CybelAngel

SRE Meetup #8

Building custom NAT for GKE

January 19th, 2021

Summary

01

CybelAngel

Short context presentation

02

Cloud NAT and 2020 context

Motivation and target

03

Custom NAT Setup

Architecture and deployment

04

Conclusion

Benefits and opportunities

01

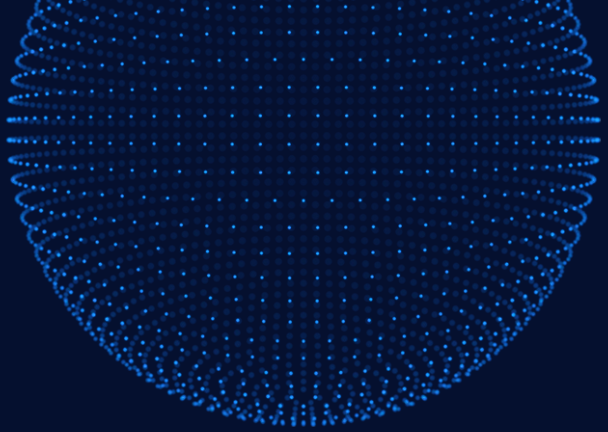
CybelAngel

Context

Leading To Devastating Costs

Marriott faces $123 Million fine for 2018 mega-breach

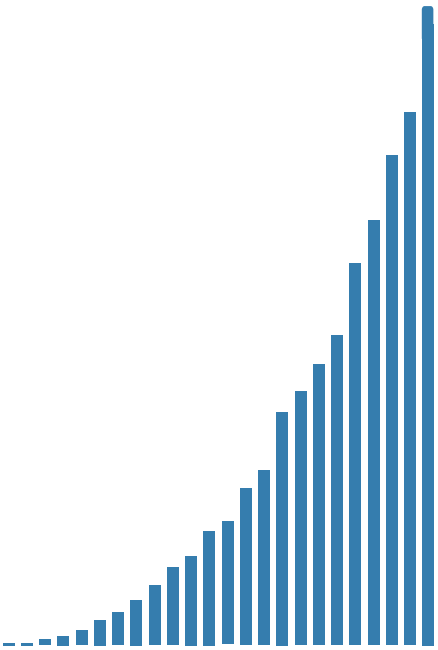
Kate O'Flaherty, Forbes, July 9, 2019



The leading digital risk management provider
detecting data leaks
outside the enterprise’s perimeter
before they wreak havoc.

The Leading Third-Party Data Leak Detection Player

Leaks are inevitable. Damages are optional



Feb. 2020
36M$ Series B Funding

3 Offices
New York - London - Paris

120
Employees

SANOFI

LOUIS VUITTON

Pinsent Masons

L'ORÉAL PARIS

A Numbers Game

AUTOMATED PIPELINE

Data harvesting
(Raw feed)

AI-filtered data processing
(Client-specific feed)

Human intelligence
(Refined feed)

SaaS delivery

LEAKS / DAY / CLIENT

BILLIONS
Of detections

THOUSANDS
Of matches

DOZENS
Of alerts

ONE
incident

30B/Year
Leaks processed

1.2B/Year
Exposed credentials scanned

02

Cloud NAT and 2020 context

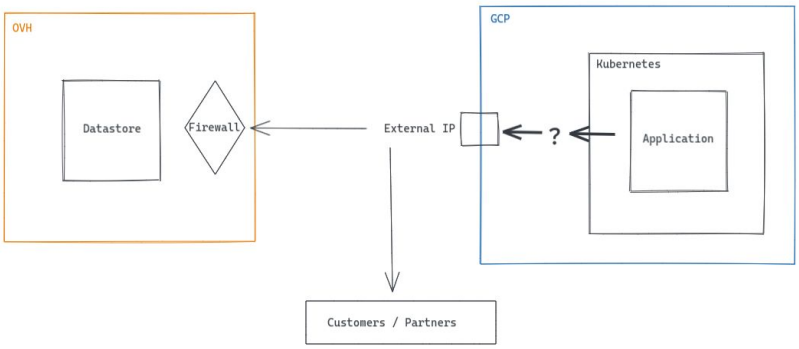
Motivation and target

NAT need and use

Following our migrations

Starting 2019, we empowered our architecture migrating from OVH to GCP. The main goal was to build a new workload orchestration with a reduced set of outgoing IPs, using private GKE

- **Migrate from DCOS to GKE**
- **Mastering our outgoing IPs**
- **Communication with our Datastores**

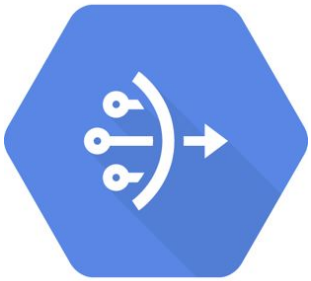


NAT need and use

Setting up Cloud NAT

First generation of our GKE cluster used a custom NAT setup based on GCP Compute Instances. After several months with some hard troubleshooting issues we decided to migrate to a new IAC based GKE with Cloud NAT enabled

- **Instability**
- **Packet loss**
- **Self-Managed and no strong IAC**

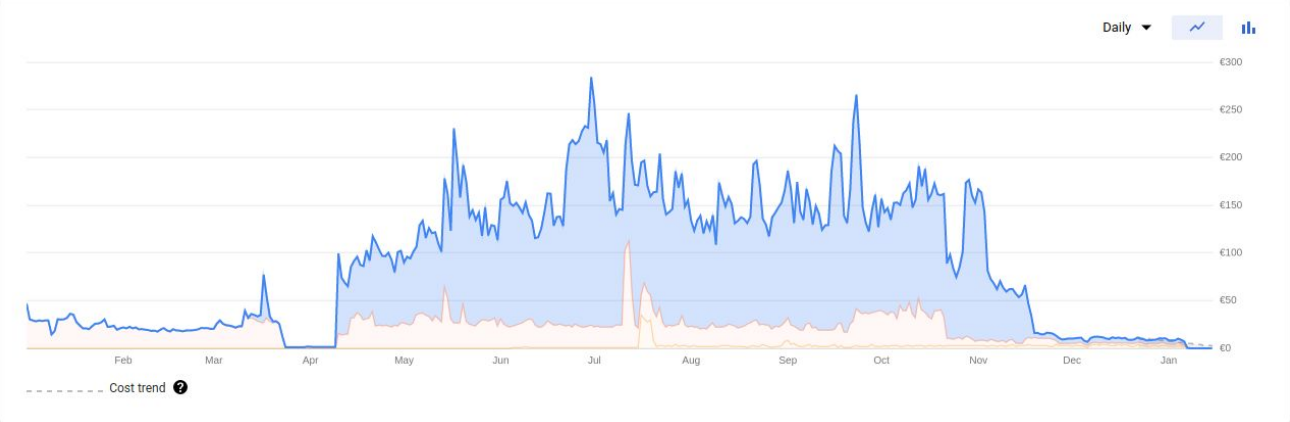


GCP Cloud NAT

Cloud NAT Costs

Cost Management and COVID impact

From March to June Cloud NAT daily cost grew until reaching the maximum value. We decided to redefine the way we would like to manage this issue, starting a new generation of GKE Clusters based on our two years experience



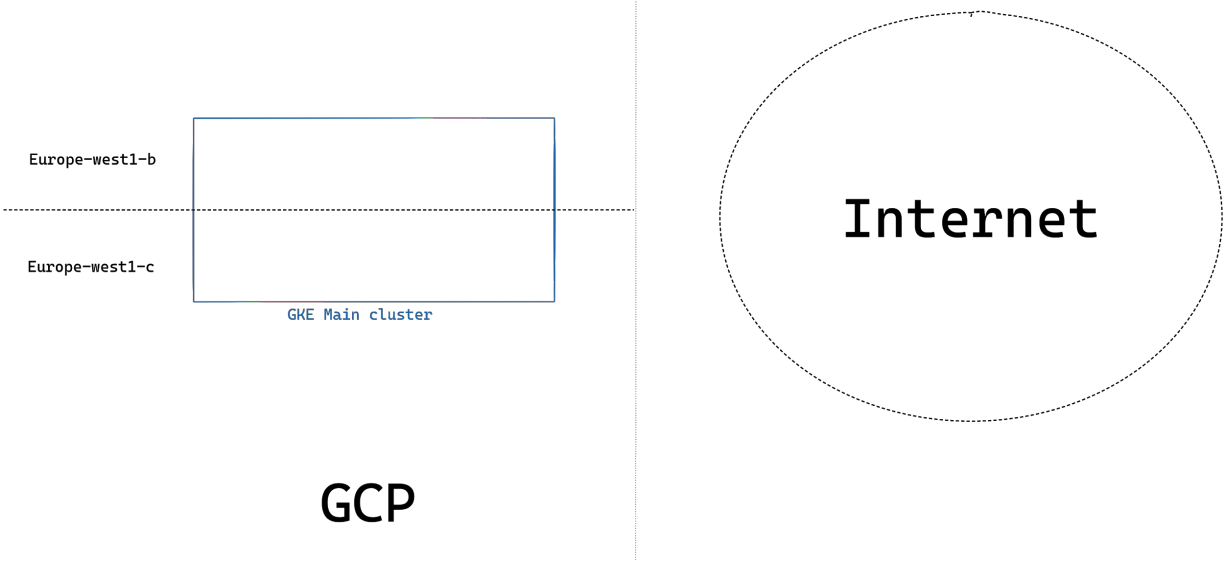
03

Custom NAT setup

Architecture and deployment

Custom NAT setup

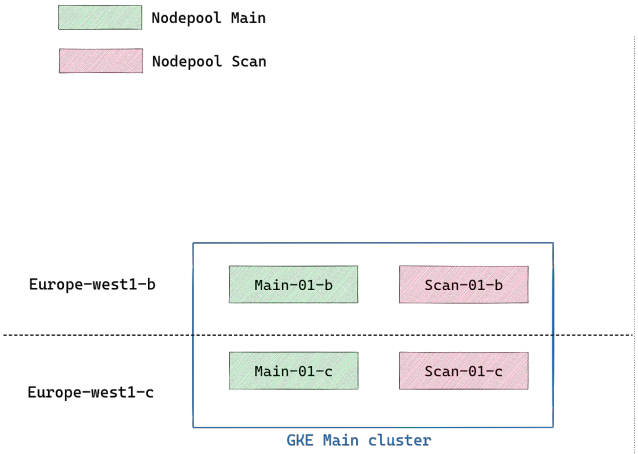
Simpler is better



GCP

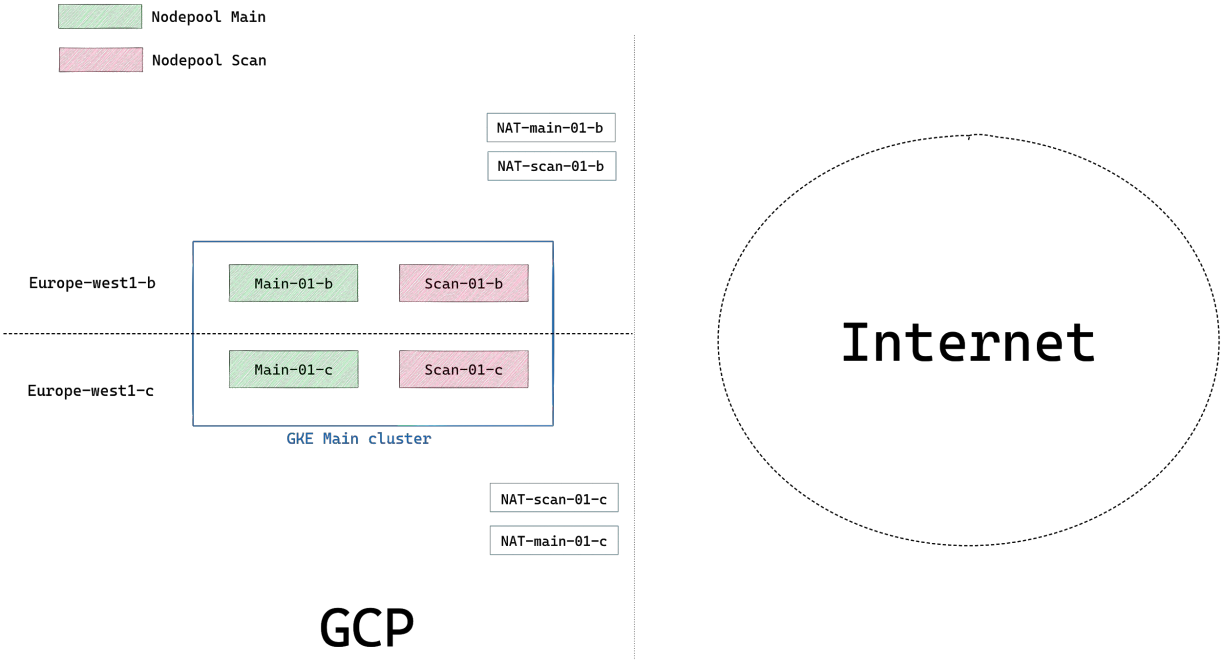
Custom NAT setup

Simpler is better



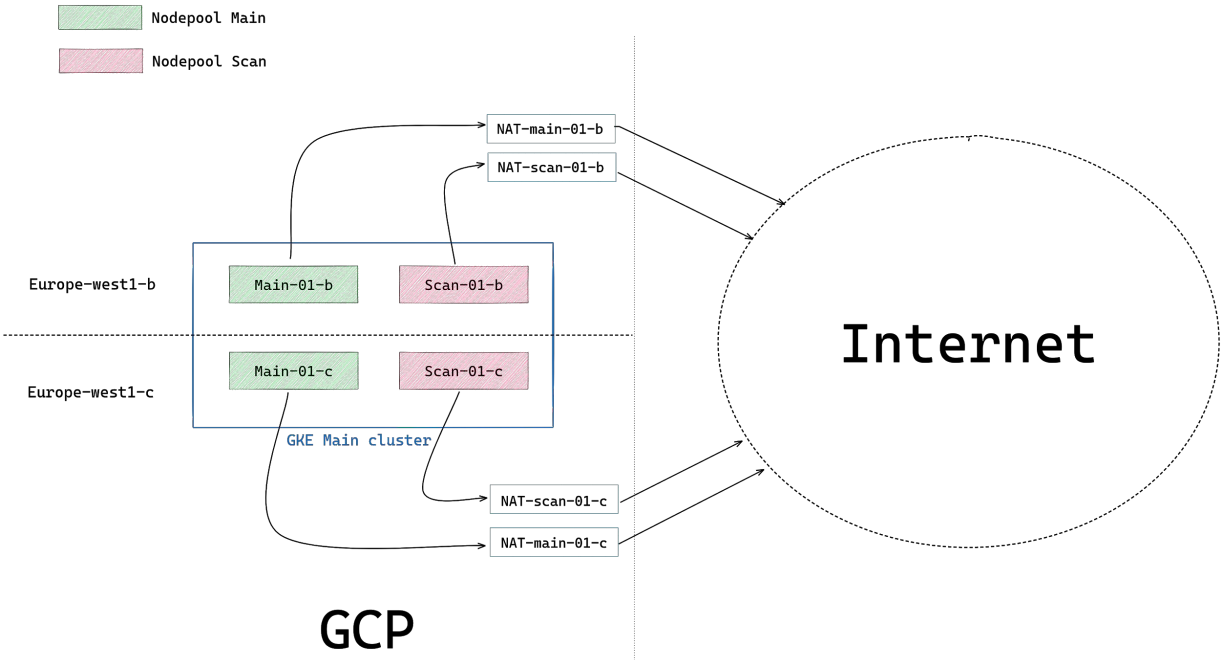
Custom NAT setup

Simpler is better



Custom NAT setup

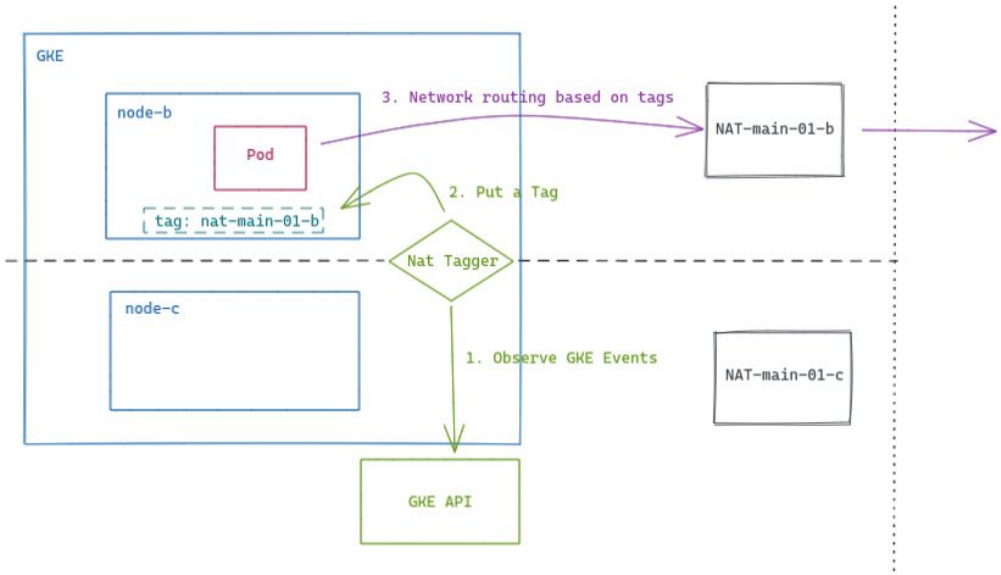
Simpler is better



Custom NAT setup

Network tagging

- NAT assignation is done using network tags
- Daemonset called K8S-nat-tagger
- Whenever a node joins the cluster, a pod from the daemon set starts on it, list available NATs, pick one and assign the matching network tag



Custom NAT setup

Tinkering with conntrack

- Each connection takes a slot in nf_conntrack: scarce resource
- Double hash table size (-> max entries * 8)
- Decrease ESTABLISHED connection entries timeout (5 days -> 1 day)

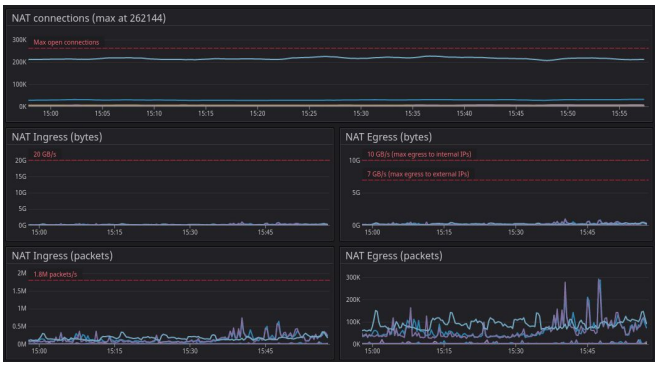
=> One NAT instance can handle ~500K connections

=> One instance per zone and per workload type is enough for us with large security margins (for now)

Custom NAT setup

Monitoring NAT usage

- Datadog based monitoring and alerting
- No incident over the last 6 month
- Robust NAT setup
- Around 100Tb / Month



☐	-	OK	[Jungle] NAT egress is too high (bytes)	service:kubernetes	team:sre	env:jungle	terraform:true
☐	-	OK	[Jungle] NAT has too many open connections	service:kubernetes	team:sre	env:jungle	terraform:true
☐	-	OK	[Jungle] NAT ingress is too high (bytes)	service:kubernetes	team:sre	env:jungle	terraform:true
☐	-	OK	[Jungle] NAT ingress is too high (packets)	service:kubernetes	team:sre	env:jungle	terraform:true
☐	-	OK	[Jungle] NAT nat-jungle-02-b-0 is down	service:kubernetes	team:sre	env:jungle	terraform:true
☐	-	OK	[Jungle] NAT nat-jungle-02-c-0 is down	service:kubernetes	team:sre	env:jungle	terraform:true
☐	-	OK	[Jungle] NAT nat-scan-jungle-02-b-0 is down	service:kubernetes	team:sre	env:jungle	terraform:true
☐	-	OK	[Jungle] NAT nat-scan-jungle-02-c-0 is down	service:kubernetes	team:sre	env:jungle	terraform:true

04

Conclusion

Benefits and opportunities

Benefits and opportunities

Costs Reduced

- Cloud NAT traffic processing cost was around 4K€/month
- Our custom NATs are ~220€/month
- Less exposed IPs and better troubleshooting abilities
- We still pay egress traffic though

Opportunities

- Flexibility on traffic routing
- Horizontal Scalability available
- Experience on Kubernetes controllers

Any questions ?

Thank you!

Notes + Directions

1. This is the master presentation template
2. **MAKE A COPY of this template to create your presentation**
3. Periodically, Marketing will update this master template with new slides/layouts/etc.
4. Remember to delete the extra/unused template slides from your final presentation.
5. If you have feedback, suggestions, or requests, you can submit them here: https://goo.gl/forms/Krgcdw5zgCxPJFiI3

Color Palette

Primary Background

Primary Accent

Secondary Accent

Text Body

Background Light

Background Accent

Inactive State

Logo Green

Logo Blue

Icon Library

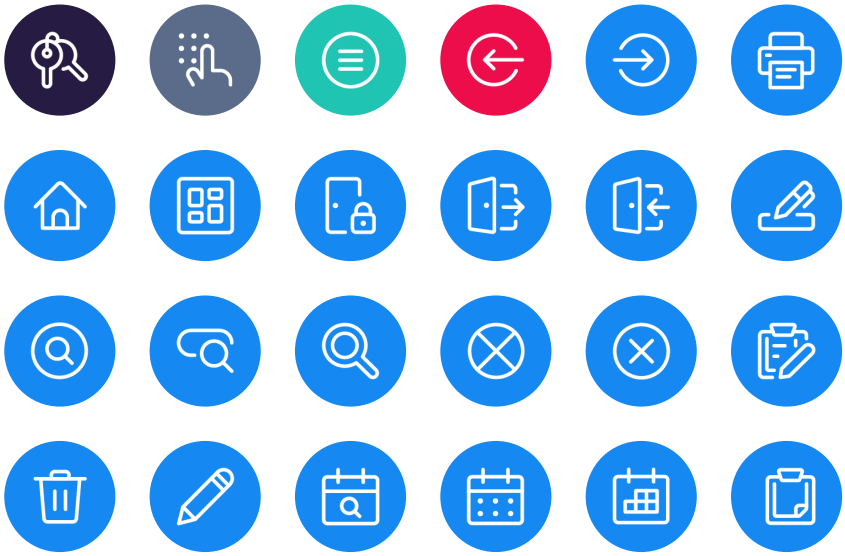
The attached icon library contains outlined white icons on colored circles.

Primarily, the icons should be on the blue circles.

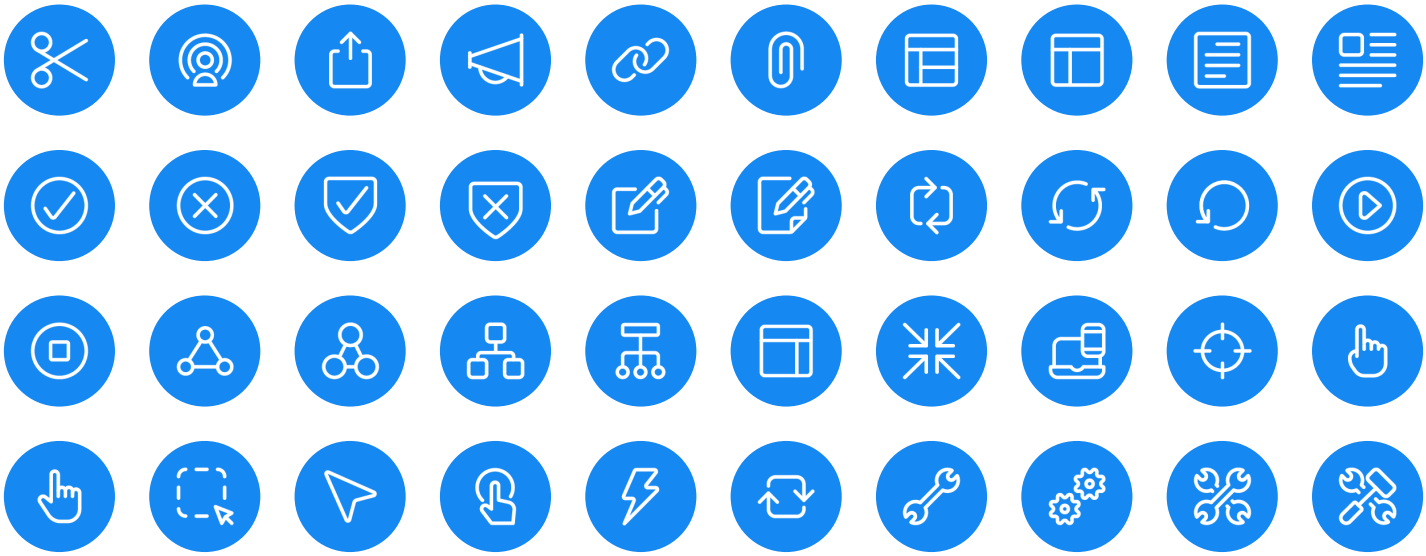
Depending on the content and background color, the other shades are acceptable.

Sizing is also dependent on the amount of content. 100% scale should be used with small amounts of content. Icons should not be smaller than 60% scale.

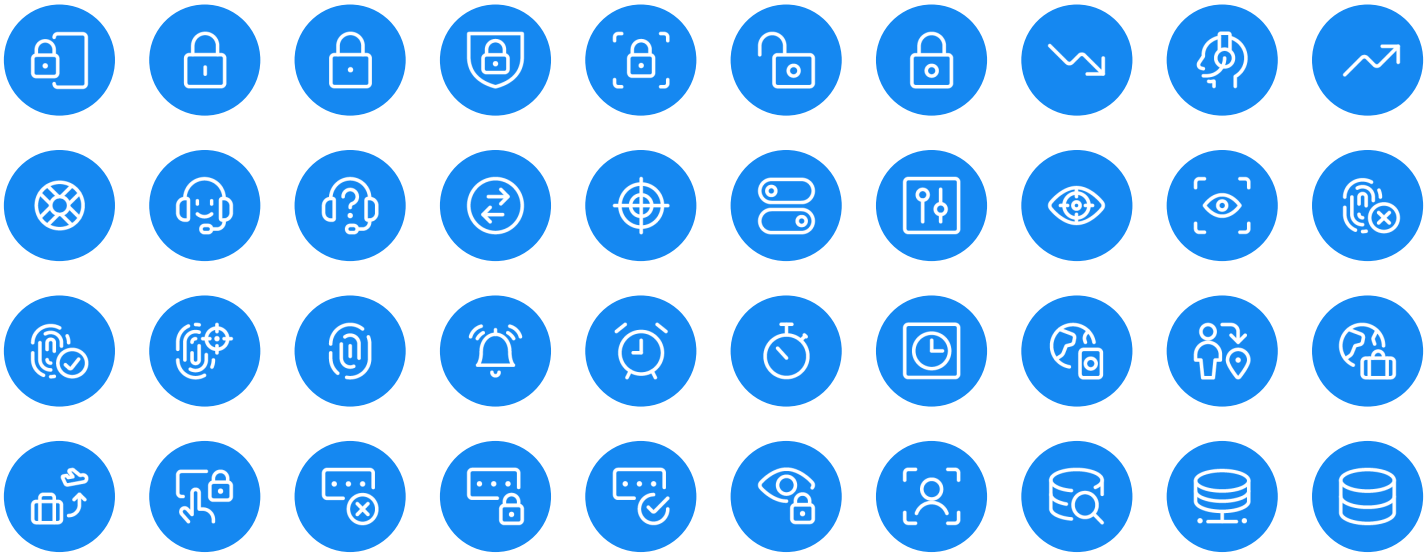
100% **80%** **60%**



Icon library



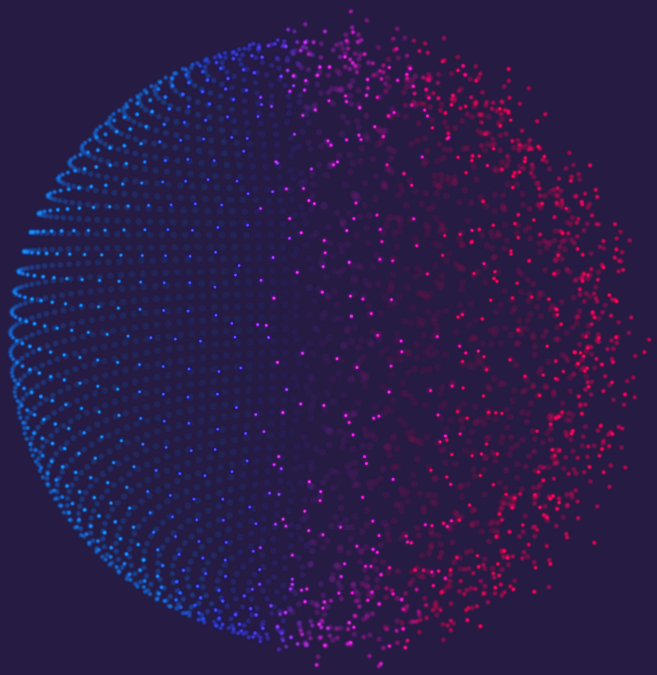
Icon library



Icon library

Icon library

CybelAngel



Presentation Title

Sub-title goes here

January 1st, 2019

CybelAngel

Presentation Title

Sub-title goes here

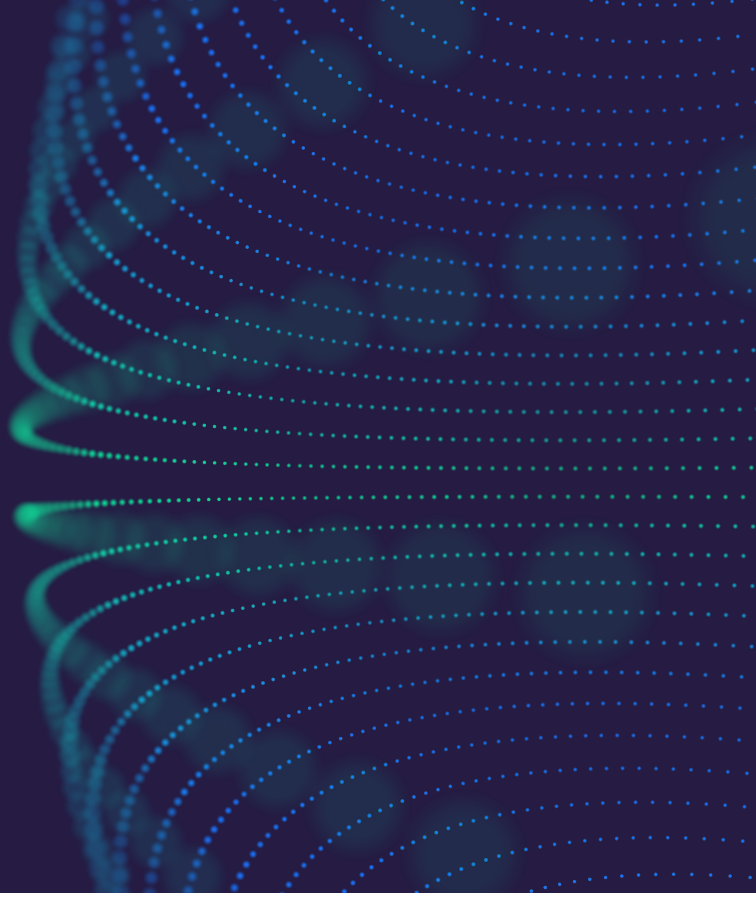
January 1st, 2019

CybelAngel

Presentation Title

Sub-title goes here

January 1st, 2019



CybelAngel

Blank Cover Page

Sub-title goes here

January 1st, 2019

Summary/Agenda

1. Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2. Lorem ipsum dolor sit amet, consectetur adipiscing elit.
3. Lorem ipsum dolor sit amet, consectetur adipiscing elit.
4. Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Summary/Agenda

01

Title of section 01

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean non ligula vulputate, sagittis orci eget, mollis libero.

02

Title of section 02

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean non ligula vulputate, sagittis orci eget, mollis libero.

03

Title of section 03

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean non ligula vulputate, sagittis orci eget, mollis libero.

04

Title of section 04

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean non ligula vulputate, sagittis orci eget, mollis libero.

Summary/Agenda

01

Title of section 01

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

02

Title of section 02

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

03

Title of section 03

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

04

Title of section 04

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

05

Title of section 05

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

06

Title of section 06

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

07

Title of section 07

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

08

Title of section 08

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Short Summary/Agenda

Part 01
Title of Part 01

Part 02
Title of Part 02

(Example) Summary/Agenda

Part 01

A Lesson In Aviation:
The Connected Storage Blind Spot

Part 02

Your Future IT Ecosystem:
Current Trends and Impending Risks

01

Title of Section 01

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean non ligula vulputate, sagittis orci eget, mollis libero.

Part 01

(Example) A Lesson In Aviation: The Connected Storage Blind Spot

Executive Summary Slide

Heading

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean non ligula vulputate, sagittis orci eget, mollis libero. Nulla facilisi. Proin ac lacus mi. Sed varius tellus non gravida scelerisque. Aliquam cursus lacus quis augue iaculis, ac malesuada tortor mollis. Fusce mollis dui a neque consectetur, sed dignissim massa eleifend. Phasellus vel varius ex, vel molestie sem.

First Name Last Name
Position / Title

PLACE IMAGE HERE

Slide with Formatted Bullet Points

Subtitle section

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi sed convallis ipsum. Cras ac dapibus dui. Praesent ultrices tristique accumsan. Duis ullamcorper mattis odio at molestie. Etiam faucibus id odio a congue. Aenean efficitur purus non ante maximus, eget mollis purus ornare.

- **FTP Protocol**
- **SMB/FTP/NFS Protocols**
- **Rsync Protocol**
- **MongoDB**
- **NFS**

Team Slide (Large)

First Name
Last Name
Position / Title

First Name
Last Name
Position / Title

First Name
Last Name
Position / Title

First Name
Last Name
Position / Title

First Name
Last Name
Position / Title

First Name
Last Name
Position / Title

First Name
Last Name
Position / Title

First Name
Last Name
Position / Title

First Name
Last Name
Position / Title

First Name
Last Name
Position / Title

Team Slide (Small)

First Name & Last Name
Position / Title

First Name & Last Name
Position / Title

First Name & Last Name
Position / Title

First Name & Last Name
Position / Title

First Name & Last Name
Position / Title

First Name & Last Name
Position / Title

First Name & Last Name
Position / Title

First Name & Last Name
Position / Title

Divider Slide

Subtitle

Short Timeline Example Slide

Title of section
Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Title of section
Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Title of section
Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Title of section
Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Title of section
Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis convallis felis at libero vulputate porttitor. Quisque nec consectetur quam, eu aliquet eros. Integer et justo leo. Morbi id malesuada dui, a euismod mauris. Etiam quis lacinia ante. Donec nec massa velit.

Screenshot Mock Slide

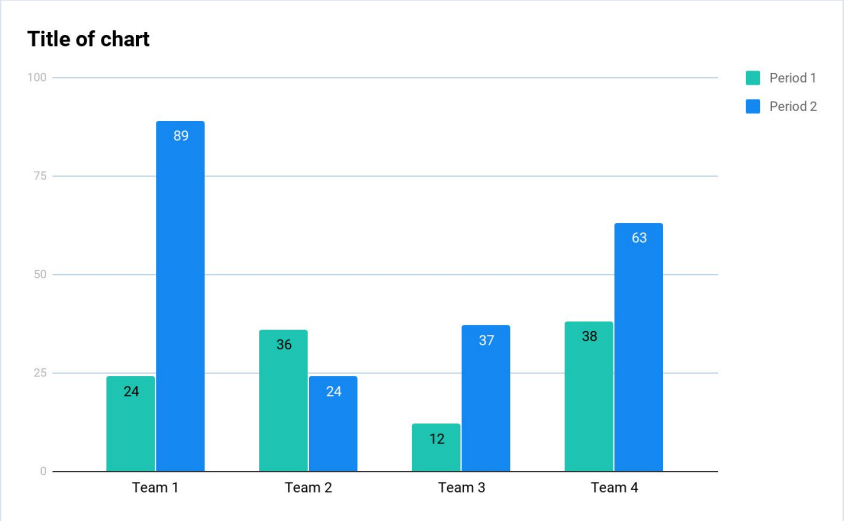
Heading

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean non ligula vulputate, sagittis orci eget, mollis libero. Nulla facilisi. Proin ac lacus mi. Sed varius tellus non gravida scelerisque. Aliquam cursus lacus quis augue iaculis, ac malesuada tortor mollis. Fusce mollis dui a neque consectetur, sed dignissim massa eleifend. Phasellus vel varius ex, vel molestie sem.

Chart Example

Heading

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean non ligula vulputate, sagittis orci eget, mollis libero. Nulla facilisi. Proin ac lacus mi. Sed varius tellus non gravida scelerisque. Aliquam cursus lacus quis augue iaculis, ac malesuada tortor mollis. Fusce mollis dui a neque consectetur, sed dignissim massa eleifend. Phasellus vel varius ex, vel molestie sem.



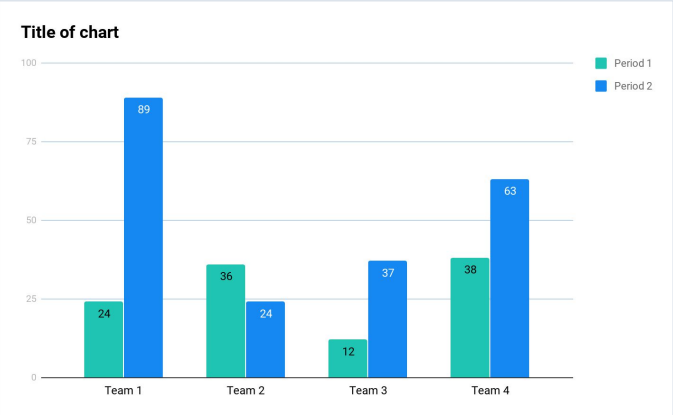
Two Sections

Heading

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean non ligula vulputate, sagittis orci eget, mollis libero. Nulla facilisi. Proin ac lacus mi. Sed varius tellus non gravida scelerisque. Aliquam cursus lacus quis augue iaculis, ac malesuada tortor mollis. Fusce mollis dui a neque consectetur, sed dignissim massa eleifend. Phasellus vel varius ex, vel molestie sem.

Heading

Lorem ipsum dolor sit amet, consectetur adipiscing elit.



(Large Title) Protect your assets from cyber threats

PLACE IMAGE HERE

(Example) Connected Storage Blind Spot

Airports Case Study

During a 5 month period of connected storage scanning, CybelAngel detected...

~ 150

Documents related to airport security badges

~ 400

Blueprints detailing airport premise

~ 350

Documents detailing security and safety procedures

Three Key Points

Heading

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut pharetra maximus mattis. Suspendisse tristique maximus nunc, in fringilla urna sollicitudin ut. Maecenas hendrerit, ligula at ornare cursus, neque tortor luctus urna, malesuada rhoncus magna velit a elit.

Heading

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut pharetra maximus mattis. Suspendisse tristique maximus nunc, in fringilla urna sollicitudin ut. Maecenas hendrerit, ligula at ornare cursus, neque tortor luctus urna, malesuada rhoncus magna velit a elit.

Heading

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut pharetra maximus mattis. Suspendisse tristique maximus nunc, in fringilla urna sollicitudin ut. Maecenas hendrerit, ligula at ornare cursus, neque tortor luctus urna, malesuada rhoncus magna velit a elit.

Your Future IT Ecosystem: Current Trends and Impending Risks

Your Future IT Ecosystem: Current Trends and Impending Risks

Table Slide

Subtitle

Title Column 1	Title Column 2	Title Column 3	Title Column 4	Title Column 5

Multiple Table/Point Slide

Subtitle

Section Title	Section Title	Section Title
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi sed convallis ipsum. Cras ac dapibus dui. Praesent ultrices tristique accumsan.	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi sed convallis ipsum. Cras ac dapibus dui. Praesent ultrices tristique accumsan.	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi sed convallis ipsum. Cras ac dapibus dui. Praesent ultrices tristique accumsan.

(Example)
100% of the following was found on internet connected storage

(and was shared with the FBI)

(Example)
100% of the following was found on internet connected storage

(and was shared with the FBI)

(Example) The CybelAngel solution

Our technology

INTERNET-WIDE SCAN

Continuously scans data from the whole internet

MACHINE LEARNING & AI

Our technology filters, scores and scans & classifies leaked documents based on your keywords

DEEP ANALYTIC SKILLS

Our cyber analysts qualify threats before conducting investigation and providing contextual analysis

---

1 billion detections
per day

100 potential threats
per day

1 qualified alert
per day

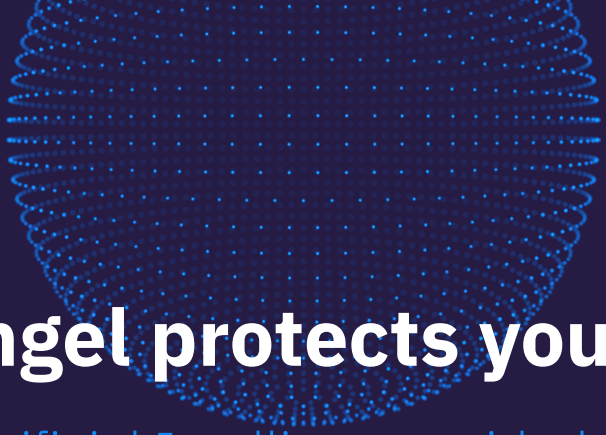
(Example) New Joiners

Marketing Team

Brian Smith

Marketing & Communications Manager

Start date: January 1, 2019
City: Paris
Manager: Jesse Kliza



CybelAngel protects your assets

Combining Artificial Intelligence with the expertise of cyber security analysts, CybelAngel's SaaS platform gives you instant and actionable insight into cyber threats before they wreak havoc.

CybelAngel protects your assets

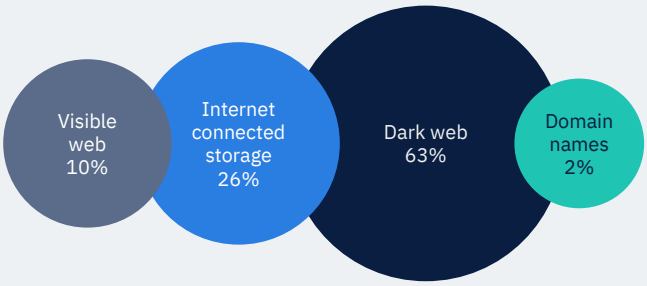
Combining Artificial Intelligence with the expertise of cyber security analysts, CybelAngel's SaaS platform gives you instant and actionable insight into cyber threats before they wreak havoc.

(Example) The Layers of the Internet

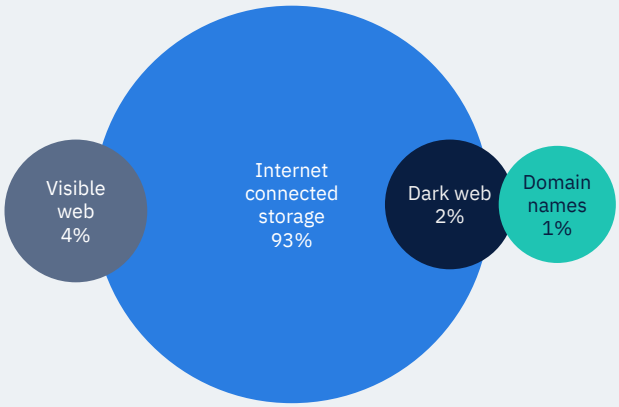
We scan all of it

The leaks we find on **Connected Storage** are the most critical

Where we find leaks by source



Where we find our most critical leaks by source

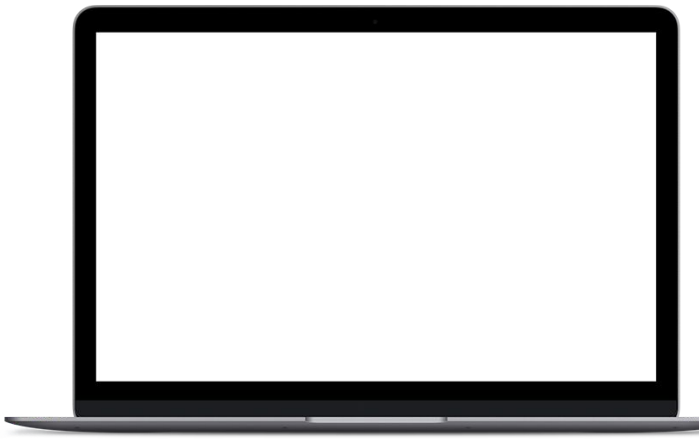


(Example) The CybelAngel solution

Your benefits

Alerts delivered via a SaaS platform

- **RELEVANT**
  98% accuracy rate (less than 2% false positives)
- **VALUABLE**
  Focused on business-sensitive assets
- **ACTIONABLE**
  100% of leaks have context & attribution
- **RESOURCE LITE**
  Built on innovative AI and superior human intelligence



"CybelAngel is the best-performing data leak detection technology known today"

Jean-Yves Poichotte, Global Head of ITS Cyber Security at Sanofi

SANOFI

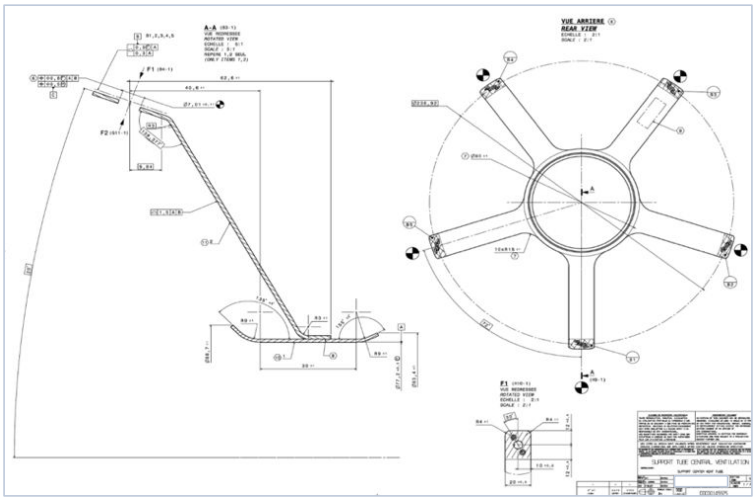
(Example) Aeronautic // Connected Storage

Subtitle

Context
Aeronautic industry

Kind of risks
R&D, Intellectual property

Kind of document
Industrial drawings



(Example) Our Features

Product overview

Round the clock detection
24/7 detection powered by automated crawlers and machine learning algorithms

Powerful AI automation
Proprietary scanner and crawler, AI powered classification and scoring

Secure interface & API
We adapt to your needs thanks to a flexible collaboration through API/data feed, SAAS or managed service offer

Dedicated expert contact
Dedicated cyber risk analyst for account management and in-depth investigation and periodic meetings

Unlimited keywords and brand monitoring
Exhaustive list of keywords and brands to cover the whole spectrum of your data security

Continuous updates
Constant improvement of technology and interface through feedback loop and agile methodologies

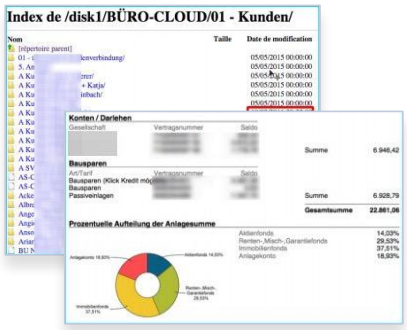
(Example) More Examples // Connected Storage

Subtitle

WHERE DID CYBELANGEL FIND IT:
Unprotected Supplier Server

KIND OF RISK:
Safety & Burglary

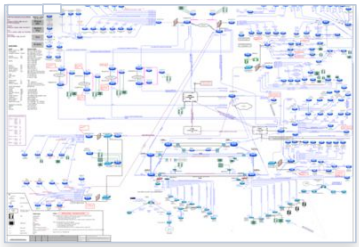
KIND OF DOCUMENT:
Blueprint



WHERE DID CYBELANGEL FIND IT:
Unprotected Supplier Server

KIND OF RISK:
Legal Liability, Business Intelligence

KIND OF DOCUMENT:
Customers' Data



WHERE DID CYBELANGEL FIND IT:
Personal NAS of a VP

KIND OF RISK:
IT & Threat Intelligence

KIND OF DOCUMENT:
Network Plan

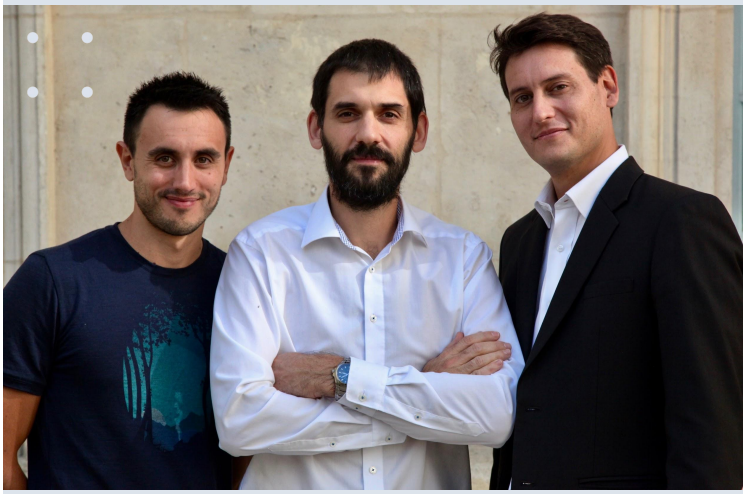
CybelAngel

Subtitle goes here

$12 M raised on October 11 2018

- Founded in 2013
- 70 employees
- >40 customers in 5 countries
- Established US entity in 2018

Short title goes here



Stevan Keraudy
CIO &
co-founder

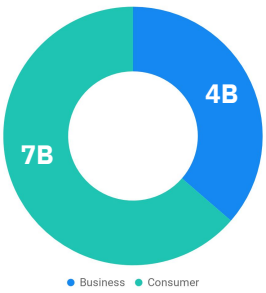
Matthieu Finiasz
President &
co-founder

Erwan Keraudy
CEO &
co-founder

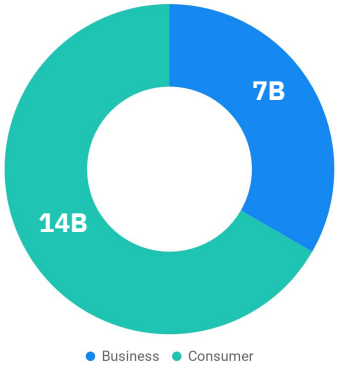
Trend 1/3: Surge in Connected Devices Generally

of Internet Connected Devices

Today: 11 Billion



2020: 20 Billion



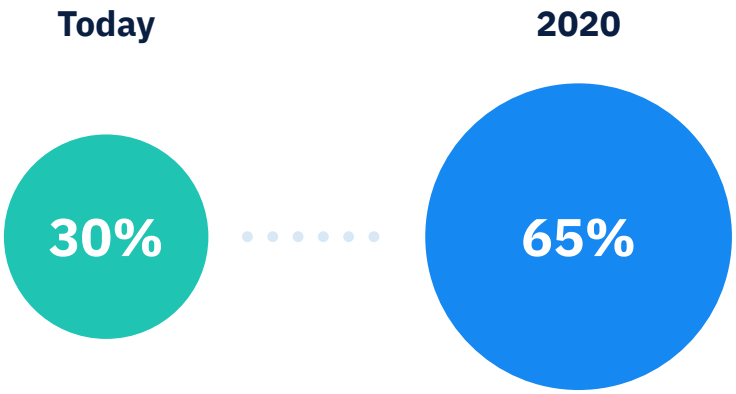
Digital Transformation

Internet of Things (IoT)

Source: Gartner

(Example) Surge in Connected Devices Generally

% of Enterprises Adopting Internet of Things (IoT) Products

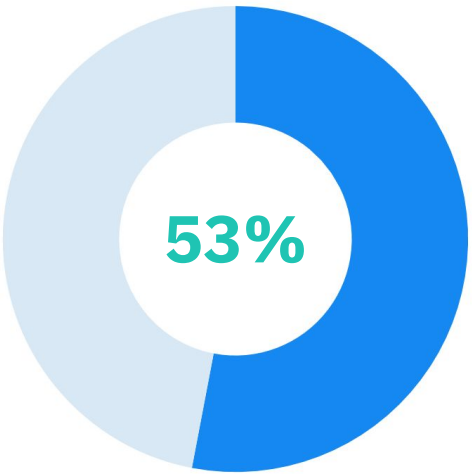


YET! **46% of Companies are Adopting IoT Technologies Without Assessing the Associated Risk**

(Example) The risk landscape is expanding

It’s not just malevolent leaks – negligent and accidental leaks are becoming bigger threats

Your information is already outside your network, and outside your direct control.



OF DATA LEAKS COME FROM THIRD PARTIES *

VISION / MISSION

To help organizations protect their intellectual property, brand, and reputation, through the use of superior artificial intelligence and human expertise.

(Example) Map

(Quote Slide)
“It’s not about ideas. It’s about making ideas happen.”

- Quote Author

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut pharetra maximus mattis. Suspendisse tristique maximus nunc, in fringilla urna sollicitudin ut. Maecenas hendrerit, ligula at ornare cursus, neque tortor luctus urna, malesuada rhoncus magna velit a elit.

- Quote Author

"It's not about ideas. It's about making ideas happen."

"Lorem ipsum dolor sit amet, consectetur adipiscing elit."

- Quote Author

- Quote Author

"Lorem ipsum dolor sit amet, consectetur adipiscing elit."

- Quote Author

"Lorem ipsum dolor sit amet, consectetur adipiscing elit."

- Quote Author

"Lorem ipsum dolor sit amet, consectetur adipiscing elit."

- Quote Author

Thank you!