ANOMALI

Data Sheet

ANOMALI PREMIUM DIGITAL RISK PROTECTION

Defend Your Brand. Protect Your People.

Anomali Premium Digital Risk Protection (PDRP) delivers continuous brand protection intelligence by monitoring the open, deep, and dark web for threats targeting your organization's brands, executives, domains, and employees — and surfaces those alerts directly inside Anomali ThreatStream Next-Gen.

Unlike generic threat feeds that tell you about attackers in general, Anomali PDRP tells you when someone is targeting you. It tracks lookalike domains impersonating your brand, fake social accounts pretending to be your company, leaked credentials for your staff, rogue apps masquerading as yours, and unauthorized use of your logo and visual brand identity.

The Anomali PDRP Intelligence Channel provides a real-time, global feed of customer-specific alerts relating to five threat categories: Brand Protection, Social Media Impersonation, Mobile App Monitoring, Credential Exposure, and VIP/ Executive Monitoring.

The intelligence derives from continuous monitoring of five major app stores, seven social media platforms, underground forums, paste sites, breach dumps, and infostealer/ malware logs. This ensures you can efficiently manage threats specific to your organization based on reliable tagging, risk scoring, and enriched context.

KEY BUSINESS VALUE

- Increased visibility and early warning of brand-targeted threats
- Reduced exposure to phishing campaigns and credential theft
- Increased productivity and reduced burnout of Threat Intelligence and SOC teams
- Increased SIEM/SOAR ROI
- Streamline CTI team workflows
- Value pricing extends capabilities of CTI and SOC teams

KEY PDRP INTELLIGENCE CHANNEL BENEFITS

Anomali PDRP is built around a unified set of capabilities that cut the tool sprawl and alert noise of standalone digital risk products, with every finding scoped to your brands, people, and infrastructure:

- Customer-specific monitoring scoped to your assets, brands, domains, and executives
- One pane of glass — no second portal to monitor or manage
- Monitors five threat categories plus Managed Takedowns
- VIP/executive-scoped dark web and underground forum coverage
- Broad social media coverage across seven platforms
- Mobile app monitoring across five major app stores (Google Play, Apple App Store, Huawei App Gallery, Samsung Galaxy Store, Xiaomi Store)
- Rich context with embedded screenshots — analysts see exactly what they're dealing with
- Extensive tagging and risk scoring for efficient triage and downstream routing
- Unified Threat Model reporting natively inside ThreatStream Next-Gen
- Dedicated PDRP dashboard for real-time risk posture visibility
- Self-service asset configuration — no support ticket required

KEY USE CASES

Anomali PDRP is built to support the full range of CTI and SOC workflows, from automated dissemination to hands-on investigation:

CTI/SOC AUTOMATION

Extensive tagging and scoring provide an easy way to collect and disseminate customer-scoped intelligence downstream.

THREAT HUNTING

Customer-specific intelligence on brand impersonation, compromised credentials, and executive exposure.

TELEMETRY ENRICHMENT

Comprehensive tagging, WHOIS data, device forensics, and classification scoring.

INCIDENT RESPONSE

Rich threat context including similarity scoring, malware classification, and embedded evidence.

BRAND PROTECTION

Identify and remediate lookalike domains, fake social accounts, and rogue mobile apps before they damage brand reputation.

CREDENTIAL MONITORING

Detect compromised employee credentials from malware infections with device forensics and password strength analysis.

THREAT CATEGORY COVERAGE

Anomali PDRP monitors continuously across five threat categories and Managed Takedowns, each scoped to your specific assets and designed to surface findings before they become incidents:

CATEGORY	WHAT ANOMALI MONITORS	TYPICAL FINDING
Brand Protection	Lookalike & typosquat domains, impersonation phishing URLs, brand-abuse SSL certs, and logo / visual brand misuse	Newly-registered acmecorp-login.com before it goes live
Social Media Impersonation	Fake brand & executive accounts across X, LinkedIn, Facebook, Instagram, TikTok, Snapchat, YouTube	Fake customer-support account on X running refund scams
Mobile App Monitoring	Rogue & impersonating apps across 5 major app stores	Rogue Android APK impersonating your banking app
Credential Exposure	Brand-wide leaked credentials attributed to your domain, delivered via API — malware / infostealer logs, ULP & combolists, marketplaces	Employee credentials from an infostealer log tied to your domain
VIP / Executive Monitoring	Named-executive impersonation plus executive company-email credential leaks; tier-allocated VIP slots	Spoofed CEO profile on LinkedIn; leaked CFO credentials on a leak site
Managed Takedowns	Analyst-overseen removal on risk-classified alerts; tier-allocated volume	Malicious lookalike domain removed within SLA

ANOMALI PDRP THREAT REPORTS

Anomali PDRP findings are delivered as a fully formed Threat Reports, importing directly into ThreatStream Next-Gen as a Threat Model with associated observables. Reports are published continuously, with a 90-day backfill on activation so your team has immediate historical context from day one.

REPORTS INCLUDE:

- Customer-Scoped Threat Models: Each alert imports as a Threat Model with associated observables
- Rich Embedded Context: Screenshots, WHOIS/DNS/SSL analysis, device forensics, malware classification, similarity scoring
- Risk Scoring and Classification: Threat level indicators, confidence scores, password strength analysis, analyst recommendations
- Actionable Intelligence: Auto-created observables, consistent tagging taxonomy, ML classification scoring, and takedown eligibility flagging
- Published Continuously: Real-time ingestion with 90-day backfill on activation

SEE ANOMALI IN ACTION

Request a Demo