Seqrite
Digital Risk Protection Services (DRPS)

Overview

Seqrite DRPS provides 24×7 monitoring of digital threats across the surface, deep, and dark web. It continuously detects and analyses risks to protect your brand, customers, and digital footprint.

In an era where digital presence defines brand trust, threats no longer stay within the firewall.

Fake domains, data leaks, impersonation pages, and dark-web activity can cripple your reputation before you even know it.

Seqrite Digital Risk Protection Services (DRPS) is a SaaS platform that gives enterprises real-time visibility and control over external cyber risks.

Key Challenges Addressed

Brand Impersonation and Fraud

Fake domains, social media profiles, or mobile apps deceiving customers.

Data Exposure and Leaks

Compromised credentials and confidential data traded on the dark web.

Supply-Chain Vulnerabilities

Risks emerging from partner or vendor ecosystems.

Intellectual Property Theft

Unauthorised access to proprietary assets and algorithms.

Online Counterfeiting

Fake listings and counterfeit products are damaging brand equity.

Infrastructure Threats

Targeted DDoS, ransomware, or API exploits impacting business continuity.

Key Features

Surface, Deep and Dark Web Monitoring
Monitors the surface, deep, and dark web to identify any mentions, threats, or leaked data linked to your organisation.

Social Media Surveillance
Detects impersonation, misinformation, brand misuse, and threat signals across social platforms.

Sentiment Analysis
Analyses online conversations to identify negative sentiment, emerging risks, and reputation issues.

IT Infrastructure Monitoring
Continuously tracks your external-facing digital assets to identify weaknesses before attackers do.

Third Party Risk Management
Assesses and monitors risks originating from vendors, partners, and external entities.

Real-Time Alert Dashboard
Provides instant threat notifications categorised by severity for faster decision-making.

Domain and Brand Protection
Tracks and secures domain activity to prevent brand abuse, spoofing, and identity misuse.

Data Leak Detection
Identifies exposed credentials, sensitive information, or breaches across public and covert sources.

VIP Monitoring
Protects high-profile executives from impersonation, targeted attacks, and digital harassment.

Takedown Services
Swiftly initiate for bringing down impersonation domains, fake profiles, phishing pages, or harmful content targeting your organisation.

Compliance-Ready Reporting
Delivers structured, audit-friendly reports aligned with regulatory and compliance frameworks.
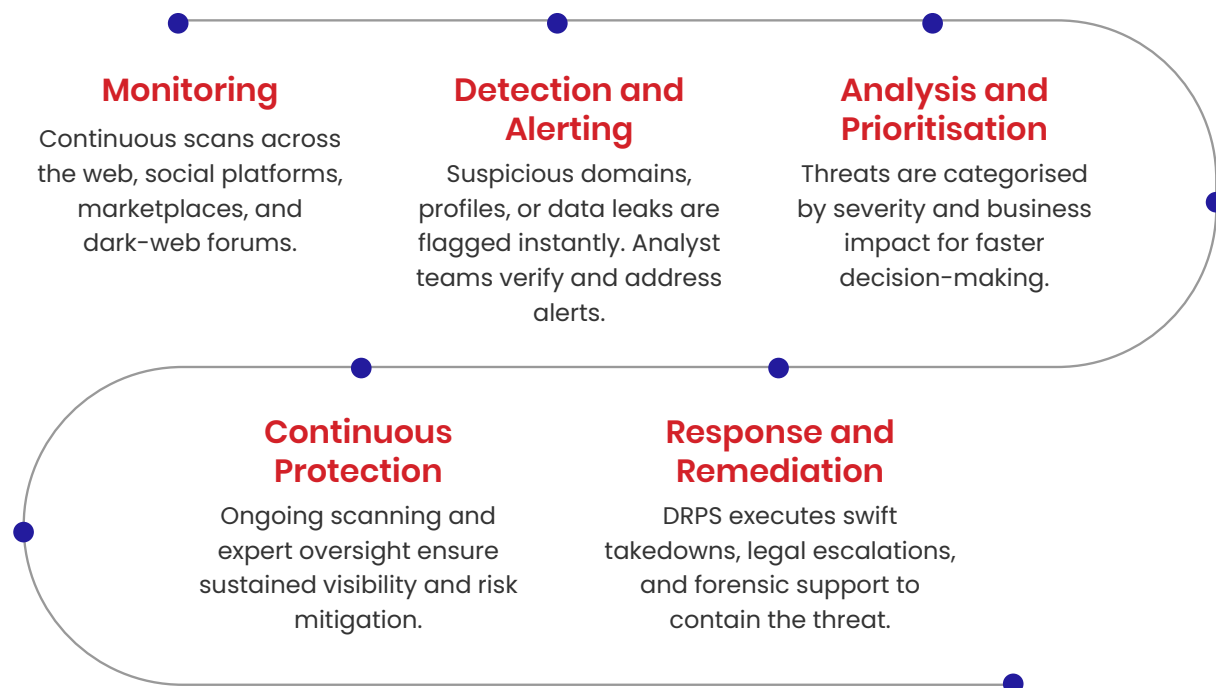
DRPS War Room with Cyber, Legal & Digital Experts
Offers expert-led investigation, interpretation, and coordinated response for complex digital threats.

How DRPS Works

Monitoring
Continuous scans across the web, social platforms, marketplaces, and dark-web forums.

Detection and Alerting
Suspicious domains, profiles, or data leaks are flagged instantly. Analyst teams verify and address alerts.

Analysis and Prioritisation
Threats are categorised by severity and business impact for faster decision-making.

Continuous Protection
Ongoing scanning and expert oversight ensure sustained visibility and risk mitigation.

Response and Remediation
DRPS executes swift takedowns, legal escalations, and forensic support to contain the threat.

Business Benefits

360° Digital Visibility
Get comprehensive coverage across all online channels — web, dark web, social, and mobile — with real-time risk alerts.

Enhanced Cyber Resilience
Predictive detection and continuous monitoring prevent external breaches before they occur.

Comprehensive Brand Protection
Protect trademarks, creative assets, and IP from impersonation and counterfeiting.

Rapid Incident Response
Seqrite's War Room Team ensures swift containment, takedown, and crisis management for brand or data incidents.

Why Choose Seqrite DRPS

Backed by Seqrite's proven cybersecurity expertise.

Human intelligence and legal actionability in one platform.

Scalable, SaaS-based model suitable for both enterprises and mid-market organisations.

Ensures data sovereignty and regulatory compliance.

Technical Specifications

Category	Description
Deployment	SaaS (Cloud-based)
Coverage	Surface, Deep, and Dark Web
Alert Levels	Low / Medium / High / Critical
Integration	REST APIs
Reporting	Automated, Compliance-Ready Reports
Support	8 x5 DRPS War Room (Cyber, Legal, and Digital Analysts)
Data Locality	Regional Compliance (DPDP Act)

About Seqrite

Seqrite is a leading enterprise cybersecurity solutions provider. With a focus on simplifying cybersecurity, Seqrite delivers comprehensive solutions and services through our patented, AI/ML-powered tech stack to protect businesses against the latest threats by securing devices, applications, networks, cloud, data, and identity. Seqrite is the Enterprise arm of the global cybersecurity brand, Quick Heal Technologies Limited, the only listed cybersecurity products and solutions company in India.

Today, 30,000+ enterprises in more than 70+ countries trust Seqrite with their cybersecurity needs.

SEQRITE

Quick Heal Technologies Limited
Phone: 1800-212-7377 | info@seqrite.com | www.seqrite.com | in X f /seqrite