flare

WHITE PAPER

Securing Your Organization's Digital Footprint

Securing Your Organization's Digital Footprint in 2022 and Beyond

In the modern age of online connections, organizations rely heavily on digital channels to share, store and communicate information internally and externally.

A worldwide pandemic, a fully remote or hybrid workforce, the rapid acceleration of digital transformation, and the increasing sophistication of cyber-attacks have continued to threaten corporate security landscapes on a global scale. Therefore, navigating ever-evolving cyber risk has become more complex and costly than ever, as it is challenging to have a holistic view of an enterprise's digital footprint.

Table of Contents

1 | The Growing Digital Footprint

Increasing access points to the internet and reliance on the cloud for business operations has resulted in an exponential increase in organizations' digital footprint. A digital footprint is composed of any publicly available asset, service, data, or other exposed element owned by or associated with an organization, whether it's on the dark, deep or clear web.

What is Your Digital Footprint?

An organization's digital footprint is composed of any piece of information that is publicly available on the dark, deep and clear web. This footprint grows without a company's knowledge and leads to data such as personal information, vulnerabilities, intellectual property, technical and business information being disclosed to anyone, including malicious actors. This new facet of an organization quickly becomes part of its attack surface and must be monitored and controlled.

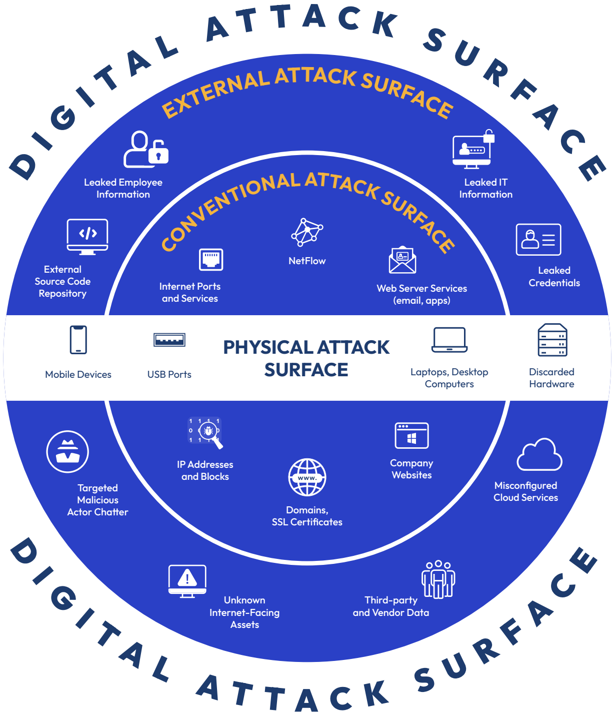
Your digital footprint evolves over time and includes exposed assets that can increase certain business risks for your organization. As your digital footprint rapidly expands, cybercriminals have access to a vast amount of information that they can use when launching increasingly targeted and effective attacks.

Do you know your digital footprint risk exposure?

The Edge of the Traditional Attack Surface

An integrated cybersecurity strategy consists of multiple layers of security to identify, understand, prevent, and mitigate threats posed by cyber risks. The first step in building a comprehensive cybersecurity program is identifying an organization's vulnerable data, risk profile, existing controls, and security landscape. Extensive mapping of this diverse digital footprint helps security teams better understand their attack surfaces and implement a proactive approach to cyber risk remediation.

An attack surface refers to the total number of possible attack vectors (or points) through which an attacker or unauthorized user can gain access to a system and use that access to extract data or insert malicious code.


DIGITAL ATTACK SURFACE
EXTERNAL ATTACK SURFACE
Leaked Employee Information
Leaked IT Information
External Source Code Repository
CONVENTIONAL ATTACK SURFACE
NetFlow
Internet Ports and Services
Web Server Services (email, apps)
Leaked Credentials
Mobile Devices
USB Ports
PHYSICAL ATTACK SURFACE
Laptops, Desktop Computers
Discarded Hardware
Targeted Malicious Actor Chatter
IP Addresses and Blocks
Company Websites
Misconfigured Cloud Services
Domains, SSL Certificates
Unknown Internet-Facing Assets
Third-party and Vendor Data
DIGITAL ATTACK SURFACE

To gain a complete picture of their cyber risk, however, it is essential for companies to go beyond conventional attack surfaces and proactively monitor anonymous sharing sites and source code repositories for external attack vectors, including:

- Leaked IT Information
- Leaked Intellectual Property
- Leaked Employee Information
- Leaked Credentials
- Misconfigured Cloud Services
- Third-Party Vendor Data
- Unknown Internet-Facing Assets
- Targeted Malicious Actor Chatter

By leveraging considerable cybersecurity experience in offensive security and red teaming activities, Flare has developed an Expert System combining AI-drive data collection to monitor an organization's digital footprint and alerts them to risk events in real-time. This allows organizations to get a complete view of their entire attack surface (on-site and in the cloud) and identify their cyber risk weaknesses and exposures. After the overall mapping is complete, organizations can then categorize these findings and reduce the time required to triage. It is imperative that organizations gain insight into and proactively understand and investigate potential threats to defend against all types of cyberattacks.

2 Increasing Visibility

Developing a robust cybersecurity program requires an in-depth understanding of the types of data the organization collects, the amount of data collected, and the network security measures in place. In their role, security teams utilize various threat monitoring and reporting tools to assess risk.

However, these solutions often fall short in terms of providing sufficient visibility and data for internal teams to make well-informed decisions about an organization's cyber risk posture. Nevertheless, many organizations fail to consider the information outside their internal network. Once you have a succinct categorized and prioritized list, a process to automate the dissemination of this information to the appropriate security team members is integral to quickly securing your data and shoring up your organization.

At a high level, an effective threat contextualization process will assist in:

- Building a comprehensive list of the actors involved in the event
- Determining the intent of the parties (malicious or accidental)
- Understanding the sensitivity of the exposed data
- Identifying where the threat has occurred
- Connecting malicious actor behavior across various platforms

The Flare Platform helps companies gain visibility into threats inside and outside of an organization by scanning the dark, deep, and clear web and quickly identifying exposed credentials, account takeover schemes, technical data leaks, and other critical external security threats. This tailored approach to cyber threat intelligence helps SOCs (Security Operations Centers) become more efficient in immediately detecting, prioritizing, and remediating internal and external threats and digital risks.

Cloud Adoption, Shadow IT, and the “Unknown Unknowns”

Cloud-based applications provide powerful and flexible services that allow organizations to make informed decisions, accelerate production and stay competitive. Because the cloud has become so integral to daily business operations, cybersecurity professionals are called upon to authorize, roll out and support cloud-based applications on a regular basis. However, behind these innovative services can lurk a severe threat to your cyber security.

Shadow IT is the acquisition and use of software or hardware without the express approval of IT departments. Most commonly, Shadow IT involves cloud services, including SaaS (software as service) and IaaS (infrastructure as service), but it can also include off-the-shelf packaged software and storage devices.

80%

of workers **admit to using SaaS applications at work**

(G2 Track)

The rise of remote and hybrid workers due to the COVID-19 pandemic has significantly accelerated the adoption of cloud-based applications. Almost overnight, employees worked from home, adopted new cloud services, and used personal devices to accomplish their tasks efficiently. Nearly 80% of workers admit to using SaaS applications at work without prior approval from their IT departments to get their job done. Generally, shadow solutions are implemented by an employee, or a team, with the intent to increase their effectiveness and productivity. For example, if an employee discovers a more efficient and effective file-sharing solution than the officially permitted one, they may begin to use it as shadow IT. As a result, IT and security teams lack visibility and control, introducing new cyber risks for organizations.

While the exposures and challenges associated with pandemic-related remote work and Shadow IT are relatively new developments, Shadow IT of any kind represents a significant risk for any company. Security risks associated with these services are often unknown to employees, leading them to adopt inadequate rights management practices. Unauthorized cloud services may also pose industry violations, resulting in costly investigations, fines, and brand damage. The faster IT departments and security teams are alerted to these threats, the faster they can make educated decisions and mitigate problems as soon as they arise.

In 2002, Donald Rumsfeld introduced the idea of ‘knowns’ and ‘unknowns’ during a DoD briefing, a concept that now regularly appears in discussions centered around cyber intelligence. An ‘unknown unknown’ is a risk that an organization is not currently aware of and does not have the opportunity to mitigate before it has a significant business, financial, or reputational impact.

While IT and security professionals inherently accept a certain level of ‘known’ risk, the goal of every organization should be to identify as many ‘unknown unknowns’ as possible to protect themselves adequately. However, many companies struggle with the sheer volume of information needed to identify, categorize and prioritize threats to make an informed decision. It can take hours to investigate a single warning thoroughly, making cyber risk remediation a daunting task. In the face of escalating cyberattacks and a rise in breach attempts, it is imperative for companies to implement best practices for cyber resiliency, but often, the most dangerous threats lie within an organization.

Human Error and Cyber Risk

Despite existing prevention techniques, many organizations discover that attacks are increasing in number. Malicious actors are constantly evolving their techniques to leverage human error and infiltrate an organization. Recently, IBM conducted a wide-reaching study into cyber breaches. According to the study, human error was the major contributor to 95% of all breaches.

There are several ways in which human error can manifest itself. For example, employees often fail to promptly initiate software security updates or reset passwords, which potentially exposes sensitive data and emails. The misuse of cloud-based applications or the misconfiguration of tools and services meant to enhance productivity and collaboration is also cause for concern among cyber risk professionals.

Unfortunately, a remote workforce, lack of training, or the absence of security best practices, lead to unintended security breaches, which jeopardize your company's security, data, financial, and brand reputation. Skilled cybercriminals understand that security measures are only as effective as the humans who implement them; therefore, the key to an organization's cyber security strategy must include the proactive mitigation of human error.

95% of all data breaches involve **human error**

— **IBM Cyber Security Intelligence Index Report**

Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) is an essential aspect of business strategy for many organizations. Unlike methods where cyber security professionals use data from their internal security systems to build awareness of the threats they face, CTI looks outward, searching for potential threats. In essence, organizations gain visibility into the world of malicious actors, opening a window into who they are, where they operate, and what malicious activity they are executing.

While this data is essential, threat intelligence has limitations. For example, intelligence collection from a vast network will yield a great deal of information that may not pertain to your specific organization and will take an exorbitant amount of time to analyze, making it hard to know the precise and actionable value of the data. To improve the effectiveness of their cyber security strategy, companies must turn unknown threats into identified and mitigated issues through a proper understanding of the threat landscape.

Security Ratings

In the same manner that credit ratings offer a quantitative measurement of a borrower's credit risk, security rating tools provide a quantitative measure of cyber risk - the greater the security rating, the higher the company's security posture.

Security ratings are objective data-driven measurements derived from a verifiable and independent platform that provides an accurate indicator of an organization's cyber security performance. When communicated properly, both IT and non-IT professionals can "speak" the same language about these ratings and how they impact an organization's cyber security strategy.

Unfortunately, analyzing data from numerous tools introduces another challenge in measuring the effectiveness of cyber security performance. For example, for chief security information officers (CISOs) to properly define a strategic security performance management plan, actionable real-time data is needed to determine a proactive strategy. Often, these tools may provide your organization or security teams with feedback that is not actionable and is therefore irrelevant to your security program and its impact on the business as a whole. Without meaningful metrics, companies cannot measure and communicate the effectiveness of their strategy, as they drown in data they cannot contextualize.

The cornerstone of an effective security performance management plan includes identifying, contextualizing, and prioritizing strategic risk-focused metrics in real-time. In addition, articulating the effectiveness to business stakeholders helps demonstrate the security team's integral value within their organization.

Flare actively collects data from illicit platforms that malicious actors use and provides security teams with real-time alerts and intelligence reports prioritized by context and threat level. Prioritization allows security teams to filter out the noise and immediately focus on remediating genuine threats while continuing to monitor the situation. Rapid threat detection combined with effective alert prioritization increases an organization's security posture while creating time and cost efficiencies.

3 | The Main Cyber Risks

Due to rapid digital transformation and the advancing sophistication of hacking techniques, the proactive detection and analysis of cybersecurity threats is a fundamentally challenging landscape to navigate. Attacks often originate and evolve in different patterns and threat levels, differing in complexity, scale, and overall goal. Here, we will discuss the most prevalent cyber risks that organizations face.

Targeted and Non-Targeted Cybercriminal Attacks

When monitoring the dark web in an attempt to identify and protect against cyberattacks, it is essential to consider the two types of attack your organization may face:

Untargeted Attacks

An untargeted attack is a cyberattack that is not specific to an organization. A constant threat for B2B businesses is ransomware attacks, in which cybercriminals hold data hostage for a ransom. This type of malicious attack attempts to modify a system to benefit the attacker and restrict an organization's access to critical data and systems. Examples of this include exploiting unpatched vulnerabilities, social engineering, distributed denial of service attacks, malware, and viruses.

Targeted Attacks

A targeted attack is often far more convincing due to its level of sophistication. For example, in a targeted scam, a malicious actor may probe the firewall defenses of an organization to determine where vital files are stored on the network so that they can launch a devastating ransomware attack.

133,000+
C-Level Executives
of Fortune 1000 Companies

Had credentials on the dark web

22
BILLION
New Records

Were added to the dark web in 2020

– Dark Web Index investigation by Privacy Affairs

According to a recent investigation by Privacy Affairs, secure data from NASA, McDonald's, Visa, MasterCard, Microsoft, and Google was found on the dark web. In addition, the investigation discovered hundreds of data samples containing confidential information being sold at prices ranging from $25-$6,000, depending on the sensitivity of the data.

While most companies are not exposed on the dark web, malicious actors utilize large-scale markets, forums, and chat rooms on the dark web to buy and sell stolen sensitive information and share their attack methods.

Traditionally, dark web monitoring is a function of a threat intelligence program. Yet, apart from a few large enterprises, most companies lack the resources and personnel to implement a fully-fledged threat intelligence operation; and given the volumes of non-organizationally specific data surfaced as previously mentioned, these platforms are cumbersome and do not contain actionable alerts for most organizations. Nevertheless, active monitoring of the dark web is imperative as it aids in the discovery of criminals who have accessed employee accounts as part of account takeover schemes or if your company's financial information is on the dark web.

> Digital Risk Protection (DRP) software protects an organization's digital assets from external threats, improves the efficiency of security teams, and safeguards brand reputation by identifying unwanted exposure in real-time.

To safeguard digital assets from external threats, it's important for organizations to implement a digital risk protection strategy that involves a comprehensive solution to meet the ever-changing needs of your expanding digital footprint. Digital Risk Protection (DRP) software protects an organization's digital assets from external threats, improves the efficiency of security teams, and safeguards brand reputation by identifying unwanted exposure in real-time.

Similar to how Google indexes data, a DRP solution indexes the dark web and other clear web online sources. It looks for links to identify new risks, detect leaked data, and deploys techniques and algorithms to enrich results. This capability enables the prioritization of alerts and remediation for the most severe problems. Information is then stored for security teams to review and implement an action plan.

Dark web monitoring detects ongoing and previous malicious attacks so companies can quickly and efficiently identify constant and previous malicious attacks and prevent threat actors from continuing access to your corporate network. Additionally, by preparing for an attack scenario, a company can protect its reputation and brand and take proactive steps to mitigate threats.

While beginning or enhancing an existing dark web monitoring program may seem overwhelming, Flare's Digital Risk Protection software can improve visibility transparency and reduce mean-time-to-remediation (MTTR) by detecting and prioritizing technical data leaks and remediating digital risks in real-time by continuously monitoring your organization's digital footprint.

Leaked Employee Credentials

According to the 2021 LastPass Psychology of Passwords survey, password reuse across all or most platforms is employees' most significant security error. When asked how frequently respondents reuse the same password (or a variation), 66% responded "always" or "mostly" - an increase of 8% compared to the 2018 survey. Unfortunately, reused passwords are fodder for malicious activity on the dark web.

PASSWORD REUSE is the #1 SECURITY ERROR committed by employees

– 2021 LastPass Psychology of Passwords Survey

66% of respondents **reuse passwords**

8% **increase** from the 2018 survey

It is common for malicious actors to exploit leaked or purchased credentials to gain unauthorized access to online accounts through credential stuffing attacks. For example, they often access large enterprise networks using stolen employee accounts. Upon login, the attacker may make fraudulent purchases and steal personal and financial information. In addition to financial losses, account takeovers harm a company's reputation and brand, causing your customers to lose trust in the digital experience organizations aim to provide.

Regulatory and organizational pressure is increasing on IT departments and business leaders to protect access to corporate resources on a daily basis. Consequently, they can no longer rely on manual and error-prone processes for assigning and tracking user privileges. Implementing an Identity and Access Management (IAM) process will empower IT managers to control user access to critical information within their organizations. Single sign-on systems, multi-factor authentication, and privileged access management are some IAM processes that should be in place within your organization.

These technologies ensure that identity and profile data are securely stored and provide data governance functions that guarantee only relevant and necessary information is shared. In addition, IAM enables granular access control and auditing of all corporate assets, both on-premises and in the cloud, by automating these tasks.

The IAM framework has a growing list of evolving features - such as biometrics, behavior analytics, and artificial intelligence - that are well suited for navigating the ever-changing security environment. IAM's ability to control access to resources in highly distributed and evolving environments is in line with the industry's transition from firewalls to zero-trust models and the security requirements of the Internet of Things (IoT).

Companies can gain numerous competitive advantages by implementing IAM tools and effectively communicating best practices. For example, IAM technologies can secure a business' network across mobile apps, on-premises applications, and SaaS without compromising the security of users outside the organization. The result is enhanced collaboration and productivity, increased efficiency, and reduced operating costs.

Source Code and Intellectual Property Leaks

Developing or working with custom software can expose your organization to the risk of secrets or source code leakage. This exposure can result in sensitive data going to one or more of the 29 million GitHub repositories. In addition, today, many development teams often consist of in-house employees and external third-party contractors. Although this increases productivity and allows organizations to fill talent gaps with part-time workers, it also significantly increases companies' risk of technical data leaks.

It is highly challenging to monitor different development applications for source code, passwords, API keys, and other types of technical leakage. Lack of visibility can also lead to situations where every potential leak is a possible data breach. Therefore, it may be challenging to prioritize data leaks.

Malicious actors frequently scan GitHub environments for secrets, API keys, and other valuable information. Additionally, malicious actors may sell illegally obtained information on the dark web or utilize it to compromise an organization if they discover the leak first. Therefore, companies that rely heavily on customer source code should be concerned.

GitGuardian's recent study on GitHub shows:

2 MILLION
Corporate Secrets

Published on the source code repository in 2020

(Includes passwords and API keys)

20% YOY GROWTH

In the number of private information that caused monetary and data integrity losses

It is common for employees to use organizational assets to participate in open source projects directly. Unfortunately, sensitive metadata is often in the config, build, and log files when these assets commit. As a result, internal usernames, asset names, IP addresses, and domain names are inadvertently made visible during these unintentional data leaks.

Flare's solution automatically scans GitHub and identifies instances in which source code, secrets, API keys, or other leaked sensitive information. This approach can make the process of detecting and remediating technical data leakage more accessible by this approach instead of requiring periodic manual checks. In addition, the functionality provided by Flare is far more robust than the basic search available through GitHub's website or using their API.

First, the software monitors GitHub's live feed for any commits made by an email address matching an identified domain or individual. Then, if secrets are detected, a further investigation is conducted throughout that repository for mentions of a domain or keyword identifier. A real-time alert is issued when both a secret and a relation to an organization are detected.

Customer Account Takeover

Fraudsters are constantly finding new ways to steal customers' financial and personal data; therefore, account takeovers are on the rise, and account takeovers are extremely common. Over sixty percent of account takeover victims reuse their passwords across multiple accounts, which provides attackers with many opportunities to compromise different services. For example, if a customers' account is compromised, they may reuse the same password for their business accounts. This information can be up for sale on the dark web.

287 DAYS

Average time to identify and contain a data breach

$4.87 MILLION

Average cost of a breach with a lifecycle over 200 days

– IBM's 2021 Cost of a Data Breach Report

Account takeover attacks can be among the most damaging types of security risks your organization faces. A compromised account can take weeks or even months to discover, by which point malicious actors may steal data, distribute ransomware, or perform other malicious activities.

The two significant causes of data leaks center around an organization's processes and the personal and financial information relating to employees and customers. As a result of the remote workforce, cloud-based collaborative software usage has increased and malicious actors actively steal this data to resell it on illicit markets for profit. In most cases, security teams do not manage access rights to data, resulting in leaks.

It can be challenging to prevent account takeover attacks. Although many companies have implemented stringent password policies, customers' accounts still face hacking. Even if an organization's customers use highly sophisticated cybersecurity programs and 24/7 monitoring, an unauthorized individual with stolen credentials can still cause a data breach or ransomware attack.

Flare continuously collects leaked credentials from the dark, deep and clear web. As a customer creates an account or resets his password, his new credentials are compared in real-time with those stored in Flare's platform. Upon finding a match, the customer is informed that their credentials are not secure and should change their passwords. As a result, organizations can proactively identify stolen account credentials to prevent ransomware attacks and data breaches. They also gain visibility into their external footprint to see where and when malicious actors sell their data on the dark web. Furthermore, companies can proactively identify stolen customer credentials and information, thus reducing the burden placed on support to help victims of identity theft.

70%

of **all data center outages** can be traced to **human error**

(according to the Uptime Institute)

Infrastructure Exposure and Attack Surface Vulnerability

Companies often have difficulty obtaining a complete picture of their digital footprint and managing their digital assets confidently. Even with the utilization of robust asset mapping and vulnerability management tools, organizations still face the challenge of comprehending what that external view of all cyber threats and data leaks represents.

Malicious actors often access unauthorized areas that hold confidential information, core code, and application infrastructure to commit a cyber attack. A successful malicious intrusion commonly involves sophisticated techniques, including Malware-as-a-Service (MaaS), artificial intelligence (AI), machine learning (ML), and others though they start with a search for application weaknesses.

Today, these intrusions now pose a greater risk as an organization's attack surface is broader than ever before. Consequently, cybercriminals are more likely to exploit vulnerabilities with malicious cyberattacks. Having a clear understanding of where an organization's data ends up when it leaves its infrastructure allows them to gain a complete view of their external data usage. Real-time monitoring of exposed endpoints is critical to an effective cyber risk remediation strategy.

Flare's solution actively and automatically scans for targeted attacks on the deep, dark, and clear web and generates real-time alerts if a company or assets are mentioned, creates a dynamic map of your digital footprint, and uses proprietary technology to cache information from the dark web, providing anonymity as well as allowing you to gather threat intelligence with far less risk than if a security team was actively monitoring the dark web themselves. The platform also offers an AI-based prioritization and scoring platform that enables analysts to spend less time sifting through data and focus on actionable insights.

Database Exposure

Data breaches can be far more reaching than just a temporary issue - they can fundamentally change the course of an organization. Businesses, governments, and individuals alike can experience massive complications from exposed sensitive information. A minor vulnerability can cause a massive data breach without proper attention to detail.

It can be challenging to have a holistic view of an enterprise's entire external attack surface at all times, and many organizations are currently reactive when it comes to responding to cyber threats. Without a proactive threat remediation process, organizations leave their network vulnerable to attacks and the potential for significant legal, financial, and reputational ramifications, often making it challenging to regain customer trust after a breach.

$4.24 MILLION The global average cost of a data breach

$5.33 MILLION The total average cost of a breach for organizations with **over 25,000 employees.**

– IBM's 2021 Cost of a Data Breach Report

In the first nine months of 2021, 281.5 million people were impacted by data breaches, data exposures, and data leaks, more than 90 percent of 2020's total figure of 310.1 million victims, according to the Identity Theft Resource Center (ITRC).

Security teams should implement real-time digital footprint monitoring to detect potential data breaches caused by human error and shadow IT applications. As part of this practice, employees, customers, and intellectual property mentions are visible in real-time. Monitoring your digital footprint will help an organization streamline its investigation, reduce incident costs, and significantly lower the stress and impact of data breaches.

In addition, properly trained employees will understand the importance of a robust/t cyber posture and the dangers of shadow IT, which will help them refrain from using unauthorized applications, even if it is tempting to do so. Data breaches, for example, could be turned into a powerful signal that forces change and prevents shadow IT applications from being used.

Third-Party Data Breaches

When the network of an organization's vendor or business partner is compromised and sensitive data is exposed a third-party data breach occurs. Cybercriminals can attack any vendor in a business's ecosystem, and industry experts estimate that approximately 60 percent of all data breaches occur through third parties. Credit card companies, email service providers, Internet service providers, and cloud providers are considered prime targets.

$4.33 MILLION

Average cost of vulnerabilities in third-party software

– IBM's 2021 Cost of a Data Breach Report

Third-party targeting is one of the common tactics malicious actors utilize to maximize ransomware profit. Despite best practices and extensive security measures, third-party vulnerabilities, business partners, and clients can compromise the security of a business.

Since ransomware groups started targeting third-party vendors, partners, and even regulators, companies have experienced a loss of control over their data. While businesses can request that third parties adhere to specific security standards, these standards are often difficult to enforce and verify before a breach occurs.

The need to share confidential information with partners, vendors, and suppliers, makes third-party attacks challenging to prevent. In doing business, larger companies are more likely to interact with multiple third parties. In addition, due to poor security in third-party networks, large companies are most at risk. Unfortunately, the more famous the company is, the more media attention the breach will be given, as we recently saw with the Microsoft breach in February of 2022.

Another primary concern with a third-party data breach is the leak of confidential information to competitors. A cyber extortionist often threatens to sell fraudulently obtained data to competitors, who would access the data if made public. In several manners, this can affect a company's market position in ways that ransomware has never been able to. The loss of a company's trade secrets, strategies, and client lists is an evolving 21st-century threat to an organizations' value and operations.

The average enterprise works with several hundred partners and third parties, so it isn't a question of "if" data will be exposed, but "when" and how badly a breach will damage a company's reputation. Therefore, companies must continually monitor third parties for potential vulnerabilities to identify actual data that a third-party inadvertently exposed and enable immediate remediation.

51% of organizations have experienced a **data breach caused by a third-party**

— "A Crisis in Third-party Remote Access Security" report from SecureLink

Brand Impersonation

Brand impersonation has become a popular method of online fraud in recent years and is steadfastly becoming extremely problematic. In impersonation, hackers or phishers pose as well-known companies who entice unsuspecting users into providing sensitive information.

The practice of impersonating a brand is a type of cyber-phishing attack that uses the image of a reputable company as a form of communication. A cybercriminal will likely pose as a company that the target would interact with or expect to receive news from regularly. Often the message emphasizes some important call-to-action, such as email password resets, data breaches, and account termination notices, and the victim unknowingly clicks on a malicious link.

Domain Monitoring

Domain monitoring is the process of employing software to identify when domains containing or closely resembling your company names are registered. Most organizations register common variations of their domain (.net, .co, .io), etc. However, thousands of top-level domains are available, and registering them all can be time-consuming and expensive. That is where domain monitoring software comes into play.

Active monitoring of your domain can inform you of targeted attacks before they occur, allowing you to prepare for an intrusion in advance. Taking this proactive step can make the difference between a ransomware attack or a security incident and prevent your organization from losing millions of dollars.

> Flare's platform can identify new or similar domain names that contain information about your organization and potential spear-phishing campaigns, typo-squatting, and other cyberattacks that could cost you time and money.

Flare's software can alert you of new or similar domain names that contain information about your organization. In addition, the process can alert you to potential spear-phishing campaigns, typo-squatting, and other cyberattacks that could cost you time and money.

While organizations could routinely run searches for variations on their domain on ICANN to identify new potential registrations, this manual process is highly time-consuming and prone to error. Flare's platform actively monitors the criminal underground and provides prioritized cyber threat intelligence in real-time. This innovative technology automatically collects and distills large amounts of data from every corner of the dark, deep, and clear web, enabling your cyber security team to detect cyber threats, save mitigation time, and protect your data, financial resources, and brand reputation. Gaining a holistic view of your entire external corporate IT footprint can enable better mean time to respond and reduce the risk of data breaches.

4 | Flare Systems: A Single Lens for Prioritized Threats and Issues

Since 2017, Flare Systems has been developing AI-driven technologies to protect companies against malicious activities and human errors. Our solution analyzes and prioritizes billions of data points to deliver actionable intelligence through its powerful yet easy-to-use platform to automate your company's dark, deep and clear web monitoring to provide you with real-time actionable intelligence.

Digital transformation offers the potential for greater innovation, productivity, operational efficiency, and customer engagement but has also created new vulnerabilities in the enterprise. Therefore, it is vitally important for CISOs and security professionals to make cyber risk a corporate responsibility that requires support and oversight of all employees and the c-suite and should advocate strongly for a shift from reactive to proactive cybersecurity postures by 2022.

With security leaders focusing on mitigating threats now and in the near future, focus should shift on improving the preventative capabilities of the highest growth threat vectors, including cloud security, access management, cloud workload, and hybrid work. In the absence of an active dark-web monitoring program, it is near-impossible to identify whether your company has exposed credentials, financial information, or proprietary information to the dark web for sale. This can result in preventable data breaches, ransomware attacks, and financial fraud.

We invite you to learn more about how Flare's continuous monitoring of an organization's evolving digital footprint and external threats can assist in identifying and remediating threats and potential data leaks in real-time in the following use cases.

CUSTOMER SUCCESS STORIES

5

Successful Risk Mitigation Based on Threat Contextualized Prioritization: Customer Success Stories

Since 2017, Flare Systems has been developing AI-driven technologies to protect companies against malicious activities and human errors. Our solution analyzes and prioritizes billions of data points to deliver actionable intelligence through its powerful yet easy-to-use platform to automate your company's dark, deep and clear web monitoring to provide you with real-time actionable intelligence.

Digital transformation offers the potential for more significant innovation, productivity, operational efficiency, and customer engagement but has also created new vulnerabilities in the enterprise. Companies now have a wealth of information living online, making it difficult to keep track of their digital footprints.

We invite you to learn more about how Flare empowers organizations to take a proactive approach to information security to help stop security incidents before they become breaches, and streamline their internal threat process protocols in the following use cases.

SUCCESS STORY

flare

How Flare Helped a Top North American Investment Firm Prevent a Significant Portfolio Company Breach

Flare's customer, a top North American investment firm that prefers to remain anonymous, explains why they chose Flare and how they prevented a significant portfolio company breach.

The Challenge

Any attack vector has the potential to lead to the loss of large amounts of data for a business. Here, we describe how Flare helped our client manage this digital risk by discovering and alerting the organization to bots for sale on the Genesis platform. This bot contained cookies for a webmail server within the company's internal network. Organizations can benefit from DRP platforms such as Flare not only by monitoring these external risks but also by accelerating remediation efforts and enhancing the efficiency of their cybersecurity teams.

Implementation

Flare platform was used for a red-team mandate, which resulted in raising alerts about a bot for sale on the Genesis platform that contained cookies for a company's internal webmail server, as well as credentials for banking and payment applications.

Impacts and Outcomes

Based on the highly specific subdomain shown in the Genesis listing (webmail.companyname.com), the red teamer had a high level of confidence the infected computer belonged to a company employee. Upon receiving approval from the portfolio company, access to the credential for sale was obtained.

This allowed the red teamer to access the employee's corporate mailbox. An attacker could easily exploit the attachments, personal information, and other documents contained in this email. According to both the investment company and their portfolio company, this infected computer access, which was sold on the Genesis market for about USD$100, could have disastrous effects.

Prioritized Digital Risk Detection

Flare's system returns much-needed bandwidth to security teams and service firms in two ways:

1. First, our research team ensures they are up-to-date on the latest trends, methods, and tools malicious actors use.
2. Second, we add new tools and intel sources into our Flare monitoring and alerting platform. As a result, we can enrich the collected data with our industry-leading prioritization scoring to reduce noise and alert our customers in real-time when data found publicly on the internet could be leveraged by malicious actors.

SUCCESS STORY

flare

Large North American Bank Streamlines Sensitive Data Leaks Monitoring; Cutting Incident Response Costs BY 95%

The Challenge

Threat Intelligence Directors at large banks face various challenges when dealing with threat actors and cybercriminals. For example, various internal errors can lead to the leakage of credentials, API keys, personally identifiable information (PII), and intellectual property. While these risks aren't malicious, they can cause just as much damage as a cyberattack and require proactive mitigation efforts.

The rate at which new data posts to the clear web is rapidly increasing, and accidental or non-malicious leaks come from various data sources. Any leaked data must be promptly collected and contextualized to determine the risk each data leak poses. Noise reduction is essential as these potential leaks come from different sources at different speeds. Collecting these leaks and aggregating them is inadequate; prioritizing them is critical.

Find and remediate potential databreaches proactively

Bringing context to an alert that helps remediate faster

Higher-risk alerts are managed quickly thanks to the unique Flare scoring system

Implementation

The Cyber Threat Intelligence (CTI) team tested multiple monitoring solutions to enhance monitoring and response capabilities; however, the noise and false positives burden many tools. Flare's solution is the only platform to combine state-of-the-art data collection with a noise-reducing prioritization engine. This feature empowers our client with the necessary context to classify each data leak's criticality level without excessive hours of work.

Armed with a comprehensive data collection and prioritization alert system in place, the CTI team now uses their newly gained bandwidth to optimize downstream processes of incident response. Using the platform and its scoring system, the CTI team developed a powerful strategy that allows them to handle higher-risk alerts promptly, and clear guidelines for different types of data leaks are in place. As a result of this new efficiency and insight, managers and employees are made aware of the situation and any remediation actions.

Impacts and Outcomes

Cost-effectiveness: 95% Cost Reduction Per Incident

The CTI team was able to operationalize and proactively deal with technical data leaks through the combination of the platform and the newly built processes, resulting in a 95% cost reduction per incident. As a result, there is no need for a war room. It is sufficient in most cases for the CISO to receive updates in weekly briefings about remediation actions taken. Still, their active involvement is not necessary unless a very-high-risk leak is immediately detected.

Proactive Remediation

Rather than responding to leaks reactively, the CTI team became more proactive. For example, during a recent investigation, Flare identified sensitive data posted by a previous employee. CTI promptly identified and notified the superior of the ex-employee, who contacted the individual concerned to request the removal of the article. Within thirty minutes of the Flare alert, the leaked content was removed from GitHub. Overall, team morale improved, and the client achieved remediation without significant overhead.

Internal Security Processes Improvement

In addition, it became apparent that external consultants were among the major contributors to public technical leaks at the end of a mandate. As a result, the CTI team has since established internal initiatives to upgrade consultants' security records.

Increased Detection, Greater Protection

Currently, the CTI team at the bank works with Flare to identify complex data leaks that, even for domain experts, can be tough to detect. For example, Flare enables the bank to remediate issues such as API key leakage in a code file where the organization's domain name is not even present. Some of these have been integrated into the solution's monitoring system, increasing the number of findings while reducing unnecessary noise.

> Whereas other solutions would present us with thousands of potential leaks which were impossible to work with for our small team, Flare was the only one that could successfully filter and prioritize data leaks with their 5-point scoring system.
>
> — CTI Director

SUCCESS STORY

flare

North American Security Service Provider Reduces Dark Web Investigation Time by 10x and Unlocks New Revenue Streams

Flare's client, a leading Managed Security Service Provider (MSSP) who offers risk assessment, penetration testing, incident response, post-breach remediation support, and ongoing posture monitoring, sees success in streamlined dark web investigations.

The Challenge

The majority of managed security service providers strive to expand their services for their clients. An example of a service that MSSPs may provide is monitoring of the dark web. However, MSSPs face two main challenges:

Dark Web Monitoring Requires Additional Knowledge

Security professionals in the field often lack sufficient knowledge of the dark web to keep up with the pace at which new dark web sources appear. Therefore, a lack of experience regarding dark web monitoring in the cybersecurity sector persists.

Dark Web Monitoring Takes Time MSSP

Those MSSP employees with dark web monitoring experience face an additional challenge when monitoring the dark web. Manually creating accounts (that often get banned), paying fees in Bitcoin for access to some sites, and using deprecated search bars take a long time. In addition, various other factors make the economics of offering this service challenging to justify.

Implementation

Since Flare's inception, our team has taken dark web monitoring very seriously. As part of our dark web monitoring method, we use three complementary components to ensure our data is accurate, up-to-date, and stays current with new dark web platforms:

1. **Our threat hunting and research team follow trends and news about illicit websites.**
2. **Our technical experts provide new data sources for our collection engine.**
3. **Our automated collection engine crawls every source every day, saves the results in our local databases, and archives dark web posts and platforms.**

Using our three-factor approach, customers can easily query any data they need to make better-informed decisions regarding their security posture.

In only a few days of using Flare's solution, a senior penetration tester realized the value Flare could bring to his organization. Flare was chosen by this customer after he utilized competing products for six months without finding much actionable information. It took just two weeks for Flare to uncover high fidelity and actionable findings for this client.

> *Firework allows me to empower junior analysts to do dark web investigations that were previously impossible, hence liberating bandwidth.*
>
> *— Senior security specialist, North American MSSP*

Impacts and Outcomes

Time Efficiency and Greater Coverage

In addition to saving time due to alert prioritization, the senior penetration tester expanded his coverage to more relevant areas of the dark web. In addition, the client has reported a significant reduction in time, as they can now complete in one week, which previously took 1500 hours.

Dark Web Monitoring Skills Improvement

The ease of use of Flare made it possible for team members with close to no knowledge of the dark web to handle the initial data discovery process and upskill the team on dark web monitoring processes. In addition, the senior penetration tester and his team had more resources to support dark web investigation projects, allowing them to offer dark web assessments and monitoring to more customers, generating more revenue

6 | The Future of Cyber Risks

Business leaders have placed a high priority on cyber security for many years. However, cyber-attacks continue to occur despite investments in security controls. We have seen a monumental change in how we interact with technology and how it affects our everyday lives over the past few years. With the rapid digitalization of technology, our work and personal lives have become more connected, and we face a new set of global challenges.

Threat Remediation in 2022 and Beyond

Cybercriminals have taken advantage of the changing world we live in since the outbreak of the global pandemic in 2020. There is no better illustration of this than the SolarWinds hack, described by Microsoft president Brad Smith as the most sophisticated hack in history, whose effects have been felt throughout 2021 and into 2022.

Unfortunately, cyberattacks are on the rise, and IT professionals and security professionals must be alert as never before. At Flare, we focus on how the ever-evolving and expanding digital footprint of an organization provides an increasing attack surface, and the need for contextualized monitoring to provide real-time cyber risk assessments. During our interactions with customers, conversations with industry professionals, and discussions with our experts, we continuously learn new findings of the current state of cybersecurity.

About Flare Systems

Since 2017, Flare Systems has been developing AI-driven technologies to protect your companies against malicious actors and human errors. Flare 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.

www.flare.systems

hello@flare.systems

1751 Rue Richardson, Unit 3.107
Montreal, Quebec, H3K 1G61

Free Trial

Book a Demo

flare