Take control of your digital footprint

Our Digital Risk Protection (DRP) solution protects against external threats and continually identifies where your assets are exposed whilst providing sufficient context to understand the risk and options for remediation.

Unwanted exposure leads to digital risks
Every organisation is becoming more interconnected with their supply chain, customers and partners. As a result the data they seek to protect increasingly becomes exposed. This exposure presents more opportunities to adversaries, who understand how to leverage and manipulate an organisation’s digital footprint. Adversaries make use of breached employee credentials to perform account takeovers, imitate your brand to target employees and customers as well as exploit vulnerabilities in your expanding attack surface.

The need for digital risk protection
Unmanaged, an organisation’s exposure to cyber-attacks can lead to regulatory fines, damaged reputation, loss of intellectual property and reduces your competitive advantage. Security leaders rely on their teams to protect against these risks, but their limited visibility outside their perimeter means they fall short of communicating the full risk landscape to the business. Digital Risk Protection reduces risks that emerge from digital transformation, protecting against the unwanted exposure of an organisation’s data, brand and attack surface as well as providing actionable insights on threats from the open, deep, and dark web.

A managed service enables you to minimise your digital risk by detecting data loss, securing your online brand and reducing your attack surface. Unrivalled coverage, expertise and relevance makes our DRP Solution the leading solution. A powerful, easy-to-use search engine that combines structured technical data with content from the open, deep, and dark web. The powerful syntax and configurable alerts enable you to quickly investigate security incidents and identify adversaries targeting your business and brand.
## Service description

### Detailed description

- The Digital Risk Protection service reduces risks that emerge from digital transformation, protecting against the unwanted exposure of a company's data, brand and attack surface as well as providing actionable insights on threats from the open, deep, and dark web.

### Opening hours

- Alert Delivery Systems: 24/7
- Reporting, Support, Training: Business hours

### Service level agreements

- Agreed delivery time for the automated alert report

### Operational follow-up

- Kick-off meeting with customer for pre-requisites
- Automated Alerts Delivery (platform, email, API)
- Periodic meetings for strategic orientations decisions

### Deliverables

- Alert Platform Access
  - Customer Onboarding: Portal creation, User management, Asset data collection, Customer training
  - Alert Delivery
    - Unlimited assets, unlimited users, unlimited API Keys
    - All system use cases locating client specific risks:
      - Data Loss Detection: Employee Credentials, Sensitive Marked Documents, Customer Data, Technical Data Loss
      - Online Brand Security: Impersonating Domains, Mobile App Risks, Spoof Social Media Profiles
    - Alert Triage
    - Regular Reports (Native or custom service activity reports)
    - Support (First Line & Product)
    - Ongoing Training
  - RFI Reports (Request For Information)
  - Managed Takedowns: Cover takedowns of domains, social media profiles, documents and mobile applications.

### Pricing

- Alert Delivery: Packaged price per company employee account and service level
- Alert Triage: Initial risk assessment of alerts
- RFI Reports: Upon request (RFI rate card available)
- Managed Takedowns: Packaged price per period and account takedown