OUTSEER
An RSA Company

Outseer™ FraudAction

Protect your brand and your customers with our 24/7 fraud intelligence and cyberattack takedown service

As businesses embrace digital transformation, they face increasingly sophisticated cyberattacks. Outseer FraudAction™ continuously monitors the threat landscape to give you unprecedented visibility into external threats targeting your company or impersonating your brand. Our industry-leading takedown service rapidly shuts down the phishing and malware sites, rogue mobile apps, and fraudulent social media pages used to launch these attacks.

At a Glance

- 24/7 end-to-end visibility and protection against phishing, Trojans, rogue mobile apps and social media pages
- Detailed attack reports via a cloud-based dashboard or API integration
- Intelligence reports and feeds on the latest online threats and fraud trends
- No integration required; simple and quick setup process

According to the FBI, cybercrime rose an astonishing 69% in 2020, accounting for more than $4.2 billion in direct financial losses in the US alone. Phishing-based brand impersonation is the primary driver in more than half of all cybercrime losses.

These scams hijack your brand identity and reputation to fool your employees or customers into paying money or inadvertently revealing login credentials and other sensitive information.

What's more, cybercriminal organizations are becoming more sophisticated by the day. In addition to phishing, a growing number of attacks involve fraudulent social media pages and malicious mobile apps distributed by trusted app stores. The good news: As fraudsters adapt their tactics, so do we.

24/7

Anti-Fraud Command Center led by our detection automation and multilingual cybercrime experts in two global centers

Rapid Detection, Swift Takedown

With Outseer FraudAction, your organization enjoys comprehensive activity monitoring, and detection and takedown services against the fraudulent websites, apps, and social media pages used in cyberattacks.

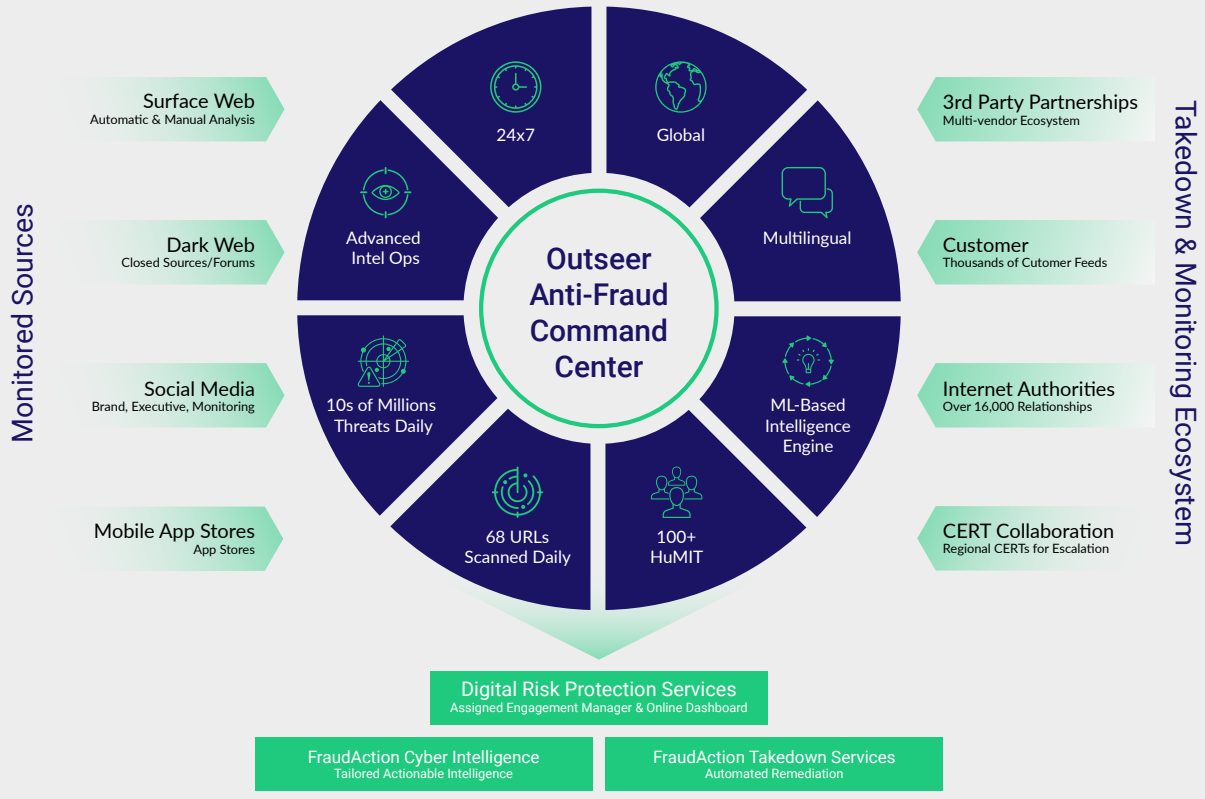
You also gain deeper visibility into emerging threats against your business and tailored intelligence that can be translated into actions.

At the heart of Outseer FraudAction lies our 24/7 Anti-Fraud Command Center. This 24/7 operation is led by our detection automation and multilingual cybercrime experts across two global centers. Tens of millions of potential threats are analyzed each day to protect millions of businesses and consumers worldwide.

With Outseer FraudAction integrated service, you can streamline your resources and management of external threats while obtaining comprehensive fraud protection across many attack vectors.

With Outseer you have the ability to manage 24/7 external threat detection and takedown all with one vendor budget. This means you can reduce your risk of financial and reputational damage from brand impersonation scams and other cybercriminal activities easily and cost effectively so you can focus on growing your business.

Outseer Anti-Fraud Command Center



Our Mission

Our mission is to eliminate threats to your company, customers, suppliers, and others before they do damage

How It Works

Our mission is to eliminate threats to your company, customers, suppliers, and others before they do damage. Here's how we do it.

Phishing & malware site takedown

Outseer FraudAction identifies phishing attacks via a broad, global partner network. We scan millions of URLs (including newly registered domains), and assess thousands of malware samples, daily. Through data science, Outseer experts, and industry partnerships, we are able to confirm attacks and take immediate steps to shut down the sites used to perpetrate them.

Rogue mobile app detection & removal

Outseer FraudAction uses proprietary, advanced detection techniques to monitor major app stores and dozens of unofficial alternative app stores in search of apps marketed under our customers' brand names. This gives you visibility into your organization's mobile presence and allows you to stay ahead of any potential damage caused by unauthorized use.

Fraudulent social media page removal

Fraudulent brand social media pages can be used to deceive users into clicking through to phony login pages impersonating trusted brands. Some are used to distribute malware. Some may be designed to infiltrate e-commerce accounts and their attendant payment card numbers and loyalty points. Still others may aim to spread disinformation or simply to tarnish your brand. Outseer FraudAction identifies bogus social media pages and works with platforms such as Facebook, LinkedIn, Instagram and Twitter to remove the threat.

Cyberattack mitigation

Once an attack has been detected and confirmed, we alert you to the threat and work to quickly neutralize it. Leveraging our long-standing relationships with over 16,000 different domain hosting services worldwide, we're able to quickly shut down attacks on a global scale. In instances involving phishing, trojan and other forms of malware used in man-in-the-middle and man-in-the-browser attacks, our strong partnering with Google, Microsoft, and others enables us to block attacks globally on all major browsers, preventing other users from falling victim.

Intelligence feeds

The Outseer FraudAction cyber-intelligence operation provides insight into cybercrime trends and in-depth investigations on fraud methods and operations within the global cybercriminal underground. Our experts monitor fraudulent activity everywhere cybercriminals trade personal identifiable information, credit card numbers, mule accounts, Fraud-as-a-Service (FaaS) offerings, malicious tools and more. Through deep investigations our researchers provide actionable intelligence you can use to protect your business and stop fraud before it occurs.

Our Intelligence feeds include:

- **Compromised Cards:** Full or partial card information associated to your organization's BINs
- **Compromised Credentials:** Credentials reported are associated with your organization's corporate email or websites

The scale and depth of Outseer FraudAction's insights and visibility keep you one step ahead, allowing you to:

Stop fraud before it occurs

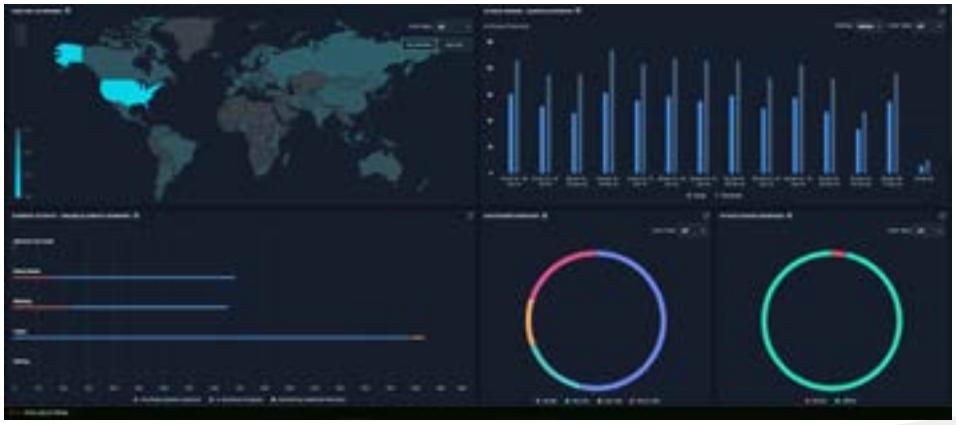
Gain comprehensive insight into external threats

Focus on your business priorities while we protect your brand and customers

- **Indicators of Compromise:** Generic data feeds (e.g., IPs, Emails, URLs) which may help your organization identify, prevent or mitigate a threat in your network or your customer facing website.
- **Open source monitoring:** Data associated with your organization, gathered from a range of open source sites that are known to be used also by cybercriminals
- **Cybercriminal assets:** Generic data pertaining to and used by cybercriminals and may help identify fraudulent activity within your organization. This category includes: mule accounts and mule addresses.
- **Executives Monitoring:** Informs you on cyber threats such as identity theft, reputational damage and extortion on key executives in your organization.

Real Time Dashboard

You can track the status of detected attacks in real time through an online dashboard. The dashboard includes attack forensics such as recovered phishing kits used to set up imposter phishing sites, associated malware triggers and configuration files. In addition, the Intelligence feeds are accessible and downloadable from the dashboard, that includes (but not limited to): Compromised Cards, Compromised Credentials and Indicators of Compromise (IoC).The dashboard can also be accessed via API integration to allow automated machine-to-machine access to this data from your SIEM, SOAR or other cybersecurity interfaces.



Outseer FraudAction Dashboard

About Outseer

Outseer empowers the digital economy to grow by authenticating billions of transactions annually. Our payment and account monitoring solutions increase revenue and reduce customer friction for card issuing banks, payment processors, and merchants worldwide.

Leveraging 20 billion annual transactions from 6,000 global institutions contributing to the Outseer Data Network, our identity-based science delivers the highest fraud detection rates and lowest customer intervention in the industry. See what others can't at outseer.com