CybelAngel

DATASHEET

ASSET DISCOVERY AND MONITORING

Prevent attacks against vulnerable shadow assets

Is your digital infrastructure fully protected against hackers? Unsanctioned assets, decommissioned services and partners' vulnerable products extend your attack surface outside of your purview. These shadow assets may remain invisible to you, but not to your attackers; 30% of successful cyber-attacks target vulnerable shadow assets (Gartner).

Traditional vulnerability management solutions are incapable to guarantee the safety of shadow assets at scale. Hence organizations worldwide rely on CybelAngel to prevent harmful attacks by detecting and securing vulnerable shadow assets before they are breached.

LOWER YOUR EXPOSURE WITH CYBELANGEL

- **Discover Shadow Assets** set up by employees, third and fourth-parties.
- **Focus On Highly Vulnerable Machines** with a risk-driven approach, not an inventory approach.
- **Protect In The Long Run** by putting newly discovered IPs under surveillance.

KEY TECH BENEFITS

4.3B	IPV4 scanning with in-depth, risk-driven matching.
>7	CVEs only. Focus on highly critical vulnerabilities to secure the most exposed assets.
<2h	Set-up time. No additional FTE, no probe or sensor required.

KEY BUSINESS BENEFITS

0%	Zero false positives. Avoid losing time and money sorting feeds of false alerts.
0	Additional FTE required on your side. Investigation is led by your CybelAngel analyst.
4	Quick return on investment, with average 4-week payback.

VULNERABLE SHADOW ASSETS INCLUDE

- **Connected File Servers**: IPv4+ connected storage, NAS drives, FTP servers, RSync backups, etc.
- **Databases**: ElasticSearch, Cassandra, Redis, CouchDB, RethinkDB, etc.
- **Industrial Systems:** telemetry systems, hardware machines, heating systems, etc.
- **DevOps Tools**: infrastructure control servers, container management softwares, etc.
- **Remote Desktop Services**: RDP, vnc, Team viewer, etc.
- **IoT**: medical imagery equipment, etc.

"CybelAngel is the only solution that detects a potential crisis before it effectively becomes one."

Thierry Auger, Deputy CIO and CISO, Lagardère International

GET NOTIFIED WHEN

Internet-facing RDPs are providing information to attackers in recon phase.

Misconfigured Industrial protocols are leaving your buildings vulnerable to hacking.

Shadow web servers are exposing you to ransomware attacks.

No Probe Required

Zero False Positives

Dedicated Analyst

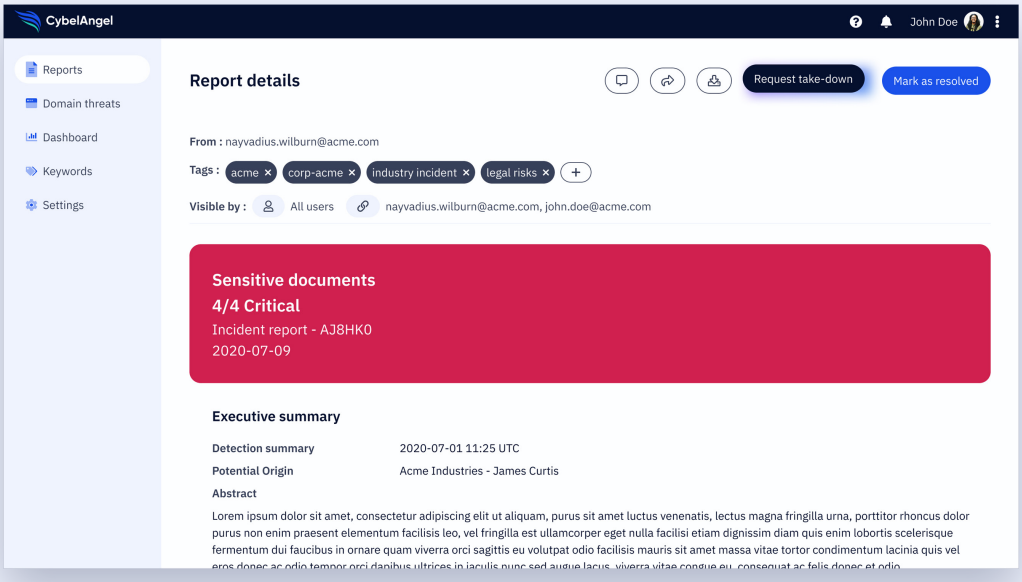
Fully Actionable

Severity Indicator
Focus your efforts on the most critical incidents first.

Details of the exposed asset
Authentify service or device.

Incident Origin
Pinpoint incident response.

Risk assessment
Anticipate potential attackers' next move.



Integrate CybelAngel In Your Toolstack

KEY FEATURES

- Fully documented RESTful API. Build a robust and scalable asset discovery workflow.
- Real-time synchronization. Retrieve, manage, resolve all Incidents Reports.
- Custom connectors on-demand. Map Incidents detected in CybelAngel to events in your SOAR, ITSM or SIEM platforms.

KEY BENEFITS

- Scale your digital risk protection by integrating realtime, zero false-positive asset discovery and monitoring capacities with your existing toolstack.
- Streamline your incident response by building simplified workflows.
- Enrich your threat intelligence strategy by correlating CybelAngel incidents with alerts from other digital risk protection solutions.

Book Your Free Trial Now CYBELANGEL.COM

Paris | New York | London

CybelAngel

DATASHEET

DATA BREACH PREVENTION

We detect data leaks others don't.

How much of your intellectual property and confidential information now exists outside of your IT perimeter? Nearly 60% of businesses have experienced a major data breach caused by a third party, resulting in an average total cost of $4.29 million (source: Ponemon, 2020). Traditional IT solutions are incapable to guarantee the safety of critical data across complex, digitized supply chains. That's why organizations worldwide rely on CybelAngel to monitor, detect, and resolve data leaks across connected storage devices, databases and cloud ecosystems, keeping their business, brand and reputation secure.

YOUR DATA BREACH PREVENTION SOLUTION

- **Leaker Identification.** CybelAngel provides the name of the potential leaker for every incident, when available.
- **Dedicated Analyst Manager.** Your go-to expert for analyzing and contextualizing every alert targeting your brand and business.
- **On-request take-down.** Your end-to-end solution, from detection to remediation.

KEY TECH BENEFITS

4.3B IPs monitored with daily in-depth, document-centric scanning.

800k Exposed documents detected per minute, making CybelAngel's dataset the largest in the market.

<2h Set-up time. No additional FTE, no probe or sensor required.

KEY BUSINESS BENEFITS

0% Zero false positives. No additional resources are required on your end.

85% Time-to-take-down reduced by 85% with end-to-end solution.

4 Quick return on investment, with average 4-week payback.

DATA LEAK SOURCES INCLUDE:

Connected Storage Devices
File servers and NAS, network virtual drives, web servers, etc.

Cloud Applications
Cloud storage services, cloud drive services, code-sharing platforms, file-sharing platforms, project management tools, etc.

Databases
Unprotected databases

"CybelAngel is the only solution that detects a potential crisis before it effectively becomes one."

Thierry Auger, Deputy CIO and CISO, Lagardère International

GET NOTIFIED WHEN

An employee shares financial data on a publicly-accessible collaborative tool.

A supplier stores your customers PII on an unsecured database.

A contractor saves your intellectual property on a NAS drive set to default configuration.

Fully Actionable

Zero False Positives

Dedicated Analyst

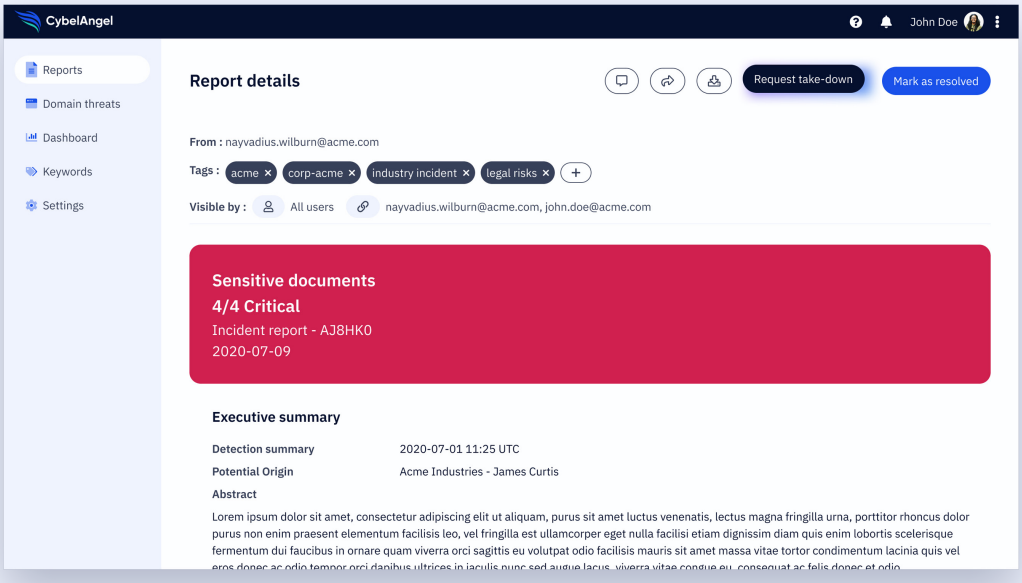
Take-down services

Severity Indicator
Focus your efforts on the most critical incidents first.

Sample of the exposed data
Authentify leaked documents.

Incident Origin
Pinpoint incident response.

Take-down
Offload your IR team when needed.



Integrate CybelAngel In Your Toolstack

KEY FEATURES

- Fully documented RESTful API. Build a robust and scalable data breach prevention workflow.
- Real-time synchronization. Retrieve, manage, resolve all Incidents Reports.
- Custom connectors on-demand. Map Incidents detected in CybelAngel to events in your SOAR, ITSM or SIEM platforms.

KEY BENEFITS

- Scale your digital risk protection by integrating realtime, zero false-positive data leak detection capacities with your existing toolstack.
- Streamline your incident response by building simplified workflows.
- Enrich your threat intelligence strategy by correlating CybelAngel incidents with alerts from other digital risk protection solutions.

Book Your Free Trial Now CYBELANGEL.COM

Paris | New York | London

CybelAngel

DATASHEET

Clarity into Connected Storage Devices

Ensure your secrets are safe with CybelAngel.

In 2020, CybelAngel found that 1.2 billion documents are leaked per day on file servers alone. Because people find them so easy to use to easily access and share files, connected storage devices pose serious security risks for businesses, across their extended ecosystem.

Trust CybelAngel to scan connected storage devices in order to prevent data breaches from impacting your business. CybelAngel scans all popular ports for connected storage devices, including NAS drives, FTP servers, and web servers.

Results[1]

305 billion files

exposed due to misconfigured connected storage

-99%

reduction in time-to-detection

213 days

saved on average incident response time vs. industry standards

1. (From July 2020 - early September 2021)

What CybelAngel scans

Sources	CybelAngel	Competitors
NFS	●	●
FTP(s)	●	●
SMB	●	●
HTTP(s)	●	●
Rsync	●	●

Protect against connected storage threats

Ransomware Prevention

Prevent hackers from finding unprotected documents and then freezing storage devices.

IT infrastructure protection

Block hackers from finding unprotected databases and then freezing networks for financial gain.

Defense against information loss

Secure storage devices with documents that have credential information and allow access to your proprietary data.

Benefits

VISIBILITY

Gain visibility into the unknown.

CybelAngel scans unsecured, connected storage devices outside of your perimeter, so you understand your business's external threats.

CONFIDENCE

Be sure connected storage isn't leaking your data.

CybelAngel scans 4.3 billion IP addresses. Your security team can rest easy with the knowledge that if there is data leaking on a connected storage device, we'll find it.

SPEED

Find external threats before others do.

Teams can take 213 days to detect data breaches. CybelAngel detection rates vary depending on the connected device source, but partner with CybelAngel to reduce your time-to-detect by as much as by 99%, aka in 2 days.

Learn more