ANOMALI

Digital Risk Protection

Defend your most critical brand and digital assets in real time

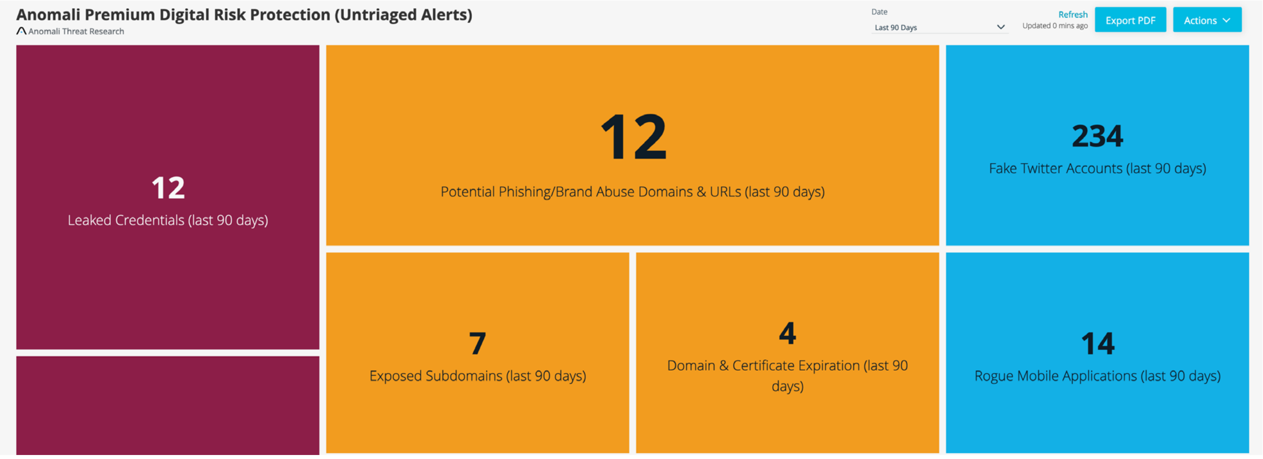
As cyberthreats accelerate, security teams have to move quickly from information to action. Many modern threats are based on fraudulent abuse of your brand and domains, or stolen or leaked information, using them to commit crime and harm you and your customers. Existing outside your infrastructure, threats like this can easily be easily missed—but they can be just as harmful as malware or security breaches.

Anomali Digital Risk Protection 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, Digital Risk Protection 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, Digital Risk Protection 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.

BENEFITS

- Defend against targeted attacks and brand abuse to maintain customer trust
- Monitor for cybersquatters and domain hijacking to prevent phishing and malware
- Prevent sensitive data leaks before they happen
- Get detailed threats alerts with recommendations for fast remediation
- Detect attacker infrastructure before it is operationalized
- Disrupt an attacker's ability to create an outbound channel
- Prevent harvesting and exfiltration of data


Anomali Premium Digital Risk Protection (Untriaged Alerts)

Anomali Threat Research

Date: Last 90 Days

Updated 0 mins ago

12 Leaked Credentials (last 90 days)

12 Potential Phishing/Brand Abuse Domains & URLs (last 90 days)

234 Fake Twitter Accounts (last 90 days)

7 Exposed Subdomains (last 90 days)

4 Domain & Certificate Expiration (last 90 days)

14 Rogue Mobile Applications (last 90 days)

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

Get real-time threat intelligence with guidance to take action

Whether you're working proactively to stop threats or responding to a potential attack in progress, security teams need to know both what's at risk and what to do about it. Anomali Digital Risk Protection provides intelligence, insight, and guidance to power fast, effective security operations.

Counter risk across your organization's entire digital footprint

Digital Risk Protection helps teams operationalize targeted threat intelligence including:

- Similar domain registration (phishing/brand abuse)
- Potential phishing URLs
- Suspicious SSL certificate registration
- Domain hijacking
- Leaked credentials
- Domain expiration
- Exposed subdomains
- Email vulnerability
- Leaked sensitive documents
- Leaked code on GitHub/Gitlab
- Rogue apps
- Pastebin brand mentions
- Employee doxing incidents
- Trademark application filing

Address digital threats quickly and effectively

Digital Risk Protection increases visibility across your digital channels, your attack surface, and the external threat landscape for potential risks. With an attacker's-eye-view of your most desirable assets, you can work quickly to strengthen your security posture.

Empower SecOps teams with actionable security analytics

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

Key Use Cases

Harden your attack surface

Identify at-risk assets and weak spots in your digital footprint to proactively prevent attacks

Prevent phishing

Track key phishing indicators like registered domains, MX record changes, and DNS reputation to cut off phishing attacks at their source

Stop potential brand abuse and fraud

Uncover fake or compromised domains, IP addresses, and apps to identify imposters and fraud schemes

Detect compromised credentials

Monitor the web for stolen credentials, passwords, and other data cybercriminals could use to access corporate systems

Catch leaks

Alert on leaked or stolen employee pr customer PII, intellectual property, code, and other sensitive information

ANOMALI