Proofpoint Digital Risk Managed Services

Monitor digital assets and protect brand reputation

Key Benefits

- Find instances of brand, impersonation, reputational or other dimensions of digital risk
- Provide your staff with direct access to Proofpoint analysts' expertise
- Minimize the risk posed by phishing sites, sites hosting malicious content, sites selling counterfeit goods and sites promoting criminal activity
- Leverage Proofpoint analysts to review, vet and escalate brand, impersonation and reputational risk identified across the social media and domain landscape
- Proofpoint analysts review, vet and escalate a curated set of highly relevant detections
- Free up your resources

Proofpoint Digital Risk Managed Services proactively monitor your organization's digital assets. They integrate with your organization to discover and mitigate fraudulent domains and social media accounts. They also protect you and your customers and prevent damage to brand reputation.

Domain Threat Analysis

Domain Threat Analysis is an add-on to Digital Risk Protection and Email Fraud Defense. With it, you can rely on expert Proofpoint analysts to monitor your organization's digital presence and eliminate the risk of domain fraud.

The add-on identifies:

- High-risk lookalike domains with email activity that may be part of a phishing or business email compromise (BEC) campaign that targets your employees, suppliers or customers
- Suspicious lookalike domains that are parked for potential weaponization
- Trademark-infringing domains that use your logo and might violate your trademarks and service marks
- Domains involved in litigation against your organization or that might defame your brand
- Brand-owned, shadow IT and other defensively registered domains to prevent typo-squatting and other attacks
- Domains involved in targeted attacks toward your employees, customers or business partners

How the process works

Proofpoint analysts set up searches using your brand's domains. They classify lookalike and other derivative domain names. They are classified according to the following risk categories:

Figure 1. How a virtual takedown works.

- **Corporate Review.** Domains named similar to domains owned by the customer that share some media, logos or other brand elements with the customer's domains. They are not deemed to be a risk. And they need customer review for legitimacy and to confirm ownership.
- **High Risk.** Domains named similar to domains owned by the customer that may use the customer's logos, colors, names or other brand elements to impersonate the customer's organization in malicious ways or have evidence of suspicious email or web activity.
- **Low Risk.** Domains named similar to domains owned by the customer that don't fall into other categories. They may use the customer's brand name or other lookalike elements. Such domains don't represent significant risk at the time of review. However, they may become high risk in time.

Virtual Takedown Service

Proofpoint Virtual Takedown is an optional add-on to Digital Risk Protection and Email Fraud Defense. It lets you submit malicious domains seamlessly. These domains include thise engaged in:

- Phishing
- Propagation of malware
- Counterfeit goods storefronts
- Criminal activity, including BEC attacks

It integrates with a wide array of:

- ISPs
- Devices
- Web services
- Security products

Apps, services and infrastructure that subscribe to these blocklists may render the domains inaccessible at the web, DNS or SMTP levels. When successful, the users can't access the web content or receive email from the blocked domain.

Virtual Takedown is an ideal pre-takedown measure. It allows fast mitigation of risks before you go through an expensive and time-consuming traditional takedown process.

Managed Social Fraud Classification

With the Managed Social Fraud Classification service, our analysts work with you continuously to identify and monitor risky social media accounts. We can use our own classification taxonomy or the customer's taxonomy to detect accounts that are fraudulent or impersonate the company's social media account. So, with this service, you don't have to use your resources.

How the process works

Our analysts classify and escalate discovered accounts according to the following risk categories:

- **High Risk.** Social media accounts that use the customer's logos, colors, names or other brand elements to impersonate the customer's organization in a malicious way.
- **Low Risk.** Social media accounts don't fall into any of the other categories, but use the customer's brand elements or accounts set up by fans. These accounts may become high risk over time.
- **Corporate Review.** Social media accounts that share some media, logos or other brand elements with the authorized customer accounts, but are not deemed to be a risk and require customer review for legitimacy.

Managed Social Fraud Takedown Reporting

Maintaining the reputation of your brand and high-profile employees' reputations is very important. You must discover and understand your social footprint to protect it. Not keeping track of your social presence may damage your brand image.

Managed Social Fraud Takedown Reporting helps you mitigate the risk of:

- Imposter accounts
- Fraudulent accounts
- Brand-damaging accounts

It facilitates takedown reporting for accounts violating terms of service. It works across platforms like:

- Twitter
- Facebook
- LinkedIn
- Instagram

How the process works

When Social Discover uncovers an offending account, customers can submit the most egregious for takedown. A Proofpoint analyst will then engage with the social network on the customer's behalf to pursue takedown of the account.

Social Discover for LinkedIn Profiles

Our analysts scan LinkedIn to find impostor user profiles affiliated with your organization. We continuously scan for any accounts that attempt to impersonate the key people within your organization. The tool also is used in auditing to identify rogue accounts.

Rogue accounts might include people who:

- Have left your organization, but still pose on LinkedIn as maintaining their affiliation
- Claim to hold regulated roles, such as a financial adviser
- Claim to have a role or job function that they do not have
- Impersonate high-profile people in your organization

How the process works

The customer provides a list of key people or job titles for Proofpoint to identify relevant LinkedIn profiles. Proofpoint curates a list of relevant LinkedIn profiles that have been identified as a rogue or impostor account.

Trusted Expertise

With Digital Risk Managed Services, your security operations center (SOC) staff and digital brand protection teams gain a trusted, expert partner. We help you safeguard your company's social media and domain investments. Our experts have design the most optimized social media and domain fraud monitoring services. Our team secures your brand and customers while providing high-quality service and industry-leading expertise. And we communicate our findings with regular service reports and meetings.

LEARN MORE

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