CybelAngel

# Use Augmented Intelligence to Detect Critical Data Leaks

WWW.CYBELANGEL.COM

# Use Augmented Intelligence to Detect Critical Data Leaks


## SUMMARY

Enterprise data is now shared on more third-party platforms than ever before:  in data centers, on mobile storage devices, in the cloud, and in online services. To detect and prevent the loss or compromise of critical data, all connected storage devices should be monitored for data leaks – as continuously as possible.

CybelAngel, a global provider of digital risk protection and management services, delivers superior detection and remediation services by combining advanced detection techniques with machine learning and the know-how of experienced security analysts. Using CybelAngel's augmented intelligence can make the difference between having a data leak versus a data breach that can disrupt a company and damage its reputation.


## Digital Transformation leads to decentralized, distributed data storage

The term Industry 4.0 was introduced in 2011 as part of an initiative to enhance German competitiveness in manufacturing. Over time, the fourth industrial revolution has been driven by advances in data and services, as well as sweeping digital trends like the Internet of Things. According to Industrie 4.0 in a Global Context, "The real-time networking of products, processes and infrastructure is ushering in the fourth industrial revolution where supply, manufacturing, maintenance, delivery and customer service are all connected via the Internet. Rigid value chains are being transformed into highly flexible value networks."[1]

With these changes, the use of IT is also changing. Seventy-five percent of companies already rely on cloud computing. In transportation and logistics, over four of ten employees (42%) use a mobile device, such as a tablet or smartphone with Internet access, to work on the move. In insurance, banking, financial services, information technology, and consulting approximately one in two employees uses a mobile device.[2]

The result is that Chief Information Security Officers (CISOs) no longer protect just data inside the corporate network, but also protect data in the cloud, on external storage, and on mobile devices. The data is processed, exchanged, and stored at locations that are no longer accessible to the corporate security team. Nevertheless, security teams are still responsible to ensure that data is secure.

[1] Henning Kagermann, Reiner Anderl, Jürgen Gausemeier, Günther Schuh, Wolfgang Wahlster (2016). Industrie 4.0 in a Global Context: Strategies for Cooperating with International Partners. Munich, Germany:  Herbert Utz Verlag, 5

[2] KPMG (2019, June 19). KPMG Cloud-Monitor 2019, Public Cloud und Cloud Security slnd keln Widerspruch. https://hub.kpmg.de/cloud-monitor-2019

## Data leaks beyond the corporate perimeter

Increased requirements for data security affect Security Operations Centers and Incident Response Teams that are often understaffed and overwhelmed. Forty-two percent of the CISOs surveyed have practically given up proactive defense against malicious players.[3]

Many security teams are stretched thin by attempting to detect internal data leaks. Expecting security teams to also scan for data leaks at external storage locations, such as cloud services, storage media and web-hosted databases, can be futile.

Example of Data Leaks

**Open Databases:** In August 2019, Health IT Security reported that "Health vendor Medico and Amarin Pharma recently reported data breaches caused by misconfigured databases, which potentially exposed the data of thousands of patients. According to the UpGuard Data Breach Research Team, a misconfigured database exposed 14,000 documents containing medical, personal, and financial data from Medico, a healthcare billing and insurance data processing vendor."[4]

**Connected Storage:** In May 2020, CPO magazine reported that "GoDaddy CISO and engineering vice-president Demetrius Comes said an unauthorized individual gained access to login information that its customers used to connect to Secure Shell (SSH) on their hosting accounts."[5]

**Cloud Applications:** In May 2020, Security Magazine reported that "More than 25 million user records, belonging to popular math app Mathway, are being sold on the dark web."[6]

Exposure is amplified by an increasingly complex supply chain, which has resulted in a growing number of third-party data leaks. In early 2020, an example was shared by General Electric whose contractor Canon Business Process Services "exposed reams of personal information, including direct deposit forms and tax forms containing social security numbers, scans of birth certificates and passports, applications for benefits, court orders and photos of driver's license."[7]

The increase in attack surface brought about by open databases, connected storage, and cloud applications leads many companies to seek support to detect data leaks beyond their internal data infrastructure.

[3] Cisco (2020, February). Cisco 2020 CISO Benchmark Report.
https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html

[4] Health IT Security (2019, August). 2 Misconfigured Databases Breach Sensitive Data of Nearly 90K Patients.
https://healthitsecurity.com/news/2-misconfigured-databases-breach-sensitive-data-of-nearly-90k-patients

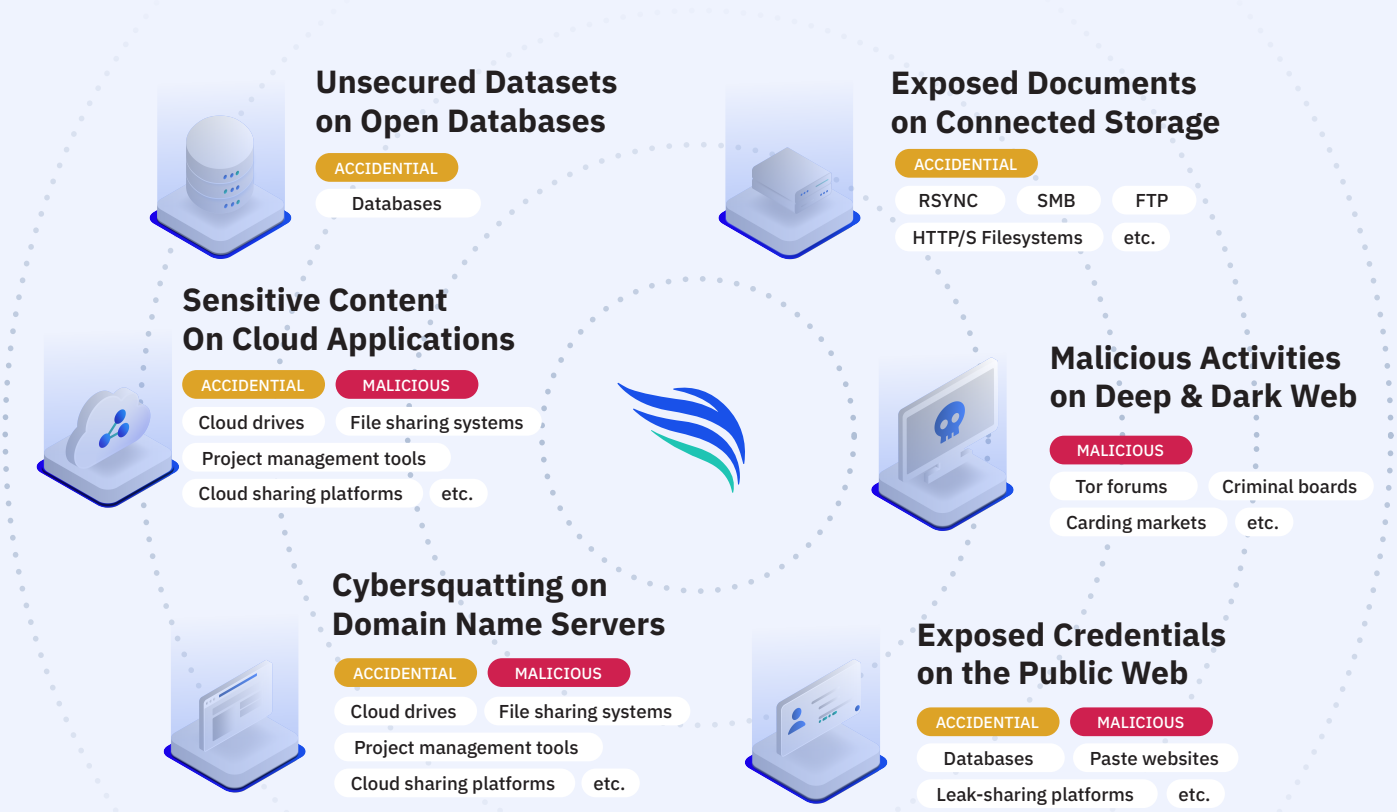
[5] Computer Weekly (2020, May). GoDaddy owns up to October 2019 data breach.
https://www.computerweekly.com/news/252482639/GoDaddy-owns-up-to-October-2019-data-breach

[6] Security Magazine (2020, May). Popular App Mathway Leaks 25 Million User Records.
https://www.securitymagazine.com/articles/92466-popular-app-mathway-leaks-25-million-user-records

[7] Security Magazine (2020, May). Popular App Mathway Leaks 25 Million User Records.
https://www.securitymagazine.com/articles/92466-popular-app-mathway-leaks-25-million-user-records

## CybelAngel scans the complete IT infrastructure for data leaks

CybelAngel, a global provider of digital risk protection services, offers a cybersecurity platform that continuously and comprehensively monitors critical IT infrastructure across Internet perimeters and sends alerts of critical data leaks to its customers. In below graphic, see how CybelAngel continuously checks six critical Internet perimeters.




When data leaks are discovered, the respective customer is immediately notified with a detailed report and best practice recommendations on how to fix the leak.

“Because more data is being stored outside the firewall on cloud services, open databases, and connected devices, the risk to enterprises has never been greater,” says Erwan Keraudy, CEO of CybelAngel. “Our platform continually detects data leaks and incidents, which we then resolve with our remediation services, so businesses can eliminate exposure before damage occurs.”

In the case of data breaches, CybelAngel security analysts offer support to customers who need to report the data protection violation according to the General Data Protection Regulation (GDPR). These reports are time critical and require comprehensive and fast reaction.

## CybelAngel Augmented Intelligence key to digital transformation

CybelAngel supports digital transformation as defined by Industry 4.0 by detecting and remediating data leaks in an environment of highly decentralized and distributed data. The Digital Risk Platform powered by Augmented Intelligence offers dashboards and specialized management reports that inform customers when a data leak occurs, its criticality, and how to remediate these breaches.

## About CybelAngel

CybelAngel reduces global enterprise digital risk by detecting critical data leaks outside the firewall before these leaks become major data breaches. Leveraging its Augmented Intelligence, a unique combination of proven machine learning capabilities and superior cyber analysts, CybelAngel analyzes billions of data sources, thousands of files, and hundreds of threats across all layers of the internet to discover critical data leaks for their customers. Global organizations rely on CybelAngel every day to detect critical data leaks before wreaking havoc on their business.

Learn more at www.cybelangel.com

PARIS, FRANCE | NEW YORK, NY