CybelAngel

ISMG INFORMATION SECURITY MEDIA GROUP

Exposed Databases: When It Leaks, Hackers Breach

Open database leaks are responsible for the exposure of more sensitive records than hacking.

WHITE PAPER

TABLE OF CONTENTS

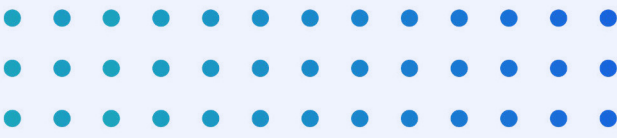
Executive Summary

Is your organization leaking sensitive data? If you have not looked for open databases on your network, then it's likely that you have a breach just waiting to happen, with all the regulatory, legal and reputational costs that entails.

A data leak refers to when any private digital data is publicly available without any identification requirement. It becomes a breach when an unauthorized entity accesses your critical data. Therefore, it is imperative to detect and identify any data leaks from internal or external sources before they become data breaches.

This paper will:

- Describe the extent of the "Open Database Leaks" problem.
- Identify what and where the main vulnerabilities are.
- Illustrate the ways in which they are exploited.
- Explain how CybelAngel's Digital Risk Protection Platform and cybersecurity expertise can be used to discover and fix exposure before leaks become breaches.



Awash With Leaks

Extent of Open Database Leaks

Data breaches are a widespread and serious business risk that must be addressed and mitigated. But how widespread is the problem?

In 2020, over 36 billion records were exposed globally.[1] In December of 2020, CybelAngel[2] shared that it had found more than 45 million medical imaging files publicly accessible on the internet. 2021 offers no reprieve, with an undisclosed number of customers at Internet of Things tech vendor Ubiquiti having their information exposed due to unauthorized access of a database via a third-party cloud provider. In January, right-wing U.S. social media app Parler found 70TB of data leaked after issues with its technology providers. That same month, an unsecured Elasticsearch database at Chinese social media management company SocialArks led to the leak of personal information of 200 million Facebook, LinkedIn and Instagram users. 2021 has also seen 1.9 million records leaked from Pixlr, and the records of 83 million users of stock photo site 123RF have been found for sale on the dark web after a breach.

Open databases allowing unauthorized access are reportedly responsible for 86% of all publicly accessible sensitive records.

Billions of these documents leave an enterprise's perimeters through unsecured databases due largely to misconfigured servers. Open databases allowing unauthorized access are reportedly responsible for 86%[3] of all publicly accessible sensitive records.

These open databases result in organizations of all sizes, unknowingly, leaving back doors to their data open, which can be exploited to devastating effect by hackers. 2020 Risk Based Security[4] finds misconfigured databases and servers are the leading cause of leaked records. 77.5% of leaks are attributable to hacking events originating outside the victim organization. Of the approximately 17% of breaches Risk Based Security identifies as originating from within the organization, the overwhelming majority – 67% – result from errors such as misconfiguration. It is likely that your organization has unsecured assets that are exposed to the internet, putting you at risk of a breach that could cost millions, assuming you survive the reputational hit.

Which Databases Get Attacked

Attackers will understandably go for the low-hanging fruit, and many organizations are making breaches far too easy. Most of the databases attacked are completely open, meaning they require no logins or passwords to be accessed online.[5]

Rank			DBMS	Database Model	Score		
Mar 2021	Feb 2021	Mar 2020			Mar 2021	Feb 2021	Mar 2020
1.	1.	1.	Oracle	Relational, Multi-model	1321.73	+5.06	-18.91
2.	2.	2.	MySQL	Relational, Multi-model	1254.83	+11.46	-4.90
3.	3.	3.	Microsoft SQL Server	Relational, Multi-model	1015.30	-7.63	-82.55
4.	4.	4.	PostgreSQL	Relational, Multi-model	549.29	-1.67	+35.37
5.	5.	5.	MongoDB	Document, Multi-model	462.39	+3.44	+24.78
6.	6.	6.	IBM Db2	Relational, Multi-model	156.01	-1.60	-6.55
7.	7.	↑ 8.	Redis	Key-value, Multi-model	154.15	+1.58	+6.57
8.	8.	↓ 7.	Elasticsearch	Search engine, Multi-model	152.34	+1.34	+3.17
9.	9.	↑ 10.	SQLite	Relational	122.64	-0.53	+0.69
10.	↑ 11.	↓ 9.	Microsoft Access	Relational	118.14	+3.97	-7.00

Table 1. Database ranking by popularity. Source: db-engines.com

Elasticsearch and MongoDB appear in the top 10 databases. (See Table 1.) They are the two most popular distributed datastores used to manage NoSQL data, but they are also the most frequently attacked. (See Table 2.) CybelAngel research[6] found that MongoDB databases are the type most often accessed and ransomed by criminals. They are also more likely to be online and unprotected.

It's clear that, whatever database you use, you are likely to be leaking data. That data leak will likely become a breach the instant it's subject to unauthorized access. The cost to your organization will depend on the sector and the nature of the data leaked, but the damage to systems, actual financial losses, the cost of remediation, fines, litigation or reputation will be costly.

PROTOCOL	3 MONTHS	6 MONTHS	1 YEAR
Mongo (unique)	45,672	68,704	119,931
Elasticsearch (unique)	37,341	54,148	86,398
SQL (unique)	21,012	35,335	60,948
TOTAL (unique)	**103,115**	**156,173**	**260,957**

Table 2. Database leaks by volume. Source: CybelAngel

Speed of Attacks

Attackers are on the prowl for open databases. Whether their goal is data theft, ransomware or cryptomining, open databases are quickly targeted.

One researcher sought to answer a question: “If one leaves a database unsecured on the web, how long does it take hackers to find and steal it?” As an experiment, they created a honeypot, in the form of an unsecured database located on an Elasticsearch instance, and recorded the results. Over 11 days, the unsecured database was attacked 175 times, roughly 18 times a day, beginning a mere eight hours after launch.

Before the database was even indexed by search engines, three dozen attacks occurred. Once indexed by search engines such as Shodan.io and BinaryEdge, the frequency of attacks increased and within a single minute of the database being indexed by Shodan, two attacks took place.[7]

Malicious attacks included ransom demands and attempts to install cryptomining, as well as theft of secrets. The results of this experiment show attackers are proactively searching for open databases and that risk of a breach increases with each minute.

Cost of Breaches Rises

The consequences of failing to act are increasing, and the cost of breaches continued to rise in 2020 and 2021. Breaches in which over 50 million records were compromised saw costs jump from $388 million in 2019 to $392 million in 2020. Breaches with 40 million to 50 million records exposed cost companies an average of $364 million, which is $19 million higher than in 2019.[8] The largest breach of Q3 2020 was attributable to an open Elasticsearch server, which exposed approximately 6 billion records and 6.4TB of data, and affected approximately 700,000 individuals.[9] One reason for the staggering scale of such losses is that data breaches typically stay undetected for an average of 280 days.[10]

Lawsuits from individuals suffering identity theft and draining of bank accounts can amount to millions in losses, especially if a class-action suit is filed.

Such data breaches can also result in regulatory fines and legal costs for the database owner running into millions - up to 4% of global revenue under Europe's General Data Protection Regulations. CCPA in California and other regulatory bodies have also introduced heavy fines and penalties. As an example, the Marriott Hotel group was fined £18.4 million by the U.K. ICO after it reported leaking of its customer database in 2018 following its 2014 purchase of the Starwood Hotels group, whose systems were compromised prior to the acquisition.[11]

Other substantive impacts from data breaches include having your organization's reputation irreparably damaged and its share price fall. In addition, lawsuits from individuals suffering identity theft and draining of bank accounts can amount to millions in losses, especially if a class-action suit is filed. Finally, organizations can also find themselves in political difficulties if sensitive government data falls into the hands of adversaries.

Once the high and increasing cost of a breach due to unsecured databases is appreciated, it is clear that this fixable risk is one that needs to be prioritized immediately as an easy win, where the returns on investment are almost immediate.

Why Databases Are Targeted

SUMMARY

The reasons for targeting databases include:

- Financial gain, particularly via ransomware and ID theft;
- Account takeover, particularly for espionage and to steal secrets or IP;
- Purposes of destruction, sabotage, malice, “fun,” vigilantism, reputational damage.

Financial Gain

If data is the new oil, then databases are the reservoirs of this valuable resource, and they can be drained remotely, quickly and surreptitiously. Databases are the knowledge base at the heart of any organization – storing customer records, contacts, prices paid and other confidential business data. They may include processes, designs, formulae or other valuable IP, including financial details; politically or legally sensitive information; staff details, including HR records; or government secrets.

Your adversaries can extract value from the previously private information your open databases are leaking. They might demand a ransom, most often payable in bitcoin, from your organization. At first, the payment of the ransom may be required to access your data and to enable business operations. Later, the ransomers may threaten to attack your reputation by leaking the data publicly if the ransom is not paid or political/hacktivist demands are not met.

In addition, CybelAngel analysts saw a sharp rise in the number of unprotected databases being hit with ransomware since May 15, 2020 – up nearly 75%, as compared with 1% to 3% in the previous 12 months. For example, during March 2021 it was reported that the z0Miner cryptomining botnet is now targeting and attempting to take control of Jenkins and Elasticsearch servers to mine for Monero (XMR) cryptocurrency.

Account Takeover

Even innocuous information, such as stolen email addresses and logins, can be used by criminals for credential stuffing to attempt to access various kinds of accounts. This can result in account takeover. As a result, it's not just the information in the initial database accessed that matters, but what doors that data opens within the network.

In the case of nation-states obtaining access to government secrets, such vulnerabilities could undermine negotiations or enable espionage, including in time of hostilities, with access potentially providing a route to account takeover.

31%

of data breach victims later have their identity stolen.

Personally identifiable information (PII) from staff and others can include Social Security numbers, driver's license numbers, bank account information and dates of birth, which can be used to open new lines of credit, commit identity theft and make fraudulent financial charges. It is reported that 31% of data breach victims later have their identity stolen.[12]

Sabotage and Vigilantism

Some attacks seem senseless. In the case of Meow attacks,[13] which only target databases that do not have security access controls enabled, Meow wipes files without asking for a ransom or any demands and without providing any form of notice or attribution.

According to one report,[14] these Meow attacks may be vigilante attempts to stop data disclosure from unsecured databases, but they actually cause damage and open databases to further attack in the process.

In March 2021, an Elasticsearch server belonging to U.K.-based data analytics company Polecat was hacked, after it was found to have no authentication or encryption in place. This led to the exposure of an estimated 30TB of data, including 12 billion records related to social media. The day after the server was exposed, a Meow attack erased half of the data. It is believed that the remaining data was later hacked by a third actor, who left a ransom note, asking for 0.04 bitcoin (around $550 at that time) to get the data back.

Causes of Open Databases

SUMMARY

The causes of open databases include:

- Human factors, negligence, misconfiguration, excess workload;
- Open API abuse or misuse;
- Open-source software flaws;
- Backup media storage;
- Third parties with extra access privileges.

The main cause of database exposure depends on the technology behind the particular database software. Some are unprotected by default, and the security is sometimes deliberately lifted to ease processes within a company. But based on CybelAngel's experience, misconfiguration due to human error is the number one cause.

Human Negligence

There are a range of technical attacks to be aware of, but human negligence is the root cause of up to 30% of data breach incidents,[15] which manifest as misconfigurations and other lapses. Often companies struggle to maintain an accurate inventory of their databases and the critical data objects contained within them. Forgotten databases may contain sensitive information, and new databases can emerge without visibility to the security team. Sensitive data in these databases will be exposed to threats if the required controls and permissions are not implemented.[16]

One reason for these lapses is that shortages of specialist staff persist, and workloads remain high among IT and security staff. Their work includes the complex and time-consuming patching and maintenance of databases, which may take months to patch, during which time they remain vulnerable. It can also be difficult to get downtime on critical systems to implement maintenance fixes.

Open API Access

Openness may be good for business, but it is not always good for security. Data democratization, where relevant data is made accessible to everyone from end users and developers to the traditional banks and financial institutions, is not a free-for-all. It has to comply with privacy laws and regulations (e.g., GDPR) as well as legitimate business concerns (e.g., IP protection, enterprise financials). But it has made more data available to more entities, and those granted access to consumer data have a responsibility to act with good faith and in the best interest of the enterprise – its business, employees and consumers. Open API access to allow new services to be interoperable, such as under open banking, is a concern if wrongly configured by the accessing third party.

Nearly all commercial databases – 99%, according to Synopsis – contain at least one open-source component, and nearly 75% of these code bases contain open-source security vulnerabilities.

Open-Source Software

Another source of third-party impact is open-source software. Nearly all commercial databases – 99%, according to Synopsis – contain at least one open-source component, and nearly 75% of these code bases contain open-source security vulnerabilities.[17] When fragments are reused, the audit trail of the original software becomes overly complex. Vulnerabilities unnoticed by developers can be exploited by hackers. Security vulnerabilities often go undetected for more than four years before being disclosed.[18] Once they are identified, the package maintainer and security community typically create and release a fix in just over four weeks.

When open-source vulnerabilities are made public, such as via the National Vulnerability Database (NVD),[19] attackers pounce before patching is done. Equifax was breached because it used part of the source code of Apache Struts, whose vulnerabilities had been published. Less common than simple errors in open-source code are backdoors, or "bugdoors," which are software vulnerabilities that are intentionally planted in software to facilitate exploitation. And there can be flaws in the OpenSSL cryptographic software library. Leaked secret keys allowed attackers to decrypt any past and future traffic.

While license compliance defines guidelines that allow source code to be used, modified and shared, most of these licenses do not meet the strict OSI and SPDX definitions of open source. There are more than 200 types of open-source licenses and, as organizations are required to comply with each individual one, they can sometimes be overwhelmed. One study[20] of 1,253 applications found that about 67% of code bases were subject to license conflicts and 33% of code bases contained unlicensed software.

Backup Storage Media

Another cause of data leaks is backup storage media that are completely unprotected from attack, are unmonitored and have unrestricted access. Some users may have been granted an excessive level of privileges, which can combine with the internal threat of misuse of database privileges by insiders.

Two major types of database injection attacks used by external attackers are SQL injections that target traditional database systems and NoSQL injections that target "big data" platforms. Both can give an attacker unrestricted access to an entire database.

Third-Party Leaks

Even when you are following best practices, your supply chain can be your weak link. Some 60% of businesses have experienced a major data breach caused by a third party with an average total cost of up to £3.86 million, according to the IBM Cost of a Data Breach Report 2020.[21]

Even when you are following best practices, your supply chain can be your weak link. Some 60% of businesses have experienced a major data breach caused by a third party.

It's not just your own staff's errors that you need to worry about. Almost two-thirds (63%) of the 4.1 billion records exposed in the first half of 2019 were exposed by third parties. These were also the most expensive kind of data leak,[22] according to Ponemon Institute. A third-party leak costs $370,000 on average compared with other kinds of data leaks. The added costs for third-party data leaks amount to over $4.26 million each year.

It seems incredible, but Ponemon notes,[23] on average, companies allow 583 third parties access to their data and says that 53% of organizations

have experienced at least one data breach caused by a third party, costing an average of $7.5 million to remediate. CybelAngel research[24] also found that third parties played an integral role in 62% of all critical-level incidents, 93% of all leaked documents from unprotected file servers and 39% of all code data leaks. All of these breaches were caused by negligence (e.g., misconfigurations) and in 81% of cases, a company's supplier was at fault.

A Real-World Solution

So what can be done? Of course, companies should continue to keep patching up to date by having an adequate supply of human resources with the appropriate skills. Misconfiguration should not happen, and implementation procedures should be thorough. Product and service providers should have stringent DevSecOps quality control and default settings that do not allow vulnerabilities to be introduced. But we are not in an ideal world. Staff shortages do exist. Third parties have variable standards. We may acquire a company and inherit its infrastructure but not the people who built it. People will make mistakes.

Security teams no longer primarily think about securing their corporate perimeter. Mature CISOs know that some of their confidential data has escaped the perimeter and is already out there. The actions you can take start with deploying specialist expertise and tools to identify and close data leaks in your network.

We are not in an ideal world. Staff shortages do exist. People will make mistakes.

How CybelAngel Can Prevent Leaks from Becoming Breaches

Borrowing terminology from the military, CybelAngel disrupts an attacker's kill chain – the logical progression of actions needed to achieve their objective – enabling defenders to take pre-emptive action that thwarts an attacker's progress. Looking at Table 3, CybelAngel's Digital Risk Protection Solutions, we can see that the crux of the service is to prevent attackers gaining an initial foothold, by identifying what exposures you have on your network, closing that access, expelling intruders, strengthening your defenses and minimizing the risk of becoming a breach victim.

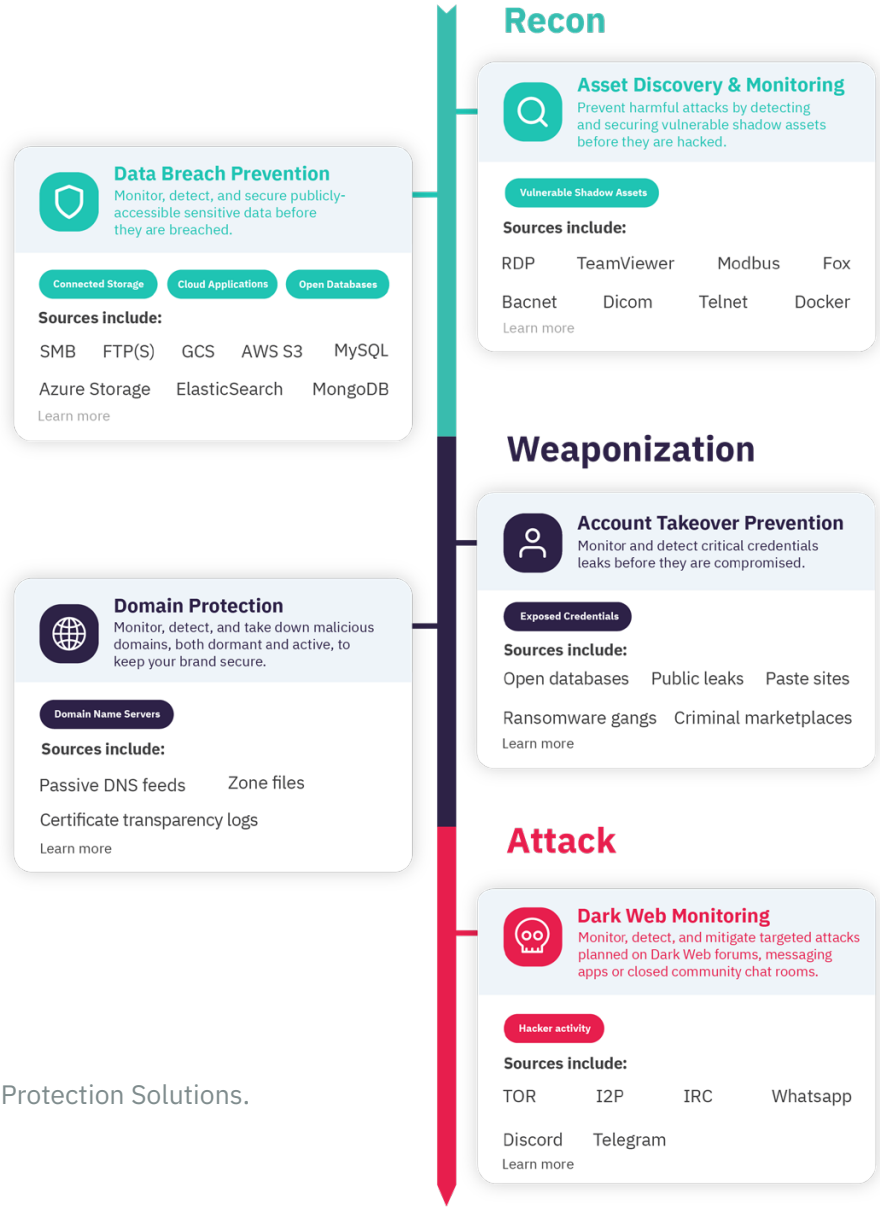


Table 3: Digital Risk Protection Solutions.
Source: CybelAngel

Comprehensive IP Scanning

To secure your vulnerabilities, you must first find what and where they are. CybelAngel monitors some 4.3 billion IPs (See Tables 4 and 5.) with weekly, in-depth, document-centric scanning of every layer of the web to detect leaks of sensitive or confidential data, whether from a cloud provider, vendor, contractor or a past or present supplier. It scans the entire IP spectrum, so it will scan any internet-connected device. This includes OT, IoT, connected storage devices, cloud applications and code repositories, as well as databases, locating all your internet-exposed assets.

Focusing solely on open databases scanned by CybelAngel monthly, Table 4 shows the total number of lines scanned by CybelAngel within open databases over four months in 2020.

DATE	NUMBER OF OPEN DATABASE LINES SCANNED PER MONTH
APR 2020	2,635,149,153,461
MAY 2020	3,709,750,847,730
JUL 2020	1,608,934,310,339
SEPT 2020	516,518,437,070

Table 4. Total number of lines searched by CybelAngel. Source: CybelAngel

The cyber exposure of an organization's strategic suppliers is assessed in five business days, detecting up to 800,000 exposed documents per minute. Table 5 shows the amount of unique IPs of open databases, per protocol, scanned by CybelAngel over a few months.

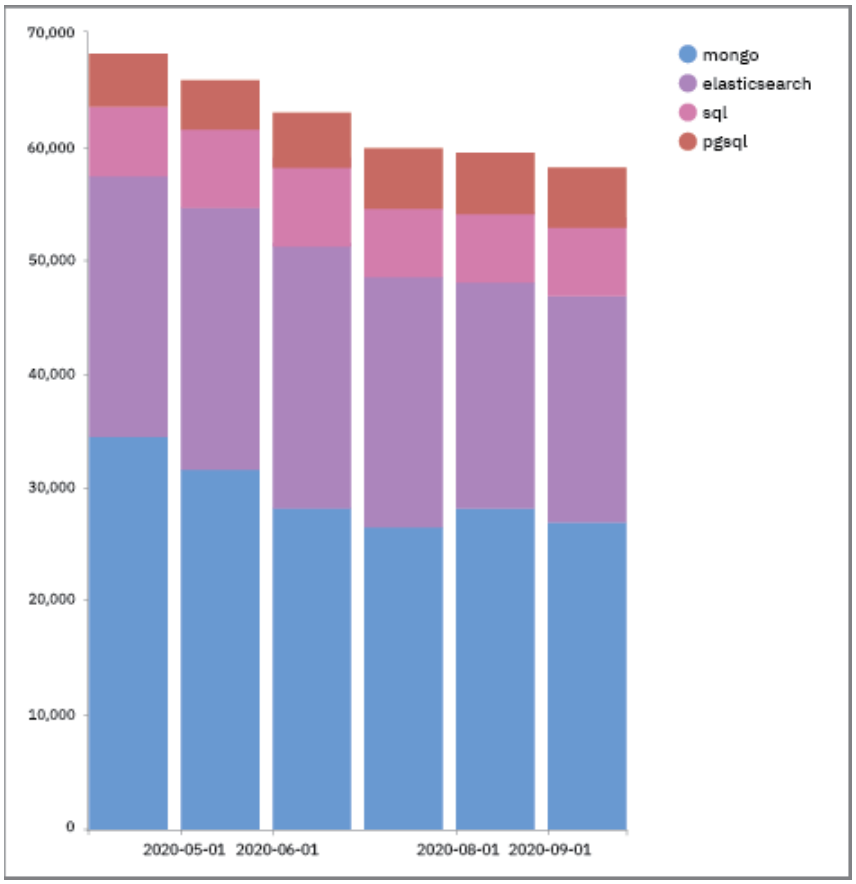


Table 5. April to November (partial month), number of unique IPs per protocol. Source: CybelAngel

Excellent Cloud Detection Capabilities

CybelAngel is the only Digital Risk Protection solution providing data leakage protection across the top three bucket cloud storage providers: Amazon Web Service S3, Google Cloud Storage and Azure Blob Storage. They scan active, publicly accessible cloud containers at the file-path level for critical documents. They create custom matching rules with your teams to alert you on what matters, quickly. To cover all ground, they also detect leaking API access keys and cloud credentials on code repositories.

Detecting Shadow IT

In January 2021, CybelAngel launched its Asset Discovery & Monitoring solution, which enables customers to regain control over their critical assets by detecting and securing unknown – often shadow IT – physical devices, cloud storages or productivity apps. These are continuously monitored for vulnerabilities that expose the organization to potentially devastating data breaches.

Timely Alerts and Remediation

Billions of assets are now exiting the enterprise's perimeter. Without the appropriate technology stack in place, sorting the true positives from the overwhelming false positives has become simply impossible. Many providers have been slow to apply a data science-backed approach to this new context, leaving organizations with a considerable amount of efforts to eliminate noise.

CybelAngel uses Augmented Intelligence from the start, where machine-learning algorithms combine with human expertise to eliminate all false positives. CybelAngel provides high-impact, actionable alerts, allowing threat teams to focus on what's critical. This is a unique approach on the market to scale your security operations without having to hire additional security headcounts. (See Table 6.)

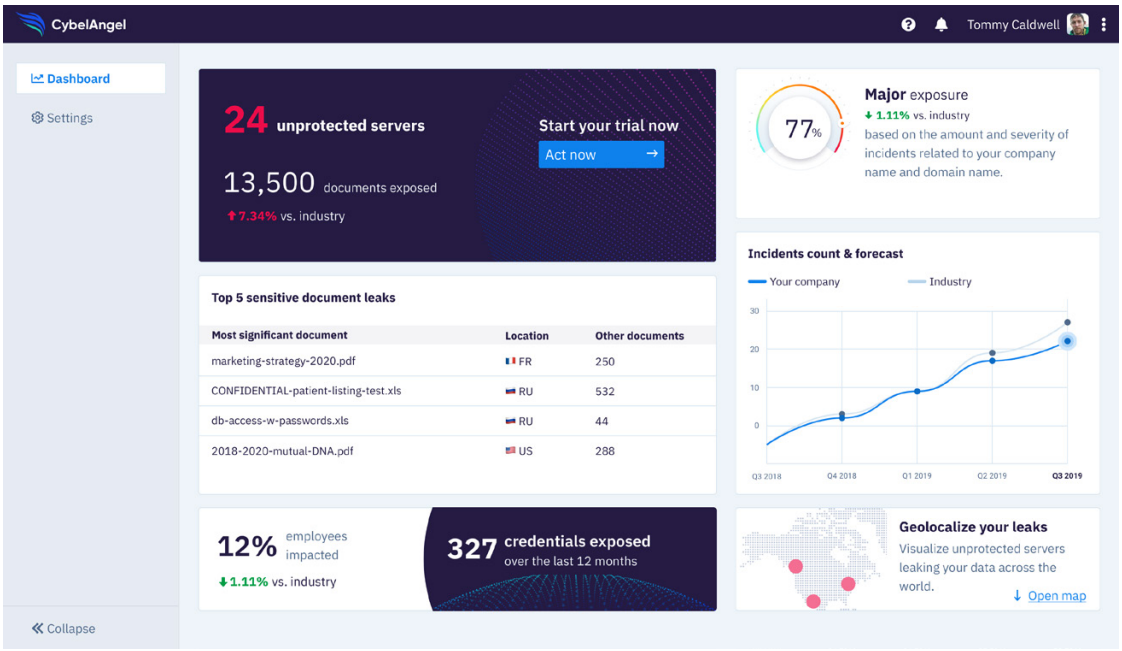


Table 6. Source: CybelAngel

Integrating SIEM and SOAR

While CybelAngel's early detection abilities are a boon, they work best if they are integrated into the cybersecurity stack and workflows of an organization. By integrating CybelAngel with SIEM and SOAR, you can, for instance, ensure password changes are automated, rather than manually alerting every employee facing a credentials leak. Active Directory is updated immediately after CybelAngel alerts are received, and automated notifications can be sent to affected employees to remind them of appropriate professional credentials use.

Return on Investment and Customer Perspectives

CybelAngel delivers value in three important ways: improved efficiency, enhanced visibility and increased agility. Our Data Breach Prevention enables the unrestrained use of cloud technologies or data exchanges by eliminating security concerns creating greater efficiencies. With CybelAngel, your executive team gains greater visibility and immediate awareness of exposed assets, compromised supply chains, pending business risks and possible ways of mitigation, reducing the costly time wasted. Finally, CybelAngel provides greater agility for SOC and CERT teams in reducing their incident backlog.

With CybelAngel, average time-to-takedown is 11 days, while the industry average is 85 days. The typical payback on investment, based on CybelAngel's ROI calculator, is four weeks. CybelAngel customers report obvious satisfaction at having been able to identify and close data leaks before they became breaches:

> "CybelAngel is the only solution that detects a potential crisis before it effectively becomes one."
>
> –Thierry Auger, Deputy CIO and CISO, Lagardère

> "With CybelAngel, we establish a new border of detection outside of our architecture, encompassing the world of our partners and suppliers, where we can't, by design, take control of their security."
>
> –Jean-Yves Poichotte, Global Head of IS Security, Sanofi

Across six years of operations, CybelAngel's customer retention rate is greater than 98%, while ratings on Gartner Peer Insights reach 4.9. This is the best proof that CybelAngel's customers demonstrate measurable ROI to their executive boards.

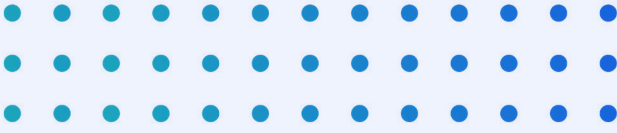
Conclusion

If your organization connects to the internet, it is likely that you have exposed databases. Exposed databases are leading to endemic data loss across all businesses, with personal data, intellectual property and credentials being left unprotected till after a breach occurs. This means every business is living under the constant threat of a breach leaving them vulnerable to fraud, theft, fines, reputational loss and even the end of an organization.

The main causes of exposed databases are known; human error from misconfigurations and onerous workload, excess third-party privileges, open API abuse and open-source software flaws. With multiple factors leading to data exposure and potentially devastating consequences, a business must seek to proactively find and remediate leaks before they evolve into breaches.

Specialist skills and tools can conduct deep scans to identify vulnerabilities to be remediated. Using ongoing automated IP scanning, including alerts and remediation, will enable staff to identify key weaknesses, take action and protect against future threats.

CybelAngel enables companies to protect against data leaks becoming devastating breaches, regardless of where the data lives. By using advanced machine learning, CybelAngel detects leaks of customers' sensitive data, whether these occur on third-party servers or in cloud storage. The Digital Risk Protection platform scans for confidential and proprietary data and its location, instantly alerting clients when their sensitive data is at risk. To fix data leaks, clients take action internally or rely on CybelAngel's security experts to resolve the risk. CybelAngel customers often see full ROI in a matter of weeks.



References

[1] 2020 Q3 Data Breach QuickView Report.pdf: riskbasedsecurity.com
[2] https://cybelangel.com/blog/medical-data-leaks/
[3] 2020 Q3 Data Breach QuickView Report.pdf: riskbasedsecurity.com
[4] 2020 Q3 Data Breach QuickView Report.pdf: riskbasedsecurity.com
[5] 1 in 3 Databases have been hacked: https://cybelangel.com/blog/one-three-databases-hacked/
[6] 1 in 3 Databases have been hacked: https://cybelangel.com/blog/one-three-databases-hacked/
[7] Unsecured databases attacked 18 times per day by hackers, We setup a honeypot to see how long for hackers find unsecured database: comparitech.com
[8] 2020 Q3 Data Breach QuickView Report.pdf: riskbasedsecurity.com
[9] https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/
[10] https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/
[11] https://www.bankinfosecurity.com/interviews/analysis-are-marriott-bas-gdpr-fines-big-enough-i-4791
[12] Experian SelfKey blog: 30 Eye-Watering Identity Management Statistics - SelfKey
[13] CPO Magazine: https://www.cpomagazine.com/cyber-security/new-meow-cyber-attack-that-wipes-unsecured-databases-is-a-malicious-throwback/
[14] CPO Magazine: https://www.cpomagazine.com/cyber-security/new-meow-cyber-attack-that-wipes-unsecured-databases-is-a-malicious-throwback/
[15] Ponemon/IBM Cost of a Data Breach Report: https://www.ibm.com/security/data-breach
[16] Ponemon/IBM Cost of a Data Breach Report: https://www.ibm.com/security/data-breach
[17] 3 Open-Source Security Risks and How to Address Them: towardsdatascience.com/3-open-source-security-risks-and-how-to-address-them-82f5cc776bd1
[18] Octoverse GitHub, Securing the world's software: https://octoverse.github.com/static/github-octoverse-2020-security-report.pdf
[19] National Vulnerability Database: https://nvd.nist.gov/
[20] 2020 Open-Source Security and Risk Analysis Report: Synopsis
[21] Ponemon/IBM Cost of a Data Breach Report: https://www.ibm.com/security/data-breach
[22] Ponemon/IBM Cost of a Data Breach Report: https://www.ibm.com/security/data-breach
[23] Ponemon/IBM Cost of a Data Breach Report: https://www.ibm.com/security/data-breach
[24] CybelAngel. How to Manage Third Party Digital Risk: https://cybelangel.com/whitepaper-how-to-manage-third-party-digital-risk/

About CybelAngel

CybelAngel is the world-leading digital risk protection platform that detects and resolves external threats before these wreak havoc. Because more data is being shared, processed or stored outside the firewall on cloud services, open databases and connected devices, the digital risk to enterprises has never been greater. Organizations worldwide rely on CybelAngel to discover, monitor and resolve external threats across all layers of the Internet, keeping their critical assets, brand and reputation secure.

Learn more at www.cybelangel.com or connect with us on LinkedIn.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io