywords search for: Email address

+ Add new location

Content

Unsaved

TRENDS OVER TIME

15

POLICIES: NEW DATASET

APPLIED FOR LOCATION CATEGORY	RISK LEVEL	INCIDENT	RESPONSE	ALERTS
• Key competitors	High Low Approved	<input checked="" type="checkbox"/>	Set up	+
• Personal email, IM, and social	High Low Approved	<input checked="" type="checkbox"/>	Set up	+
• Personal file hosting	High Low Approved	<input type="checkbox"/>	N/A N/A	+
• Removable media	High Low Approved	<input checked="" type="checkbox"/>	Set up	+
• Risky SaaS services	High Low Approved	<input type="checkbox"/>	N/A N/A	+
• Unauthorized local apps	High Low Approved	<input type="checkbox"/>	N/A N/A	+
• Uncommon domains	High Low Approved	<input type="checkbox"/>	N/A N/A	+
• Approved email domains	High Low Approved	N/A N/A N/A	N/A N/A N/A	+
• Authorized local apps	High Low Approved	N/A N/A N/A	N/A N/A N/A	+

CANCEL PREVIEW

KEY COMPETITORS: REAL-TIME RESPONSE

Enable user warnings ☒

User warning settings:

- ☒ Show the dialog title
- ☒ Require the user to provide a justification
- ☒ Require the user to acknowledge the warning
- ☐ Allow the user to request a policy review
- ☐ Prevent the user from accessing the destination after

1 warning(s) within 1 month(s) for the period of
1 day(s)

! Restricting user access to destinations is only supported for websites and endpoint applications. Restrictions are not supported on MacOS.

- ! Users will receive at most one warning per minute.
- ! User warnings are not yet supported for user actions performed in SaaS applications.

Warning message preview

Please edit the warning message below:



Warning: You have violated Acme Corp security policy

You have just {{action}} {{source}} {{destination}}. The data you {{action}} may contain {{dataset}}. You are not allowed to send, store, or share this data to {{category}}.

Required: Please, provide a justification for your action

- ☐ I acknowledge that I have read and understood this message

I UNDERSTAND

Thank You!

www.cyberhaven.com

Additional questions?
jared@cyberhaven.com

