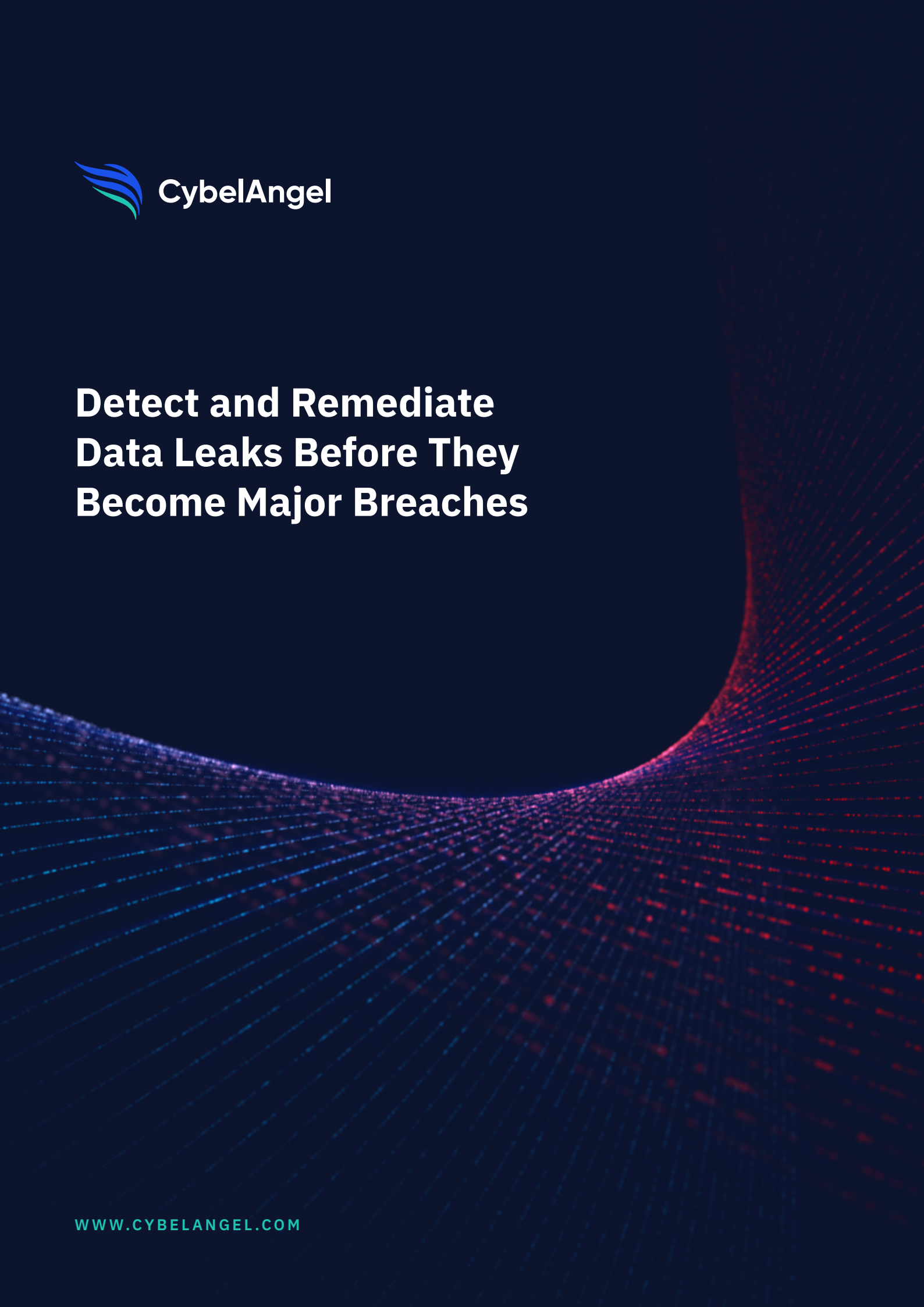
CybelAngel

Detect and Remediate Data Leaks Before They Become Major Breaches



WWW.CYBELANGEL.COM

Detect and Remediate Data Leaks Before They Become Major Breaches

SUMMARY

The proliferation of corporate data, growing use of cloud services, and an increasing reliance on third parties introduces new ways to expose corporate information and personal data. From detection to resolution, CybelAngel offers an end-to-end solution to address data leaks. Through executive dashboards, actionable reports and connectors with ServiceNow® and Splunk® companies can protect digital projects on the go.

As Businesses Connect, Risk Rises

Increasingly connected business means increased opportunity to leak sensitive corporate data. For Chief Information Security Officers (CISOs), the resources needed to detect and mitigate potential breaches often goes far beyond capabilities at their disposal.

An issue that most cybersecurity teams face is the need for speed, the inability to respond to incidents fast. Teams are pressured to identify and remediate threats quickly, but the backlog of threats continues to increase over time. What can you do when each day brings more incidents to investigate, and massive remote work leaves you more exposed than ever to data leaks?

Cybel Angel Detects and Resolves Data Leaks

CybelAngel's clients are provided with executive dashboards, actionable reports and relevant connectors with ServiceNow® or Splunk®. empowering them to protect their digital projects by updating data leak protection information on the go. Clients can manage their incident response capabilities with takedown support at the click of a button.

A comprehensive four-step process backed by augmented intelligence combines machine learning with insight provided by the world's best cybersecurity analysts to detect and remediate data leakage.

Four Steps to Detect Data Leaks

Julia Osseland, Product Marketing Manager at CybelAngel, outlines the four critical steps to detect data leaks:

1. The first stage is data harvesting, building a data lake to detect billions of documents.

2. Next, CybelAngel uses data processing and machine learning to filter documents by applying keywords specific to clients, such as their name and IP address. “We have points of focus that the client wants us to look at,” says Osseland. This focus on the client and expert knowledge of the customer’s business is critical to CybelAngel’s success in detecting data leaks that are relevant to each organization.

3. The third step considers the thousands of matches critical to the client and is when human intelligence and contextualization from machine learning comes into place. “Machine learning will have filtered out the noise before matches are sent to an analyst,” says Osseland.

4. The fourth step allows analysts, dedicated to a client account with deep knowledge of the customer’s environment, to apply their skills to ensure that only actionable data leak alerts are sent to the CISO. “Our analysts are experts in political and human sciences and know the challenges faced by customers. They go through the alerts and can separate actual threats and risks that require action, from what is noise. An incident report is then sent to the client via the platform in real time,” says Osseland.

Finding Data in the Clouds

Will Brown, UK Country Manager at CybelAngel, says “A key differentiator is the unique capability to detect business-sensitive documents and the databases where they are exposed on the internet, often unintentionally, perhaps through the pursuit of digital change projects.”

“Businesses are going through a digital transformation process. There is internal pressure to move physical boxes from within the company-owned perimeter and controlled datacenter to the cloud. When mistakes are made such as misconfigured cloud services, the result is data leaks,” says Brown.

Digital risk is not a reason to halt migration of data to cloud-based apps; it is a necessity in the evolution toward digital infrastructure. But when mistakes happen, deploying CybelAngel’s platform dramatically minimizes the risk of exposure.

Misconfiguration Leads to Exposure

According to Dark Reading, “We are seeing large numbers of cloud-based databases such Elasticsearch® left wide open through misconfiguration.”[1] While organizations use change and configuration control methodologies to reduce errors, ultimately, mistakes happen. The question is how can you detect the error and remediate it before it’s too late? The value CybelAngel brings is letting customers know that their data has been exposed so they can close the leak before it can be weaponized by malicious actors, bring regulatory fines or damage the company’s reputation.

CybelAngel has detected more than 1 billion *sensitive* files over the last six months. Corporate boundaries are a thing of the past, and there is a real need for speed to detect leaks as enterprises race to connect and transform digitally.

Managing the Risk of “Shadow IT”

Another challenge arises from “Shadow IT”, when employees, without sanction from the CISO, decide to pursue their own projects, which often exposes large amounts of data.

CybelAngel is focused on locating and safeguarding confidential documents that were negligently made available on corporate and third-party connected storage.

Peter Regent, Sales Director at CybelAngel UK, explains how employees may, for example, use unstructured databases such as MongoDB® or Elasticsearch, an open source search and analytics solution, for big data and cloud-based databases to spin up projects without the same security focus that is used for production systems. “Shadow IT working at development speed with agile capability can go outside the restrictions of a big corporation and expose corporate data -- for example, developing a new front end to an e-commerce site. Integrating cloud components can be a juggling act and it is hard to make secure in a world demanding speed and agility,” says Regent.

Troubleshooting Problems

CybelAngel can identify and troubleshoot sensitive content leaking through collaborative tools, repositories and cloud applications used by staff and third parties. It can also combat cybersquatting on domain name servers; exposed credentials on the public web; and malicious activities on deep and dark web sites.

[1] Dark Reading, Informatech (2019, March). Misconfigured Elasticsearch Instance Exposes More Than 5 Billion Records. https://www.darkreading.com/attacks-breaches/misconfigured-elasticsearch-instance-exposes-more-than-5-billion-records/d/d-id/1337368

However when it comes to exposed data, if cloud components are not made secure, there is no sympathy from the criminal world. “If you don’t secure critical perimeters, leaks will be found. Shadow IT often means individuals work quickly and flexibly, which increases the risk of leaks,” warns Regent. Part of the problem is that organizations have experienced four decades of using structured databases such as Oracle® and MySQL®, and often only a few years with unstructured databases, with only 10-15% of consultants experienced in the newer technologies.

Brown says it is one thing to detect an open server; it is another thing to understand the level of exposure and risk of that server. This is where CybelAngel’s solution excels at detecting and remediating a data leak.

“When an open server is detected it can often contain thousands of records. The ability to detect is one thing, but to understand, categorise, and express the risk almost instantaneously puts CybelAngel streets ahead,” Brown says.

The Importance of Data Science

CybelAngel has focused its efforts on recruiting data scientists and sees the challenge as a data science problem, which is why it can move so quickly to remediate and end leaks.

Data scientists can optimize learning capacity and hone in on what is important to ensure no false positives are sent to organizations, so they can take immediate and effective action to end leaks.

“We focused the lens on data leaks and cybersecurity as a problem that has to be solved mathematically by algorithms, so as not to send rubbish over. Machine learning’s ability to assist humans is key to what we do,” says Regent.

CybelAngel detects over one billion documents per day, relying on machine learning and human expertise to manage digital risk by detecting leaks across six critical internet perimeters. After filtering by machine learning, the additional contextualisation that the analysts provide across these perimeters is critical to knowing what action is necessary.

Remediating Data Leaks

Remediation can be executed by the client organization or by CybelAngel, depending on resources and what is required. CybelAngel’s Remediation Services are a complement to our detection services and give clients the option for CybelAngel to take down a leak expeditiously rather than take it down themselves.

Enterprises risk exposing their sensitive data when they share data with third parties who do not have effective security measures in place to detect leaks. These leaks can damage the enterprise’s reputation, incur regulatory scrutiny, and destroy trust with customers. Regardless of how or where the leak occurs, remediating the leak adds to the organization’s workload. “Information security departments are often under-resourced. We can take down their data leak. The benefit of us having responsibility for takedown is we can alleviate their workload,” says Osseland.

Enterprises may utilize CybelAngel's Remediation Services in a variety of ways. In some cases, a client may require CybelAngel to address less critical incidents, while they remediate more critical threats. Another company may have a team to remediate data leaks after receiving an incident report from CybelAngel. In this case, the data leak is handled by the organization because they are in the best place to speak to the culprit.

"CybelAngel is efficient at detecting critical leaks of acutely sensitive data, as well as remediation of the incident. In some cases, it is best to have the business handle the resolution of the data leak, as they have the relationship with their third-party provider. Cybel Angel's Remediation Service is purposefully-built for this level of flexibility and collaboration with our customers; it is an end-to-end solution.

If your company has been exposed to ten data leaks of sensitive information across three different internet perimeters over the last month -- such as connected devices, cloud applications, domain servers, public internet, deep and dark web, open databases or data sets -- you can expect to have between 100 and 150 incidents to remediate over the next year.

When security teams have a need for speed, CybelAngel meets the challenge. With experts in augmented intelligence, machine learning and data science, CybelAngel can offer data leak detection with zero false positives. If an organization needs a data leak taken down, CybelAngel offers remediation services, which can reduce the time from detection to takedown by as much as 85%. From detection to resolution, CybelAngel offers enterprises an end-to-end solution to address data leaks.

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