ANOMALI

# Anomali Premium Digital Risk Protection

Defend your most critical brand and digital assets in real time

## Leverage customized tools and expertise to stop cyberthreats

Cybercriminals have become highly skilled at hijacking your brands, domains, or information to commit crimes and victimize your customers. Existing outside your infrastructure, threats like this can be easily missed—but can be just as harmful as malware or security breaches.

Anomali Premium Digital Risk Protection (PDRP) helps you identify and defend against targeted attacks with real-time visibility, actionable insights, and detailed prompts to guide your response. Continuously monitoring both the threats targeting your organization and your digital footprint, Anomali PDRP combines expert human analysis with AI and ML insights to help you understand which assets are most at risk, which threats pose the greatest danger, and how you can prevent an attack before it happens.

Going beyond phishing, Anomali PDRP also monitors for fake domains, social media accounts, or apps impersonating your brand, stolen PII or intellectual property, fraud or extortion campaigns, and other threats to your business and its reputation.

Anomali PDRP is individually implemented and expertly configured by Anomali professional services to meet your unique requirements. By leveraging the full value of threat intelligence, attack surface management, and AI-powered security analytics powered by the Anomali Security Operations Platform, you can safeguard your organization from all types of digital risks—before they impact your business.

## Stop attacks, leaks, and fraud

### Brand protection

Monitoring for cybersquatters, domain hijacking, and fake or compromised apps helps prevent phishing brand abuse to maintain customer trust

### Proactive defense

Web monitoring for stolen credentials and passwords helps prevent data breaches and exfiltration of data

### Actionable analytics

More than just another dashboard, PDRP delivers AI and ML-powered insights in real-time to help SecOps teams translate threat intelligence into action

### Customized deployment

Expert implementation and configuration by Anomali professional services is tailored to your unique requirements

## Get real-time SecOps intelligence, insight, and guidance

### Address digital threats quickly and effectively

Gain full visibility across your digital channels, attack surface, and external threat landscape. With an attacker's eye view of your most desirable assets, you can work quickly to harden weak spots in your digital footprint and proactively prevent attacks.

### Empower SecOps teams with actionable security analytic

Translate threat intelligence into action with real-time, AI and ML-powered insights. Anomali PDRP leverages Anomali ThreatStream, the world's largest threat repository, to correlate IOCs and IOAs with relevant telemetry across your environment.

### Stop data theft, leaks, and other breaches

Alert on leaked or stolen team member or customer PII, intellectual property, code, and other sensitive information while there's still time to prevent damage. Tracking for key phishing indicators like registered domains, MX record changes, and DNS reputation helps cut off attacks at their source. Continuous web monitoring for stolen credentials, passwords, and other data cybercriminals prevents unauthorized access to corporate systems.

### Stop potential brand abuse and fraud

Protect customers, employees, and your business reputation by uncovering fake or compromised domains, IP addresses, and apps that imposters can use for fraud schemes.

## Key capabilities

- Expert human analysis to understand which assets are most at risk
- AI and ML-powered insights in real-time to help teams translate threat intelligence into action
- Detailed threat alerts with recommendations for fast remediation
- Tracking for key phishing indicators like registered domains, MX record changes, and DNS reputation
- Continuous monitoring for:
  - Similar domain registration (phishing/brand abuse)
  - Fake social media accounts
  - Compromised IP addresses
  - Potential phishing URLs
  - Suspicious SSL certificate registration
  - Domain hijacking
  - Leaked credentials
  - Domain expiration
  - Exposed subdomains
  - Email vulnerability
  - Leaked or stolen sensitive documents
  - Leaked code on GitHub/Gitlab
  - Rogue apps
  - Pastebin brand mentions
  - Employee doxing incidents
  - Trademark application filing

## The Anomali Security Operations Platform

### Anomali ThreatStream

The world's largest threat repository, Anomali ThreatStream captures raw threat data in real time to power the LLM at the heart of the Anomali Security Operations Platform. IOCs and IOAs are immediately correlated with relevant telemetry to drive actionable insights.

### Anomali CoPilot

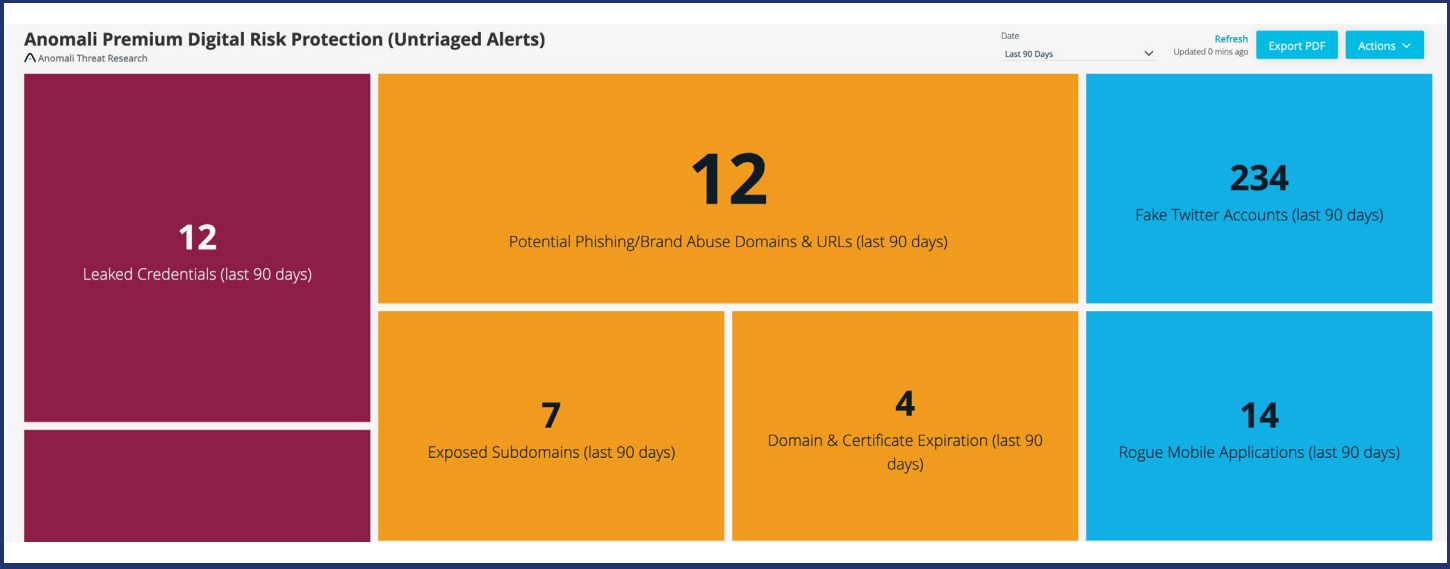
The integrated generative AI capabilities of CoPilot makes our Security Operations Platform the fastest and most comprehensive solution in the market. Based on an LLM using the industry's largest threat repository, CoPilot mitigates hallucinations for accurate, actionable insights in plain language.

### Anomali Security Analytics

Built in the cloud for massive scale and speed, Anomali Security Analytics consolidates SIEM, SOAR, UEBA, and TIP capabilities into a best-in-class, AI-driven solution at a fraction of the cost of competing offers.

### Anomali ASM

Anomali Attack Surface Management provides comprehensive visibility into all your IT assets, including shadow IT, to fuel actionable security analytics. Real-time monitoring flags outdated policies, misconfigured assets, and other at-risk entities.






ANOMALI