

Dark Web Monitoring Service

Proactively Identify and Mitigate Dark Web Risks

Cyber Security Services 



The Challenge

Cyber criminals exploit the Dark Web to trade stolen credentials and sensitive information, which they can then use to target organisations through phishing attacks, ransomware, and unauthorised access. With over 80% of breaches involving compromised passwords, businesses face significant risks if these threats remain undetected. The financial and reputational damage caused by data breaches can lead to operational disruptions, loss of client trust, and compliance violations.

Aztech IT's Dark Web Monitoring service continuously scans the Dark Web to identify stolen credentials and other sensitive data linked to your organisation to help keep your business secure.

Key Business Outcomes:

Improved Security Posture:

Detect and address compromised credentials before they can be exploited.

Reduced Risk of Breaches:

Act on real-time insights to prevent data breaches and safeguard sensitive information.

Operational Continuity:

Minimise disruptions caused by cyber incidents with proactive threat detection.

Informed Decision-Making:

Gain actionable insights to strengthen cyber security strategies.

Enhanced Employee Awareness:

Improve cyber security practices through expert advice and training.

Why Choose Us?



Proven Expertise: Over a decade of experience in Dark Web Monitoring and threat analysis.



Actionable Insights: Clear recommendations empower businesses to act swiftly and effectively.



Customised Approach: Tailor monitoring to your organisation's unique security needs.



"If you're looking for IT Support, you need a company that listens to its customers and provides solutions it needs rather than solutions it believes you may want – we have found Aztech do that."

Alan Clarke, Financial Director (MiniClipper Logistics)





Service Overview

Our advanced monitoring techniques and expert analysis enable proactive risk identification, providing actionable insights and recommendations to mitigate potential breaches. We help you address vulnerabilities early and protect your business from escalating cyber threats.

Continuous Dark Web Scanning: Monitor the Dark Web 24/7 to identify stolen credentials and sensitive data.

Advanced Monitoring Techniques: These techniques cover platforms frequented by cyber criminals, including private websites, peer-to-peer networks and black market sites.

Detailed Reporting: Provide insights into detected threats, helping you prioritise actions and mitigate risks effectively.

Expert Consultation: Deliver expert analysis and guidance to address vulnerabilities and enhance security.

Predictive Threat Intelligence: Leverage patterns and trends to anticipate emerging threats and act pre-emptively.

Example Use Cases



Identify compromised credentials: Detect stolen passwords and login details before they lead to breaches.



Mitigate targeted phishing risks: Use real-time insights to prevent phishing attacks on employees.



Strengthen security policies: Inform policy updates and employee training with threat intelligence.

How It Works:

Initial Assessment:

Identify critical assets and potential risks to maximise monitoring capabilities.



Continuous Monitoring:

Deploy advanced scanning tools to track compromised data in real-time.



Threat Detection:

Analyse detected risks and determine their impact on your organisation.



Actionable Reporting:

Provide detailed reports and recommendations to mitigate risks.



Ongoing Support:

Offer expert consultation and updates to maintain strong security practices.

What's Next?

Take proactive steps to protect your organisation from cyber threats. Book a consultation call to learn more about Aztech IT's Dark Web Monitoring service and how it can safeguard your business.