UpGuard

UpGuard CyberResearch

Data Leak Detection Datasheet

The cloud has changed cybersecurity. Rapid cloud adoption is now the norm, as organizations move at the speed of digital transformation. The UpGuard platform empowers cloud-enabled organizations to proactively mitigate cybersecurity risks and securely operate in an evolving threat environment. By combining world-class expertise with our AI-assisted platform, UpGuard data leak detection capabilities are able to detect sensitive data exposed by employees, contractors, or third-parties.

What is Data Leak Detection?

Detect exposed data

Monitor keywords relevant to your business and always be notified if there is a data leak for your keywords. Failure to detect exposed data can have serious consequences on your business, from enabling corporate espionage to customer identity theft.

How UpGuard detects data leakages

Organizations provide UpGuard with a set of keywords, such as brand names, internal project names, company names. Our data leak detection engine and our analysts scour the web and notify you of any data exposures.

Monitoring multiple sources of exposures

UpGuard monitors hundreds of vectors, encompassing billions of exposed records, including:

- Publicly-available online file storages, such as Amazon S3, Azure Blob Storage, SMB, FTP, and RSync,
- Databases like MongoDB and Firebase,
- Company websites that include content hosting services, such as indexed folders and CDNs,

and hundreds more.

UpGuard's data leak detection continually monitors the Internet for a set of keywords important to your business that you have provided to UpGuard's analysts.

At a glance

- ✓ Detect sensitive data exposed by employees, contractors, or third-parties.
- ✓ UpGuard combines data leak detection engine and UpGuard analysts who reviews and investigates the findings, reducing the number of false positives.
- ✓ Get help to remediate the data leakage alerts with remediation workflows.

> Security posture dashboard and data leak detection tool that you need.
>
> Gartner Peer Review
>
> August 2020

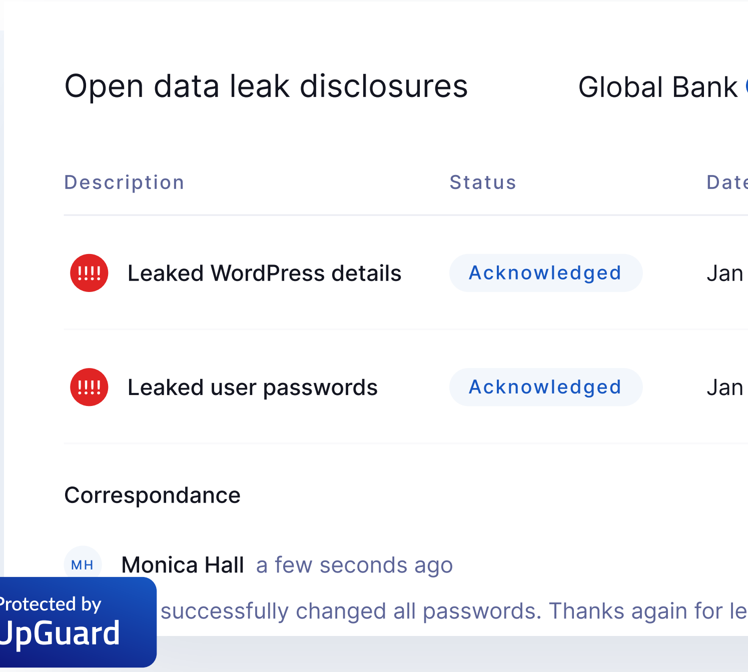
Gartner peerinsights™ 5.0 ★★★★★

Key features and benefits

Detect leaked employee credentials	Leaked employee credentials enable attackers to gain unauthorized access to your organisation's systems.
Monitor sensitive documents and customer data	Exposed documents and customer details can create business, reputational and regulatory issues. Detect exposed customer data such as PII, protected health information, and leaked payment data.
Vendor data exposures	UpGuard data leak detection can also monitor your third-party vendors for data exposures, including those that contain references to your organization.
Instant context	For every data leak alert, UpGuard provides context that enables you to make better decisions, including source, severity, and significance.
All findings reviewed by an analyst	Our analysts review and analyze each data exposure by hand, only notifying you of verified and risk-assessed leaks.
Risk remediation	UpGuard can help you remediate your data leakage alerts with remediation workflows through the platform and through our API.

We're processing over 800 billion data points each day and are directly responsible for securing over 1.9 billion records.

UpGuard is a cybersecurity platform that helps global companies prevent data breaches, monitor third-party vendors, and improve their security posture. Through proprietary security ratings, world class data leak detection capabilities and powerful remediation workflows, we proactively identify security exposures for companies.



Open data leak disclosures Global Bank

Description	Status	Date
!!!! Leaked WordPress details	Acknowledged	Jan
!!!! Leaked user passwords	Acknowledged	Jan

Correspondance

MH Monica Hall a few seconds ago

successfully changed all passwords. Thanks again for le