

Seqrite

Servizi di protezione dal rischio digitale (DRPS)

SECURITE





Panoramica

Seqrite DRPS offre monitoraggio 24x7 delle minacce digitali attraverso la superficie, il deep web e il dark web. Rileva e analizza continuamente i rischi per proteggere il tuo marchio, i clienti e l'impronta digitale.

In un'epoca in cui la presenza digitale definisce la fiducia nel marchio, le minacce non restano più all'interno del firewall.

Domini falsi, fuga di dati, pagine di impersonificazione e attività nel dark web possono compromettere la tua reputazione prima ancora che te ne accorga.

Seqrite Digital Risk Protection Services (DRPS) è una piattaforma SaaS che offre alle aziende visibilità e controllo in tempo reale sui rischi informatici esterni.



Principali sfide affrontate



Marchio Impersonificazione e frode

Domini falsi, profili sui social media o mobili app ingannevoli clienti.



Esposizione dei dati e fughe

Credenziali compromesse e dati riservati scambiate sul dark web.



Vulnerabilità della catena di fornitura

Rischi emergenti dagli ecosistemi di partner o fornitori.



Furto di proprietà intellettuale

Accesso non autorizzato a beni e algoritmi proprietari.



Contraffazione online

Gli annunci falsi e i prodotti contraffatti danneggiano il marchio equità.



Minacce infrastrutturali

DDoS mirati, ransomware o exploit API che influenzano la continuità aziendale.





Caratteristiche



Monitoraggio della superficie, profondo e dark web

Monitora la superficie, il deep e il dark web per identificare menzioni, minacce o dati trapelati legati alla tua organizzazione.



Sorveglianza sui social media

Rileva impersonificazione, disinformazione, uso improprio del marchio e segnali di minaccia sulle piattaforme social.



Analisi del sentiment

Analizza le conversazioni online per identificare sentiment negativo, rischi emergenti e problemi di reputazione.



Monitoraggio dell'infrastruttura IT

Monitora costantemente i tuoi asset digitali esposti all'esterno per identificare debolezze prima che lo facciano gli attaccanti.



Gestione del rischio di terze parti

Valuta e monitora i rischi provenienti da fornitori, partner ed esterni entità.



Cruscotto di avvisi in tempo reale

Fornisce notifiche di minaccia istantanee classificate per gravità per decisioni più rapide.



Protezione del dominio e del marchio

Monitora e mette in sicurezza l'attività del dominio per prevenire abusi del marchio, spoofing e uso improprio dell'identità.



Rilevamento delle perdite di dati

Identifica credenziali esposte, informazioni sensibili o violazioni su fonti pubbliche e fonti occulte.



Monitoraggio VIP

Protegge dirigenti di alto profilo dall'impersonificazione, attacchi mirati e molestie digitali.



Servizi di rimozione

Avvia rapidamente l'azione per eliminare domini di impersonificazione, profili falsi, pagine di phishing o contenuti dannosi mirati alla tua organizzazione.



Reporting conforme alle normative

Fornisce rapporti strutturati e audit-friendly allineati a normative e conformità quadri di riferimento.



Sala operativa DRPS con esperti di cybersicurezza, giuridici e digitali

Offre indagine, interpretazione e risposta coordinata guidate da esperti per minacce digitali complesse.





Come funziona DRPS

DRPS

Monitoraggio

Scansioni continue sul Web, sui social, sui marketplace, e forum del dark web.

Rilevazione e Allerta

domini sospetti, profili o fughe di dati vengono segnalati immediatamente. I team di analisti verificano e intervengono avvisi.

Analisi e Prioritizzazione

Le minacce sono classificate per gravità e impatto sull'azienda per una decisione più rapida.

Protezione continua

Scansioni in corso e supervisione esperta garantiscono visibilità continua e rischio

mitigazione.

Risposta e rimedio

DRPS esegue rapidamente takedown, escalation legali e supporto forense a

contenere la minaccia.



Benefici aziendali

✔ Visibilità digitale a 360°

Ottieni copertura completa su tutti i canali online — web, dark web, social e mobile — con avvisi di rischio in tempo reale.

✔ Resilienza cibernetica migliorata

Rilevamento predittivo e monitoraggio continuo prevengono intrusioni esterne prima che si verifichino.

✔ Protezione completa del marchio

Proteggi marchi, asset creativi e IP dall'impersonificazione e dalla contraffazione.

✔ Risposta rapida agli incidenti

Il team War Room di Seqrite assicura contenimento rapido, rimozione e gestione della crisi per incidenti di marchio o dati.



Perché scegliere Seqrite DRPS



Supportato dall'esperienza comprovata di Seqrite in cybersecurity.



Intelligenza umana e applicabilità legale in un'unica piattaforma.



Modello scalabile basato su SaaS adatto sia a grandi aziende che a imprese di medie dimensioni.



Garantisce la sovranità dei dati e la conformità normativa.

Specifiche Tecniche

Categoria	Descrizione
Distribuzione	SaaS (basato su cloud)
Copertura	Superficie, Deep Web e Dark Web
Livelli di Avviso	Basso / Medio / Alto / Critico
Integrazione	API REST
Reporting	Rapporti automatizzati e pronti alla conformità
Supporto	Sala di Guerra DRPS 8 x 5 (Analisti Cyber, Legali e Digitali)
Località dei Dati	Conformità regionale (Legge DPDP)



Informazioni su Seqrite

Seqrite è un importante fornitore di soluzioni di cybersecurity per aziende. Con un focus sulla semplificazione della cybersecurity, Seqrite offre soluzioni e servizi completi tramite il nostro stack tecnologico brevettato alimentato da IA/ML per proteggere le aziende dalle minacce più recenti, mettendo in sicurezza dispositivi, applicazioni, reti, cloud, dati e identità. Seqrite è la branca Enterprise del marchio globale di cybersecurity, Quick Heal Technologies Limited, l'unica azienda quotata di prodotti e soluzioni cybersecurity in India.

Oggi, oltre 30.000 aziende in più di 70 paesi si affidano a Seqrite per le loro esigenze di cybersecurity.

SEQRITE

Distribuito da s-mart.biz

Telefono: +39 055 43 03 52 | cs@s-mart.biz | www.seqrite.it |

 /Seqrite Italia