DATA SHEET

proofpoint.

PROOFPOINT DIGITAL RISK PROTECTION: WEB DOMAIN FRAUD MONITORING

PROTECT YOUR DOMAIN INVESTMENTS AND IDENTIFY LOOKALIKE DOMAINS

For every brand-owned domain on the internet, 20 suspicious lookalikes are potentially defrauding your customers.[1]

That's why monitoring your company's domain presence should be a key part of your digital security strategy. But legacy tools can leave your analysts and security teams overwhelmed. Manually sifting through results—and determining which ones are false positives—is tedious and time consuming.

KEY BENEFITS

- Gain visibility of suspicious domains, dormant domains and defensive domain registrations (lookalike domains registered by your organization to preempt spoofing attacks)
- Quickly detect domains that are part of active phishing campaigns
- Get real-time monitoring and alerts to ensure your brand-owned domain registrations and SSL certificates don't expire
- See when someone is misusing your corporate logo on infringing domains
- Receive instant alerts when spoofed brand domains move from parked to a live, weaponized state
- Automatically detect lookalike domains that use your brand to sell counterfeit goods

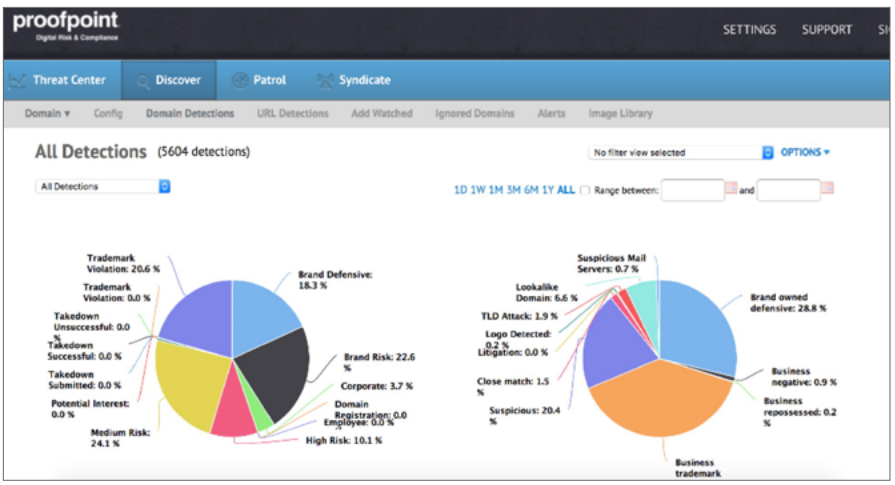
Proofpoint Digital Risk Protection identifies domain squatters and phishing campaigns and stops them from targeting your brand, customers and even your own employees.

Using machine learning and artificial intelligence, Digital Risk Protection analyzes a vast body of domain data to uncover domain fraud and infringing domains. At the same time, real-time alerts let you know when your domains and SSL certificates are expiring to help keep your brand-owned domains secure.

COMPREHENSIVE DOMAIN DISCOVERY

We use a highly scalable detection system that continually analyzes more than 350 million domains in the WHOIS registration directory. With high-quality intelligence and wide coverage, you get accurate details of any domains or subdomains that pose a security, trademark or other risk to your company and customers.

We also show you when your logo appears on websites that are hosted on infringing domains. This insight helps you quickly find scammers and cyber criminals impersonating your brand. Our automated domain discovery tool gives you a detailed view of your domain presence. It shows suspect domains by threat type and risk levels to help you prioritize your response.



DIGITAL RISK PROTECTION GIVES YOU THE INDUSTRY'S BEST THREAT INTELLIGENCE ON CROSS-CHANNEL ATTACKS

It starts with insights from our award-winning security solutions, including:

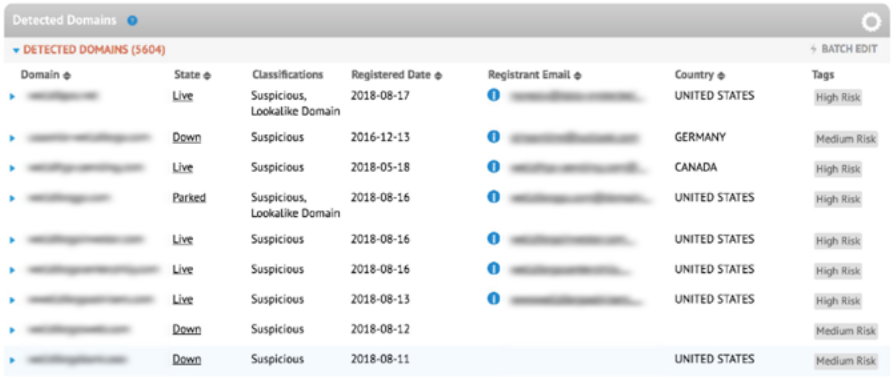
- Targeted Attack Protection for Email
- Email Fraud Defense
- Email Security and Protection

By connecting the dots between suspicious domains and active malware, phishing, email fraud and other attacks, Digital Risk Protection gives you a full picture how attackers are undermining your brand.

We'll alert you when a lookalike brand domain is sent as a malicious URL in email attacks. And we'll uncover fraudulent domains used in email fraud attacks. With Digital Risk Protection, you can even reveal fraudulent emails sent to your employees and customers.

DISCOVER DOMAINS QUEUED FOR PHISHING COMMUNICATIONS

Our research has found that nearly one-fourth of domains imitating corporate brands also have active MX records. In other words, these domains are ready to communicate with your unsuspecting customers and employees. Digital Risk Protection gives you deep visibility across digital channels. Armed with this insight, you can better protect against these potential phishing attacks.



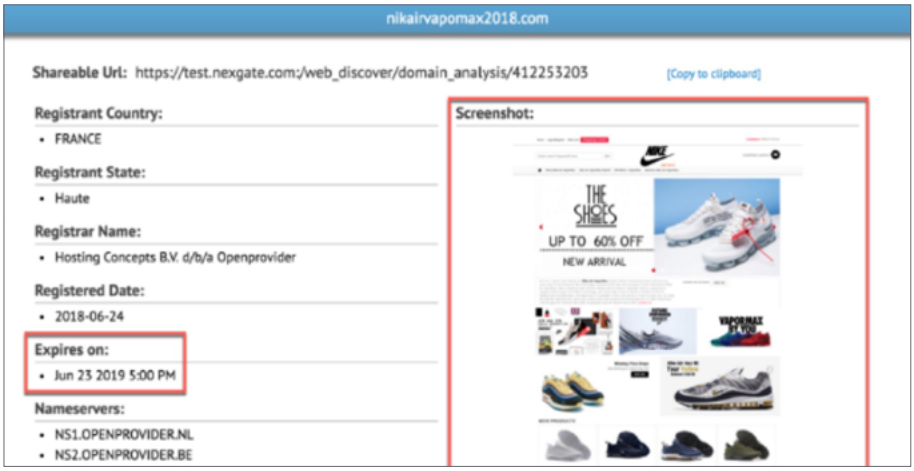
Our solution also monitors for infringing domains that are sending out email. When this is discovered, you'll receive an alert so you can act quickly to stop this harmful activity.

It also identifies security-risk domains that use Punycode. Punycode takes advantage of a quirk in the internet's domain naming system to create lookalike URLs. For example, Punycode for domain "xn--9naa4azkq66k5ba2d.com" is displayed as "BITCOIN.COM" in Unicode. Attackers use this technique to mask their phishing campaigns.

VISIBILITY TO QUICKLY ASSESS RISK

We protect against domain fraud with detailed visibility into domains that infringe on your brand. With automated tags categorized by risk level, you can quickly assess:

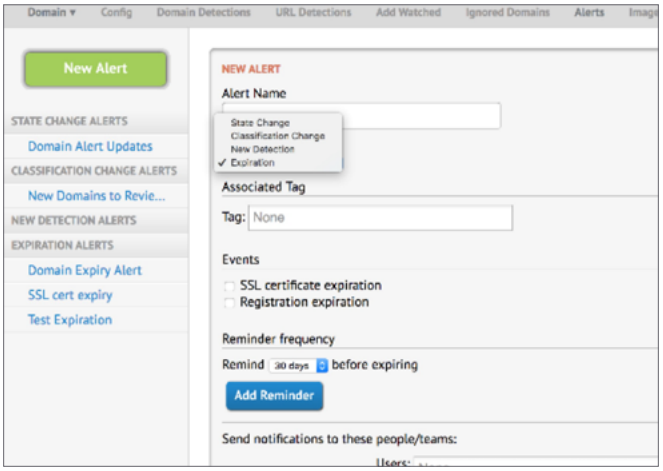
- Security risk domains that have MX records and are part of a phishing or cyber attack
- Suspicious domains that are parked for a potential future attack
- Trademark-infringing domains that use your logo and violate your brand trademarks, and lookalike domains that use your brand to sell counterfeit goods
- Brand-owned, defensively registered domains (used to prevent typosquatting and other tricks)



SAFEGUARD YOUR DOMAIN INVESTMENTS

Companies like yours often use many web domains. They're used for sub-brands, sales regions, operational departments, customer-engagement channels and more. These critical brand investments must be documented and monitored so that the domains and associated SSL certificates don't expire.

We monitor the expiration dates of your domains and SSL certificates and alert you when a date is nearing. With Digital Risk Protection, you can ensure that your web presence isn't interrupted or hindered by lapsed registrations.



BUILT-IN MITIGATION WORKFLOW

We make it easy for you to take down risky domains and URLs. Automated reports let you know about suspicious new domains that require enforcement. What's more, our integration with takedown providers and remediation workflow make it easy to track outcomes.

DOMAN FRAUD

Primary Use Cases	
Identifies legitimate and fraudulent domain assets associated with a brand	✓
Identifies brand-infringing web domains actively sending phishing emails	✓
Identifies trademark-infringing domains that use your logo and violate your brand trademarks	✓
Monitors for brand-infringing web domains selling counterfeit goods	✓
Ensures brand-owned domain registrations and SSL certificates do not expire	✓
Auto-detects high-risk domains and accelerates awareness for security teams	✓

OUR UNIQUE VALUE

With Digital Risk Protection, you get comprehensive protection from security, brand and compliance risks across domain, social media and mobile. We provide the most effective and complete protection for digital risk across all your engagement channels.

MORE INFORMATION

To learn more, visit proofpoint.com.

[1] Based on Proofpoint research.