flare

Digital Risk Protection Guide

Are You Aware of Your Organization’s Digital Footprint?

https://flare.systems

Executive Summary

A lot has changed in 2020. A global pandemic outbreak has transformed the way companies operate, increasing reliance on remote work and cloud-based services. These transformations, however, increase the number of digital risks enterprises are exposed to. The overall lack of control and visibility of cloud-based services, shadow IT, and unsecure internet connections have created a need for enhanced transparency into a company's digital footprint.

Considering the average cost of a data breach has neared USD$4 million, companies are looking into adding digital risk protection (DRP) solutions to their cybersecurity strategy to optimize risk coverage and prevent reputational and brand damage. Digital risk protection should be a long-term investment in any corporate cybersecurity strategy to prevent malicious actors from infiltrating enterprise networks.

Cyber criminals can take advantage of data and technical leaks to conduct illicit operations such as account takeover, phishing attacks, and fraud. In this white paper, you will learn about digital risks, specifically what their root causes are and how to detect them in the wild. You will get a comprehensive overview of how malicious actors can infiltrate your network, what role human errors play in an attack, and how to identify if an attack was successful.

A holistic cybersecurity strategy involves multiple security layers that help you identify, understand, and mitigate the digital risks threatening your brand, reputation, and customers. Even though the industry is predicting a higher number of sophisticated attacks, there are silver linings: a wide portfolio of user-friendly tools to help you detect, prevent, and remediate risks.

Table of Contents

1. How Has the Digital Risk Landscape Changed? 4

Remote workforce 4

Reliance on cloud-based services 4

Personal, financial, and confidential data collection 4

2. Digital Risks: Root Causes and Detection in the Wild 6

The Root Causes of Digital Risks 6

How Malicious Actors Infiltrate Enterprises 6

How Human Errors Invite Malicious Actors Into Your Company 7

What Happens After a Malicious Attack or a Human Error? 7

3. What Is Digital Risk Protection? 9

Digital Footprint Monitoring on the Dark Web 10

Data Leak Detection 11

Technical Leak Protection 12

Brand Protection 13

Account Takeover Prevention 14

Financial Fraud Prevention 15

4. Why Digital Risk Protection Is a Long-Term Investment in Your Cybersecurity Strategy 16

5. The Industry's Current Strategy 18

Identify 18

Understand 18

Mitigate 18

6. The 4 Key Actions to Protect You Against Digital Risks 19

Superior Coverage 20

Digital Risk Contextualization 22

Digital Risk Prioritization 23

Digital Risk Remediation 25

7. About Flare Systems 27

1 How Has the Digital Risk Landscape Changed?

High competition, digital transformation, and, more recently, a global pandemic, have been pushing for business evolution and innovative business models. These transformations take on many forms but **three stand out as top digital risk enablers for your company:** a rapidly expanding remote workforce, reliance on cloud-based services, and personal, financial and confidential data collection.

Remote Workforce

As many as **64% of employees would accept lower pay** in exchange for the quality-of-life working from home offers. Due to COVID-19, at least **4.7 million Canadians** are working from home in 2020 , according to Statistics Canada. Social distancing guidelines will make returning to work unlikely for many of them.

A remote workforce introduces a number of cybersecurity challenges, especially in terms of network security visibility. Employee use of work devices on unsecure connections, as well as BYOD (bring-your-own-device) **increase your company's susceptibility to attacks.** This could jeopardize critical data and proprietary code, whose security may be out of your control.

Reliance on Cloud-Based Services

While they help your company be more flexible and lower the costs of running infrastructure, the **overall lack of control and visibility of cloud-based services** turns risk management into a challenge. Cloud-based services manage information access rights and are difficult, if not impossible, to audit from a cybersecurity point of view.

Departments and individual employees may also **adopt unlicensed cloud-based services** to bypass your company's central systems. Also known as **"shadow IT,"** BYOC (bring-your-own-cloud) has gained popularity among employees, despite causing a third of successful enterprise attacks.

Personal, Financial, and Confidential Data Collection

Business processes are actively relying on the analysis of data associated with customers, competitors, markets and trade secrets. Your company **needs to protect its information pool** from malicious actors who want to commit financial and identity fraud.

It is challenging to protect this information since many employees need to access it for legitimate reasons. Malicious actors can **hide their access requests and exports among the many day-to-day requests for data.** The skill needed to attack databases has become of the most sought-after skills on hacker forums.

Any Company Can Fall Victim to Data Breaches and Cyber Attacks

Large corporations, such as British Airways, leaked the personal details of over **400,000 customers** in 2018, which led to a **£20 million (USD$25.8 million)** fine.

More recently, the largest mobile operator in Greece also lost control over the personal information of thousands of customers.

Malicious actors are also opportunistic and **target small and medium businesses (SMBs)**. A recent report shows that over 4,800 companies, many of them SMBs, suffer data breaches every month. **The impact on SMBs is likely even higher,** given they lack large corporations' resources to handle data breach responses.

The average **cost of a data breach has now reached almost USD$4 million**. Large breaches, such as that of Dickey's Barbeque Restaurant locations in the U.S., may generate higher costs, since information linked to over three million credit cards was put up for sale on the dark web.

An effective cybersecurity strategy relies on **multiple layers of security to prevent and mitigate data breaches.** According to research conducted by Forrester in 2018, companies include **digital risk protection** (DRP) solutions in their cybersecurity strategy to optimize risk coverage and prevent reputational and brand damage. Digital risk removal and remediation, C-level executive and VIP protection, and enhanced transparency and security into their digital footprint and assets are other DRP drivers, as we explain below.

2 | Digital Risks: Root Causes and Detection in the Wild

Gartner **defines digital risks as** "potential threats to critical assets." A broad definition to begin with, digital risks include **all external threats, malicious actors and human errors** pose. Threats vary based on your industry, number of employees, and your security team's maturity. However, root causes, shape and size, and visibility have some common characteristics.

The Root Causes of Digital Risks

Security teams have so far focused on malicious actors outside the company perimeter. These cyber criminals can be anywhere on the globe and be motivated by greed, personal or political reasons. Political motivations were behind the Anonymous movement that targeted hospitals, amusement parks and financial institutions. Recently, though, greed is the driver for most, which helps security teams understand the target and type of attack to expect.

Human errors should also be a major concern for security teams. Usually related to employees, **human errors jeopardize your security**, data, financial assets and brand reputation. They are hard to predict and prevent, because any employee could be the source to a successful attack.

How Malicious Actors Infiltrate Enterprises

Looking at infiltration through the prism of digital risks, there are **four ways malicious actors can infiltrate your company,** based on the MITRE ATT&CK framework. This is only the first step in a long process that may lead to a visible data breach (see below).

Technical Vulnerability

Drive-by Compromise (T1189)
Exploit Public-Facing Application (T1190)

Malicious actors take advantage of a weakness, a bug, a glitch or a design vulnerability to take control of a computer system. The attack can be proactive with malicious actors attacking your network. It can also be passive where malicious actors wait for one of your employees to visit an infected website to attack them.

Supply Chain Attacks

Supply Chain Compromise (T1195)
Trusted Relationship (T1199)

Supply chain attacks are indirect attacks in which malicious actors compromise software used by your employees. Employees then download and install the infected software, which opens the door for malicious actors. Popular open-source software is often a target, given its wide adoption and high number of downloads.

Phishing

Phishing (T1566)

Phishing attacks are part of social engineering strategies based on electronic communications. Malicious actors send email, SMS txts and even social media messages to your employees under false pretenses to extract sensitive information or gain access to your network. Phishing attacks can be targeted to a specific individual or company (spearfishing) or non-targeted and opportunistic.

Legitimate Accounts

External Remote Services (T1133)
Valid Accounts (T1078)

Malicious actors can download or purchase from various online sources a large number of valid credentials to log in to your network. They can also test leaked credentials from other services to check if your employees are reusing known leaked passwords.

How Human Errors Invite Malicious Actors into Your Company

Human errors are unintended employee actions that jeopardize your company's security, data, financial assets and brand reputation. No security training or the lack of time to implement the best security measures often lead to human errors.

Misuse of Cloud Collaborative Platforms

Even though your company may offer a number of cloud-based services such as Microsoft Office and file-sharing (ex. Dropbox), employees may prefer different tools. This is also known as shadow IT, because your security team cannot monitor the communication and data sharing process.
Free trials could expose confidential documents by default.

The use of licensed cloud-based services does not guarantee protection against human errors. Most cloud-based services allow data sharing with individuals outside your company. Each user is responsible for information security because a lack of training may lead to costly human errors.

Misconfiguration of Tools and Services

Security teams have to secure large computer networks in an environment shifting towards remote work and collaboration. Employees are also pushing for the approval of new tools and services to enhance their productivity.

Each of these need to be properly configured and reviewed by a risk assessment process. This can be time-consuming, especially when there is no proper documentation.

Tool and service misconfigurations can have dire impacts on a large number of employees and even expose databases online. Employees may gain access to confidential information about customers and other staff.

What Happens After a Malicious Attack or a Human Error?

Malicious actors are trying to infiltrate your systems, while some employees introduce additional risks through misused cloud collaborative platforms and the misconfiguration of tools and services. However, **not all digital risks lead to successful attacks,** because they require a vulnerable target, a motivated offender and the absence of a capable guardian.

According to this model, a digital risk is a theoretical threat, as long as a motivated offender does not discover it, and decides to take advantage of it. Malicious actors have plenty of companies to choose from when it comes to attacks, so this may give your security team a chance to **remediate digital risks**. The absence of a capable guardian is crucial because a security team cannot prevent all digital risks. It can only **reduce digital risk detection time** and implement effective measures to eliminate them.

> *A recent study on Github shows that 200,000 passwords and API keys were published on the source code repository over a six-month period. Over 80% were accessible for the entire study span, leading to monetary losses, confidential information leaks and loss of data integrity.*

A random factor dictates which theoretical threats become successful attacks. Successful attacks can have a differential level of impact when detected early on. Since malicious actors are not likely to publicize their attacks, traces of their activities must be collected.

Data Leaks

Data leaks are the most common evidence of successful attacks. When listed for sale, malicious actors publish either samples of the stolen data or the entire information set once commercial value is lost.

Data Leaks Typically Include:

- **Executives' personal and financial information** used for impersonation and identity fraud. It can also be used in fraudulent wire transfers from the company to the malicious actors' bank accounts.
- **Customers' personal and financial information** used for financial and identity fraud.
- **Technical secrets and assets** such as passwords, API keys, and trade secrets. This information is useful to gain further access to your company's network and computers. It can also be used to steal your company's computational resources to feed large botnets.

Unauthorized Access

Unauthorized access to computers, company services and accounts is also evidence that an attack was successful. Malicious actors will publish screenshots to prove they have taken advantage of your digital risks. Unauthorized access can last for months and **lead to continued data theft**, as your company enlists new customers.

Fake Online Presence

Fake company presence online is another confirmation that an attack was successful. Suspicious domain names and certificates similar to yours are used to **launch phishing attacks**. They are valid even when the phishing campaign has ended. Fake social media profiles are another source of false online presence. They are used in phishing attacks against your customers, but also against your employees who might believe they are talking to a co-worker on social media.

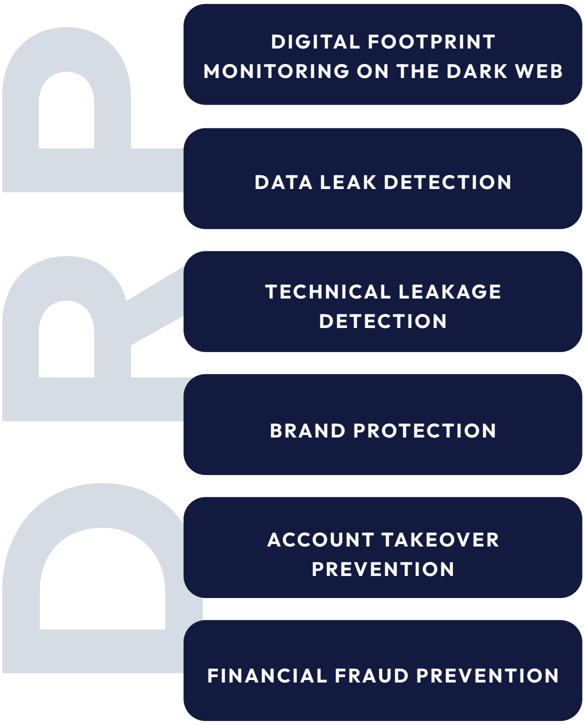
3 What Is Digital Risk Protection?

In its 2020 report titled “Emerging Technologies: Critical Insights in Digital Risk Protection Services,” Gartner **defines Digital Risk Protection (DRP)** as “a key technology solution that supports” digital risk management (DRM) capabilities. A digital risk protection solution is an **additional security layer** that safeguards corporate digital assets from external threats, improves security team efficiency, and protects brand reputation by **identifying unwanted exposure in real-time.**

The research company has defined six major use cases Digital Risk Protection (DRP) can assist with:

- **Dark Web Monitoring**
- **Data Leak Detection**
- **Technical Leakage Detection**
- **Brand Protection**
- **Account Takeover Prevention**
- **Financial Fraud Prevention**

How does the concept of DRP apply to each use case? How can DRP help your company prevent malicious attacks, human errors, and reduce detection time of successful attacks?



DIGITAL FOOTPRINT MONITORING ON THE DARK WEB

DATA LEAK DETECTION

TECHNICAL LEAKAGE DETECTION

BRAND PROTECTION

ACCOUNT TAKEOVER PREVENTION

FINANCIAL FRAUD PREVENTION

Digital Footprint Monitoring on the Dark Web

Most companies have no presence on the dark web. Malicious actors, however, use the dark web as an anonymous communication **network to buy and sell stolen information** and to share effective attack methods. They are no longer lone wolves, but have grouped into organized crime units that operate in large-scale illicit markets, forums and chat rooms. Considering it is easier than ever to purchase hacking tools and personally identifiable information (PII) online, dark web monitoring is essential in maintaining visibility over your company's digital footprint.

How Does It Work?

Digital risk protection solutions create their own indexing robot just like Google, though it seeks to **index the criminal underground** instead of legitimate websites. The indexing robot goes through all web pages and online resources, looking for links to content that could identify new digital risks. DRP keeps a history of all online resources to revisit later, if found to be of value. It also logs in to websites to **access content that is not available publicly** which makes them more sophisticated than Google indexing robots.

How Does It Help?

Dark web monitoring **detects ongoing and past malicious attacks.** Its role is to quickly identify if your company has suffered a data breach and to prevent malicious actors from maintaining access to your corporate network. Your company can prepare a response to a successful attack, protect your brand and reputation, and proactively remediate threats.

In 2019, darknet market activity outperformed previous years, as sales grew to more than $790 million

A study conducted by the University of Surrey in 2019 claims 60% of dark web listings could directly damage businesses

Data Leak Detection

Malicious actors are actively trying to steal corporate confidential data and employees' and customers' personal and financial information. **Human errors,** however, are also behind data leaks. The shift to remote work has increased the use of cloud-based collaborative tools that employees can use to create accounts and **store data without company knowledge**. The access rights are often not managed by security teams and may lead to leaks.

How Does It Work?

Digital Risk Protection solutions leverage indexing robots that monitor your company's digital footprint on the dark web to also monitor legitimate websites where your employees are active and may leak data. DRP analyzes the data from both the criminal underground and legitimate websites to **identify specific data leak patterns** such as customers' names and contact information and credit card numbers. They then send real-time warnings about a newly published digital risk.

How Does It Help?

Data leaks involve costly investigations into root causes, which may hinder normal business operations and cause downtime and productivity loss. When leaks include customer data, companies can be fined, forced to pay legal fees, and suffer a drop in brand reputation. Leaked passwords and API keys can be used to launch new attacks.

Some 1.6 billion records have been leaked since 2005

Over 163 million records were leaked in 540 security events in 2020 alone

Technical Leakage Detection

Software engineering teams use multiple open-source and cloud-based solutions in their DevOps applications. Whether the team is made up of in-house developers or a mix which includes external contractors, they might mistakenly leak source code and access keys on code repositories such as Github or GitLab, paste sites such as Pastebin, or support forums such as Stack Overflow. World-renown companies have experienced technical leakage, as no company is exempt. What's more concerning is detection time, because quite often technical leaks could go undetected for months, allowing malicious actors enough time to download the code.

How Does It Work?

DRP performs custom regexes and queries that would not be normally run directly in the Github search function. It expands search coverage by monitoring both recent commits and repositories' entire commit tree and reduces the number of alerts and noise by regrouping alerts based on repositories, projects, and developers.

How Does It Help?

Technical leakage compromises the most sensitive secrets your company depends on: its passwords and access keys. Once they get access to either, malicious actors can easily infiltrate your corporate network to steal confidential information. The larger your development team gets, the higher the risks for technical leakage to occur, due to weaknesses in secure coding practices.

In July 2020, 50+ international companies suffered a source code leak due to software development misconfigurations

More than 100,000 repositories had leaked API and cryptographic keys on GitHub in 2019

Brand Protection

Your online **brand reputation is in sync with your digital footprint.** Ever since business has moved online, companies have been collecting tons of data, making them an attractive target for external hacking attacks. When a data breach compromises customer and business partner information, you may damage your reputation and lose your partners' trust.

Poor infrastructure security could expose your company to phishing attacks which may result in reputation damage and fines from privacy regulators. Cybercriminals register domain names and security certificates similar to yours to redirect followers to phishing and malware-distributing websites. By identifying attacks against your brand and data leaks early, you can **mitigate reputational risk** and negative media attention from publicized breaches.

How Does It Work?

The dark web digital footprint monitoring and data leak detection capabilities instantly alert you when a security event could damage your brand. DRP also monitors new registrations for domain names and security certificates to **identify phishing campaigns** that use your company's names. DRP helps you take down those domain names and security certificates to eliminate digital risks.

How Does It Help?

Digital Risk Protection services **inform you about data leaks and phishing campaigns** as soon as they happen. This provides you with the time you need to react and prepare your public responses. Your brand and reputation are valuable assets, so protecting them ensures core business activities can continue, even when under attack.

Between 2018 and 2019 alone, phishing attack frequency grew by 250%

81% of customers say they need to trust a brand before they make a purchase

Account Takeover Protection

Malicious actors have access to specialized, automated software to test whether leaked credentials, or those acquired on the dark web, work on different online services. When people reuse passwords, it's enough for cyber criminals to access a website's credentials to use them in **credential stuffing attacks** and take over multiple accounts. To take a better guess at passwords for online accounts, malicious actors can also profile the passwords individuals would use.

How Does It Work?

Digital Risk Protection services **download credentials leaked online** and on the dark web, which are then assimilated into sprawling databases of billions of credentials. You can query that database in real-time to flag employees and customers using leaked credentials. An initial investigation can also be conducted to find the leaked credentials in your database and force user reauthentication.

How Does It Help?

Account takeovers result in **direct financial losses,** because you need to refund your customers when their funds or loyalty program points are stolen. Your customers may also lose trust in the digital experience you provide them, which could **damage your brand and reputation.** Customers' switching costs are generally low online. Bad experience with an account takeover attack could push your customers toward competition.

Account takeover fraud went up 72% in 2019

40% of account takeovers occurred within 24 hours of a criminal's access to a victim's account

Only 35% of users have unique passwords for each account

Financial Fraud Prevention

Personal and financial data collected from phishing attacks, skimming and card-not-present fraud are sold on the dark web. A single identity can be used for multiple credit card fraud schemes, to open new bank accounts or apply for loans. Hackers sell stolen credit card information on the dark web for anywhere between USD$1 and USD$45 each, depending on whether it contains the complete personal and financial information of the victim.

How Does It Work?

Digital Risk Protection **compiles a financial fraud victim directory** based on leaks on the dark, deep and clear web, as well as identifies the information for sale on illicit markets. Personally identifiable information is shared with the victim's financial institution to flag their account as potentially vulnerable to fraud.

How Does It Help?

One of the least reported crimes, identity fraud has a high dark figure that limits preventive measures. Financial fraud prevention helps your company **identify potentially vulnerable accounts.** Increased vigilance can lower fraudulent charges and protect your brand and reputation.

47% of companies suffered from fraud in the past 2 years causing a total loss of USD$42 billion

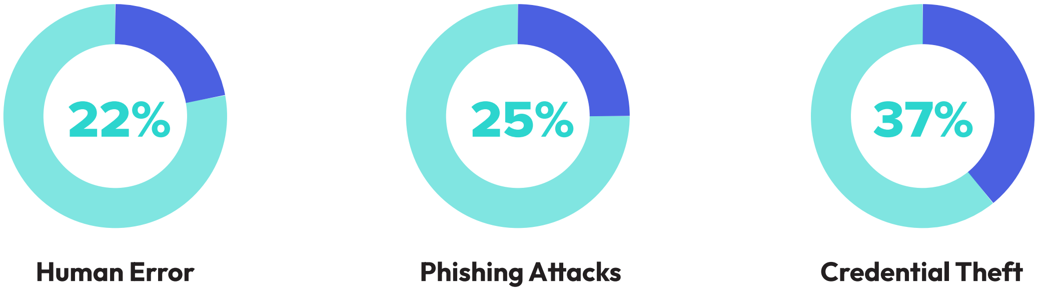
Canadian financial services firms and lending platforms encountered an average of $3.46 in costs for every dollar lost in fraudulent transactions

The total cost of fraud for U.S. financial services and lending firms has increased by 2.8% year-over-year

4 | Why Digital Risk Protection Is a Long-Term Investment in Your Cybersecurity Strategy

In 2020, the **average cost of a data breach** was USD$3.86 million, according to independent research conducted by the Ponemon Institute. The highest cost was detected in the United States, which ranks as the most expensive country (USD$8.64 million), whereas healthcare is the most expensive industry (USD$7.13 million).

Top Data Breach Causes in 2019



As companies grow, threat vectors expand. According to Verizon's 2020 Data Breach Investigations report, the **most targeted industries** are Manufacturing, Retail, Finance and Insurance, Educational Services, Healthcare and the Public Sector.

Gartner estimates that "by 2025, the target audience for **digital risk protection services will increase to 10%,** up from 1% today." Given the current threat landscape, Digital Risk Protection (DRP) is an investment which organizations of all shapes and sizes should consider to **safeguard their digital assets.**

DRP leverages **Artificial Intelligence and Machine Learning** to help security teams minimize risks, reduce cost through process automation, and protect revenue and brand reputation. Over two-thirds of breaches remain unknown for months, making it even harder for your company to measure the impacts of external threats. External threat management allows your internal security team to monitor and eliminate risks exponentially.

Companies spent an average of 280 days to identify and contain a breach.

Companies struggle to attract new business once a security incident is public news. Loss of trust and brand tarnishing could take your company years to rebuild. Besides negative press attention, **stock market share prices drop** an average of **7% within 14 days of a data breach** and are likely to underperform for three years.

Downtime, productivity loss, security consultants hired to clean up the mess, protection services and regulatory non-compliance are **additional costs** you will have to handle following a data breach. Addressing the security problems, delays in business operations, specialists hired for attack investigation and remediation, and credit monitoring and identity theft prevention services will generate a decrease in ROI. Regulators are proactive in external threat investigations, raising corporate negligence costs to millions.

What if you could get **actionable cyber threat intelligence for billions of data points** generated by interactions between cybercriminals? Any company can fall victim to cyber security incidents, but there are tools available to help mitigate cyber threats and improve your security hygiene. To assist you, these tools use real-time **monitoring the deep, dark and clear web.** Deep web monitoring ensures all content is analyzed, even when it's not indexed by search engines, including websites that require membership or sign-in.

> *Organizations need to redefine their cybersecurity strategies by combining threat intelligence with digital risk protection*

Organizations need to redefine their cybersecurity strategies by **combining threat intelligence with digital risk protection,** especially as third-party vendors and partners expand attack vectors. **AI-driven digital risk protection software** expands digital platform coverage and your security perimeter to enhance visibility into threats targeting your company.

5 The Industry's Current Strategy

At a high level, most Digital Risk Protection solutions adopt a somewhat similar approach to the digital risk problem. Their approach is based on an "identify, understand and mitigate" approach.

1. Identify

This step requires your security team to identify its **critical assets that need protection against digital risks.** These assets are not necessarily computer networks, systems or even databases, but include key personnel, customers and even business processes. Partners and third-party vendors such as payment processors are part of your company's critical assets.

2. Understand

The second phase requires **understanding malicious actors' tactics** and procedures, as well as the specific opportunities they may take advantage of. Your security team also needs to **understand which systems your employees are using.**

It is important to know if they are accessing collaborative cloud-based services without your security team's approval and knowledge. The latter could create opportunities for malicious actors to generate digital risks.

This simple yet effective approach has generated some interesting results in protecting against digital risks. It puts, however, an equal emphasis on identifying, understanding and mitigating digital risks. Of the three, the "understand" step stands out for two reasons.

> By virtue of size or industry, many companies are attractive targets. **Malicious actors will actively monitor human errors and digital risks** to manipulate them for corporate access. The security team is probably drowning in alerts from various vulnerability scanners and intrusion detection systems.
>
> Your company has to conduct a differential analysis to redirect resources to the most urgent risks, because malicious actors are not equally threatening. Smart solutions are essential in keeping digital risk protection effective.

> Smaller companies might wrongfully believe that their size of industry could not draw much interest from malicious actors. They might also believe they lack the resources to invest in digital risk protection services, which may have previously been expensive or time consuming.
>
> Malicious actors are opportunistic, so they don't focus only on large corporations or on healthcare and finance. **All companies that have personal and financial information databases are at risk.** Partnerships with larger names in business can turn them into targets for access to confidential information and secure networks. Understanding your company's digital risks should not be limited by resources, because it is a vital part in any company's security hygiene.

3. Mitigate

The last stage involves **taking action against the digital risks identified** in the previous steps. These wide-ranging measures vary based on industry, company size and risk profile. Removing offending content from public sources, relacing leaked credentials and introducing new security measures to prevent data breaches and attacks are part of the mitigation process. New integrations with incident response processes and a closer monitoring of certain digital risks maybe be introduced.

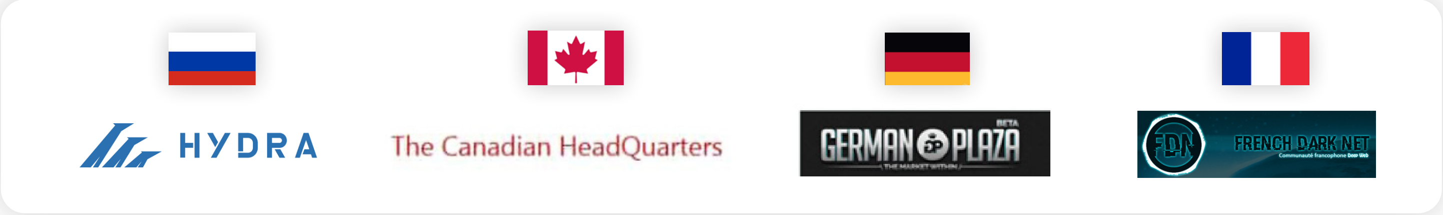
6

Flare Systems' **4 Key Actions** to Protect Against Digital Risks

Flare Systems protects your digital risks by providing you with Firework, an intelligent solution capable of contextualizing, prioritizing, and remediating digital risks.

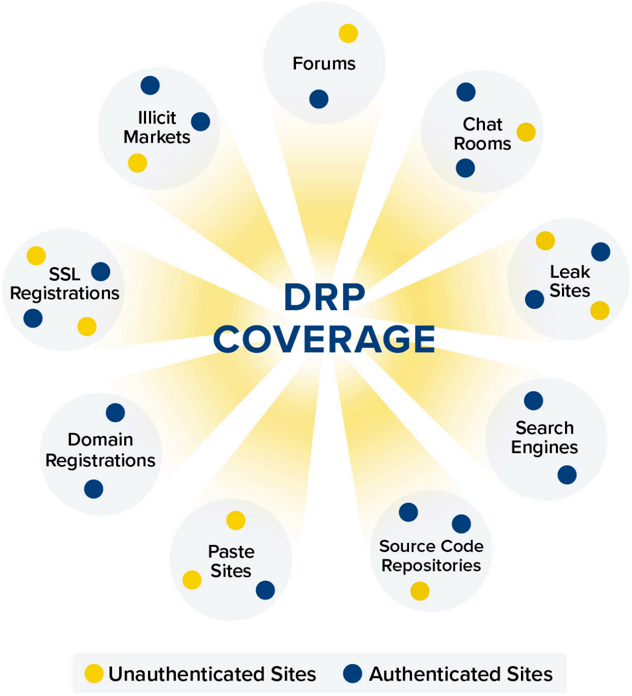
Superior Coverage

Our Digital Risk Protection begins with **transparent and quantifiable digital risk monitoring** of your company's activity. The extent to which digital risks are monitored is known industry-wide as coverage. Coverage is most often the number of websites indexed by DRP to identify digital risks. This is an important metric, as malicious actors cluster in niche websites with peers from the same geographical region, or active in the same type of fraud. The many **dark web markets** that cater to the needs of specific malicious actors are the best example:



Intelligence collection from multiple websites helps tap into multiple criminal underground communities and get a **holistic view of the threat landscape.** Coverage, on the other hand, is much more complex, because there are several factors that need to be addressed, not just the number of websites.

Measuring the Coverage of a DRP Solution



Malicious actors are known to be active on the dark and clear web, but also on instant chat messaging systems (ex. ICQ), voice systems (ex. Discord) and social media (ex. Facebook). The above figure presents the sources of information that a good coverage implies. It shows that for each source, there are many platforms that need to be monitored. Some platforms require that we authenticate ourselves, while others are open to anyone. Malicious actors share different types of information on each source, and connecting the dots between them has the potential to improve the quality of digital risk intelligence.

While single platform indexing could provide some answers to fend off digital risks, indexing a **vast number of platforms ensures a superior threat intelligence level** and enhances defense output.

Authentication Crawlers for Top Coverage

No matter the platform, authentication plays a crucial part in understanding coverage. Authentication involves platform access with a username and a password. Online content protected by authentication is allegedly 500 times larger than the content that is not, meaning coverage without authentication has limited value for intelligence.

Often too costly for some DRP providers, manual labor is necessary to develop authentication crawlers. Similar to platform coverage, different types of malicious actors are likely to be active on different authentication levels. As a result, DRP platform coverage varies, depending on providers' willingness to pay for authentication and engage with malicious actors for invitation codes.

Flare Systems has developed a unique and custom infrastructure that establishes platforms and authentication as the main coverage axes. **The high number of platforms we monitor provides complementary intelligence, combined into a valuable set of actionable intelligence.**

Firework's sophisticated crawlers can handle captchas, anti-bot defenses and all types of authentication to gain access to valuable intelligence. The online dashboard lists the most relevant platforms we are indexing and pinpoints if intelligence collection is running smoothly, experiencing difficulties, or in maintenance mode, for each of these platforms. Firework is built around accountability for you to evaluate monitoring quality and show peers and C-level executives how reliable their digital risk protection solution is.

Digital Risk Contextualization

Extensive digital footprint coverage will help better understand the digital risk landscape. As coverage improves, so does the number of potential digital risks identified. This makes **contextualizing digital risks** an essential part of DRP.

Firework uses a mix of keywords, regexes and artificial intelligence to identify your digital risks among the intelligence collected. You can **build an unlimited list of queries** (identifiers) to help the tool identify the digital risks that specifically target you. The solution extends whatever identifiers you select, by making sure only relevant intelligence is analyzed. For example, you can enter the first six numbers of a credit card number and label it as such. Firework will only return strings of numbers that match those of a credit card and begin with those six numbers, discarding the rest.

To make this possible, data point structuration is important because it involves extracting specific information on each content we collect. This translates into identifying the vendor name, contact information and status from all illicit market advertisements. As a result, you can cross match threats and actors, and derive analytics and actionable intelligence as described below.

Contextualization centers around the following elements:

Malicious actor profiles: on any given day, tens of thousands of malicious actors advertise a supposedly new data breach affecting a North American company. To understand how credible this threat is, Firework builds profiles. Malicious actor profiles determine how long they have been active, what feedback they received, how much reputation they have gained and what products they advertised in the past. Combined, these details generate a profile for each malicious actor to contextualize the level of threat it poses.

Threat profiles: contextualizing is also possible at threat level, rather than malicious actor level. At threat level, Firework seeks to understand when the threat appeared, who had access to it, who is responsible for posting the threat (attribution), as well as the nature of the threat. Firework connects this threat to others that are similar, to provide more context. If a specific company or system is mentioned in multiple threats, compromise odds increase drastically.

Risk-based automated labelling: Firework uses artificial intelligence to automatically label threats and actors. These labels indicate targeted industries, as well as the type of threat. This intelligence is essential to reduce noise and to make sure that our prioritization engine is able to classify the digital risks that impact your company.

Activity correlation across platforms: on average, malicious actors are active on 3 different platforms on the dark web. To contextualize their activities, it is essential to connect their identities across platforms used. This provides a fuller picture of the threat posed and improves profiling, in general. Firework leverages a unique mix of personal identifiers and usernames to eliminate noise and match identities, even when malicious actors are using completely different usernames.

Digital Risk Prioritization

Even after adding contextualization, many companies are likely to receive tens, if not hundreds, of alerts per day. Each alert takes anywhere from a few minutes to a few hours to investigate. Firework helps your company manage those alerts first, **grouping them by threat and malicious actors.**

Malicious actors tend to repost the same advertisement for an illicit service (ex. Access to a corporate network) on multiple platforms, as well as on the same platform at regular intervals. **Each of these postings would generate an alert** that needed to be handled. By grouping similar alerts, your security team saves time and resources. More importantly, it takes the repetitiveness out of your security team's daily grind, **so they focus on new threats every time.** This is an essential piece in keeping your security team alert and ready to handle your digital risks.

Digital risk scoring is another aspect of prioritization. Firework uses a proprietary algorithm that generates a risk score for each new threat it detects. The digital risk scoring process is based on the imminence and scope of digital risks, to help your security team prioritize their handling of new threats.

Firework's Five-Point Scoring System

Score	Description	Example
1	Validated not-sensitive	A list of domain names that includes yours
2	Public information	A Github commit or posting on Pastebin that mentions your company
3	Potentially sensitive data based on source or query	Company mentioned on a dark web marketplace, a known pattern of a password posted by one of your developer accounts
4	Potential leaked data or threat identified	Personally identifiable information, configuration files, and credentials tied to your company
5	Potential serious leaked data or threat identified	Large data breach coming from your company, sensitive passwords to computer network components

Prioritization can be used when defining an identifier to eliminate digital risks with a score level lower than a specific threshold. If it delivers not enough or too many alerts, the threshold can be updated in real-time. The adaptability of our systems allows different thresholds to be set for different identifiers, to ensure your security team will focus on those more sensitive.

Prioritization is also integrated in Firework's online dashboard to filter all manual searches based on risk score. The risk score evolves through time. Our proprietary algorithm is refined regularly based on our team's and our customers' experience. To build our risk scoring system, we take into account **what our own customers have flagged as most urgent and important,** as well as our investigations and assessments of the current threat landscape.

You can override our scoring system at any point and assign an ignore tag to any of the digital risks that we find. This effectively removes a digital risk from your alerts and online dashboard to ensure only what's relevant remains in your view.

Digital Risk Remediation

A contextualized and prioritized list of digital risks needs to be communicated efficiently and rapidly. To do so, Firework interacts with customers either through their machines or through their analysts:

APIs

Data contextualization and prioritization are available through APIs connected to your existing security tools to feed into your analysis systems and internal communication tools. This provides automated ingestion of our information, as well as seamless integration into your existing business practices.

Alerts

Our systems are configured to alert you and your colleagues based on your specific needs. Each of the identifiers you set up can be configured to alert you in real-time, once per day or once per week. Each alert can be sent to a single person or to a group of people in or outside your organization.

In both cases, the aim of our solution is to help you remediate the digital risks your company is facing.

To achieve this goal, our solution helps your security team:

Take down online content

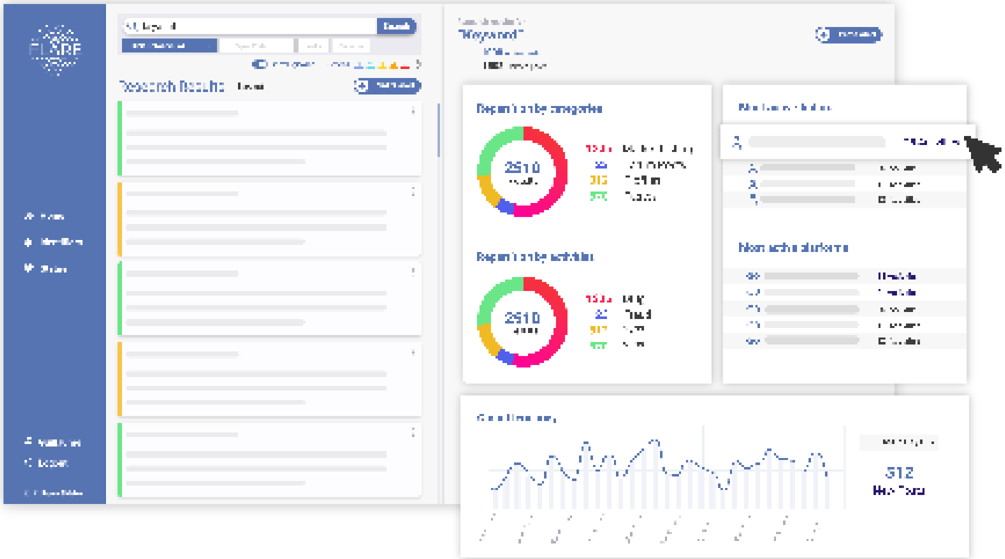
Our solution identifies specific information that is creating a digital risk for your company. It helps you understand where the information comes from, who is responsible for posting that information, and the extent to which this information is creating a digital risk. These are key pieces to sending out a take-down notice to the hosting platforms.

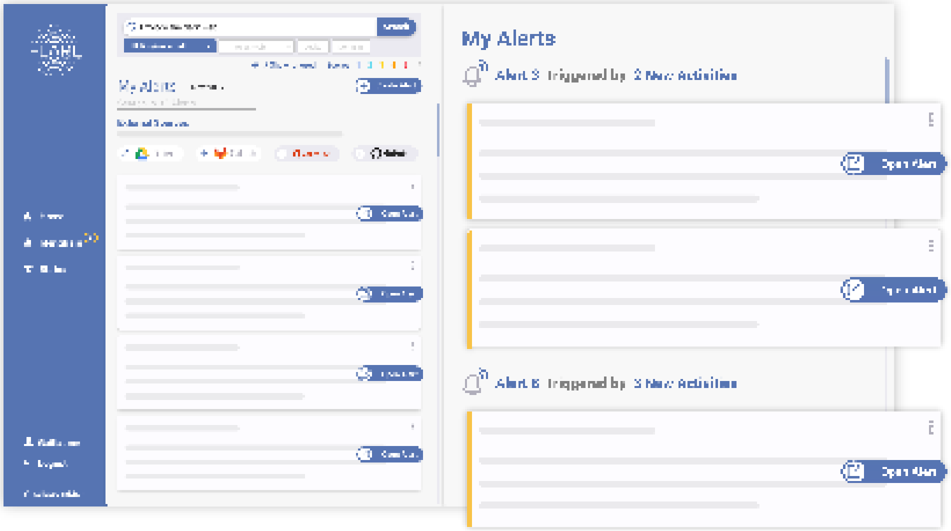
Automatically flag potentially defrauded accounts

Data structuration enables Firework to identify not only the digital risk your company faces (ex. An account was taken over by a malicious actor), but also the account at risk. This empowers you to flag potentially vulnerable accounts, to increase verifications before any transactions are authorized. This process is automated through our APIs to prevent fraud that could happen mere hours after an account becomes vulnerable.

Digital risk remediation is a collaborative task that requires multiple people in your organization. In larger companies, team leaders are likely to assign tasks to their analysts who need to review each alert. A small and large team, a single analyst is unlikely to have the necessary expertise to address all alerts and must collaborate with others within their organization.

Flare Systems enables this collaboration by offering the concept of notes that can be attached to digital risks right on our platform. These notes make it easy for your team members to collaborate with each other and that no digital risk is left behind. They are confidential and can only be accessed by your security team.




FLARE
My Alerts
My Alerts
Alert 3 triggered by 2 New Activities
Open Alert
Open Alert
Alert 6 triggered by 3 New Activities
Open Alert

About Flare Systems

Since 2017, Flare Systems has been developing AI-driven technologies to protect your companies against malicious actors and human errors. Firework offers an easy-to-use platform that gets you the right information before risks become unmanageable. Reduce digital risk and fraud with Firework, the digital risk protection (DRP) platform that automates your dark, deep and clear web monitoring to deliver real-time actionable intelligence.

David Hétu is a co-founder and Chief Research Officer of Flare Systems. David has a Ph.D. in criminology from the Université de Montréal. His main research interest is in online illicit markets and the impact of technology on crime, whether it be from the offenders' point of view or from a regulation point of view. David's research has been published in the highest academic journals (ex. British Medical Journal) and presented at leading conferences (Botconf, HOPE). He is regularly invited to share his analysis of cybercrime in media outlets. David has developed the DATACRYPTO software tool to monitor darknet activities and has co-developed the BitCluster software tool.

Luana Pascu is a cybersecurity writer and researcher at Flare Systems. Luana has a MA in New Media from the University of Amsterdam and a MA in Marketing from the Academy of Economic Studies in Bucharest. For over six years, Luana's work has been focused on discussing cybersecurity, IoT, data privacy and biometric security. Luana is a supporter of women in tech and has a passion for entrepreneurship, technology, and startup culture.

Free Trial

Book a Demo

flare.systems
hello@flare.systems

1751 Rue Richardson, Unit 3.107
Montreal, Quebec, H3K 1G6