Solution Brief

BlueVoyant Digital Brand Protection

Secure your brand's digital assets with industry-leading proactive cyber threat detection and unlimited takedowns.

Traditional endpoint security solutions are capable of shutting down cyber attacks and mitigating the damage they can cause. But this is reactive defense – the hackers have already infiltrated your network, and your security team is left chasing them with limited visibility beyond the perimeter. The endpoint defense solution cannot detect threats as they emerge – phishing domains being registered on hosting providers, malicious apps popping up in app stores, social media impersonations of your brand, etc.

Security teams need a proactive cyber defense approach leveraging Digital Brand Protection to disrupt cyber attacks before they hit a company's perimeter.

BlueVoyant Digital Brand Protection uses a machine learning, data analytics, and human expertise combination to help security teams proactively expose websites, social media accounts, and applications impersonating your brand. BlueVoyant equips security teams with the tools they need to detect and validate cyber threats with minimal false positives, analyze threat data to pinpoint and adapt to emerging cybercriminal patterns, and ultimately shut down threats at the source.

With BlueVoyant Digital Brand Protection, your team can gain visibility into emerging threats, take down threats at the source before they even turn into full-fledged attacks, and anticipate future attacks using insights gleaned from threat data.

Key Differentiators

- Advanced phishing detection of malicious web domain registrations across hosting providers, app impersonations across 170-plus app stores, and brand impersonations on social media platforms.
- Unmatched, comprehensive data sources including DNS data sets, instant messaging channels, breach data, and exclusive cybercrime forums.
- Unlimited 24-hour phishing takedown capabilities leveraging exclusive partnerships with domain registrars.
- Automated alerts, threat prioritization, and continuous monitoring supported by our cyber threat analyst team.
- Fully automated product that can be deployed out of the box, backed by expert analysts assigned to each client.

Features

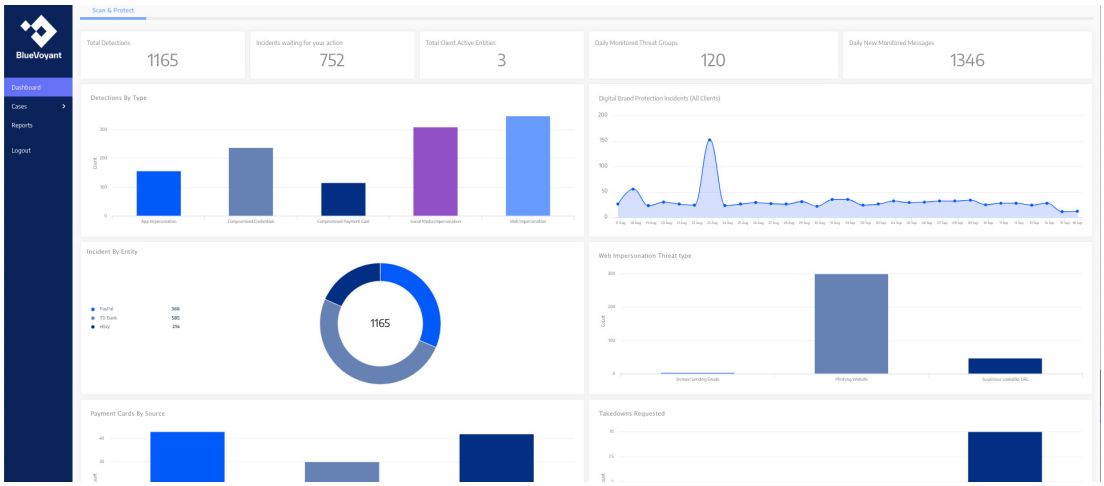
Domain Spoofing and Web Impersonation
Detection of phishing sites leveraging the brand's logos, imagery, messaging, and any other digital assets.

Social Media Impersonation
Identification of fraudulent social media profiles attempting to impersonate the brand or a high profile corporate executive.

Malicious Apps
Detection of malicious apps designed to lure unsuspecting users across 170-plus app stores.

Unlimited Takedowns
Maps to CIS Implementation Group 3 requirements to maximes protection against advanced threats. Designed for companies that secure sensitive information, have supply chains that will suffer significant impact from successful attacks on the company, and organizations that are likely to be subject to targetted attacks.

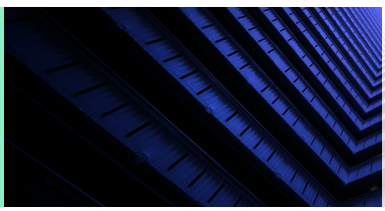
Continuous Monitoring
24×7 monitoring of the company's digital footprint and any emerging threats that use company brand assets without authorization.



Ready to get started?
Schedule a demo.

BlueVoyant combines internal and external cyber defense capabilities into an outcomes-based cloud-native platform by continuously monitoring your network, endpoints, attack surface, and supply chain, as well as the clear, deep, and dark web for threats. The full-spectrum cyber defense platform illuminates, validates, and quickly remediates threats to protect your enterprise. BlueVoyant leverages both machine-learning-driven automation and human-led expertise to deliver industry-leading cybersecurity to more than 900 clients across the globe.

BlueVoyant



To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**