ActiveFence Recognized for

2021

Technology Innovation Leadership

European
Online Trust and Safety Industry
Excellence in Best Practices

FROST & SULLIVAN

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. ActiveFence excels in many of the criteria in the Online Trust & Safety space.

The Internet is an Unregulated, Unsafe, and Unhealthy Place

Throughout the years, as digitalization picked up steam, governments, companies, and the general public have become increasingly reliant on the internet for the most basic activities. The internet today is as essential to the socioeconomic fabric of the world as is electricity. It is intricately intertwined with the social, cultural, and political outlook of society. Platforms, such as social media, content sharing webpages, and news outlets on the internet have a direct and fundamental impact on the evolving ideologies and situations unfolding on the ground across the globe in real time. Criminal and anti-social elements and groups have established a strong foothold on the internet to execute sophisticated and targeted campaigns that defraud individuals and companies, and can impact political revolutions and elections. The vastness of the internet and its globally distributed nature makes it incredibly difficult for authorities and website content moderation teams to police it. Thus, rampant abuse of the internet for activities such as terrorism, misinformation campaigns, child abuse, and financial fraud has been growing unchecked at an alarming rate with a lack of mechanisms to tackle this growth at scale.

The process of maintaining online integrity has several aspects to it, including but not limited to identifying bad actors, categorizing and taking down problematic content, and blocking known violators from using online platforms. However, there are several challenges in the process of maintaining online integrity:

Scale: The internet is a vast space with petabytes of content being generated by users every minute. A thorough review of content being uploaded on every platform is humanly impossible, leading to the implementation of automated review systems by platforms. Automated classifier systems need to be trained on multiple languages, and when human analysts are employed to review problematic content, they need to be trained to understand the regional and cultural nuances of the content they are dealing with.

Access & Identification: While leading social media and content sharing platforms, such as Facebook, Twitter, and YouTube have well-defined policies to identify malicious content and provide access to third parties to monitor chatter on their platform, they are just the tip of the iceberg when it comes to online threats and abuse. Platforms in the dark/deep web, underground messaging forums, and marketplaces constitute the underbelly of the internet that is incredibly hard to find and access.

Contextual Nuances: Recent years have seen heavy usage of internet platforms for the spread of hate speech, disinformation, violence and child abuse material among other online harms. Such content on the internet has played an undeniable and significant role in stoking sectarian violence and has aided political extremism across the globe among other problems. Urgent as it may be, fighting hate speech, disinformation, extremism and other abusive content is difficult as it requires the understanding of ideologies and cultural nuances, which are unique to demographics, geographies, and cultures, and is very tough for an algorithm or an automated classifier system to acquire.

Privacy & Legal Restrictions: Content platforms on the internet, by design, have very few entry barriers and fewer mechanisms to verify the identity of a user, thus making anonymity easy. Crime committed on the internet and other malicious activity often falls into a legal grey zone in a number of countries which tips the risk-reward balance in favor of criminals and bad actors. Lastly, even if identified, cases of hate speech, disinformation, extremism and other types of harmful content often fall in odds with free speech, crippling the enforcement mechanism deployed against it.

Free Speech vs. Content Guidelines: Policing content on the internet often leads to a debate between free speech and content policies. What is deemed by a platform as malicious or harmful might also be seen as an expression of free speech by a content creator and the larger user base. Platforms walk the fine line between ensuring a good and open user experience and removing harmful or malicious content.

The above list of challenges is not exhaustive when it comes to fighting online crime, but it shows that a lot more work needs to be done to make the internet a safe place and internet giants are clearly falling short of their responsibilities. The biggest victims of an unsafe internet are governments, corporations, and society at large. A successful trust and safety strategy needs to incorporate a highly nuanced understanding of numerous languages, cultural sensitivities, and complex geopolitical realities. Without significant expertise and strong tools that enable analysts to put their expertise to use; platforms will always be playing catch-up in the race to make the internet a safe place for everyone. There is a clear and urgent need for innovation in this space to fight the vices of the internet.

Commitment to Innovation and Creativity

ActiveFence is at the forefront of the battle for online integrity, trust, and safety on the internet. The company is involved in identifying malicious content and threat actors from across the internet, orchestrating the workflow of Trust & Safety teams and plays an active and instrumental role in helping organizations understand and control their exposure to malicious actors and activities. Realizing the inadequacies of current methods of fighting online threats, ActiveFence empowers a proactive approach to addressing these challenges, and has designed its platform to monitor online chatter and detect threats in their early phases, allowing potential victims to react well in advance and limit the damage.

> *"Faced with a formidable adversary, organizations found ActiveFence to be the most potent weapon in their arsenal that helped them penetrate the illusive world of cybercrime."*
>
> ***- Hiten Shah, Senior Analyst, TechVision***

ActiveFence has been working with a number of reputed organizations from the fields of social media, audio and video streaming, file sharing, and gaming in addition to consumer brands. All of these organizations face increasingly targeted and sophisticated attacks, perpetuated by attackers that are well-funded and organized with clear objectives and strategies to achieve them. Faced with a formidable and constantly innovating adversary, organizations found ActiveFence to be the most potent weapon in their arsenal that helped them penetrate the illusive world of malicious online activities. ActiveFence's AI-based solutions help provide visibility into a number of threat categories and identify the activities that need to be monitored or acted against immediately.

ActiveFence differentiated itself from the competition by both providing a complete Trust & Safety management platform and accurate content detection APIs powered by understanding the most hard-to-reach platforms that are leveraged by bad actors to plan their campaigns and to connect with other bad actors to undertake coordinated attacks. With AI that supports a robust team of intelligence analysts and domain experts, ActiveFence analyzes sources on the dark web, deep web, and in underground messaging forums to identify malicious activities and actors at the source, before they reach the mainstream internet and damage their targets. The company continuously trains its algorithms to match the policies of its clients, while adapting to ever-changing regulatory requirements, platform growth challenges, new trends, and evasion techniques of bad actors found across ActiveFence's 10 million sources of chatter, in order to stay ahead of problems before they arise. The ActiveFence platform and threat experts maintain a vigilant watch- in areas such as terrorist activities, child abuse, hate speech, and disinformation, among others- providing clients with a curated set of accurate insights. ActiveFence works across numerous languages and formats to connect the dots from various data points across sources to build a comprehensive picture of an evolving threat.

Most large organizations deploy an internal trust and safety team responsible for identifying and taking action against malicious on-platform activities. These teams usually leverage basic algorithm-based classifiers to identify malicious content based on a specific set of keywords or their combinations. Some companies that deal with high volumes of diverse content employ teams of moderators that manually validate and moderate content to determine compliance and flag malicious creators. With these approaches, the nuances and the historical or supporting context tends to get missed as pieces of

content are analyzed in isolation. To create a context-aware content moderation system, ActiveFence takes a cross-platform approach, establishing its presence at the source of malicious activities where it analyzes millions of signals, behaviors and trends from across the open, deep, and dark web to establish a comprehensive birds-eye view. In essence, most large-scale targeted campaigns related to hate speech, right wing extremism, or election influence are planned on fringe online or dark web forums before they appear on mainstream social media websites or any other surface website. Understanding such grassroot sources allows ActiveFence to track a threat as it evolves and matures to help victim organizations and companies plan and execute their actions at the right time and phase using the most appropriate method to take down not only a piece of content, but possibly the group of individuals responsible for creating and spreading it. To make such a feat possible, ActiveFence has developed an ever-evolving database that captures malicious activities on the internet. The database curated by ActiveFence captures information, such as URLs, keywords, images, behaviors, and more related to underground actors and communities.

Overall, Frost & Sullivan thinks that ActiveFence can provide its clients with an insider look at how harmful content, bad underground actors, and criminals function, along with an ability to pre-empt organized attacks and targeted campaigns. ActiveFence had a game-changing effect on how organizations deal with online safety. As defensive strategies against online malicious activities show their limitations, ActiveFence is the first step toward a proactive approach that many organizations are now adopting against online abuse.

Application Diversity & Commercialization Success

ActiveFence has developed one of the most robust and insightful databases of activities and actors in the world of malicious content detection to enable proactive action. However, signal collection is only the first piece of the puzzle. The effectiveness of ActiveFence's platform also stems from its ability to combine advanced AI technology with verifiable human intelligence to deliver insights in real time, in the format of choice to a diverse audience, customized to the policies and growth challenges of technology platforms. The company is involved with some of the largest user-generated content distributors and social media companies that have unanimously elevated content moderation to one of their top priorities.

Intelligence from ActiveFence can be configured by trust and safety teams as per their specific job roles and interest areas, after which the platform delivers curated risk and relevance scored feeds to the user with the required context to help ascertain the right counteraction. In addition, ActiveFence also built an API interface that helps clients integrate its feed into their internal review and moderation system. Throughout the years, ActiveFence has built a strong team of experienced individuals from the wider intelligence and technology world that helped them gain a firsthand view of how cross-border crime and malicious activity functions in the underground internet world. Leveraging their expertise and knowledge, ActiveFence has performed focused

> *"ActiveFence differentiated itself from the competition by developing a presence on the most hard-to-reach platforms that are leveraged by bad actors to plan their campaigns and to connect with other bad actors to undertake coordinated attacks."*
>
> ***- Hiten Shah, Senior Analyst, TechVision***

investigations and carried out extensive projects to help its clients deal with the spread of malicious activities on their platforms, or in the general internet arena.

ActiveFence has gained the praise of its clients through its noteworthy approach of enabling each of its clients to operate their own tailor-made solution, which has allowed trust and safety teams to keep up with the complexities and pace of content moderation. ActiveFence has been able to accomplish this by building adaptable algorithms that account for the nuances of the client's platform. These algorithms are enriched further with insights generated by ActiveFence's team of analysts with deep domain expertise. These insights are further enriched by cross-referencing with ActiveFence's proprietary database of open/dark/deep web activities. Collectively, the entire approach comes together to ensure that trust and safety team have the best possible tool at their hand to keep their platform free of harmful content.

In a specific instance, one of the world's largest UGC websites sought help from ActiveFence to deal with the spread of content related to terrorism on its platform. Using its robust database and systems, ActiveFence could identify and monitor the source of terrorist chatter and this information was further leveraged by the UGC platform to take down thousands of malicious content items and the accounts responsible for their spread. Similarly, ActiveFence helped companies in combating disinformation on their platforms or stopping the spread of child sexual abuse materials (CSAM) on their websites.

The robust backend technology stack of ActiveFence's current portfolio can support a wide range of use cases and applications, allowing the company to add multiple features and functionalities to their platform as per client feedback and demand. Frost & Sullivan thinks that ActiveFence has the potential to bring a transformational change in how organizations deal with harmful content, at scale.

Human Capital and Financial Performance

ActiveFence's work in the areas of terrorism, child abuse, and hate speech brings it close to individual criminals, criminal groups, and even state-sponsored cyber-offensive programs. Effectively understanding their strategies and uncovering their identities requires a nuanced understanding of global political and ideological trends, and how underground criminal networks and their finances function. ActiveFence is uniquely positioned to handle the intricacies of harmful content detection with an experienced team of analysts that have served in intelligence, technology or related fields in the past. Noam Schwartz, co-founder and CEO of ActiveFence, previously served as an intelligence analyst for the Israel Defense Forces, and was a co-founder of TapDog, which was involved in competitive intelligence based on data analytics. The founding team also has Eyal Dykan, who currently serves as the president of ActiveFence who was the head of several intelligence units for the Military Intelligence Directorate of the Israel Defense Forces. The founding team also includes Iftach Orr and Alon Porat, who serve as CTO and CPO, respectively. While Iftach was involved with scaling a number of start-ups on the technical front, Alon was on the product management side for a number of start-ups prior to ActiveFence.

At present, ActiveFence has a team of about 250 employees in six offices, globally. With a rapidly expanding client base, ActiveFence focused on onboarding a strong team of intelligence and technical experts that allowed the company to expand its expertise across a wide range of abuse areas.

The company acquired a total funding of $100 million from leading investors, including CRV, Highland Europe, Grove Ventures, Norwest Venture Partners, Vintage Investment Partners, and Resolute Ventures, among others.

Conclusion

The internet is a vast, unchartered territory with limited oversight and control, even for social media companies and user-generated content platforms that facilitate the exchange of ideas and connect individuals globally. Increasingly, the spread of malicious content, including terror, hate speech, child abuse, and disinformation on the internet has led to worrying consequences in the real world. Organizations, economies, and countries have been facing real-world consequences of malicious activities on the internet.

ActiveFence understood the shortcomings of current trust and safety strategies employed by organizations globally, and designed a platform that combats malicious content and activity at its grassroots, enabling organizations to detect, identify, and classify harmful content and individuals at an early stage, and undertake steps to neutralize them before they can reach the surface web and influence mass audiences.

With its strong overall performance, ActiveFence earns Frost & Sullivan's 2021 European Technology Innovation Leadership Award in the online trust and safety industry.

What You Need to Know about the Technology Innovation Leadership Recognition

Frost & Sullivan's Technology Innovation Leadership Award recognizes the company that has introduced the best underlying technology for achieving remarkable product and customer success while driving future business value.

Best Practices Award Analysis

For the Technology Innovation Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization Success: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

Business Impact

Financial Performance: Strong overall financial performance is achieved in terms of revenues, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Commitment to quality and to customers characterize the company culture, which in turn enhances employee morale and retention

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Engine™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fueled by the Innovation Generator™.
[Learn more.]

Key Impacts:

- **Growth Pipeline:** *Continuous Flow of Growth Opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*

The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- Mega Trend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)