FUJITSU

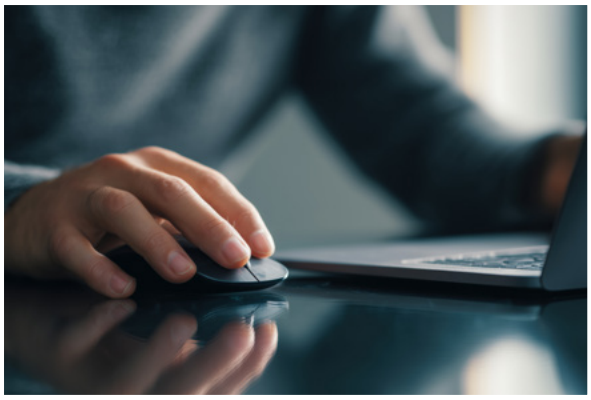
Darknet Report

A point-in-time assessment of your darknet exposure

Cyber criminals operate in hidden corners of the internet where stolen data, compromised credentials and targeted attack planning circulate long before a breach becomes public.

Fujitsu's Darknet Report gives your organisation a point in time snapshot of its exposure within these dark web communities - delivering clarity, confirmation and actionable insights without committing to continuous monitoring. It's a fast, intelligence driven way to uncover hidden risks and strengthen your security posture.

Continuous Darknet Monitoring is available for those requiring ongoing visibility as new threats emerge.



Understand what cybercriminals may already know about your organisation.

Equip your security and incident response teams with actionable intelligence, identify unprotected assets, unpatched systems and brand misuse discussed in darknet communities, and receive concise executive reporting to support informed risk, investment and remediation decisions.

- **Visibility of hidden risks**
- **Faster, more informed response**
- **Reduced exposure to emerging threats**
- **Evidence based executive reporting**

Ideal for organisations seeking rapid visibility of cyber exposure without the commitment of continuous monitoring.

How we identify risks across the darknet

Targeted Darknet intelligence search

A curated scan of darknet forums, marketplaces, leak sites and closed communities for mentions of your organisation.

Credential leak identification

Detection of exposed employee usernames, passwords and authentication artefacts circulating on underground platforms.

Sensitive data exposure analysis

Assessment of whether corporate documents, IP, internal systems or customer data appear in threat actor channels.

Brand and asset discovery

Identification of references to your brand, domains, shadow IT assets or infrastructure vulnerabilities.

Contextual risk prioritisation

Findings are ranked based on relevance, threat level and business impact - no noise, just actionable intelligence.

Integration with security operations

Insights can be fed into SOC workflows, incident response or vulnerability management to enable rapid remediation.

Why work with us?

Gain rapid intelligence on your exposure without the longer-term commitment of continuous monitoring.

Analysts validate and enrich automated findings, ensuring accuracy and eliminating false positives.

An objective, third party view of your darknet risk posture to support internal decision making and compliance.

Know what's exposed. Know what to do next - Contact us today

Visit our website