Brand Protection Tools: Domain, Social & Dark Web | Fortra

Archived: 2026-04-26 02:10:14 UTC

When your brand is targeted, your defenses must be ready. Trusted by businesses worldwide, Fortra Brand Protection proactively detects and eliminates fraud and impersonation threats before they escalate.

With industry-leading detection and rapid takedown capabilities, security teams can confidently protect their brand, customers, and employees.

Businesses Around the World Trust Fortra Brand Protection

Why Brand Protection Is Business Protection

87%

Of customers switch when data trust is compromised

90+%

Of successful cyberattacks begin with a phishing attack

$11.5 Billion

Projected Gen AI–enabled email fraud losses by 2027

Prevent Fraud and Impersonation with Brand Protection Software

Text

Identify, monitor, and remove brand impersonation, phishing, and fraud across web, social media, mobile apps, and the dark web. Fortra brand protection tools continuously monitor and automate takedowns to stop threats from reaching your customers.

Brand Protection Tools

Safeguard your reputation and revenue with brand protection software that detects, monitors, and removes threats from web and social platforms.

Text

What Fortra Brand Protection Customers Are Saying on G2

“The platform provides extensive coverage across various digital channels, making it a robust solution for protecting against a wide range of threats. Strong threat intelligence capabilities help in detecting and mitigating phishing attacks and other digital risks.” *IT Security Professional*

“Constantly monitors the internet for any instances of brand infringement or imposter sites and apps. Will automatically initiate takedowns of any unapproved usages of your brand.” *VP of Information & Bank Security*

“Fortra Domain Monitoring is helping us address the critical issue of brand impersonation and domain-based threats. The platform is intuitive, the alerts are timely and actionable, and the support team is always responsive and knowledgeable.” *Financial Services User*

FAQs about Brand Protection Services

Online brand protection secures your digital identity, customers, and revenue against impersonation, fraud, counterfeiting, and phishing. It involves ongoing monitoring, expert analysis, and rapid takedown of malicious content. Brand protection services help detect and remove threats before they reach your customers.

Brand protection solutions safeguard your reputation, customers, and revenue in a rapidly evolving digital environment. They enable early detection of threats and prevent impersonation and fraud, reducing the risk of scams, lost sales, and customer distrust.

Brand protection software counters threats such as impersonation, phishing, account takeover, and lookalike domains. It detects fraud, data leaks, and brand abuse across social media, marketplaces, and the dark web, providing visibility into risks on all major digital channels.

Phishing poses a significant risk to brand security, as attackers use fake domains and impersonation to deceive customers. These campaigns often imitate trusted brands to steal credentials or payments. Brand protection tools detect phishing campaigns early and support rapid threat takedown to minimize impact.

Yes, lookalike domains present a significant risk in internet brand protection. Attackers use them to impersonate brands, mislead customers, and launch phishing attacks, often by using subtle misspellings or domain variations that seem legitimate.

A brand protection company detects impersonations and scams across social media, domains, and websites. They use tools that provide real-time monitoring, flag suspicious activity, and enable rapid removal of fake accounts, fraudulent listings, and malicious content. Automated detection is often combined with analyst review to prioritize high-risk threats and accelerate enforcement.

Brand protection solutions use several technologies to help organizations spot, stop, and respond to threats against their identity, assets, customers, and online presence. Instead of addressing just one risk, these solutions offer layered security for fraud, data, infrastructure, and intellectual property.

Key components include:

- **AI data security solutions** to identify sensitive data exposure, detect anomalous activity, and strengthen real-time monitoring across cloud and digital environments
- **Fraud detection software** to uncover suspicious behavior such as impersonation attempts, account takeover activity, and financial fraud across digital channels
- **IP protection tools** to safeguard intellectual property, including proprietary content, brand assets, and digital materials from misuse or theft
- **Ransomware protection** to detect, block, and contain malicious activity that could encrypt systems, disrupt operations, or impact brand trust

By working together, these brand protections help organizations lower their risk from new threats and keep control of their brand and digital environment.
