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, employees, and infrastructure — 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 vulnerabilities exposed on your infrastructure.

The Anomali PDRP Intelligence Channel provides a real-time, global feed of customer-specific alerts relating to six distinct threat categories: brand impersonation, compromised credentials, social media impersonation, rogue mobile apps, SSL certificate issues, and infrastructure vulnerabilities.

The intelligence derives from continuous monitoring of 40+ app stores, seven social media platforms, underground forums, paste sites, breach dumps, and global scanning infrastructure. 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
- Six distinct threat categories covering the full digital risk surface
- Dark web and underground forum coverage for early credential and campaign detection
- Broad social media coverage across 7 platforms
- Mobile app monitoring across 40+ app stores
- Rich context with embedded screenshots — analysts see exactly what they're dealing with
- CVE correlation and CVSS scoring on infrastructure vulnerability findings
- 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 infrastructure exposure.

TELEMETRY ENRICHMENT

Comprehensive tagging, WHOIS data, device forensics, and CVE correlation.

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.

COVERAGE: THE SIX THREAT CATEGORIES

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

CATEGORY	WHAT ANOMALI PDRP MONITORS	TYPICAL FINDING
Brand Protection	Lookalike domains, typosquatting, new SSL certificates issued for impersonation domains	Newly-registered yourcompanylogin.com before it goes live
Dark Web and Credentials	Underground forums, paste sites, breach dumps, malware-harvested credentials	Employee credentials from malware infection with device forensics
Social Media	Fake accounts on X, LinkedIn, Facebook, Instagram, TikTok, YouTube, Pinterest	Fake customer-support account on X running refund scams
Rogue Mobile Apps	Unauthorized apps on Google Play, Apple App Store, 40+ third-party stores	Rogue Android APK impersonating your banking app
SSL Certificates	Certificate expiration, security misconfigurations, self-signed certificates	Expired SSL cert on customer-facing domain with 30-day notice
Infrastructure	CVE-correlated vulnerabilities on exposed servers, domains, endpoints	Critical Apache vulnerability for specific (CVE-2026-XXXX) on public web server

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, CVE correlation
- Risk Scoring and Classification: Threat level indicators, confidence scores, password strength analysis, analyst recommendations
- Actionable Intelligence: Auto-created observables, consistent tagging taxonomy, CVEs with remediation guidance, takedown eligibility flagging
- Published Continuously: Real-time ingestion with 90-day backfill on activation

SEE ANOMALI IN ACTION

Request a Demo