

# ScanX DARK WEB MONITORING



## PRODUCT OVERVIEW

ScanX Dark Web Monitoring platform by Velox Solution is an enterprise-grade intelligence platform designed to continuously monitor the open, deep, and dark web for cyber threats, data exposure, identity compromise, brand abuse, ransomware activity, and underground marketplace transactions linked to an organization and its ecosystem.

The solution combines large-scale underground data collection, identity-centric analytics, brand protection intelligence, contextual enrichment, risk scoring, and automated response integration to deliver actionable, high-confidence alerts. Velox enables early detection of compromised credentials, exposed customer data, impersonation campaigns, phishing infrastructure, third-party leaks, and extortion listings — empowering organizations to initiate immediate containment, remediation, and legal action where required.

Built for enterprise, government, BFSI, telecom, and regulated environments, Velox Dark Web Monitoring strengthens proactive cyber defense, digital risk management, and reputational protection.

## WHY CHOOSE US

### 1. COMPREHENSIVE THREAT & EXPOSURE VISIBILITY

Monitors underground forums, marketplaces, encrypted channels, paste sites, ransomware leak portals, and threat actor communities for complete intelligence coverage.

### 2. BRAND & IDENTITY PROTECTION INTELLIGENCE

Detects brand impersonation, typo squatting, phishing domains, counterfeit listings, and identity theft risks affecting employees and customers.

### 3. ACTIONABLE & PRIORITIZED INTELLIGENCE

Applies advanced analytics, contextual enrichment, and risk-based scoring to eliminate noise and focus on high-impact exposures.

### 4. ENTERPRISE-INTEGRATED & AUTOMATED

Seamlessly integrates with SIEM, SOAR, TIP, and ITSM platforms to accelerate remediation workflows.



# ARCHITECTURE OVERVIEW



## COLLECTION LAYER

Distributed crawlers and sensors gather intelligence from surface, deep, and dark web environments, including restricted and ephemeral sources.



## NORMALIZATION & ENRICHMENT LAYER

Applies language translation, entity extraction, link analysis, and contextual tagging aligned with organizational assets and identities.



## ANALYTICS & RISK SCORING ENGINE

Implements machine learning-driven prioritization, actor credibility assessment, and impact-based classification.



## INTEGRATION & AUTOMATION LAYER

Delivers enriched alerts and structured intelligence feeds to SOC platforms for automated containment and response.



## ANALYST & GOVERNANCE LAYER

Supports investigation workflows, evidence documentation, takedown coordination, and executive-level reporting.

# Core Features

1.

## UNDERGROUND INTELLIGENCE & DATA COLLECTION

- Continuous monitoring of open, deep, and dark web ecosystems including Tor/onion services
- Multilingual crawling with indexed historical archive and entity correlation
- Automated extraction of domains, emails, IPs, credentials, wallet IDs, and infrastructure indicators

2.

## BRAND MONITORING & DIGITAL RISK PROTECTION

- Detection of brand impersonation, domain spoofing, typo squatting, and phishing campaigns
- Monitoring of counterfeit product listings, fake applications, and social media impersonation
- Evidence capture with screenshot validation and coordinated takedown support

3.

## IDENTITY THEFT & CREDENTIAL EXPOSURE MONITORING

- Detection of leaked employee and customer credentials, PII, financial data, and session artifacts
- Risk-based prioritization to identify high-value or newly exposed accounts
- Automated remediation triggers including password resets, account lockouts, and access reviews

4.

## RANSOMWARE & EXTORTION INTELLIGENCE

- Monitoring of ransomware leak sites, negotiation portals, and affiliate listings
- Early identification of organization mentions in extortion campaigns
- Collection of forensic-grade evidence to support response, negotiation, and legal escalation

5.

## SUPPLY CHAIN & THIRD-PARTY RISK MONITORING

- Monitoring of vendor and partner exposure across underground channels
- Detection of supply-chain data leaks and third-party compromise indicators
- Visibility to support contractual remediation, compliance, and regulatory reporting

6.

## INTEGRATION, REPORTING & CASE MANAGEMENT

- Delivery of structured IOC feeds via STIX, TAXII, JSON, and API integrations
- Centralized web console with dashboards, search capabilities, and scheduled executive reports
- Exportable evidence packages with timestamps, metadata, and audit-ready documentation



# ADVANCED IDENTITY & DEEPPAKE THREAT MONITORING

- Identification of deepfake-based impersonation campaigns, synthetic identity abuse, and manipulated media targeting executives or brand assets
- Monitoring of underground marketplaces offering AI-driven fraud services and voice/video cloning capabilities
- Actionable alerts with forensic evidence to support rapid response and reputational risk mitigation



## CONTACT US!

**Velox Solutions Pvt. Ltd.**



[sales@velox.co.in](mailto:sales@velox.co.in)



[www.velox.co.in](http://www.velox.co.in) | [veloxworld.com](http://veloxworld.com)



+91 8828297182 | +91 9321943983



India | USA | UK | Dubai | South Africa | Singapore | Indonesia