Spirity
TOMORROW:TODAY

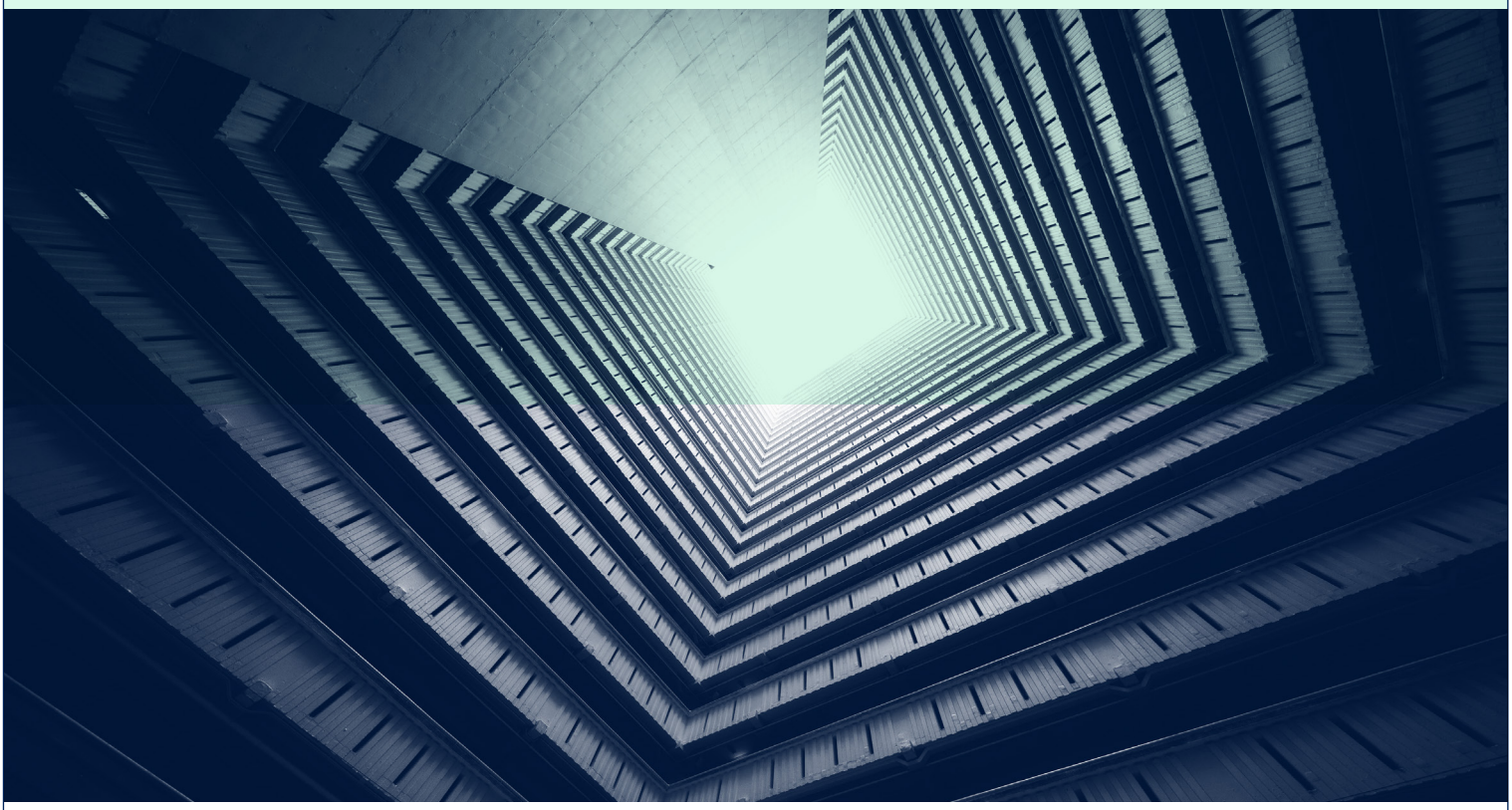
eBook

# From Reactive to Proactive Security Posture

BlueVoyant
**Sky: DRP**

BlueVoyant

# Security threats have evolved



Security threats have evolved significantly in today's world. Threat actors are experts at finding new weaknesses in even the most secure environments, and they're particularly adept at exploiting new technologies that have emerged in the era of remote work. With the cost of a data breach rising to a 17-year high[1] of $4.24 million, it's hardly a surprise that cybercriminals are stepping up their efforts.

But organizations cannot rely on manual efforts to recognize and prevent cyber threats from impacting an organization's bottom line. In fact, 64%[2] of CISOs fear their companies are at risk of a major cybersecurity attack in the upcoming year and 66% feel their organization is unprepared to handle it.

**This is where you come in.**

In this eBook, you will learn:

- Common cyber attacks used by today's threat actors.
- Recent changes to the threat landscape based on the increasing popularity of hybrid work models.
- The advantage of leveraging a Digital Risk Protection (DRP) solution to establish visibility and a proactive approach to security.

1 https://www.ibm.com/security/data-breach
2 https://www.csoonline.com/article/3628188/cisos-15-top-strategic-priorities-for-2021.html

## Common Cyber Attacks Used Today

The evolution in the way we work (and how we get our work done) has increased the threat landscape for nearly every organization. From myriad new devices accessing an organization's network to more sophisticated efforts by threat actors, our digital transformation has created a slew of common tactics your security team can—and should be—well versed on. These include:

**Phishing:** Phishing is no longer limited to suspicious emails; it now often occurs over social media, text messages and malicious USB drops. It's relatively easy for cybercriminals to trick unsuspecting users into clicking malicious links and surrendering personal information.

**Data breaches:** The most pressing aspects of data breaches are data leakage and credential stuffing. Data leakage occurs when massive databases are leaked or stolen by criminals who buy and trade the information on dark web forums or instant messaging platforms. Credential stuffing occurs when login credentials are used for brute force entry into password-protected accounts.

**Spoofed domains:** Hackers set up nearly identical domains using company branding to lure users of those products into unwittingly providing their login credentials or sensitive personal information. Domain spoofing has become increasingly prevalent during the COVID-19 pandemic, with costs rising 85% year-over-year[1] to $2 billion total losses in September 2021.

**Malware or ransomware:** Many phishing scams that include malicious links ultimately lead to malware or ransomware threats. Users unwittingly download software containing viruses, allowing hackers to steal data, gain control of their environments, or even lock a company out of its systems and demand a ransom. The FBI's 2020 Internet Crime Report[2] showed there were 2,474 reports of ransomware in 2020 with adjusted losses of $29.1 million.

**Fraud campaigns:** Once data and credentials are stolen, hackers can execute effective fraud campaigns that can put organizations at risk of being infiltrated, in addition to harming the individuals affected. These can lead to the loss of sensitive business data, and undermine consumer confidence and brand loyalty.

**Account takeovers:** Fraud campaigns are often facilitated by account takeovers; hackers use credentials to impersonate specific users. With this access, they can wreak havoc on that user's assets or company infrastructure.

**Targeted executive attacks and spear phishing:** Highly-targeted phishing attacks often use an executive's digital likeness to dupe employees or partners into clicking a malicious link or providing sensitive data. This can include spoofed email domains and social media accounts.

## Changes to the Cyber Threat Landscape

As every security team knows, social and marketplace influences have a direct impact on cybersecurity needs. In fact, the most common cyber attacks used today often lean on current events to trick the unsuspecting users into giving away sensitive information.

As a result, organizations' security teams must see cybersecurity within the context of the larger business environment to understand how reactions to current events could heighten certain threats.

### Hybrid Work

The COVID-19 pandemic changed everything from the way employees work to how consumers purchase products and what data they choose to share. Perhaps one of the most influential changes COVID had on the modern workplace is the introduction of hybrid work.

Hybrid workplaces present new security concerns and distinct challenges from pre-pandemic workplaces. Not only do hybrid workplaces use more devices, but the rise of the bring-your-own-device (BYOD) trend means security teams have less visibility and diminished control over endpoints. This disrupts the ability of security teams to spot vulnerabilities.

Compounding this challenge is the organization's increased reliance on gig workers, freelancers and third-party vendors — all of whom need a level of insider access to get the job done. To mitigate both of these unique challenges in today's modern workplace, it demands greater oversight of the cyber risks that threaten the organization.

1 https://www.ftc.gov/news-events/press-releases/2021/12/ftc-launches-rulemaking-combat-sharp-spike-impersonation-fraud
2 https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

# Data leaks & threats at a glance

**92%** of apps by online retailers actively leak sensitive data

**57%** of data breaches involved insider threats

**E-commerce Boom**
How and where people work has presented a number of security challenges, but one area that can be easily overlooked is e-commerce. Though online shopping is not new, a majority of consumers became more comfortable with purchasing everyday items online during the pandemic. From clothes to groceries, consumers leaned on various apps to take advantage of delivery or curbside pickup solutions.

But many e-commerce apps have glaring security vulnerabilities. In fact, 92% of apps by online retailers[1] actively leak sensitive data. Organizations shouldn't just be worried about their own e-commerce vulnerabilities, but those of the companies in their supply chains, as well.

**Personally Identifiable Information**
Hybrid work and online shopping paved the way for yet another security challenge: the rise of Personally Identifiable Information (PII) and Protected Health Information (PHI). As more consumers became comfortable shopping online, it spread to the use of various other health-related services, especially for providers that deliver COVID-19 testing or vaccines, such as pharmacy retailers, grocery stores, and department stores. With increased usage, these organizations have become larger targets to threat actors, increasing their need for a heightened approach to protecting their information.

**Emerging Threats**
It's not just consumer-driven behaviors that have changed the security game. Cybersecurity is constantly evolving as new threats and vulnerabilities emerge, meaning there are ever-changing security demands.

For example, the Log4j security vulnerability is easily exploited by criminals. While many security teams are rushing to patch, most organizations realistically need to shift their focus to detection and response. This is because it can be difficult to immediately understand the extent of an organization's Log4j exposure, and even after this is determined, the patching process can be incredibly labor intensive. If an organization focuses entirely on the patching process only, they can easily miss the areas where they are at risk as a result of a previous (or ongoing) exposure.

Complicating matters is the trend for cybercriminals to move away from dark web forums — that can be monitored — to private instant messaging channels. Encrypted chats are becoming increasingly popular as illicit marketplaces. And the robust security features of these messaging channels means organizations (and law enforcement) have less visibility into the activities taking place.

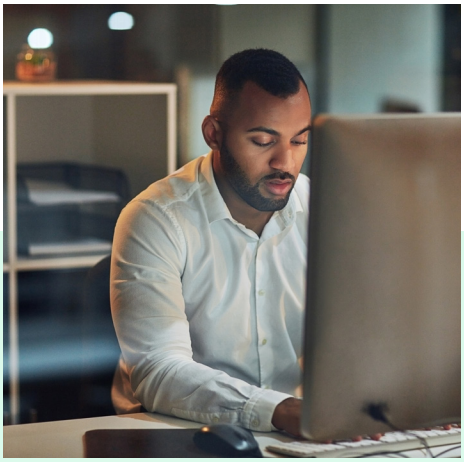
While security teams could once heavily rely on endpoint security tactics to reduce much of their risk, this isn't enough anymore. Hackers often collaborate on their own private instant messaging channels to evade detection. They can also use malicious insiders, or take advantage of mistakes made by negligent insiders, to accomplish their aims. Worth noting is that insider-led security breaches are responsible for an increasingly large number of data breaches in today's environment; Verizon's Data Breach Investigations Report[2] shows 57% of database breaches involved insider threats.

1 https://www.retaildive.com/news/almost-all-retail-apps-leak-personal-data-security-firm-warns/569939/
2 https://www.verizon.com/business/resources/reports/insider-threat-report/

**Digital risk protection is the home-field advantage**
Despite the continuous shift in the cybersecurity landscape, organizations' security teams have a major advantage over malicious outsiders: the home-field advantage. By leveraging digital risk protection to ensure proper security precautions in place, organizations can more effectively detect vulnerabilities in their own environment and fix them before hackers spot weak points. Taking this approach ensures organizations are taking big steps away from a reactive approach to cybersecurity toward a proactive security posture.

One of the most effective ways to make this shift is by using threat intelligence to identify weak points within the organization's security infrastructure. Taking this approach is typically comprised of three parts, each of which presents unique benefits:

**Conduct an attack surface evaluation.** This evaluation can provide an objective appraisal of the organization's security posture, giving security teams a head start on fixing vulnerabilities that, ideally, will head off attacks.



**Find and lock down leaked digital assets across the web.** This approach can minimize the damage of attacks that have already occurred and give security teams a unique opportunity to turn the tables on cybercriminals. In fact, threat data enables security teams to anticipate threat actor movement and activity, so even if some dark web forums are providing less useful information over time, security teams can still gain insight into criminal activity through threat data. Coupled with this is validated alerts, which provide next-level actionable intelligence for security teams to stay ahead of the game.

**Extend visibility – and control – beyond the network perimeter.** This means security teams can effectively identify threats before they become attacks. Monitoring sources across the dark web for emerging threats to the organization is crucial to succeeding with this approach.

**The BlueVoyant Difference**
BlueVoyant's Digital Risk Protection solution goes above and beyond to identify emerging threats targeting your organization, while equipping your security team with the tools to shut the threats down at the source. By leveraging the largest private sector global cyber threat detection data set, BlueVoyant's team of experts can see deep into your ecosystem to identify vulnerabilities, provide comprehensive intelligence, and arm your team with actionable insights on how to fix these weak spots.

The BlueVoyant Digital Risk Protection solution can help your organization with:

- **Brand protection:** Continuously protect against attacks targeting your digital assets with BlueVoyant's end-to-end solution.
- **External attack surface analysis:** Quickly identify stolen credentials to reduce risk and limit the consequences of a breach.
- **Data leakage detection:** Protect intellectual property, credentials, and other sensitive data from leaking on the dark web or instant messaging platforms.
- **Fraud campaigns discovery:** Defend against the use of stolen customer data, such as compromised payment cards and bank account information, among others.
- **Account takeover monitoring:** Quickly identify stolen credentials to reduce risk and limit the consequences of a breach.
- **Executive cyber guard:** Create a digital footprint, identify compromised information, and shut down digital threats specifically targeting executives.

Learn more about implementing Digital Risk Protection in your organization here.


## 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.