Proofpoint Digital Risk Protection

Monitor and protect against risks outside of the network

Key Benefits

- Protect against social accounts and web domain impostors
- Monitor for threats targeting your brand, executives and locations
- Defend your brand-owned social accounts and followers from spam, phishing, malware, account takeover, and offensive content

Your digital presence is critical to providing a cohesive customer experience. Yet, it also exposes your company to digital risks. And they can be especially dangerous and hard to combat. That's because threat actors target people on infrastructure that sits outside of your corporate environment.

Whether or not you engage in a digital channel such as social media, threat actors can create fake accounts that appear to represent your brand. Even in the deep and dark web—where corporations have clearly opted-out, bad actors can defraud your brand or plan attacks on your key personnel and physical assets.

Proofpoint Digital Risk Protection helps you identify and respond to threats targeting your employees, customers, partners and brand on digital channels. Some of these channels include web domains, social media and the deep and dark web. And they can be used to impersonate, phish, compromise accounts, host malicious content and pose physical threats to key company personnel and locations. Digital Risk Protection scans for these threats and provides you with alerts, workflows and options for responding.

Domain Discover Managed Services

- Equips your staff with direct access to digital protection expertise
- Provides high-quality, expedited service
- Tailors your service based on your domain and business needs
- Maximizes efficiency and frees your IT resources

Discover and Protect Against Social Accounts and Web Domains Impersonating Your Brand

Attackers register many web domains and social media accounts to mimic legitimate businesses. They then defraud their employees, customers and partners. That's why monitoring and protecting your company's domain and social presence should be a key part of your security strategy.

Domain Discover

Using machine learning and artificial intelligence, we analyze a vast body of domain data around the clock. This helps us to uncover infringing domains that pose a risk to your employees, partners and customers.

With Digital Risk Protection, you can:

- Gain visibility of suspicious, dormant and your owned domains
- Detect domains that are part of active phishing campaigns or other attacks
- Identify the use of your logo or logos on infringing domains
- Receive immediate alerts when domains move to a weaponized state, from parked to live

Proofpoint uses a highly scalable detection system. And it is designed to continually analyze more than 400 million domains every day. With our quality of intelligence and coverage, you get accurate details on the domains that represent a security, trademark or other risk to your company and customers.

We also give you a detailed view of your domain presence with a prioritized risk level, so you can take immediate action. We alert you when your logo appears on websites hosted on infringing domains. This allows you to quickly find scammers and threat actors who attempt to mimic your brand.

According to Proofpoint research, nearly one-fourth of domains posing as corporate brands also have active Mail Exchange (MX) records. These domains are ready to launch email attacks on your unsuspecting customers and employees.

With our unrivaled data on domains' email activity, Proofpoint provides superior security against these potential phishing attacks. Proofpoint Targeted Attack Protection (TAP) finds fraudulent domains that are used in email attacks. This helps you discover security-risk emails sent to your employees and customers. You can then take action to stop them.

Virtual Takedown

Proofpoint Virtual Discover is an optional add-on to Domain Discover. It lets you submit malicious and criminal domains, including domains engaged in phishing, propagation of malicious content or those engaged in criminal activity. It also lets you add blocklists used by a wide array of ISPs, devices, web services and security products. Apps, services and infrastructure that subscribe to these blocklists can then render the domains inaccessible at the web, DNS and SMTP levels. As a result, users cannot access web content or receive email from blocklisted domains.

Social Discover

You must be able to discover and understand your social footprint if you want to preserve your brand's reputation. You might have many social accounts. And your account sprawl could pose a security risk. It can also ruin your cohesive and consistent brand image. Social Discover helps you control account sprawl. It scans social media outlets such as Twitter, Facebook, LinkedIn, Instagram and more to find impostor accounts affiliated with your brand or high-profile executives.

When it finds these imposters, you can act immediately to protect your brand, as well as:

- Search accounts by image to detect brand fraud misuse
- Persistently scan for fraudulent brand protest accounts
- Receive alerts for risky accounts that require takedown or legal review
- Send automated alerts to other stakeholders such as legal or HR when risk accounts are detected

Monitor for Threats to Your Brand, Executives and Locations

Social Patrol

Digital Risk Protection also helps you find potential threats to your brand, executives and locations within content on digital channels. It does so by scanning the far reaches of the digital world, spanning millions of web pages and social content items daily.

Also, our darknet data consists of a broad and constantly evolving database. The database includes more than 1 billion current and historical content items. It includes dark network data. It also includes high-risk content from deep and surface web sources.

We provide safe and scalable visibility into criminal content. This includes hacker forums, dark markets, anonymous messaging, anonymous file sharing, known leaks and breaches, and other known threat actors. All of this helps you get in front of threats, whether they are planned, imminent or occurring in real-time.

Brand Threat Monitoring

Brand Threat Monitoring provides monitoring for three different types of threats:

- **Cyber.** Monitor for threats that target an organization including attack and exploit activity, credential compromise, vulnerabilities, and confidential information leaks
- **Fraud.** Monitor for threats that defraud customers including credit card compromise, scams, phishing and hacked accounts for sale
- **Physical threats.** Monitor for public safety reports, gun threat reports, protest activity, physical violence and more

Executive threat monitoring

Executive threat monitoring provides monitoring, protection and defense for your digital channels. It helps against threats on social media (Twitter), Breach Database and darknet. Some of these threats include physical violence, protest, doxing, credential compromise and confidential information compromise. It also protects you from reputation compromise by looking for content that includes hate and profanity. When a threat like doxing or account compromise is made against your key executives, executive threat monitoring delivers instant notifications.

Location threat monitoring

Location threat monitoring provides monitoring on Twitter. It helps you protect and defend against threats such as protest language and physical violence. And it also monitors gun threat reports, public safety reports, general hazard reports and weapons images. It is based on geo-coordinates or explicit location name or address. When a threat is made against your locations, location threat monitoring delivers instant notifications.

Protect Your Social Accounts Against Hacks, Phishing and Malicious Content

Social Patrol also includes social account protection. It provides protection for your brand-owned social accounts from account takeovers, phishing attacks and other malicious content.

Social account protection

With social account protection, you can:

- **Automate content remediation.** Digital Risk Protection automatically remediates social media content at an unlimited scale. It scans posts and comments for high-risk content. And it finds malware, phishing, profanity, hate speech, pornography and more. Based on the content type, you get to decide whether to log, notify, hide or delete it. There's no other technology that can detect, classify and manage content more accurately.
- **Detect account takeovers and lock down compromised accounts.** Digital Risk Protection defends your brand accounts from takeover attempts. It continuously monitors for changes in your account profiles that can indicate a hack. It also looks for publishing patterns that indicate

Darknet Data Sources

- Anonymous dark networks, such as Tor, I2P and Zeronet
- Chat applications and protocols, such as Telegram and IRC
- Anonymous file share and dump sites, such as Mega
- Forums, such as Raidforums, Bitshacking and Free Hacks
- Carding sites, such as Carderbase, CrdClub and Chknet
- Dox sites, such as Doxbin and Ghostbin
- Dark markets, such as Silk Road 3.0 and Dream Market
- Paste sites such as Pastebin, 0paste and Dpaste
- Alternate DNS
- FTP and Torrent file servers

your account has been hijacked. And Proofpoint can automatically remove unsanctioned content, revert compromised accounts to a previously approved or "known good" state, or lock down the account if account tampering is detected.

- **Enforce publishing application policy**. Most enterprise organizations use centrally managed publishing applications to publish social content across their accounts. Unfortunately, they have no way to enforce the use of their approved application. And over time, many apps, including native web publishing, can be used to publish content. Each unapproved application represents a path. Bad actors may use it to compromise your social accounts. Proofpoint's App Policies enable you to enforce least privilege publishing app access controls. This reduces this risk and ensures consistent use of approved content publishing workflow.

Leverage the Proofpoint Nexus Threat Graph

The Proofpoint Nexus Threat Graph collects and correlates more than a trillion threat data points across email, cloud, network and social media. This provides unique visibility into the ever-changing threat landscape. And it also helps drive the effectiveness of Digital Risk Protection for best-of-breed detection and response.

LEARN MORE

For more information, visit **proofpoint.com**.