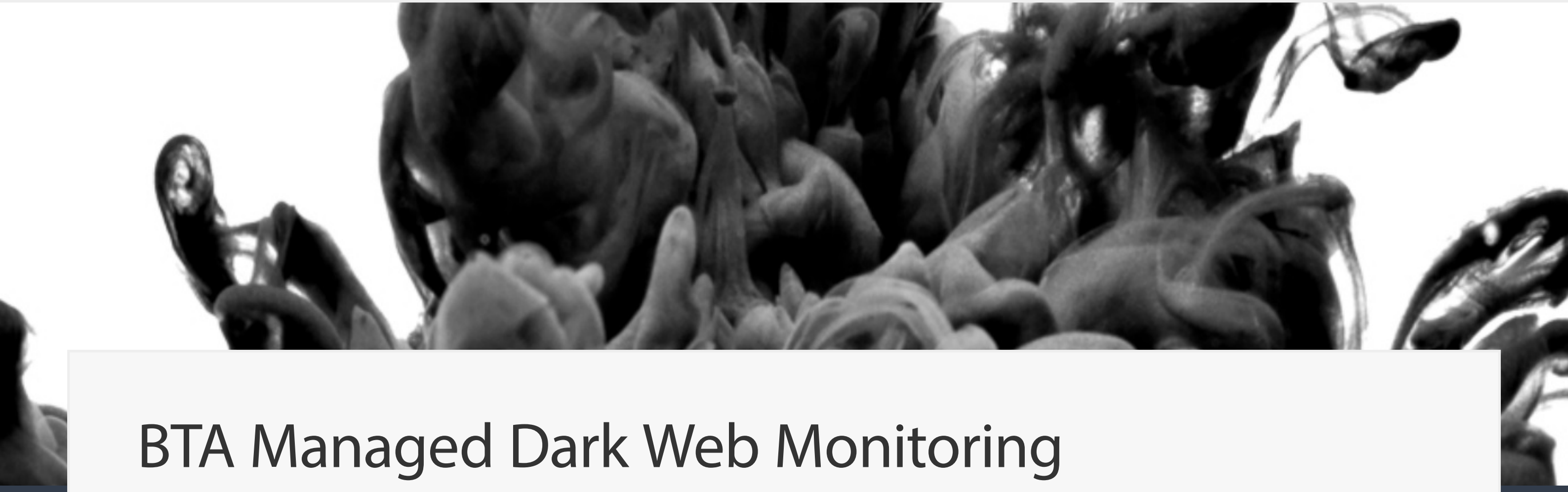
bta> The business IT experts



BTA Managed Dark Web Monitoring

BTA Managed Dark Web Monitoring provides continuous scanning and notification of your organisation's credentials on the Dark Web, so you can take action before critical digital assets are compromised.

Digital credentials such as usernames and passwords connect you and your employees to critical business applications, as well as online services. Unfortunately, criminals know this — and that's why digital credentials are among the most valuable assets found on the Dark Web.

What is the Dark Web?

The Dark Web is a hidden universe contained within the "Deep Web"— a sub-layer of the Internet that is hidden from conventional search engines. While there are legitimate purposes to the Dark Web, it is estimated that over 50% of all sites on the Dark Web are used for criminal activities, including the disclosure and sale of digital credentials. Far too often, companies that have had their credentials compromised and sold on the Dark Web don't know it until they have been informed by law enforcement — but by then, it's too late.

BTA Managed Dark Web Monitoring is a fully managed service utilising Dark Web ID by ID Agent – the industry's first commercial solution to detect your compromised credentials in real-time on the Dark Web!

ID AGENT PARTNER

BTA Managed Dark Web Monitoring combines intelligence with search capabilities to identify, analyse and proactively monitor for your organisation's compromised or stolen employee and customer data. Using a proprietary technology, this service vigilantly searches the most secretive corners of the Internet to find compromised credentials associated with your company, contractors and other personnel, and notifies you immediately when these critical assets are compromised, before they are used for identity theft, data breaches or other crimes.

With BTA Managed Dark Web Monitoring you will benefit from:

- Full set up of the service, supported by highly experienced engineers who can advise you on the right security to protect your business
- Continuous searching, monitoring and notification of your digital credentials on the Dark Web
- Fixed monthly fee for primary domain to be monitored. Reduced monthly fees for additional domains
- Up to 5 personal email addresses per organisation can also be tracked, in addition to all emails on the company domain

How BTA Dark Web Monitoring protects your business:

- Delivers the same advanced credential monitoring capabilities used by Fortune 500 companies
- Connects to multiple Dark Web services, including Tor, I2P and Freenet, to search for compromised credentials, without requiring you to connect any of your software or hardware to these high-risk services directly
- Provides awareness of compromised credentials before identity theft or data breaches occur

Prepare

Today, you have limited visibility into when your credentials are stolen; over 75% of compromised credentials are reported to the victim organisation by a third party, such as law enforcement. Extensive logging and reporting capabilities allow us to track everything that happens with your network, so there are no surprises. The monitoring also allows us to triage incidents and create effective policies and procedures to minimise risk in the future.

Predict

Compromised credentials are used to conduct criminal activity, such as corporate information leaks, or sensitive details about individual employees. It's not enough to simply be ready, you need to be ahead. This service allows us to see industry patterns long before they become trends, and offers the intelligence to keep you, your employees, and consultants more protected.

Protect

Users often have the same password for multiple services, such as network logon, social media, online stores and other services, exponentially increasing the potential damage from a single compromised username and password. Attacks on networks may be inevitable, but they don't have to be destructive. Proactive monitoring of stolen and compromised data alerts the BTA Managed Dark Web Monitoring platform as soon as it is detected, so that we can respond immediately, and minimise the risk to all affected services.