![Resecurity logo] **Resecurity**

Risk™

Measure risks to control the enterprise security posture

Resecurity provides proactive alerts and comprehensive visibility of internal and external risks targeting the enterprise. Reduce potential blind spots and security gaps with Risk.™

Accurate

In-depth risk evaluation of the entire enterprise ecosystem.

Scalable

Works on a massive scale and can monitor digital footprints of any size.

Effective

Take proactive actions to improve your security strategy.

Key Features

In-depth risk evaluation of the entire enterprise

Early-waring security notifications

Automated daily security posture reports

Data is displayed on a convenient dashboard

Protective Software-as-a-Service (SaaS)

Scan for free trial

Resecurity

Comprehensive Digital Risk Monitoring

External

Identify threats coming from outside based on high-quality threat intelligence data aggregated from over 30K+ public and closed sources.

BENEFITS

- Massive repository of Dark Web data
- Add your own threat intelligence feeds
- Detailed information with additional context

RISK VECTORS

- Account Takeover
- Botnet Infections
- Business E-mail Compromise
- Cyberespionage
- Brand Reputation Abuse
- Dark Web Activity
- Domain Squatting
- Data Breaches
- Digital Certificates
- Exposed Network Services
- Network Compromise
- Insecure Infrastructure
- Intellectual Property Exposure
- Physical Threats
- Social Media
- Supply Chain Risks
- Targeted Attacks
- Vendor Security

Internal

Integrate available security solutions to actualize the risk score of your enterprise footprint. Driven by your data, powered by Context™.

BENEFITS

- Automated enrichment of security events
- Integration with SIEM and EPP/EDR solutions
- On-the-fly analysis on the highest speeds

RISK VECTORS

- Active Directory Account Compromises
- Backdoors
- Incorrect Network Segmentation
- Security Anomalies
- Lateral Movement
- Malicious Traffic
- Vulnerable Software
- Misconfiguration Errors
- Unpatched Services

Cloud

Round-the-clock security monitoring of your cloud workloads in AWS Amazon. Prevent data breach at early stage.

BENEFITS

- Massive repository of Dark Web data
- Add your own threat intelligence feeds
- Detailed information with additional context

RISK VECTORS

- Abandoned EC2 instances running dangerous services
- Databases facing the internet with sensitive data and weak credentials
- Compromised Credentials
- Sensitive Data Identification
- Misconfigured services
- Malicious code
- Public S3 buckets containing sensitive data