CybelAngel

WHITE PAPER

Flying Blind in Third-party Ecosystems

TABLE OF CONTENTS

03 Introduction

04 Flying Blind

05 Aviation: A Case Study in Third-party Risks

06 Lessons for Other Industries

07 Contributing Factors in Third-party Data Leaks

09 Challenges in Digital Risk Management

12 Looking Ahead

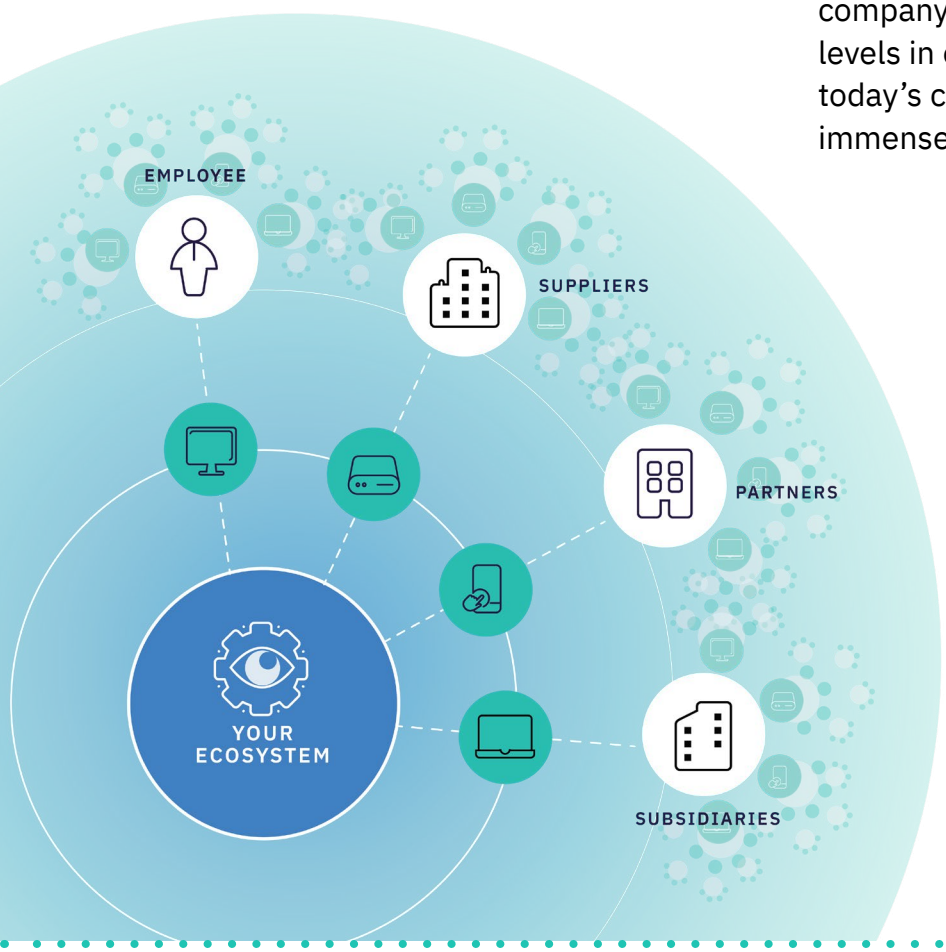
Modern Third-Party Supply Chains

Introduction

The days of local, community-driven supply chains are long gone. In a search for sourcing flexibility, improved quality, and ever-lower prices, firms have added hundreds of third parties to their expanded supply chains, which now typically extend around the globe.

In fact, supply chain logistics extend beyond third parties to fourth and Nth parties. For this reason, enterprises must be prepared for the consequence that the sensitive information they share with their closest partners and vendors will likely end up in the hands of players with vastly different information security processes, procedures, and tools. As third-party risk continues to escalate at each data point, the stakes grow exponentially.

To function efficiently, these complex third-party ecosystems require digital interconnectivity. Data must flow seamlessly from the requirement for goods or services, through procurement and order placement, to implementation or production. Whether it's a consumer goods manufacturer focused on ensuring product consistency across multiple facilities or an oil & gas company looking to optimize production levels in offshore rigs, the supply chains of today's corporations generate and share immense volumes of essential data.



BLINDNESS INTO THIRD-PARTY ECOSYSTEMS LEAVES YOU VULNERABLE

In this white paper, we will share key findings made by the CybelAngel analyst team after a comprehensive analysis of a complex web of suppliers, vendors, and contractors in the aviation industry. We expose how aviation's convoluted chain of third, fourth, and Nth parties that maintain and service aircraft, ensure passenger safety, and manage travel plans greatly expand the attack surface and the potential for data leaks. These digital risks experienced by the aviation sector are similar to those seen in most verticals, whether consumer goods manufacturing, financial services, or oil & gas production. Increasing reliance on vendors and suppliers' adoption of advanced technologies to supplement and/or integrate with legacy systems amplify the importance of digital risk protection.

Flying Blind

Obtaining oversight on the information security hygiene of all vendors in a supply chain can be a fool's errand. Contracts now contain clauses on confidentiality, access for audit purposes, and explicit conditions around data security that must be met. However, monitoring and enforcing these contracts across the entire ecosystem is labor intensive and cost prohibitive. Once an enterprise shares information with a third party, it no longer has visibility into or control over what is done with the data, despite best efforts or intentions on either side.

The Growing Challenge of Third-Party Data Leaks

Malicious Behavior Gets Attention, But...

Despite highly publicized cyber threats from malicious actors such as adversarial foreign governments, activist hackers, and profit-seeking blackmailers, organizations must understand the greatest threat to their data security is far less sinister, but much larger in scale and potential reputational damage.

Negligent Third Parties Pose a Huge Risk

The biggest risk companies face is from the data they willingly share with consultants, vendors, partners, and other third parties. This data may now sit exposed and publicly accessible outside company networks, just waiting to be discovered and exploited.

Scale of Third-party Risk

Third-party leaks are most often caused by negligence and not malicious intent. Regardless of the cause, the ramifications of any third-party breach can be profound and potentially devastating to shareholder value. A January 2020 Ponemon Institute report (via Security Boulevard) revealed that, "In the past two years, 53% of organizations have experienced at least one data breach caused by a third party. And a data breach costs an average of $7.5 million to remediate."[1] Loss of brand reputation or competitive edge (e,g, IP or product plans), and regulatory and legal financial penalties are just the tip of the iceberg in a data breach scenario.

1. Zhao J. "Automation In Compliance: Why It's a Business Imperative and Where to Start." Security Boulevard. June 23, 2020. https://www.thehackettgroup.com/wp-content/uploads/2017/12/hackett-analytics-supply-chain-digital-1711.pdf

Aviation: A Case Study in Third-party Risks

With an estimated 40.3 million flights taking off in 2020,[2] carrying over 4.7 billion passengers,[3] risk mitigation is paramount across the entire aviation ecosystem, from manufacturers through airports and flight crews. A data breach could mean the loss of travelers' confidential data, which could have significant consequences for each of those impacted. Lost airport security plans could serve as blueprints for a terrorist attack. Exposure of financial data could cause loss of shareholder value. The ramifications are varied, but each is equally damning.

As the aviation sector embraces digital transformation, it becomes more interconnected and the volume and scope of data collected, generated, and transmitted expands – as does the potential for data breaches. When an airline shares its banking information with a prepared food provider, it typically does not consider the possibility that the supplier may lack the information security posture or maturity necessary to ensure the safety of confidential data. As this scenario plays out time and time again, it puts travelers and the general public at risk for a third-party data breach.

During the five-month period of this case study on one of CybelAngel's aviation customers, our data harvesting system and machine learning identified more than 10,000 publicly accessible servers, each containing multiple, potentially sensitive files belonging to this company. The majority of these exposed and unprotected files resided on third-party connected devices or in misconfigured cloud storage around the world.

The CybelAngel digital risk platform assessed the files identified via our scanning technology for severity of risk and degree of relevance using proprietary machine learning algorithms based on a 300+ keyword list. Following this artificial intelligence assessment, CybelAngel's cyber analyst team executed proprietary processes to determine the criticality of these file leaks and prioritize them accordingly. This two-step Augmented Intelligence methodology eliminated false positives, allowing the cyber analyst team to focus on delivering the most comprehensive and accurate detections. Finally, the team investigated the content of the documents and reviewed it in conjunction with open source intelligence (OSINT) related to airport security to ensure the relevance and criticality of the exposed information.

53% **of organizations surveyed experienced a data breach caused by a third-party, with an average cost of $7.5 million**

The CybelAngel analyst team ultimately confirmed the sensitive nature of hundreds of leaked files, which included 150 documents related to airport security badges, 400 blueprints detailing airport premises, and 350 documents containing details of aviation security and safety procedures and policies.

2. Number of flights performed by the global airline industry from 2004 to 2021. Statista. https://www.statista.com/statistics/564769/airline-industry-number-of-flights/

3. Number of scheduled passengers boarded by the global airline industry from 2004 to 2021. Statista. https://www.statista.com/statistics/564717/airline-industry-passenger-traffic-globally/

AVIATION CASE STUDY RESULTS

Each of the files we found were freely accessible, stored on unprotected devices or misconfigured cloud repositories belonging to third-party entities that were legitimately connected with the airports and agencies. Far from having a single exposure source, the documents were identified on thousands of open servers located around the globe. CybelAngel worked directly with the proper authorities, namely the FBI and Interpol, and the impacted organizations to secure this information and help protect those at risk. All of the open servers were closed expediently.

Lessons for Other Industries

It is easy to believe that other industries are not as vulnerable as aviation, or the consequences are not as dire. Before settling on this conclusion, stop and think about the following:

- Who audits your company's financials? What would happen if these were leaked to the financial community? To your competitors? Your customers?
- Who prepares your payroll and employees' end-of-year tax information? How would a leak of your employees personally identifiable information (PII) impact their lives, or your ability to recruit?
- Have you shared a blueprint of your premises including entrances/exits, HVAC runs, and secure areas such as server rooms or a data center? In the wrong hands, could this result in a physical security breach or cyber incident? If so, Gartner predicts the liability for failing to protect systems from cyber incidents will fall directly onto many CEOs by 2024.
- Where is your data hosted? What would happen if there were an open port or open source CVE that allowed your competitors to download your customer list, your price book, etc.? Or worse yet, expose all of your customers' data?
- With the huge shift to working remotely from home offices, how are your employees accessing and storing information? What would the consequences be if one of these employees stored your documents on an unprotected NAS?

This list just scratches the surface of the types of information that can be leaked in mundane ways, from a phishing email that downloads employee login credentials to elaborate cyberattacks that steal the lifeblood of your company.

Contributing Factors in Third-party Data Leaks

Let's examine a variety of factors contributing to increased third-party data exposure risk through the lens of our case study while recognizing the implications across all verticals.

SCALE OF THE ECOSYSTEM

The breadth of the case study ecosystem extends from the design of an airplane engine to the inflight experience of passengers. Hundreds — if not thousands — of third parties and Nth parties are involved in the business of aviation. Highly sensitive intellectual property shared with original equipment manufacturers (OEMs), detailed maintenance logs held by repair and overhaul facilities, passenger data held by travel agents and booking sites, purchase information in airport duty free systems, even the credit card data from the purchase of inflight WIFI or meals — each of these presents the opportunity for data compromise.

Physical Aviation Security

Gaining access to airport and airline controlled facilities is paramount for a threat actor. However, this is not always an easy task because of thorough security checks by well-trained and vetted personnel. Often these physical security processes are facilitated and managed by a third-party security partner. This means the partner's handling of highly sensitive and confidential data increases the opportunity for data leakage beyond the aviation company's direct control.

In this scenario, CybelAngel found freely accessible online files containing security badge templates and active badge identifiers entirely unsecured on connected storage devices used by a third-party security firm. These files included blank security application access forms, which could be filled out by malicious actors and, if processed, would allow the threat actor access to the airport facilities. More worrisome, however, were exposed files that included completed Transportation Security Administration (TSA) badge application forms with official stamps and signatures.

A cybercriminal or potential terrorist in possession of these openly available files would not have to rely on the processing and approval of a badge application. Instead, with the approved TSA badge form, an attacker could determine the name of the third-party firm with access to an airport and learn their workers' positions within the facility. Using photo editing software, a cybercriminal could replace ID photos and names with those of his team. Now, this criminal group would have vetted and approved TSA badges — allowing them unfettered access to secured areas of the airport.[4]

4. CybelAngel worked directly with our customer and the proper authorities, namely the FBI and Interpol, and the impacted organizations to secure this information and help protect those at risk. All of the open servers were closed expediently.

Operational Third Parties

Over the course of our research, CybelAngel located an unprotected server containing the files of a third-party supplier that worked on the integration of a new security camera system for a major airport. A new technology — networked, motion-sensitive cameras — was being implemented across a legacy system, which created an additional level of complexity for the teams involved.

The robust, detailed documentation required to make this installation a success was inadvertently leaked by this third party. CybelAngel found blueprints containing all of the camera locations. The documentation also revealed which cameras are motion activated, which have facial recognition capabilities, and how each ties into the overall security access system implemented at the airport. Accompanying those files was a detailed legend, as well as spreadsheets that listed one by one each of the security cameras at the airport, its function and orientation, and precisely how to access and take control of the cameras.

This information would grant a criminal the power to manipulate security systems remotely to enhance ease of movement throughout secure areas of the airport.

INTRODUCTION OF NEW TECHNOLOGIES

Supply Chain 4.0 emphasizes the importance of collecting and leveraging data to make better decisions for the entire supply chain. The initiation of integrated supply chain management platforms — which enable multiple parties to share data for analysis and visibility along the value chain — mean that with a single credential breach, a threat actor could gain access to several enterprises' data. Adding to the risk, digital transformation of processes is generating more data than ever before across all verticals, including the aviation industry. To this point, a Thales Group study indicated that a single passenger flight now generates nearly 1TB of data.[5] Pilot flight binders have been replaced by tablets, air traffic control radar by GPS, and boarding passes by mobile devices.

Challenges in Digital Risk Management

Information is critical to the success of any threat actor's campaign. In this digital age, obtaining sensitive, insider information is no longer a matter of breaking into filing cabinets. Instead, with the increased number of third parties per company, the movement of data to storage devices connected via the internet, and use of collaborative cloud applications, sensitive data is often leaked and freely accessible to hackers and cybercriminals across the Internet. With little more than basic internet skills a hacker or cybercriminal can locate online files with a treasure trove of critical information that can help execute a ransomware campaign,

5. "Digital Transformations Impacting the Ecosystem of Flight." Thales Group. April 15, 2016. https://www.thalesgroup.com/en/united-states/magazine/digital-transformations-impacting-ecosystem-flight

disrupt a major enterprise's business, or endanger the safety of citizens. Enterprises must consider the following issues when addressing digital risk across their third-party ecosystem.

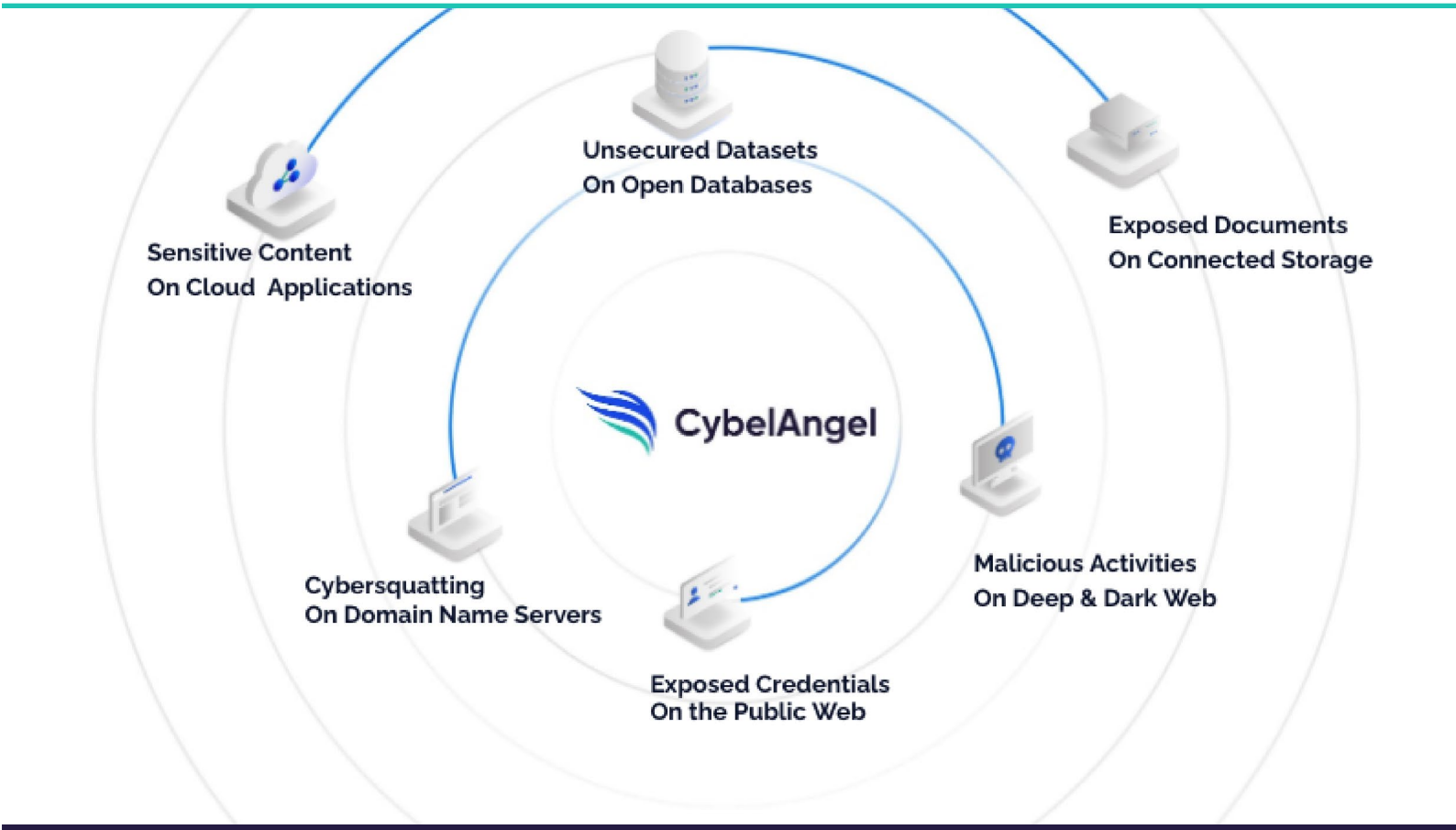
HIGH VOLUME OF DATA LEAKS

Assessing the opportunities for a data leak to occur across an entire supply chain ecosystem is daunting. Each employee within your own organization poses a risk, as well as each employee at every one of your vendors, sub-tiers, contractors, and partners. Added to that, each supply chain entity has its own complex ecosystem of third parties. The scale of digital risk is enormous. Data can be leaked negligently on multiple platforms, in multiple countries, in multiple languages. Simply detecting (let alone assessing) this volume of data for potential exposure just is not possible for most internal security teams.

Our system has detected more than 160 billion files over the last six months. On average, the system finds client data on servers or other sources in 23 countries.

Tracking leaked data after-the-fact can be like playing a digital game of whack-a-mole.

CYBELANGEL SCANS FOR SENSITIVE DATA ACROSS KEY INTERNET PERIMETERS



"While there's no going back on interconnectedness—it is a factor in today's world—every airline has to address the risk of third-party networking and the potential weakness of points of intersection."[6]

PWC, Airline Industry Perspectives

WIDE VARIETY OF SENSITIVE DATA

Any organization seeking to better understand their digital risk will cast as wide a net as possible when looking for potential data leaks. However, what is captured in that net (likely billions of files over a half-year timeframe) is useless for better understanding risk, regaining control over escaped data, or mitigating impact from the breach if this data cannot be properly triaged and analyzed. Internal security operations center (SOC) teams do a tremendous amount of sifting through alerts, but expecting them to review and correctly assess a high volume of alerts is like asking them to drink from a firehose. It is not very effective and can be demoralizing for highly motivated and well-trained team members. The ability to thoroughly and consistently assess both the relevance and risk level of files ranging from Excel and PDF documents to postings on a dark web forum is critical.

CybelAngel leverages artificial intelligence and machine learning to efficiently triage billions of documents and assess their level of criticality. For example, in the aviation industry research we conducted, our technology found nearly 10,000 freely accessible servers, each containing multiple files related to aviation. Triage via CybelAngel's machine learning algorithms, followed by assessment by a cyber analyst, refined the number of files identified as sensitive to approximately 900, including spreadsheets, PDF and image files, and word processing documents.

DYNAMIC MOVEMENT OF INFORMATION

From one day to the next, sensitive data that is exposed may change. Servers will go on and offline, posts on forums will be created or deleted, and domain names will be registered or cancelled. In short, figuring out what data has leaked from your organization, and from where it is leaked, is like finding a moving target. Digital whack-a-mole.

Speed Matters

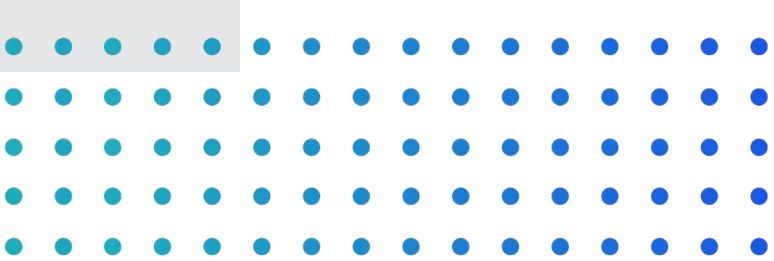
Once files are exposed and become publicly accessible, there is no way to be certain who will be downloading them and how they will be used — whether for a threat actor's own malicious plans or for sale to the highest bidder on the dark web. Fast identification of leaked files enables a company or government agency to act quickly in securing the information and mitigating any risk. Decreasing the timeframe to mitigation is particularly important, given the Ponemon Institute's assertion that the average time to takedown (mitigation) is 279 days.[7] CybelAngel's continuous scanning of the Internet and cloud and connected storage slashes average time to takedown for our clients by 84 percent; thus, significantly narrowing the digital risk window.

6. "Aviation perspectives. 2016 special report series: Cybersecurity and the airline industry." PWC. 2016. https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-airline-industry-perspectives-cybersecurity-detection.pdf
7. "IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years." IBM news release. July 23, 2019. https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

An important part of many supply chain contracts between enterprises and third parties is the former's ability to perform initial assessments of the vendor's or partner's information security capabilities and conduct occasional audits to verify compliance. While essential elements in a digital risk management strategy, these assessments and audits are simply snapshots of exposure or compliance at specific moments and may not help to address the non-stop flow (and potential exposure) of data. After an audit is completed at 10 am, a crucial file could be exposed at 10:05 am... exposed for any threat actor to find and leverage until the next audit takes place three, six, or 12 months later.

CybelAngel's scanning of connected devices, cloud storage, databases, deep and dark webs, public web, and domain names is continuous. Crawlers are working 24/7/365 to detect newly exposed files. This information is automatically assessed by our machine learning technology to ensure clients receive relevant alerts in a timely manner.

> "Companies in the aviation industry face yet another challenge. A key trend is increasing interconnectedness, whether it's between aircraft and ground control stations, airlines, airports and other aviation stakeholders, or between dispersed field-deployed assets. This same interconnectedness that provides operational efficiencies simultaneously introduces further risk..."[8]
>
> *PWC, Airline Industry Perspectives*



8. "Aviation perspectives. 2016 special report series: Cybersecurity and the airline industry." PWC. 2016. https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-airline-industry-perspectives-cybersecurity-detection.pdf

Looking Ahead

The challenges facing the aviation industry in managing digital risk across broad supply chains are the same as those facing enterprises in many other sectors. As digital threats evolve with new threat actors, new technologies, and new demands on the security posture of organizations, digital risk protection requires visibility beyond your corporate perimeter.

Leading enterprises are already investing in digital risk protection solutions to augment their cybersecurity stacks and ensure they will no longer be flying blind regarding data leaks outside of their firewalls and endpoints.

CybelAngel enables companies to protect against having data leaks become devastating breaches, regardless of where their data lives. We use advanced machine learning to detect leaks of customers' sensitive data, whether these occur on third-party servers or in cloud storage. Our data leak platform scans for confidential and proprietary data and its location, instantly alerting our clients when their sensitive data is at risk. To fix data leaks, our clients take action internally or rely on CybelAngel's security experts to resolve the risk.

Do you know the scope of your organization's risk for data leaks? CybelAngel will provide you a dashboard that indicates where your company's data is leaking and how you rank compared to other organizations in your industry—without any obligation.

Click here to get your company's complimentary Data Leak Dashboard.

If you suspect a data leak, **Contact Us.** Because data leaks are inevitable, but damage is optional.

Do you know your organization's risk for data leaks?

CLICK HERE to get your company's Data Leak Dashboard.

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