RSA FraudAction 360

About RSA FraudAction

RSA FraudAction offers its customers a holistic, all-encompassing solution for external threat management and brand protection. In addition to proactive detection and mitigation of a wide array of online threats such as phishing, Trojans and brand abuse, customers also gain deep insight into emerging internal and external threats via a broad range of intelligence reports and data feeds that provide deep visibility into the cybercrime landscape.

With an all-encompassing service, organizations can deploy fewer in-house resources to manage external threats, obtain full fraud protection without leaving any threat vector uncovered and manage only one vendor budget for 24/7 anti-fraud operations.

FraudAction caters to hundreds of global customers, diverse in size and sector, including many of the top fortune 500 companies. To support the different needs of each organization, FraudAction offers flexible subscriptions that can be customized based on attack volumes and areas of interest.

The Operations

Anti-Fraud Command Center

At the heart of RSA FraudAction lies the Anti-Fraud Command Center (AFCC), a 24x7x365 operation that is staffed by over 100 highly skilled researchers, in two global centers, analyzing tens of millions of potential threats every day to protect millions of end-users around the world.

With thousands of cyber-attacks occurring every single day, and more on the way, automation is key to keeping up. The RSA AFCC incorporates a multitude of diverse, internally developed automation programs and tools that are invaluable in helping shut down cyber-attacks fast.

You can’t fight cybercrime alone. It requires coordination and cooperation with internet hosting facilities, law-enforcement authorities and other entities around the world. Cultivating those relationships takes time, and that’s why experience counts for so much.
Since launching the first anti-Phishing service in the industry back in 2004, The AFCC has established long-standing relationships with over 16,000 different internet authorities. These connections and experience combined with extensive multi-lingual capabilities, enable the quick takedown of fraudulent sites anywhere on the globe.

Worldwide coverage and support for all languages is essential in a time when cybercrime is everywhere. Not only that, but threats can start in one part of the world and move quickly to another, making a seamless global presence imperative to responding effectively.

Finally, Threats are constantly emerging and quickly evolving. The AFCC is extremely agile and able to adapt just as fast—adopting new methodologies and techniques to root out threats and avoiding cumbersome processes and procedures that slow things down.

**Intelligence Operations**

RSA FraudAction’s Intelligence operation is built on a strong foundation of proprietary monitoring mechanisms as well as a dedicated team of highly skilled researchers.

Passive and active monitoring of fraudulent activity are conducted on a wide range of communication channels where cybercriminals congregate to trade compromised data, Fraud as a Service (FaaS) offerings, tools and knowledge.

Our researchers leverage multilingual expertise and years of underground presence to conduct deep investigations, cross reference analysis and fraudster interrogations. They have also been “grandfathered” into forums as trusted players, including some of the exclusive forums which are considered by cybercriminals to be more secure exchange platforms.

Since cybercriminals are always on the move, extending their activity and exposure to new venues, our researchers are not only keeping track of known communication channels but also constantly identifying new ones on the go. Ensuring maximal visibility and footprint are critical to the team’s mission of serving as our customers’ eyes, ears and mouth within fraudster communities.

**Engagement Managers**

Once subscribing to FraudAction, customers are assigned a dedicated engagement manager to oversee the account throughout the entire service lifecycle and serve as a trusted advisor.

The engagement management team plays a crucial role in the onboarding process and ongoing utilization of the FraudAction services, maximizing service level and customer experience. Working cross-functionally with all internal operational and technical teams, they not only help customers resolve their most pressing challenges, but also anticipate new ones.
Cybersecurity is a business, sure, but it’s not just any business. It’s a business where people are responsible for protecting others from potentially catastrophic cyber events—and we take that responsibility very seriously.

**FraudAction Dashboard**

The FraudAction Dashboard is geared to provide a single-pane-of-glass experience, allowing our customers to assess and manage their external-facing risks.

The portal is synchronized with the Anti-Fraud Command Center (AFCC) and updated in real-time as attacks are handled, providing an overview of recent and current fraud activity targeting your organization and industry.

Customers can easily drill down on information through advanced search tabs as well as view trends displayed via a wide range of graphic widgets.

**FraudAction Dashboard API**

The dashboard also offers API (Application Programming Interface) access, allowing your organization to integrate back-office applications (such as SIEMs) directly with the FraudAction Dashboard to automatically pull data into your systems.

**FraudAction 360 Service**

In order to holistically protect an organization’s online presence, FraudAction covers a wide range of cyber threats causing damage to the brand as well as fraud losses. Cyber-threat and brand monitoring are an essential prerequisite for an all-encompassing mitigation strategy.
Cyber Threat & Brand Monitoring

Domain Registration

FraudAction’s domain monitoring provides real-time alerts on newly registered or newly updated domains that potentially pose a risk to your organization.

Our proprietary monitoring system features a self-learning risk engine, scoring each domain based on a wide range of parameters indicating similarity to customers’ legitimate domains. This is highly efficient as an early-detection method and provides protection also against advanced threats utilizing Typo squatting and Punycode.

Monitoring newly registered domains is highly efficient as an early-detection method to warn our customers against domain registrations by cybercriminals.

SSL Registration

FraudAction’s SSL monitoring provides real-time alerts on domains and sub-domains associated to newly registered or newly updated SSL certificates that potentially pose a risk to your organization.

Our proprietary monitoring system features a self-learning risk engine, scoring each domain and sub-domain based on a wide range of parameters indicating similarity to customers’ legitimate domains.

Monitoring newly registered and newly updated SSLs is highly efficient as an early-detection method to warn our customers against SSL certificate registration by cybercriminals.

Mobile App Stores

FraudAction’s mobile app store monitoring alerts on apps available in app markets that are utilizing our customers’ brand names.

FraudAction has developed a proprietary web-crawling mechanism that continuously scans the major official app stores as well as tens of unofficial alternative stores.

Monitoring mobile app stores grants organizations visibility into their mobile presence and allows them to stay ahead of potential damage caused by unauthorized and unsupervised apps.

Social Media

FraudAction’s social media monitoring alerts on pages and accounts on social media platforms that are utilizing our customers’ brand names.

FraudAction has developed a proprietary web-crawling mechanism that continuously scans the major social media platforms, including Facebook, LinkedIn, Instagram and Twitter.

Monitoring social media platforms grants organizations visibility into their social media presence and helps them stay ahead of potential damage.
caused by unauthorized and unsupervised pages or accounts misrepresenting their organization.

**Malware**

FraudAction monitors the web for “Bankers”, malicious software unknowingly installed on computers with the purpose of stealing end-user information.

Malware infected machines are computed to send harvested data to the Cybercriminal’s server, specifically referred to as the malware’s drop point. These drops are continuously monitored by FraudAction to recover compromised credentials belonging to an organization’s end-users and employees.

**Phishing**

FraudAction monitors the web for phishing sites, websites mimicking our customers’ legitimate site attempting to dishonestly acquire sensitive personal information from end-users.

Sub-categories related to this fraud method include Smishing, phishing URLs spread via SMS, and Vishing, the collection of sensitive personal information from end-users over the phone.

**Email Scams**

FraudAction monitors the web for a wide range of email scams including advance-fee fraud (also known as the 419 scam or Nigerian scam) and CEO fraud which involves the use of tailored and targeted emails designed to steal sensitive personal information from end-users.

**Mitigation Process**

**Detection**

FraudAction utilizes a large network of global detection partners comprised of organizations in several technology areas, including consumer antivirus firms, email security companies and internet gateways. In addition, FraudAction uses proprietary technology to monitor external resources as well as the customer’s environment. Many of these methods not only significantly enhance visibility but are specifically geared to achieve early detection of Phishing attacks before they are launched by Cybercriminals.

**Abuse Mailbox**

Most organizations provide a dedicated email address known as an Abuse Mailbox that enables their customers to report suspicious emails.

FraudAction offers 24/7 monitoring of our customer’s Abuse Mailbox in order to quickly detect and act against attacks reported by their end users.
Web Logs

FraudAction web logs monitoring is a simple and effective method designed to enhance phishing detection.

Web logs are access logs that in most cases are automatically generated by web servers and they keep records of the different events the server handles.

Most phishing attacks interact with the legitimate website and these references and redirections are recorded in the web server log files; the most pertinent information in this use case is the referrer URL. The referrer URL is the address of the website that referred the visitor to your site.

FraudAction offers 24/7 monitoring of our customer's web logs in order to quickly detect and act against phishing attacks.

E-pixel

FraudAction ePixel monitoring is a simple and effective method designed to enhance phishing detection, also known as digital watermarking.

Cybercriminals who create phishing kits often use automated tools to "rip" an organization's legitimate web page to create up-to-date looking phishing attacks to easily trick victims. In addition, Cybercriminals often end an attack by redirecting victims to the legitimate site using the original links from the copied pages. With the covertly embedded ePixel code on the legitimate page, Cybercriminals unknowingly copy it into their attack pages, creating a trail that will ultimately reveal the web location of the phishing page targeting your brand(s). The invisible, watermark-like detection code connects to a dedicated server in real-time and provides FraudAction with details regarding the web location of the embedded code and the referrer URL of HTTP requests.

Qualification

FraudAction performs both automated heuristic and manual qualification of hundreds of millions of suspicious resources a day. URLs are first run through proprietary risk engine and are scored based on multiple parameters. URLs that pass the risk threshold are sent to human analysts for manual qualification.

FraudAction is committed to the highest level of accuracy when it comes to the qualification of an attack. We are obligated not only to our customers, but also the partners with whom we collaborate, to a negligible percent of false positives. As such, AFCC analysts abide by a strict qualification procedure, which includes verifications such as comparing to a customer’s whitelist, Whois lookup, examination of SSL certificate details and more.

Blocking

Exposure to a Phishing site directly impacts fraud losses, which makes blocking a crucial part of our mitigation strategy. As such, the AFCC acts immediately to distribute qualified Phishing URLs to FraudAction blocking partners.
Blocking is typically implemented within the hour, depending on the partner itself, ensuring that hundreds of millions of online users are prevented from accessing confirmed Phishing sites until they are completely removed.

More on FraudAction’s blocking Network:

FraudAction has established one of the largest Global Blocking Networks in the industry. Our network integrates with Google’s Safe Browsing Platform and Microsoft’s Windows Services Safety Platform amongst others, providing an immediate first line of defense for 96% of the world’s browser traffic. As a result, end-users surfing through any of the major browsers (Internet Explorer, Chrome, Firefox, or Safari), will be presented with a blocking warning, which is also supported on mobile devices. FraudAction’s blocking network also includes leading security vendors and local ISPs.

Takedown

The AFCC leverages its long-standing relationships with over 16,000 different internet authorities and its multi-lingual capabilities to enable the quick takedown of fraudulent sites anywhere on the globe.

To ensure best results the AFCC has established the following approach:

**Takedown is commenced immediately upon attack qualification**

Thanks to the expertise of the AFCC analysts and their manual qualification of each attack, further qualification from customer is not required and there is no hold up in the takedown process.

It is important to mention that the AFCC does request customer approval before acting on brand abuse cases. This is a crucial layer of verification to assure that no measures are taken against legitimate third-party affiliates.
Take down is commenced on each resource related to an attack
Attacks are analyzed to identify additional resources including redirections, frames, and drop points. The AFCC commences takedown on each of the resources involved in an attack.

All hosting authorities related to an attack are contacted
Attacks are analyzed to determine all the involved authorities: ISP, webhosting, registrar, registrant, hijacked website owner, etc. As part of the takedown process, each authority is contacted separately.

Follow-up is conducted with the relevant authorities
In addition to initial takedown request, follow-ups are conducted via email, instant messaging and phone calls. In cases of noncooperative hosting authorities, the AFCC also reaches out to the local CERT or Cyber Police.

Multi-lingual communication
Communication with the authorities, including C&D letters and follow-up calls, is conducted in the local language to convey a clear message and optimize results.

Forensic Analysis
AFCC analysts use several methods to reveal Phishing kits and decrypt the information they contain. Analysis of the kit may reveal valuable information about an attack such as the drop email used by the Cybercriminals to collect compromised credentials, and the actual compromised credentials.

In addition, Trojan samples undergo dynamic and static analysis to uncover triggers, communication points, and other information including the Trojan's modus operandi on an infected system.

All forensic data gathered from an attack is uploaded to the FraudAction dashboard and may be used by fraud teams to conduct additional investigations.