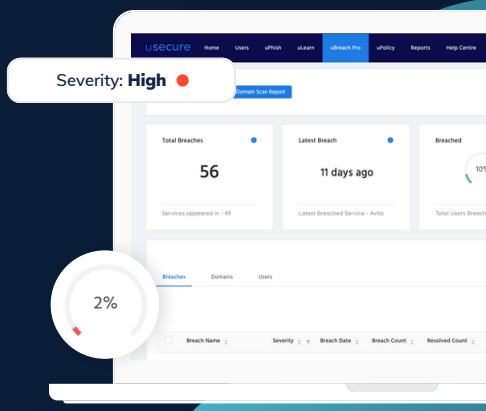
usecure | uBreach Pro

Defend your business with proactive breach monitoring

Secure your business against the hidden dangers of the dark web through actionable dark web monitoring and instant breach alerts.



Reduce existing risks

Identify sensitive user data that is currently accessible to attackers.

Prevent future breaches

Get instant email alerts when users are found in the latest breaches.

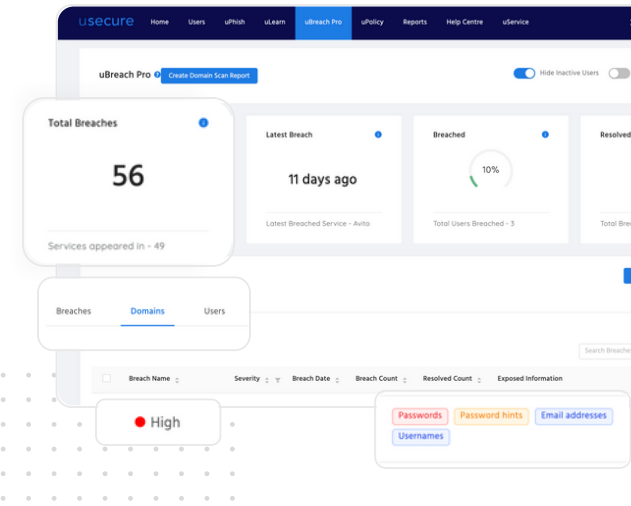
Achieve compliance

Demonstrate your data protection efforts and regulatory compliance.

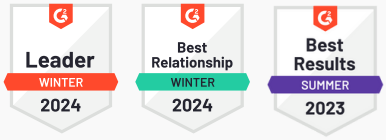
Prevent cyber threats early in the attack lifecycle

In an era where digital security is paramount, businesses cannot afford to be blind to the dangers lurking in the shadows of the dark web. User credentials and sensitive data, once exposed, become tools for cybercriminals, leading to potential security breaches, financial loss, and reputational damage.

uBreach Pro serves as a critical line of protection, proactively identifying and mitigating these risks before they escalate into crises.



uBreach **leads the way in dark web monitoring**



Rated as a Leader on G2.com

Enhanced cybersecurity

Significantly reduce human cyber risk and prevent costly security breaches.

Comprehensive coverage

Extend protection across all user email accounts associated with your domain.

Proactive breach alerts

Keep ahead of threats with instant email notifications for affected users and admins.

Understand the risk impact

Reduce your ongoing human risk score by quickly resolving user breaches.

Get started with uBreach Pro

	uBreach Starter *Reactive monitoring for breach remediation.*	uBreach Pro *Proactive intelligence for breach prevention.*
Dark web monitoring	✔	✔
Extensive breach database	✔	✔
Domain monitoring	✔	✔
Alert notifications	✔	✔
Advanced reporting	✔	✔
Set breaches as ‘resolved’	✔	✔
View exposed data values	✔	✔

usecure

Upgrade to uBreach Pro today

Head over to uBreach in your usecure portal to upgrade in a few simple steps, or, book a call with your usecure Account Manager.

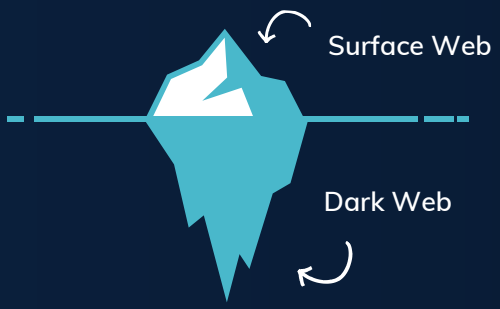
Grab a quick tour

Head over to usecure’s YouTube channel to watch a quick 2-minute tour of uBreach Pro.

Watch Product Tour



The Dark Web: A breeding ground for targeted attacks



In today's digital landscape, where cyber threats lurk in every corner, safeguarding your business's sensitive information is not just a necessity – it's an imperative. As the dark web becomes a thriving marketplace for stolen user credentials and confidential data, businesses without robust monitoring solutions stand at a crossroads of escalating risks and potential crises.

24.6B

A Digital Shadow report found 24.6 billion complete sets of usernames and passwords circulating in cybercriminal marketplaces.



Those 24.6B username and password combinations offered for sale on the dark web show an increase of 65% since 2020.



Google Cloud's 2023 Threat Horizons Report found that 86% of breaches involve stolen credentials, incl. usernames and passwords.

Why should your business focus on addressing dark web threats?

Increased risk of unauthorized access

With stolen user credentials freely available on the dark web, businesses face a heightened risk of unauthorized access to their systems and sensitive data.

Targeted social engineering attacks

The availability of personal and corporate information on the dark web enables cybercriminals to deceive employees and compromise security.

Regulatory and compliance risks/fines

The exposure of sensitive data on the dark web can lead to breaches of regulatory compliance, resulting in fines and damage to reputation.