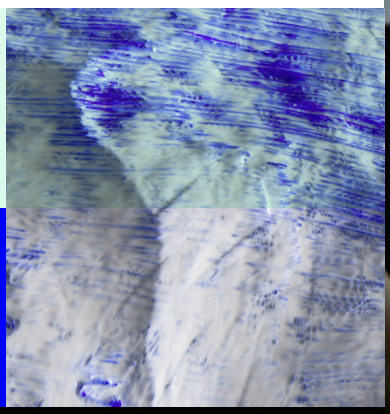
Spirity
TOMORROW:TODAY

eBook

Digital Brand Protection

Revolutionize Your Phishing Response with Proactive Threat Detection

BlueVoyant
Sky: DRP™



BlueVoyant

A Proactive Approach

A high-traffic website. Popular social media networks. A frequently downloaded mobile app. A thriving remote workforce. Communicative emails. These are all crucial elements for business success, but they're also easy targets for cybercriminals while fast becoming phishing hot spots.

This is challenging for today's enterprises because they must increase their digital presence to stay competitive. But as they do, threat actors are also increasing their use of web domains and social media channels to launch phishing and spoofing attacks against brands and their customers. And with plug-and-play phishing kits now sold on the dark web, scammers with little technical skills can launch unsavory campaigns, lowering the barriers of entry into cybercrime.

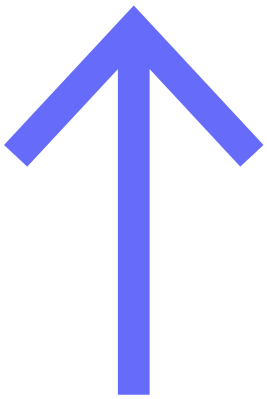
According to Verizon's 2021 Data Breach Investigations Report, 36% of all data breaches in 2021 involved phishing, an 11% increase from the year before.[1]

And make no mistake: Successful phishing and spoofing campaigns erode customer trust, brand reputation, and the bottom line. According to industry research, one out of every three consumers would hold a duped company responsible for getting personally phished – and then take their business elsewhere.

Though typical endpoint security solutions can limit the severity of phishing and spoofing attacks, this approach is reactive. Organizations can be much more proactive in detecting phishing and spoofing attacks, and stopping them, before they can happen.

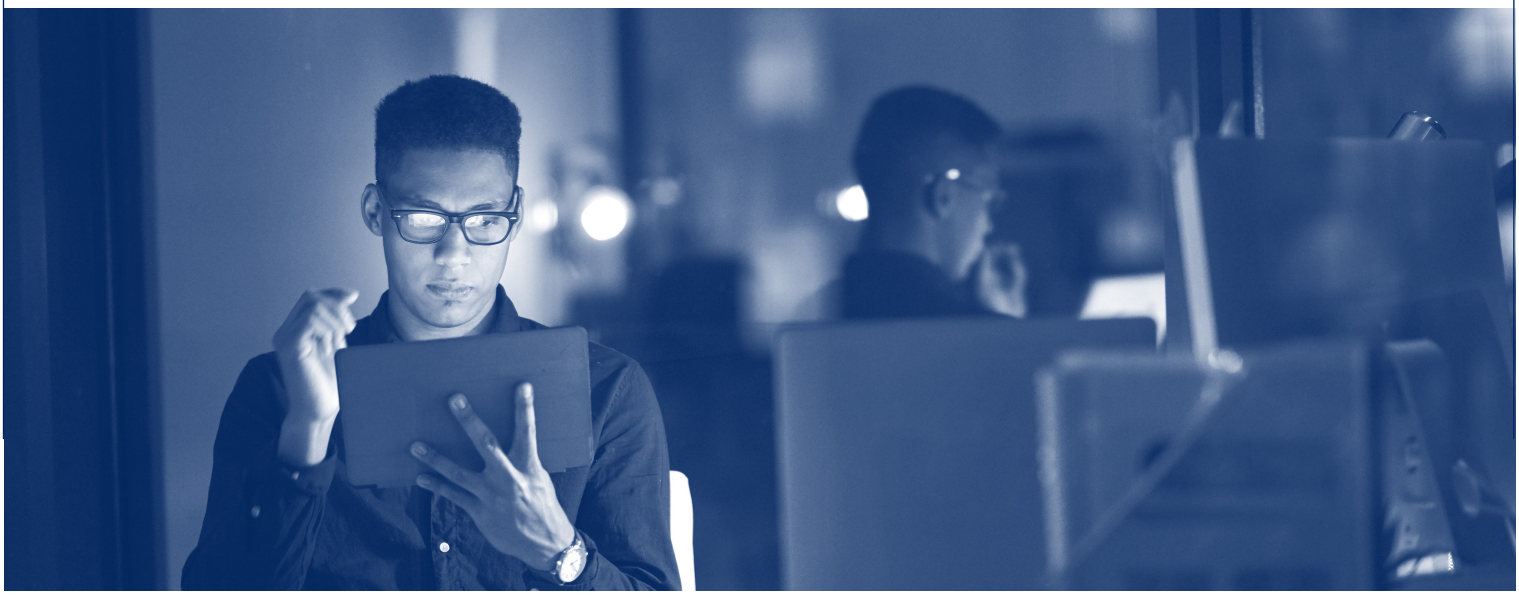
Key Takeaways

- Common cyber attacks used by today's threat actors
- The advantage of establishing a proactive approach to phishing and spoofing campaigns
- How security teams can discover if brand data is exposed to cyber attacks



36%

of all data breaches in 2021 involved phishing, an 11% increase from the year before.[1]



Cyber Attacks that Target Brand Assets

- **Phishing**
  This is the most common attack vector and, though well known, has become increasingly sophisticated. Cybercriminals are adept at tricking users into clicking malicious links and surrendering personal information. Phishing is no longer limited to emails; it now happens over social media channels, text messages, and malicious USB drops.
- **Spoofed domains, social media networks, and mobile apps**
  Hackers set up fake web domains, social media accounts, and mobile apps using company branding to lure customers into providing login credentials. Spoofing can compromise brand reputation and trigger successful fraud campaigns. Spoofs became more prevalent during the COVID-19 pandemic, with costs rising 85% year-over-year to $2 billion total losses between October 2020 and September 2021.[2]
- **Ransomware**
  Many phishing scams ultimately lead to ransomware threats. Users unwittingly download software containing viruses that allow hackers to gain control of networks and lock a company out of its systems until a ransom is paid. The FBI's 2020 Internet Crime Report showed there were 2,474 reports of ransomware in 2020 with adjusted losses of $29.1 million.[3]
- **Spear phishing**
  These are highly targeted phishing attacks that often use an executive's digital likeness to trick employees into clicking a malicious link or providing sensitive information. This can include spoofed email domains and social media accounts.

2,474 reports of ransomware in 2020 with adjusted losses of $29.1 million.[3]

Leaked data used by cybercriminals to levy attacks and take over accounts include:

- Confidential documents
- Personal health information
- Intellectual property
- Email addresses
- Usernames and passwords

Beyond the Perimeter

Staying ahead of cyber attacks and data leaks

Traditional endpoint security solutions are capable of stamping out.most phishing attacks as they breach your systems, but this is passive and reactive defense. These solutions don't offer insights for a security team to determine where an attack originated. They also don't provide visibility into whether an infiltration may be part of a larger, multi-tiered attack.

With reactive defenses, the financial and reputational damage is usually already done. Organizations will still be responsible for fines, repayment of fraudulent charges, and lost business from angry customers who closed their accounts after getting personally duped.

A proactive digital brand protection strategy disrupts cyber attacks before they hit a company's perimeter.

They are include two main parts:

1. **Continuous monitoring for phishing plots in the wild**
   While it's important to safeguard your internal systems, security teams need to see what threats are coming from outside the perimeter so they can be notified about phishing and spoofing attacks in advance.

   A digital brand protection solution provides this proactive, external eye. By continuously monitoring dark web forums or black markets for mentions of a company's name, for example, threat analysts can validate whether the threats are legitimate. If so, they can take action by immediately shutting down fake domains or spoofed social media sites.
2. **Finding leaked data and locking it down**
   Leaked data opens up a path to serious data breaches. If a hacker gets hold of admin credentials, they can wreak havoc on corporate security networks, leading to a full-blown ransomware or spear phishing attack on a CEO, for instance.

   A proactive approach to protecting digital brand assets also requires knowing what private employee and company information is exposed to threat actors on the dark web, paste sites and social media platforms.

   When security teams are alerted in advance about leaked digital assets, they can plug any holes attackers were hoping to exploit.

Protecting Your Brand

Using a combination of machine learning, data analytics, and human expertise, BlueVoyant helps security teams proactively expose websites, social media accounts, and applications impersonating your brand. This approach equips security teams with the tools they need to shut down threats at the source.

As part of the BlueVoyant Sky: Digital Risk Protection™ (DRP) solution, BlueVoyant's Digital Brand Protection helps your organization address the following:

Web Impersonation

BlueVoyant analyzes more than 100 million potential phishing domains daily by using data sources that include active and passive DNS records, domain registration data, and advanced web-crawling capabilities.

Social Media Impersonation

BlueVoyant identifies fraudulent social media accounts that mimic your brand and employees across Facebook, Twitter, Instagram, and LinkedIn.

App Impersonation

BlueVoyant actively detects third-party modifications of legitimate apps and rogue applications, both for mobile devices and desktop. This includes scanning Google Play, the Apple App Store, and more than 170 different unofficial app stores to uncover illegitimate applications.

Continuous Monitoring

BlueVoyant provides ongoing monitoring of suspicious domains and real-time alerts once phishing campaigns are live. With BlueVoyant's continuous monitoring, you'll be alerted of any active phishing campaigns and the recurring risk they pose to your organization.

Effective Takedown

BlueVoyant offers an unlimited takedown service that leverages our team of expert cyber threat analysts to take immediate action on your behalf. This ensures threats are removed quickly, reducing the time to remediation.

Data Leakage Detection

BlueVoyant provides detailed information about leaked digital assets, such as confidential documents and intellectual property. This includes the source in which the information was leaked, which helps security teams minimize the impact of attacks.

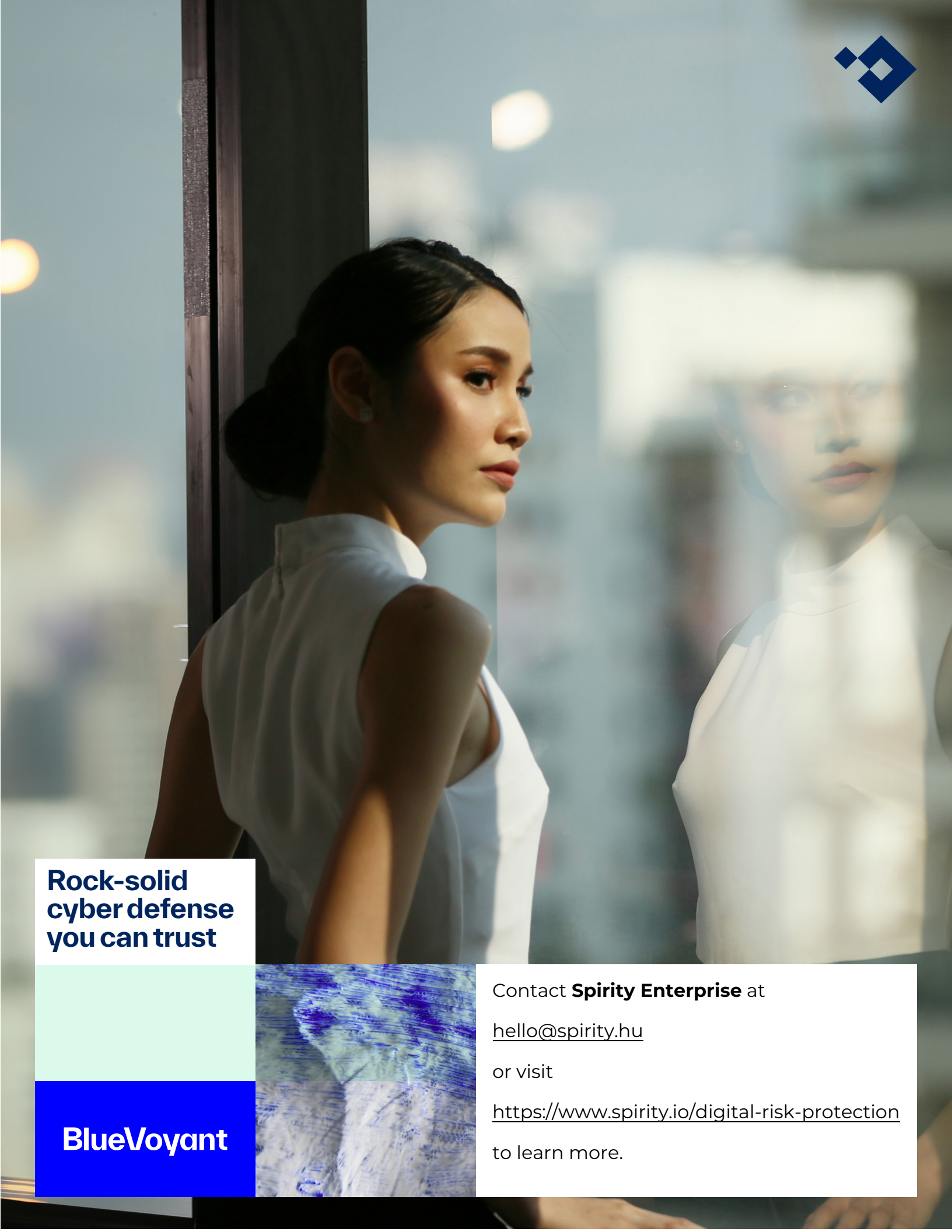
Account Takeover Monitoring

BlueVoyant continuously monitors the clear, deep, and dark web for threat actor activity to help prevent emails, usernames, and passwords from being compromised or sold by threat actors.

BlueVoyant analyzes more than 100 million potential phishing domains daily.

Sources

1. (PDF) 2021 Verizon Data Breach Investigations Report. (2021, July). Retrieved May 23, 2022, from https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report
2. FTC Launches Rulemaking to Combat Sharp Spike in Impersonation Fraud. FTC. (2021, December). Retrieved June 1 2022, from https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-launches-rulemaking-combat-sharp-spike-impersonation-fraud
3. (PDF) Federal Bureau of Investigation Internet Crime Report 2020. FBI. (2021, April). Retrieved June 1, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf



Rock-solid cyber defense you can trust

BlueVoyant

Contact **Spirity Enterprise** at

hello@spirity.hu

or visit

https://www.spirity.io/digital-risk-protection

to learn more.