UpGuard

Whitepaper

Data Leak Detection

UpGuard CyberResearch sets a new standard for
Third-Party Risk Management and Data Leak Detection.

Trusted by hundreds of companies worldwide

Bill.com MORNINGSTAR NASA NYSE iag ICE Akamai

UpGuard

Table of Contents

UpGuard

Introduction

The price of leaked data

The inexorable dependence on data and its continued proliferation creates an appreciating commodity sending criminals into a frenzy.

The increasing value of sensitive data means that criminals will always be on the hunt for it. This translates into a substantial financial burden when data breaches occur.

The numbers are astronomical.

According to a May 2020 report from IBM and the Ponemon Institute, the average cost of a data breach has risen to $3.92 million. This is a 1.6% increase in cost compared to 2018 and a 12% increase over the last 12 years.

The effects are not only directly monetary. An organization could suffer irrevocable reputational damage after a data breach. A study by Gemalto showed that 70% of consumers would switch brands in the event of a data breach.

The increased prevalence of data breaches has resulted in increased regulatory compliance pressure to mandate data leak vigilance. Examples include GDPR, CCPA and Australia's Privacy Act. The healthcare and finance sector are under particular pressure to expunge all data leak vulnerabilities.

But the vulnerabilities that facilitate data breaches are not only internal.

Organizations have a 27.7% chance of suffering a data breach (an increase of 2.7% compared to 2019) and 58% of these breaches are linked to third parties.

This offset from traditional attack vector surfaces creates a complex challenge that surpasses conventional capabilities, demanding a reformative response to data leak prevention.

The transition to a higher standard of data leak due diligence is only possible by overcoming the following limitations of conventional solutions.

- Lack of continuous vendor monitoring
- Lack of access to cybersecurity talent
- Lack of solutions that are cloud-native and target vendors

58%

Of data breaches occur within a vendor network.

27%

Organizations have a 27.7% chance of suffering a breach.

Traditional Digital Risk Protection Services (DRPS)

The truth about traditional Digital Risk Protection Services

Currently, DRPS solutions only monitor for data exposures within an organization's own footprint. Such information only covers a single dimension of the data leak spectrum.

UpGuard have been pioneers in the DRPS landscape with the first fully SaaS-based solution to help organizations detect and close their own data leaks. Having discovered and helped remediate data leaks for Facebook/Cambridge Analytica, the Republican National Convention, Amazon, GoDaddy and Tesla, UpGuard has been pioneering the effort in this new threat landscape.

But with 58% of data breaches occurring within a vendor network, organizations are currently overlooking a majority of the threat landscape. Without broadening the DRPS focus to include third-party vendor monitoring, the risk of a data breach will always be greater than its successful prevention, despite innovations in data leak prevention methods.

UpGuard

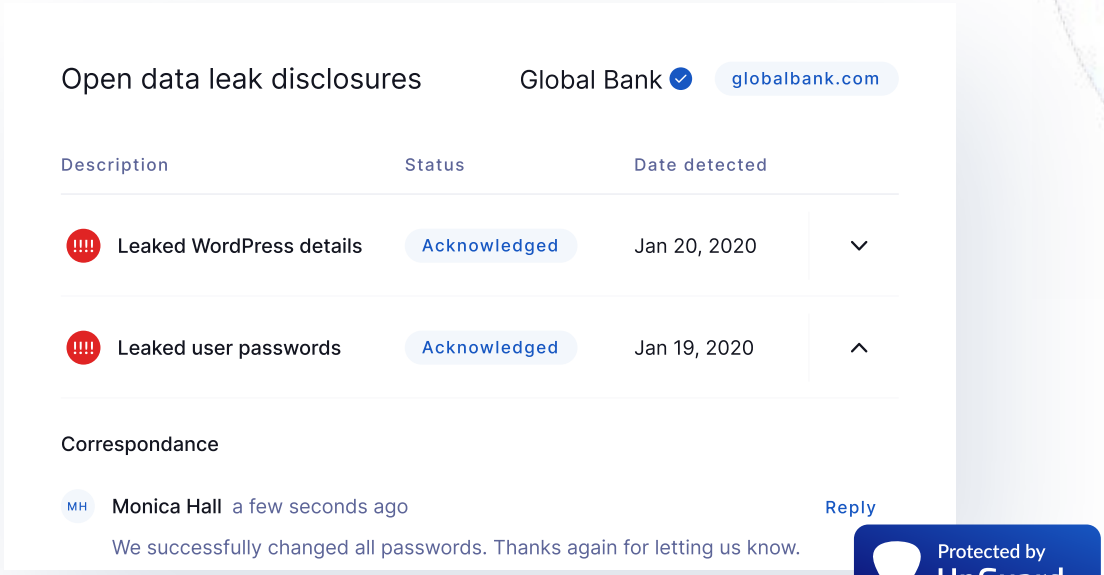
Traditional DRPS do not monitor for data leaks in the vendor network

Existing third-party risk solutions list publicly disclosed breaches for each vendor, but none are continuously monitoring for breaches that aren't publicly disclosed. These seemingly innocuous instances could develop into devastating data breaches.

- Only focused on monitoring internal endpoints, emails and networks.
- Majority of threat landscape overlooked.
- Data breach prevention methods are reactive rather than proactive.
- Costly data leak prevention solutions only protect against 40% of breach occurrences.

40%

Costly data leak prevention solutions only protect against 40% of breach occurrences.



UpGuard

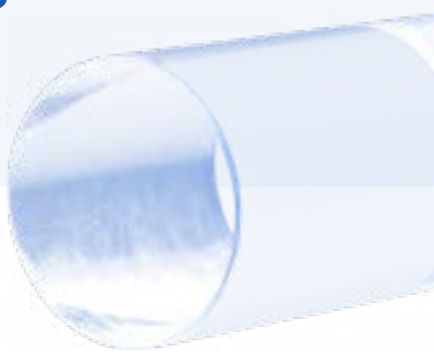
Traditional DRPS do not connect organizations to data leak analysts

The evolving complexity of data leak vulnerabilities means that organizations lack the necessary erudition to effectively manage threats. This is the primary reason for non-compliance with regulatory standards, resulting in significant fines.

Filling knowledge gaps with an in-house security team is an extremely difficult and costly solution.

- An internal security team could cost at least $1.4 million annually.
- Without a contextualized approach to data leak analytics, remediation efforts will not be targeted.
- Expert guidance prevents costly misinterpretations of data leak vulnerabilities, wasted effort assessing false positive results, and noncompliance with regulatory standards.

The evolving complexity of data leak vulnerabilities means that organizations lack the necessary erudition to effectively manage threats.



UpGuard

Traditional DRPS do not monitor external infrastructure

Traditional security solutions only focus on internal infrastructure such as email, directory services and endpoints. They lack the ability to continuously monitor the cloud and vendors for leaks.

There is also a severe deficit of cloud-native solutions that could dramatically decrease the onboarding time of necessary defences.

- **Static event-centric policies provide a negative user experience.**
- **Internal security teams are overwhelmed with superfluous requests.**
- **Full scope of regulatory standards are often not met, resulting in costly regulatory fines.**

A 900 / 950

Armed with security ratings and data leak detection, you'll be able to proactively identify, quantify and manage first, third and fourth-party risk instantly.

Data breach detection

Audit trail

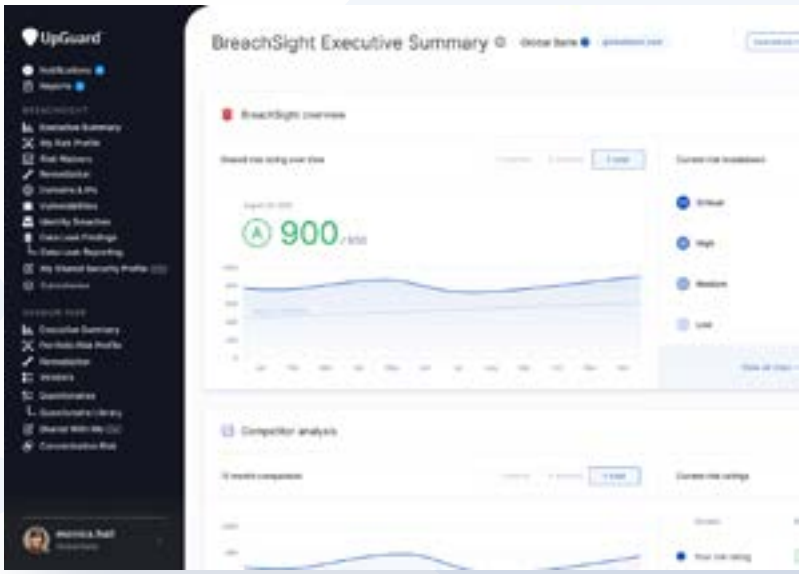
Vulnerabilities detection

Vendor security ratings

Data leaks

Automated questionnaires

Risk remediation

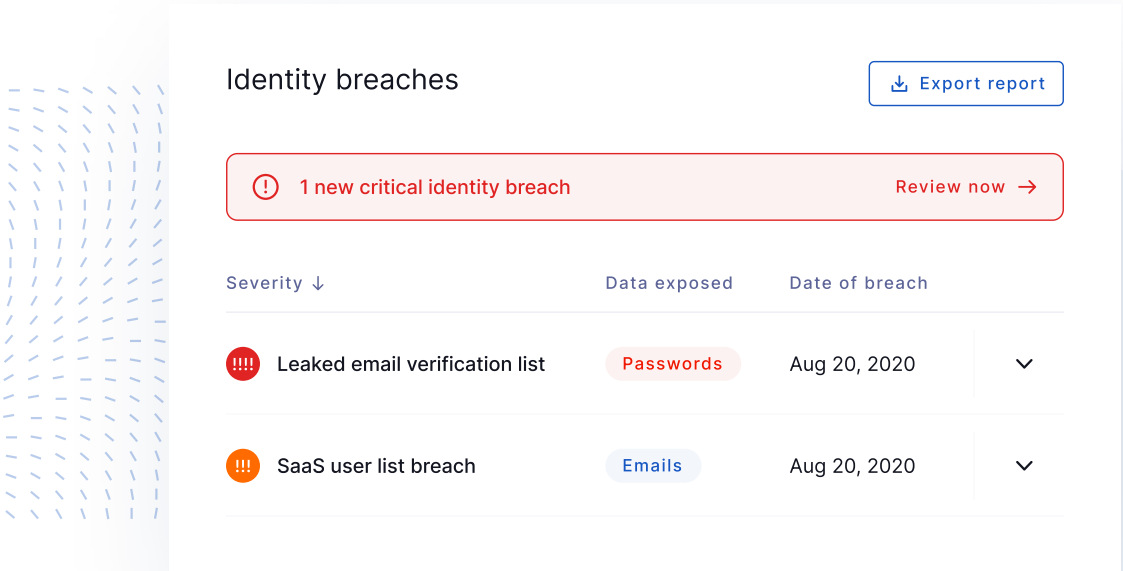


UpGuard

CyberResearch: The superior Digital Risk Protection Service

Conventional Digital Risk Protection Services limit their potency with a narrow assessment of the problem statement. Sharpening threat detection methods solely focused on internal infrastructure, will always leave a business vulnerable to data breaches through its overlooked third-party network.

The solution is a complete reformation of the conventional DRPS framework. This involves significantly broadening monitoring parameters to include the vendor network and connecting organizations with world-class security analysts to correctly interpret identified data leaks.



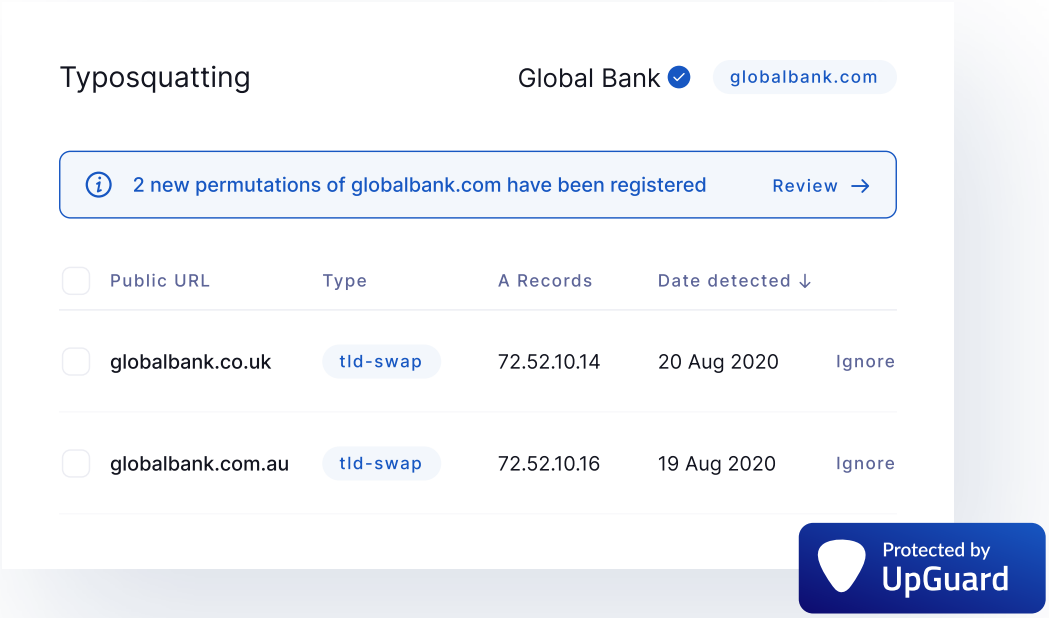
CyberResearch: The Superior DRPS

Expert security analyst support

CyberResearch removes the costly requirement of an internal security team. Organizations are supported with dedicated cybersecurity analysts to assist with the complexity of data leak detection and interpretation.

These world-class analysts have helped discover and secure some of the world's most high-profile data breaches, further ensuring compliance with strict regulatory requirements.

- Exclusive access to a dedicated cybersecurity analyst for focused reporting and threat interpretation.
- Vendor data leak notification, to identify vendors at greatest risk of a data breach.
- Unlimited data leak monitoring for a nominated list of keywords to continuously strengthen detected vulnerabilities.

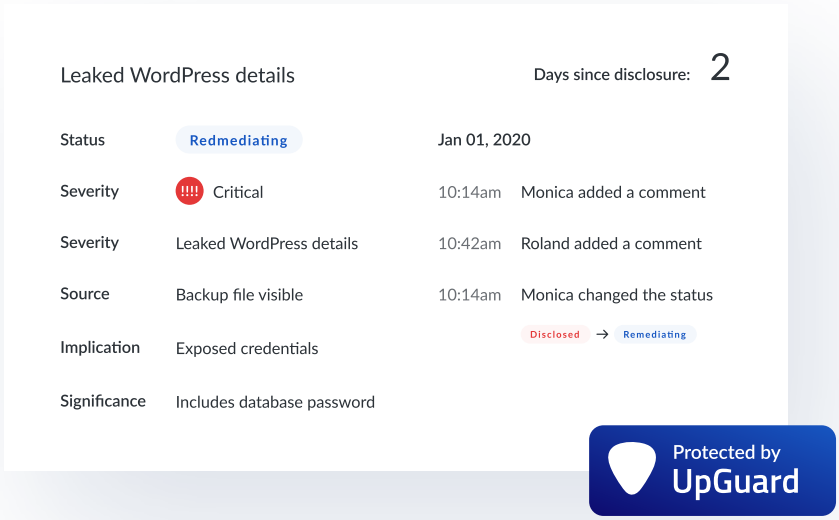


CyberResearch: The Superior DRPS

Cloud-native data leak protection

A SaaS solution acutely decreases onboarding time, giving customers instant data leak protection. Within a 45 minute onboarding call a complete index of all potential leaks is created for immediate global monitoring.

- The UpGuard platform has been intentionally designed for ease-of-use to dampen the learning curve and accelerate expertise.
- The SaaS solution combines the power of AI-based data leak surfacing with world-class analyst expertise, completely removing the need for a costly internal security team.
- Dedicated cybersecurity analysts can assist with nominating the most relevant data leak keywords for the most efficient data breach protection.



45 min

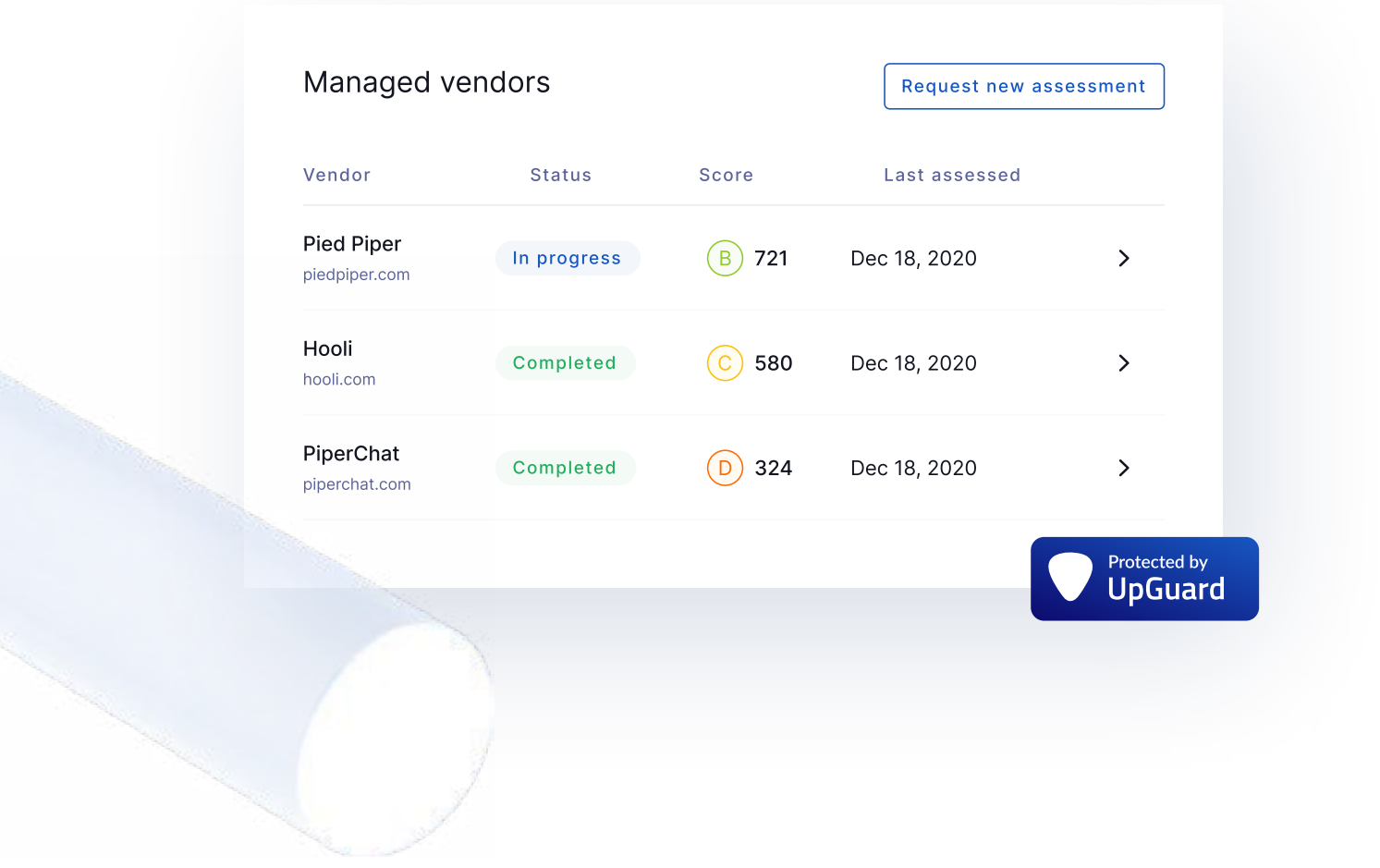
Within a 45 minute onboarding call a complete index of all potential leaks is created for immediate global monitoring.

UpGuard

The secure choice for data leak protection

Expanding data leak detection parameters to also include third-party vendors addresses the overlooked majority of data breach instances. The addition of world-class cybersecurity analysts creates the most authoritative and cost-effective data leak security solution.

UpGuard CyberResearch gives organizations deeper visibility into their third-party attack surface, empowering them to identify and address third-party data leaks before they develop into catastrophic data breaches.



UpGuard

Questions? We have answers

We're here to help, shoot us an email at sales@upguard.com

Know your vendors. Secure yourself.

Looking for a better, smarter way to protect your data and prevent breaches?

UpGuard offers a full suite of products for security, risk and vendor management teams.

Contact sales | Free demo →

Trusted by hundreds of companies worldwide

Bill.com MORNINGSTAR NASA NYSE iag ICE Akamai

www.upguard.com

+1 888-882-3223

650 Castro Street, Suite 120-387, Mountain View CA 94041 United States