



# External Cybersecurity Platform



# I Table of Contents

<b>ZeroFox: The First End-to-End External Cybersecurity Platform.....</b>	<b>3</b>
<b>The ZeroFox Platform.....</b>	<b>4</b>
<b>Global Intelligence Collection .....</b>	<b>5</b>
<b>Data Source Coverage .....</b>	<b>5</b>
<b>Digital Risk Protection: Protect Vulnerable Assets Beyond the Perimeter .....</b>	<b>6</b>
<b>Top Threat Use Cases .....</b>	<b>8</b>
<b>Full-Spectrum Threat Intelligence .....</b>	<b>10</b>
<b>On-Demand Investigations &amp; Dark Ops .....</b>	<b>13</b>
<b>Adversary Disruption .....</b>	<b>14</b>
<b>Dedicated Response.....</b>	<b>15</b>
<b>Incident Readiness .....</b>	<b>16</b>
<b>Digital Forensics &amp; Incident Response .....</b>	<b>17</b>
<b>App Library &amp; Integrations .....</b>	<b>19</b>
<b>AI Analysis &amp; Platform Capabilities .....</b>	<b>20</b>
<b>Customer Success .....</b>	<b>21</b>
<b>Get Started With ZeroFox .....</b>	<b>22</b>
<b>About ZeroFox .....</b>	<b>23</b>

# ZeroFox: The First End-to-End External Cybersecurity Platform

*Protect your revenue, reputation and customer engagement from threats that originate outside of the corporate perimeter*

## The Problem

Commerce, customers, and threat actors are converging outside the corporate perimeter, creating a new attack surface that traditional security teams cannot see or control. This leaves external assets like brands, domains and people vulnerable to a host of cyber-threats that can result in fraud, impersonations, reputational damage, data breaches, and even physical harm.

Modern protection demands a robust external cybersecurity program that finds and disrupts threat actors where they operate – across social media and the surface, deep, and dark webs – before they can attack important assets. In today's threat landscape, organizations must prioritize a robust external cybersecurity program to effectively protect revenue, reputation and customer engagement from threats originating beyond the perimeter.

## The Solution

ZeroFox is the architect of the world's first end-to-end external cybersecurity platform to help security teams regain the advantage against emergent threats. We combine market-leading solutions – digital risk protection, cyber threat intelligence, adversary disruption and incident and breach response services – into a single platform experience backed by a global managed services team 24/7/365.

ZeroFox customers gain unprecedented visibility into the external attack surface and complete protection over vulnerable external assets including domains, social platforms, executives, forums, job posting sites, mobile apps, BINs, marketplaces, intellectual property, physical locations, code repositories, third-parties and more. In addition, our team of SOC analysts and embedded dark web personas provide regular curated findings and a steady stream of relevant threat reports packed with important context, analysis and recommendations.

ZeroFox is also built to disrupt and takedown threats at scale. Upon threat detection, time-sensitive disruption actions, such as offending content moderation, dismantling of attacker infrastructure, in-house takedowns of malicious domains and social profiles, move into action. And, should an incident occur within your organization, our on-demand incident response team helps prepare, detect, and respond to any situation, while our breach response services provide flexible solutions to notify and protect the impacted population. ZeroFox is committed to helping our customers return to normal business operations as quickly as possible.



# I The ZeroFox Platform

The ZeroFox Platform is an always-on, full-spectrum external threat intelligence, digital risk protection and response solution that provides organizations with comprehensive visibility and control across social media and the surface, deep and dark webs. Trusted by 4 of the Fortune 10 and hundreds of the Global 2000 across all industries, the ZeroFox Platform automatically detects and takes remediation actions to resolve many dozens of threat use cases including fraudulent brand and social media accounts, domain-based phishing attacks, customer scams, exposed PII, compromised credentials, physical security threats and more.

Built on easy-to-integrate APIs, our fully-managed platform integrates with existing security tools, Business Intelligence, social media management, and other technologies. The Platform's flexibility ensures near real-time delivery of every data point, IOC, remediation action, metadata blob, and contextualized alert within existing security workflows, infrastructure, and toolsets.

## The ZeroFox Platform

### ➤ OMNICHANNEL VISIBILITY

Safeguard your enterprise from dynamic security risks across the industry's broadest range of public platforms including the surface, deep and dark web, social media, mobile apps, code share repositories, forums and much more.

### ➤ AI-ENABLED THREAT DISCOVERY

Using machine learning techniques and artificial intelligence-based analysis achieved at global scale, the ZeroFox Platform automatically identifies hidden threats that evade traditional detection within objects, images and video, accelerating the remediation of targeted phishing attacks, credential compromise, impersonations, brand hijacking, executive and location threats and more.

### ➤ FULL-SPECTRUM THREAT INTELLIGENCE AND THREAT HUNTING

Enrich your security program with strategic, operational, and tactical threat intelligence uniquely focused on social media and across the surface, deep, and dark webs. ZeroFox enables API-integrated or in-platform threat hunting via a petabyte-sized data lake of curated, exclusive intelligence, along with a team of threat researchers, analysts, and embedded dark web operatives, who augment your team to tackle the scale and sophistication of external threats.

### ➤ COMPREHENSIVE ADVERSARY DISRUPTION AND TAKEDOWN AUTOMATION

ZeroFox leads the industry in disruption with unparalleled depth and breadth of coverage across 100+ networks, playbooks across 20+ threat use cases, and support from 50+ partners, including Google Cloud and GoDaddy, as part of our Global Disruption Network (GDN). Our comprehensive, in-house takedown services that enable quick and direct action to block and remove malicious content while disrupting attack campaigns at scale. In just a few clicks, you can automate the submission of a takedown request with convenient in-platform tracking, notifications and status change updates.

### ➤ DEDICATED RESPONSE

With the increasing frequency and complexity of cyber attacks, organizations often require a dedicated, experienced partner to help manage the risk across all response stages. ZeroFox's unified and complete response management will cover any threat or support need tailored to your organization's requirements. Our world-class Incident Response team delivers incident readiness, threat hunting, digital forensics, investigations, incident remediation, and ongoing monitoring. In the event of a data breach, we deploy notification solutions and flexible best-in-class protection packages for the impacted population. With more than 20 years of expertise managing incidents, ZeroFox is the go-to-partner for your response needs.

# I Global Intelligence Collection

ZeroFox provides comprehensive, “outside the firewall” threat intelligence for the digital business platforms you depend on. We offer automated and human intelligence collection for protected assets from all relevant OSINT (Surface) and Deep/Dark Web data sources. This provides the ability to surface and address threats early before damage can be done.

ZeroFox covers a broad range of data sources, from social networks and domain registrations, to email, surface, deep and dark web sites, forums and marketplaces. As new threats emerge, we continue to expand our coverage and capabilities to meet the needs of security teams.

ZeroFox is committed to full transparency surrounding data source coverage. Our Global Intelligence Collection framework ingests billions of pieces of social and digital content and ensures that protected entities are streamed in near real-time. ZeroFox leverages the networks’ APIs for data ingestion, ensuring timely and the most accurate data possible.

# I Data Source Coverage

ZeroFox’s data source coverage includes the following but is not limited to:



**Social Media**



**Domain Registries**



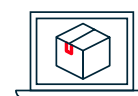
**Mobile App Stores**



**Forum, Blogs & News**



**Recruitment & HR**



**Web Marketplaces**



**Deep & Dark Web**



**Collaboration Platforms**



**Code Sharing**

# Digital Risk Protection: Protect Vulnerable Assets Beyond the Perimeter

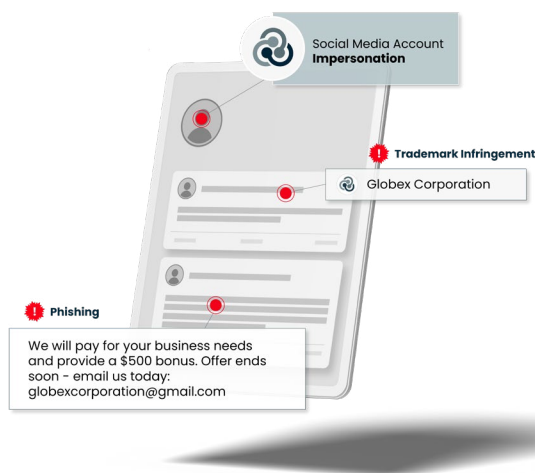
Protection only works if it is tailored to the specific risks and threats that an organization faces every day. ZeroFox starts by defining the assets that matter most — including brands, employees, executives and VIPs, locations and corporate pages. These assets are composed of a variety of “objects” such as profiles, names, keywords, images, domains, hashtags and more. This governs how and where ZeroFox gathers data; ensuring what is ingested is only the data that is relevant to your organization. During the onboarding process, our team of launch specialists helps to correctly configure and personalize the platform instance to your specifications.

## Brand Protection

ZeroFox Brand Protection empowers security teams of all sizes to proactively mitigate external threats to revenue, reputation, and customer engagement. We monitor for threats targeting your brands, sub-brands, products and intellectual property across all the surface, deep and dark web. This includes: brand impersonations, fraud, scams, abuse, piracy and counterfeiting, attack chatter, breach evidence relating to branded terms, compromised account credentials, BIN number exposures, rogue mobile apps and more.

## Domain & Malicious URL Protection

ZeroFox safeguards companies’ owned domains and protects employees and customers from malicious domains, URLs, and phishing attacks to ensure positive brand engagement. We continuously monitor and process hundreds of millions of websites across the dark and surface web for instances of trademark infringement, phishing, spoofing and more.



## Executive Protection

We protect executives and VIPs against account takeovers (ATOs), impersonations, personally identifiable information (PII) exposure, cyber threats (doxing, swatting, credential compromise), and physical threats (location and travel related threats). Our VIP protection service specializes in threat assessments, 24x7 monitoring, alerting and escalation, vetting of physical security threats, and PII removal coverage for immediate family members and more.

## Corporate Social Account Protection

ZeroFox provides governance and security for corporate owned social media accounts and business pages. We help prevent account hacking and gain early warning into hijacking attempts via continuous monitoring across owned accounts. ZeroFox enables inline content moderation across owned and authenticated accounts for remediating offensive comments or inappropriate content postings.

## Deep & Dark Web Monitoring Protection

We continuously monitor closed forums to detect new information on the dark web and provide wide coverage over unindexed digital channels. We gain visibility over compromised credentials and other sensitive information, uncover sensitive data leaks and gain insight into threat actor tactics and attack planning.

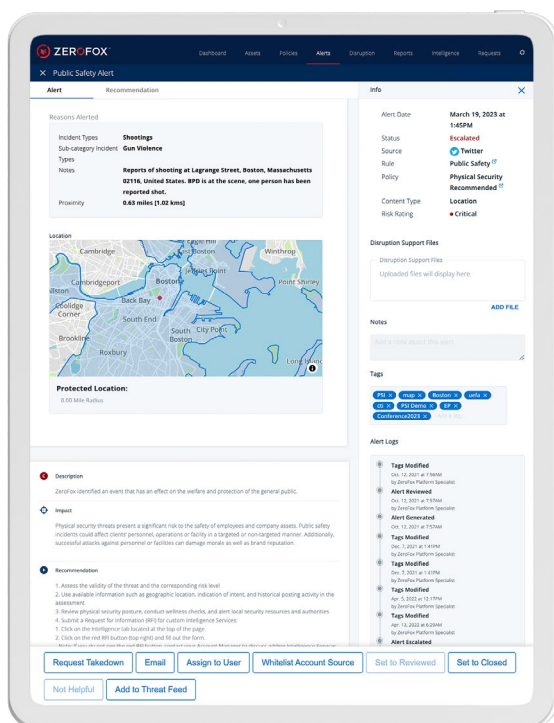


## Physical Security Intelligence (PSI)

We provide near real-time alert notifications for global incidents that threaten the physical security of your executives, VIPs, partners, team members, and facilities. ZeroFox's 24/7 Physical SOC team continuously researches and validates events that pose an immediate public safety risk or disruption (such as acts of violence, civil unrest, protests, natural disasters, emergency response situations, travel advisories, etc.) from various disparate HUMINT and OSINT sources across the surface, deep, and dark web.

## Event Protection

ZeroFox provides protection for location-based assets, such as corporate headquarters, manufacturing facilities, distribution and storage warehouses, offices and stores, and homes or temporary destinations for executives and their families against travel-related mentions, physical, and location-based threats. Additionally, our customers gain near real-time situational awareness and rapid alert notifications of attack planning, public safety incidents, or nearby threats to your locations and events.



## Third Party Monitoring

We enable you to monitor for threats and risks facing your supply chain and partner ecosystem. ZeroFox enables you to monitor and alert on expired SSL certificates, open ports, inferred vulnerabilities, and infected hosts within your vendor community. Additionally, we are able to discover risky or threatening content across the surface web and dark web channels that mention third party brands or related terms of your suppliers, contractors or other key partners.

## Top External Cybersecurity Risks

- Impersonations and Abuse of Executives, Brands and IP
- Fraud & Scams
- Phishing & Malicious Domains
- Hosted IP Infringement
- Hosted Malware
- Cybersquat URLs
- Cyber Threats & Harassment
- Physical Threats & Public Safety Incidents
- Reputational Risks
- Counterfeiting & Piracy
- Credit Card Exposure
- PII Exposure & Leaks
- Botnets
- Account Takeover
- Internet Infrastructure Exposure
- Third-Party Risk
- Attack Chatter and Planning on Covert Sites

# I Top Threat Use Cases

ZeroFox provides information security, corporate security, physical security and brand protection teams with the critical visibility, intelligence and automated response necessary to safeguard against:

## Brand & Executive Impersonations

Fraudulent accounts and spoofed domains leverage the implied trust across social media, email and the surface web to launch and spread phishing attacks, perpetrate scams and damage brands. We identify and remove accounts and domains impersonating your brands or people.

## Targeted Phishing & Malware

Attackers use shortened or obfuscated URLs as the primary attack delivery mechanism, exploiting social media to bypass security measures and target both your employees and customers. Other domain phishing tactics include domain squatting, typosquatting, and homoglyph attacks. We identify and remediate malicious URLs in your social media environment.

## Ransomware

Address early indicators of ransomware attacks — from early warning of credentials on the dark web to direct engagement with bad actors within the criminal underground. Additionally, we serve as an intermediary to negotiate asset reacquisition or crypto payments when necessary.

## Compromised Credentials & Information Leakage

After attackers steal employee credentials and corporate information, they advertise, sell and distribute this sensitive data on the deep and dark web. ZeroFox continuously scans these channels to identify where this data or other sensitive company IP has been exposed, quickly alerting you when your protected domains are found in breach data.

## Executive & Corporate Threats

Executives and corporate assets are exposed to risks on the surface, deep, and dark web, such as doxxing, PII exposure, and physical threats. We monitor executive and corporate accounts and the digital world for malicious activity, threats or sensitive content.

## Account Compromise

Social media accounts are trusted sources of corporate information, yet unlike websites, they lack security and protection beyond a simple password. We alert you to any suspicious behavior or posts and block all outgoing content from the compromised account.

## Customer Fraud & Scams

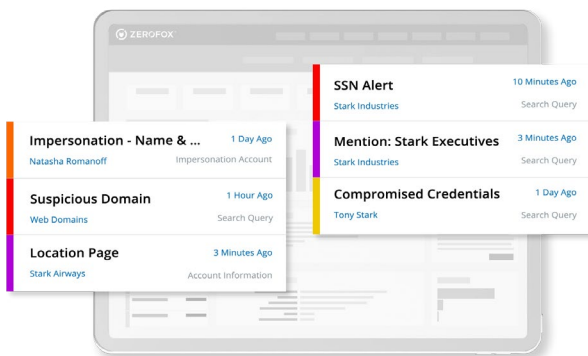
Whether financial fraud, job and HR scams or fake offers, social media and digital platforms can expose your customers and brand reputation to exploitation. We identify and remove instances of fraud and scams that leverage your protected brands to target your customers and employees.

## Covert Attack Planning & Chatter

Threat actors often leverage covert channels and unindexed sites across the deep and dark web to plan, coordinate and discuss upcoming attacks. We help cut through the noise and pinpoint attack chatter that mentions your protected brands, executives and assets and automatically detect covert communications that indicate malicious intent or sentiment.

## Piracy & Counterfeit Goods

Fake or stolen content shared on marketplaces, dark web markets and promoted on social media can seriously undermine your organization's bottom line and reputation. We automatically identify proprietary content, posted intentionally or not, circulating on social media.





## Global Physical Security Incidents

Real-world incidents and events can often threaten the physical security of key executives at home or while traveling, and their organization's physical assets. Stay on top of public safety incidents and disruptions near your protected locations with rapid alerts of events that threaten the safety of your worksites and people. We monitor for organization-specific phrases and terms, attack chatter, and malicious posts targeting your organization, assets, employees, executives, and key stakeholders.

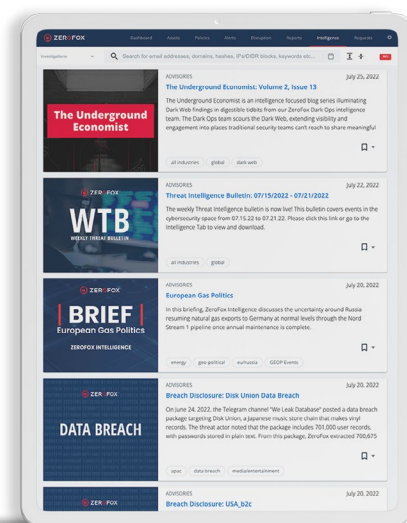
## Malicious Content

Trolls, spammers, competitors, cybercriminals and unwitting customers post malicious, offensive or sensitive content to corporate pages. We immediately block, hide or remove undesirable content, such as slurs, credit cards numbers, scams and phishing links.



# Full-Spectrum Threat Intelligence

As digital footprints expand, so does cyber-risk, leaving security leaders struggling to keep ahead of a torrent of threats. Regain the advantage against adversaries with ZeroFox intelligence solutions that are purpose-built to deliver timely insights with finished reports, searchable access to petabytes of threat data, 24x7x365 location monitoring, and the investigative services of embedded dark operatives and expert security analysts. Crafted by cyber security experts with decades of experience and unmatched access within the underground economy, ZeroFox tailors insights and intelligence services to empower security teams of one or one hundred.



## Global Intelligence Types

### Botnet Intelligence

Discover compromised customer and employee account credentials, and botnet malware-infected corporate hosts, in order to quickly address the risk posed by this pervasive threat vector.

### Dark Web Intelligence

Access deep and dark web chatter and data that helps you identify exposed or stolen credentials, PII, IP and more before it's weaponized and directed at your organization.

### Fraud Intelligence

Find data sets, websites, tools, fraud specialists and their TTPs and social engineering methods aimed at undermining your business and clients.

### Geopolitical Intelligence

Gain rapid situational awareness and relevant insights of threats to your organization, assets, or operations from a particular region in the world, including political, cultural, regulatory, health, and other related topics.

### Internet Infrastructure Intelligence

Distinguish between legitimate and suspicious providers for domains and hosting/VPS infrastructure. Find current infrastructure exploits and TTPs, suspicious hosts, IPs and domains used in attacks.

### Malware & Ransomware Intelligence

Quickly track down malware, adversaries, and tactics, techniques and procedures being used to gain access, escalate privileges, exfiltrate sensitive data, and ransom your organization.

### Physical Security Intelligence

Monitor potential threats or events affecting specific geographic areas of operation or specific executives. Track TTPs affecting cybersecurity and physical posture with analyst-vetted alerts and rapid situational awareness.

### Strategic Intelligence

Track geopolitical events, social, health and economic indicators to inform long-term decision-making.

### Third Party Intelligence

Scope potential risk of vendors and partner companies in your supply chain across the threat intelligence spectrum.

### Vulnerability Intelligence

Track the latest vulnerabilities being released publicly by vendors. Monitor vulnerabilities and exploits being prioritized by the security research and adversary communities.

# Global Intelligence Reports & Deliverables

ZeroFox's threat researchers curate and contextualize relevant breaking news stories, delivering them to users directly within the ZeroFox Platform as well as to your email inbox via our Daily Intelligence Brief.

## On-Demand Investigations

Address persistent digital threats and access in-depth threat research and investigations. Our team of expert analysts provide access to custom threat research and in-depth threat investigations based on your organization's unique threats, business cases, new, incoming RFIs and/or persistent issues.

## Advisories

New publications throughout the week ensure your security team remains up to date on the latest threat actors and campaigns. Advisories include data breach notifications, targeted attack information, research reports and more.

## Strategic Intelligence Reporting

Leverage periodic cyber intelligence reports and research that lend insight into security policy, planning, implementation and ongoing operations. Our targeted research enables more effective policy and compliance decisions, increases security hardening capabilities and improves ongoing security operations.

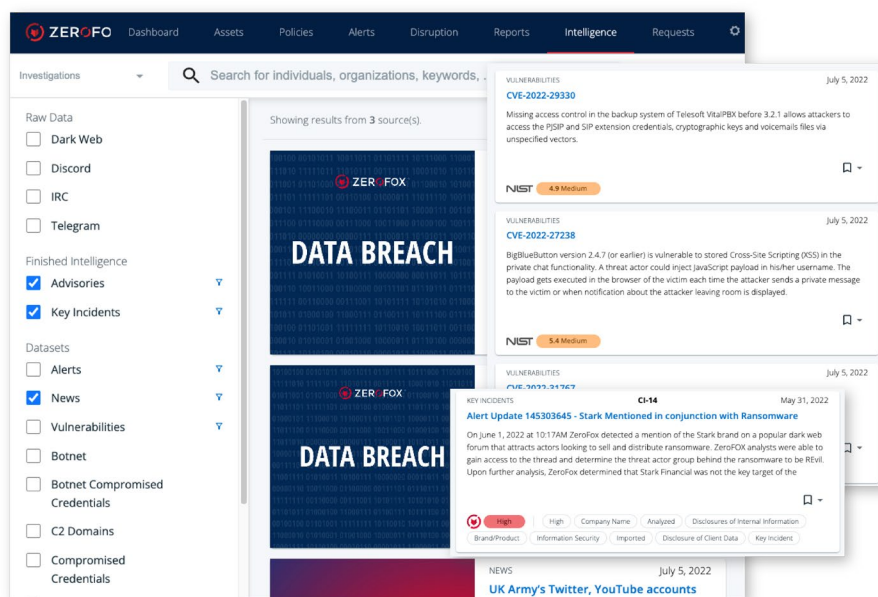
# Intelligence Data Lake

## Intelligence Search

The ZeroFox Intelligence Search module provides threat intelligence analysts unlimited search access into the complete threat intelligence data lake from within the ZeroFox Platform. Provide the ability to search ZeroFox's extensive data lake and retrieve all threat intelligence related to search terms. Easily search across: intelligence and vulnerability feeds of curated, finished intelligence and associated IoCs for Command & Control (C2), covert communication channels, compromised credentials, botnet logs, malware, etc.

## Intelligence Feeds

Delivered to the platform of your choice, ZeroFox Intelligence Feeds improves the depth and accuracy of your threat alerting, analysis and investigations. Using the ZeroFox API, ingest the threat data you require directly into your SIEM, TIP, SOAR, firewall, or IAM, adding exclusive context to expedite decision making and automate protection. Three Intelligence Feeds bundles deliver unique Identity & Fraud intelligence, Deep & Dark Web intelligence, and Network & Vulnerability intelligence, enabling automated security workflows while also providing security teams insights needed to validate IoCs, respond to attack-in-progress, and thwart impending attacks.



# OnWatch™ Managed Services

Every ZeroFox customer is fully-managed by our world-class team of threat experts, saving your security team time and resources. Whether it's triaging alerts in the ZeroFox Platform, or leveraging a fully dedicated analyst – you can rely on enhanced, hands-on protection and threat intelligence experts who help ensure optimal protection and satisfy your unique intelligence requirements.

## OnWatch™ Alert

Extend digital visibility and protection with ZeroFox OnWatch™ Alert. Our team of global SOC first-line threat experts provide 24x7x365 managed services to review, triage and escalate incidents and prioritize threats on your behalf. Protect your organization from social and digital threats while maximizing the value of the ZeroFox Platform – all while getting back more time in your day.

## OnWatch™ Expert

ZeroFox OnWatch™ Expert service provides a dedicated, named analyst who performs as a key member of your security operations team. Rely on an experienced security intelligence analyst who provides expert threat hunting, nuanced contextual analysis, routine threat reporting, and regular executive briefings. Our analysts access the world's most historically accurate data lake of threat indicators and attack data, including unique data from embedded dark web operatives. Optional support for over 25 languages is available.

### Choose the OnWatch Service Tier That's Right For Your Organization

	OnWatch™ Alert	OnWatch™ Expert
Initial Onboard Configuration & Setup	✓	✓
Global 24x7 SOC's and Expertise	✓	✓
Managed Service Alert Triage, Validation, Routing, & Escalation	✓	✓
Strategic Finished Intelligence (Geopolitical, Industry, Global Threats)	✓	✓
Customer Workflow Design	✓	✓
24x7 Customer & Platform Support	✓	✓
Expert Configuration, Tuning & Consultation	✓	✓
Platform Optimization	✓	✓
Online, On-Demand Access to ZeroFox University	✓	✓
Dedicated Senior Threat Intelligence Analyst		✓
RFI Research, Analysis & Alert Context Inquiries		✓
Advanced Alert Curation & Analysis		✓
Weekly Threat Intelligence & Monthly Threat Assessment Reports		✓
Daily Threat Intelligence Brief		✓
Quarterly Threat Intelligence Executive Briefing		✓
Language Translation Support	English Only	Additional Language Support Available

# On-Demand Investigations & Dark Ops

Gain access to teams of highly skilled intelligence analysts and researchers with experience conducting specialized risk assessments and investigations. Additionally, leverage deeply embedded dark web operatives who engage with adversaries, triage threats, and curate intelligence specific to you.

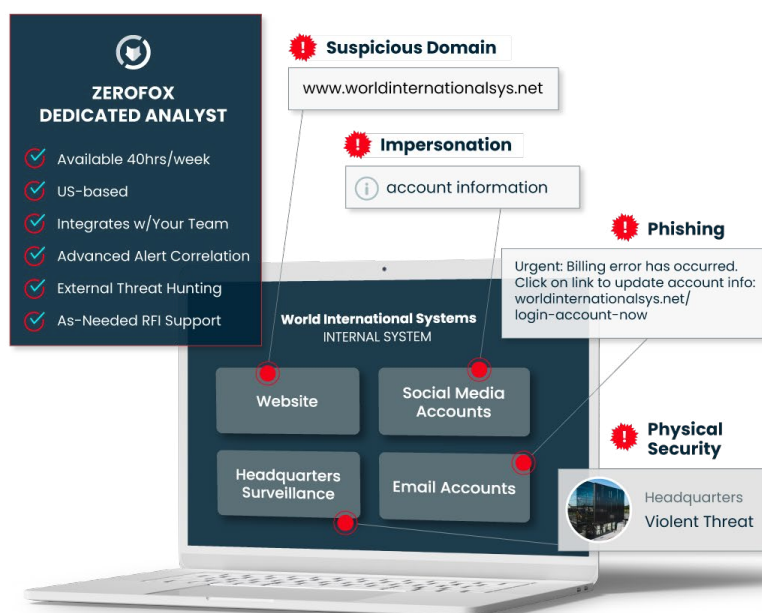
## On-Demand Investigations & Incident Support

Threats to physical and digital assets are escalating in scale and sophistication. Most organizations don't have the tools, personnel, or time to keep up, but your organization's success still rests on your ability to accurately assess and respond. ZeroFox's On-Demand Investigation and Incident Support provides highly-skilled intelligence analysts who deliver deep-dive reports, technical cybersecurity analysis, threat assessments, research projects and as-requested analytic projects tailored to your organization. Gain in-depth analysis on adversaries, campaigns, targets, red teaming on your behalf and attack surface assessments and reporting according to your SIRs, PIRs, and RFIs.

## Dark Ops Investigation & Engagement

Go deeper into the cybercriminal underground with ZeroFox's dark web threat intelligence. Our analysts work with dark web operatives to investigate and identify exposed credentials, Personally Identifiable Information (PII), intellectual property, social and Active Directory (AD) accounts available for sale on the dark web. If there are specific RFI needs, we will fulfill those as well.

Additionally, ZeroFox leverages deeply embedded dark web operatives with exclusive connections into underground communities to help you recover assets, negotiate pricing and acquire specific compromised material. Gain access to Dark Ops operatives and research when you need it. Services, reports and assessments are available via subscription and on-demand.



# I Adversary Disruption

## Disrupt Attacker Campaigns & Take Down Threats Beyond Your Perimeter

ZeroFox saves you from the manual, costly and arduous process of finding and taking down malicious profiles and dangerous content, working on your behalf to process and report directly to the source provider for successful takedown removal. We go above and beyond by working with disruption partners that block or flag malicious adversary infrastructure. The collective intelligence of our Global Disruption Network (GDN), a premier partnership with Google's Web Risk program, ZeroFox can quickly disrupt complex threat actor campaigns and prevent attacks from threatening your people, brands and critical business assets.

### Universal Takedowns

ZeroFox manages takedowns fully in-house with expansive breadth of coverage, expertise, and success across 100+ networks. Our customers can automate takedown requests directly from the platform and pursue the removal of malicious or spoofed domains, impersonating social media accounts, fraudulent mobile apps and marketplace listings, content that infringes copyright or IP, content that violates hosting provider terms of service, and more. After processing the request, ZeroFox analysts work directly with the source provider to expediently remove the violating content with transparent reporting, tracking and status updates for every step of the way.

- 100% in-house with analyst expertise for 100+ networks (and growing)
- Takedown coverage for malicious domains, impersonating social accounts, fraudulent content and more
- Automated request processing
- Transparency & notifications of takedown status changes delivered via email and in-platform

### Global Disruption Network (GDN)

For every validated takedown request submitted, ZeroFox automatically distributes associated indicators of attack (IoAs) with partnering third-party security vendors (such as Google Cloud) and network providers (such as ISPs, registrars, etc.) to rapidly block access to malicious sites and content and close threat exposure gaps. These actions trigger in significantly less time than it takes for traditional takedowns to process (ie. minutes/hours vs. days/weeks) and reduces reliance on a single provider response for remediation.

- Rapid blocking while takedown is processing
- Automated submission to 50+ partners
- Google Cloud's Web Risk Integration: Can block phishing in 15 min or less

### Uniform Domain-Name Dispute-Resolution Policy (UDRP) Solution

ZeroFox provides in-house assessments and filing of UDRP disputes on your behalf. Work with ZeroFox experts to effectively dispute cybersquat cases that put your brands and intellectual property at risk.

- ZeroFox works with the World Intellectual Property Organization (WIPO), the largest UDRP arbitration provider, on your behalf
- Detailed UDRP assessments that review domain ownership, previous filings, opposing parties, geographic conflicts, trademarks, etc.
- Full support during the UDRP filing process with status updates and recommendations to guide you

### PII Removal

ZeroFox scans over 150 data broker sites to look for assigned executives' and your employees' personally identifiable information (PII). Once the PII is identified, PII Removal automates the removal of this information from data broker websites and related Google search results. Ongoing monitoring identifies if monitored PII returns to the data broker sites. If PII does return, PII Removal initiates an automated removal process. Monthly email reporting provides easy tracking and visibility, allowing security teams to stay-on-top of potential risks to executives, employees, and the organization.

- ZeroFox provides ongoing monitoring and automated removal of PII across 150+ data broker websites
- Over 90% of successful removals occur within the first 30 days



# Dedicated Response

## Rapid Mobilization to Prepare & Recover from any Incident

ZeroFox incident response solutions help organizations identify, contain, and recover from any perceived or active cybersecurity incident. Acting swiftly and efficiently, our highly experienced team is ready at a moment's notice to help you contain the incident and provide best-in-class products and services when an incident is detected.

With cyber attacks on the rise, organizations need to be prepared to identify, analyze, contain, and recover from the latest risks. When the time comes to manage an attack, employing a time-tested leader is critical to ensure business operations are restored. ZeroFox's trusted, comprehensive response products and services are tailored to fit each organization's needs. The ZeroFox suite of Incident Response services includes incident readiness, digital forensics and incident response, and ongoing monitoring ensuring your organization has full protection from cyber attacks.

In the event of a data breach, the ZeroFox team deploys notification solutions and flexible best-in-class protection packages for the impacted population. Our end-to-end response management of any cyber attack, serves as an extension of your team building resiliency for your organization. With more than 20 years of response expertise, the ZeroFox team is the trusted, go-to partner for leading response products and services.

## Stages of Incident Response

	01 PREPARE	02 IDENTIFY	03 CONTAIN/ RECOVER	04 REVIEW	05 MONITOR
<b>ZeroFox Incident Response Offering</b>	<p>Get immediate, 24/7 assistance from a team of security experts through</p> <ul style="list-style-type: none"> <li>Clicking on the "Contact ZeroFox Response" link on <a href="https://zerofox.com">zerofox.com</a></li> <li>Emailing <a href="mailto:incidentresponse@zerofox.com">incidentresponse@zerofox.com</a></li> <li>Calling 1.855.936.9369</li> </ul>	<p><b>ZEROFOX WILL:</b></p> <ul style="list-style-type: none"> <li>Rapidly deploy technologies to gain visibility and preserve evidence</li> <li>ZeroFox will conduct preliminary analysis and work with you to develop a tailored response and remediation plan</li> </ul>	<p><b>ZEROFOX WILL:</b></p> <ul style="list-style-type: none"> <li>Contain the incident to limit its impact on your business</li> <li>Conduct root cause analysis</li> <li>Identify evidence of data access exfiltration</li> <li>Work to recover lost data (if possible)</li> <li>Assist in rapidly restoring business operations to normal</li> <li>Liaise with law enforcement and other external agencies</li> <li>Provide regular incident updates</li> </ul>	<p><b>POST INCIDENT, ZEROFOX WILL:</b></p> <p>Offer a final report covering the following:</p> <ul style="list-style-type: none"> <li>Root cause of the incident</li> <li>Methodology used</li> <li>Remediation activities performed</li> <li>Recommendations for future security enhancements</li> </ul>	<p><b>ZEROFOX WILL:</b></p> <ul style="list-style-type: none"> <li>Provide continuous dark web monitoring to collect and analyze data on a broad range of deep and dark web sites, forums and marketplaces and across covert communications networks such as TOR, I2P, ZeroNet, Paste sites.</li> <li>Deliver contextually enriched alerting for compromised credentials, sensitive data leaks and relevant attack planning and chatter.</li> </ul>

# I Incident Readiness

ZeroFox proactive incident readiness solutions help you address the increasing frequency, complexity, and speed of cyber threats. With the help of our expert team, your organization can improve its defenses by understanding the threats, tactics, techniques, and procedures most likely used to target your organization. You can assess your current security posture, discover areas for improvement, and develop effective incident response strategies enabling you to prioritize defensive measures for your organization. Preparing for an incident will also improve stakeholder confidence and raise your organization's overall cybersecurity posture.



## Tabletop Exercises

Tabletop exercises enable ZeroFox to simulate realistic cyber threats to test and evaluate your organization's response to a cyber attack or other cyber-related emergencies. Exercises are built to engage key stakeholders in discussing and analyzing a hypothetical scenario to identify strengths and weaknesses in the response effort. Tabletop exercises offer a cost and time effective way to evaluate and improve incident readiness.

## Incident Response Capabilities Assessment

Entailing a thorough analysis of the existing incident response plan, ZeroFox incident response capabilities assessment identifies any weakness or areas for improvement. This may include reviewing the incident response plan, assessing the adequacy of the response procedures, and evaluating the effectiveness of the resources and personnel available to respond to an incident.

## Ransomware Readiness Assessment

Performing an in-depth ransomware readiness assessment will evaluate your organization's systems, networks, and data to identify potential weaknesses commonly exploited by ransomware attackers. A ransomware readiness assessment provides actionable recommendations to enhance overall readiness and prevent future attacks.

## Threat Hunting

ZeroFox experts perform structured threat hunts, targeting high-risk cyber threats in the environment. Threat hunting is a proactive practice that systematically searches for potential threats and vulnerabilities within an organization's environment. Advanced tools and techniques are used to stay ahead of attackers, reducing dwell time, improving cybersecurity resilience, and helping prioritize defense.

# Digital Forensics & Incident Response

ZeroFox's experts and dedicated teams help identify, prioritize, contain, and recover from any cyber threats and security issues. Working collaboratively with any organization, we fight back against attackers by disrupting attacker infrastructure. The ZeroFox team uses industry leading tools and techniques in executing our proven response methodology to identify attacker activity, respond to and recover from incidents. Communicating with your organization through each step of the incident, you will stay apprised of each step in the process.

Our robust threat intelligence function accelerates our IR team's ability to understand what happened in an incident, how the attacker gained access and escalated their privileges, what persistence mechanisms exist and what data was accessed or exfiltrated. ZeroFox can also protect your organization's critical digital assets and data from threats by providing ongoing monitoring across the surface, deep, and dark web for sensitive data and credential leaks.

*"Organizations today are facing cybersecurity challenges that have accelerated in frequency, severity, and complexity. The rise of the Ransomware-as-a-Service cybercrime business model has become an easy way for threat actors to launch cyber-extortion campaigns and monetize their activity, and our ZeroFox threat intelligence team "anticipates a continued increase in ransomware attacks and extortion activities."*

—ZEROFOX 2022 THREAT INTELLIGENCE FORECAST

**\$4,350,000**

AVERAGE COST OF A DATA BREACH

**22B**

RECORDS WERE EXPOSED IN PUBLICLY DISCLOSED DATA BREACHES IN 2021

**82%**

OF DATA BREACHES INVOLVED THE HUMAN ELEMENT

## Breach Response

ZeroFox Data Breach Solutions provide the most consultative, tailored and flexible solutions for your organization's unique needs and industry environment. The ZeroFox team mobilizes quickly to provide flexible solutions tailored to the unique characteristics of your data breach, helping to mitigate the impact to the impacted population while restoring normal business operations. Serving as an extension of your team, we help you build resiliency to any type and size of attack. With the average cost of a data breach topping \$9 million in the US and over \$4 million globally, a time-tested leader is critical for your organization.

Our consultation and guidance will help you make informed choices about the products and services that your organization needs, avoiding those that it does not, and ultimately maximizing the efficiency of your breach response. Whether the impacted population is 10 million or just a few individuals, ZeroFox data breach response services can be built to fit your organization's needs. From digital and physical notifications, to call center services, to breach websites – we have it all ready to quickly respond to any size data breach.

## Breach Notification Services

Individuals affected by a breach need answers and advice. ZeroFox customized digital and mailing notifications and tracking help ensure the right notifications reach the right people. We will also work closely with your organization's privacy attorney to ensure all legal requirements are incorporated. Our breach information and enrollment site will be configured to meet your organization's unique needs and ensure the individuals impacted by the breach will have access to information and protection at their fingertips. Our live-trained US-based call center agents help bring peace-of-mind to breach victims helping to alleviate concerns, answer questions and enroll affected individuals in our protection services. We support more than 200 languages and unique populations such as minors, deceased, and the disabled.

## Protection for Impacted Breach Populations

Select from ZeroFox protection products and services for the impacted population that best fit the requirements and specifics of your organization's data breach. Our solutions will help the impacted population not only after an incident occurs, but also in anticipation of one. If your employees, customers or members have fallen victim to any form of identity theft, ZeroFox Identity Recovery Experts will help them restore their identities. We have a 100 percent success rate restoring affected individuals to pre-theft status.

Options include:

- Identity protection service provides single or tri-bureau credit monitoring. We give you the flexibility to make that decision based on your organization's needs.
- Proprietary dark web technology scours 24/7 for stolen identities. It targets the illegal selling and trading of personal information and alerts your employees, customers and members, enabling them to take immediate steps to protect themselves.
- Identity theft reimbursement insurance includes up to \$1 million of insurance per individual, which reimburses victims for outside covered legal and professional services.
- Our Member Services team is fully accessible to your employees, customers and members and provides state of the art, patented and trademarked tools and services that assist them in proactively reducing their risk of identity theft.

# I App Library & Integrations

## Integrated Intelligence Feeds

Delivered to the platform of your choice, ZeroFox's integrated Threat Intelligence Feeds Improves the depth and accuracy of your threat alerting, analysis, and investigations. Using the ZeroFox API, ingest the threat data you require directly into your SIEM, TIP, SOAR, firewall, or IAM, adding exclusive context to expedite decision making and automate protection. Three Intelligence Feeds bundles deliver unique Identity & Fraud intelligence, Deep & Dark Web intelligence, and Network & Vulnerability intelligence, enabling automated security workflows while also providing security teams insights needed to validate IoCs, respond to attack-in-progress, and thwart impending attacks. Improve the signal-to-noise ratio with ZeroFox's Threat Intelligence Feeds, adding exclusive context to expedite decision making and automate protection.

## Integrated Asset Configuration, Alerting & Takedowns

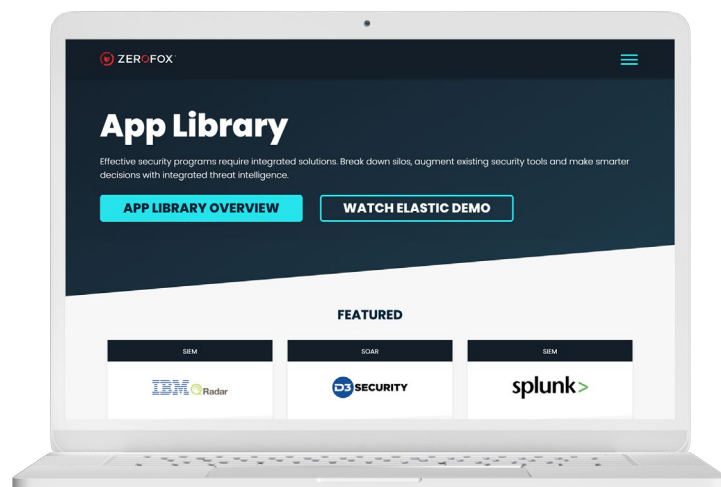
The ZeroFox App Connector provides the ability to create and configure protected assets, receive alerts, and request takedowns through integrations to other security tools such as Splunk, SIEMs, TIPs, SOARs. Leverage available partner applications to better streamline your response to external threats through effective threat intelligence enrichment, alert orchestration, and incident remediation.

## ZeroFox Partners & Integrations

Effective security programs require integrated solutions. Connect your enterprise with ZeroFox to enable integrated threat intelligence. Access 700+ data sources, disruption and technology apps, extensible RESTful APIs and pre-built connectors for the tools you've already deployed.

### The ZeroFox Platform Connects With:

- Analytics & Investigation Tools
- Blogs, Forums and Job Review Sites
- Business Intelligence Tools
- Cloud Security Tools
- Code Repositories
- Dark Web Channels
- Email and Collaboration Providers
- Endpoint Security and Management
- Existing SOC (TIP, SOAR, SIEM, Infrastructure, etc.)
- Governance and Risk Tools
- ITSM and Orchestration Tools
- Marketplaces
- Mobile App Stores
- Network and Security Management Tools
- Registrars and Hosts
- Social Media Platforms
- SSOs and IAMs
- Vulnerability and Patch Management Tools



# AI Analysis & Platform Capabilities

## AI-Driven Analysis

Dramatically reduce your risk exposure with AI-driven analytics and custom rules designed to eliminate costly, time-intensive threat hunting, manual remediation and coverage gaps that leave your organization exposed. ZeroFox deploys a variety of AI techniques such as natural language processing (NLP), sentiment analysis, optical character recognition (OCR), computer vision, anti-cloaking, logo/weapon/credit card detection, and facial matching models to enrich collection and detection across text and images. In addition, we are expanding the scope with generative AI, called FoxGPT, to accelerate the analysis of intelligence across large datasets and further enhance the identification of malicious accounts and attacks. Leverage the power of modern AI technologies to stay informed of critical threats with access in the office or via mobile device using the ZeroFox mobile app.

## Alerts

Once your asset groups have been configured and policies established, ZeroFox begins constantly identifying any new violations and triggering alerts. Bulk alerts are displayed in an easily filterable alerts table, allowing you to sort by risk rating, impacted asset, type of threat, timestamp, social network and much more. Each alert contains the content of the offending post or profile, threat metadata, adversary intelligence, alert logs and the ability to take action on the alert, including assigning the alert, emailing the alert, whitelisting the adversary and issuing a takedown of the content. All of this alert data, as well as additional enriched metadata, is available via API for organizations to pass into their existing security infrastructure (ex. SOAR, TIP SEIM, etc.).

## Foxscripts Custom Analysis

FoxScript, a part of the ZeroFox Platform, is a JavaScript-based language that opens the power of ZeroFox's data collection and analysis engines to virtually any use case. This fine-tuning capability means each organization can regulate the volume of their alerts, ensure only the most critical information is passed to the security analysts and avoid data overload.

## Dashboard & Access

The ZeroFox Dashboard provides an executive level summary of the overall state of an organization's digital risks and mitigation actions taken on behalf of the organization. The dashboard displays the total number of ingested and analyzed posts, profiles, URLs and images and gives an overarching look at the most critical alerts and most threatened assets. It also provides a summary of takedown metrics and recent advisories from ZeroFox researchers. Additionally, ZeroFox uses Role-Based Access Control (RBAC) for page visibility which enables the ability to hide or show certain pages based on existing users, user roles, or groups. This functionality helps to prevent numerous issues such as unauthorized users improperly making modifications to key platform configurations.

## Rules & Policies

Once assets have been configured, you can determine what analyses to perform for each asset, based on the associated use cases (for example, a brand will have different requirements than an employee). ZeroFox's rule engine leverages a suite of artificial intelligence, machine learning and data science techniques to address both the massive volume of ingested data and the diversity of risks. You have full control over which rules are turned on and which policies apply to which assets. ZeroFox comes out of the box with hundreds of default rules for the most prevalent challenges on the surface, deep and dark web, including malicious links, impersonations accounts, violence, offensive content, compromised accounts, compliance violations (PCI, FFIEC, HIPAA, GDPR, etc), scams, PII and much more.

## Reporting

Robust, automated summary reports demonstrate key platform statistics that show the social media and digital footprint analyzed, major threats identified and remediations implemented by the ZeroFox Platform. In addition, ZeroFox provides tools and reports to export platform data for custom analysis and input into other systems.



# I Customer Success

## Launch & Implementation

ZeroFox's expert Launch team ensures your platform is set up for continued success. Our high-touch launch program makes sure your protection is precisely configured to your organization's specific needs.

## Managed, Technical & Professional Services

ZeroFox provides a wide variety of flexible and tailored services to help you assess, analyze and reduce your organization's digital risk. Our team of experts can help build integrations, tune, optimize and configure the platform and enhance your overall platform experience.

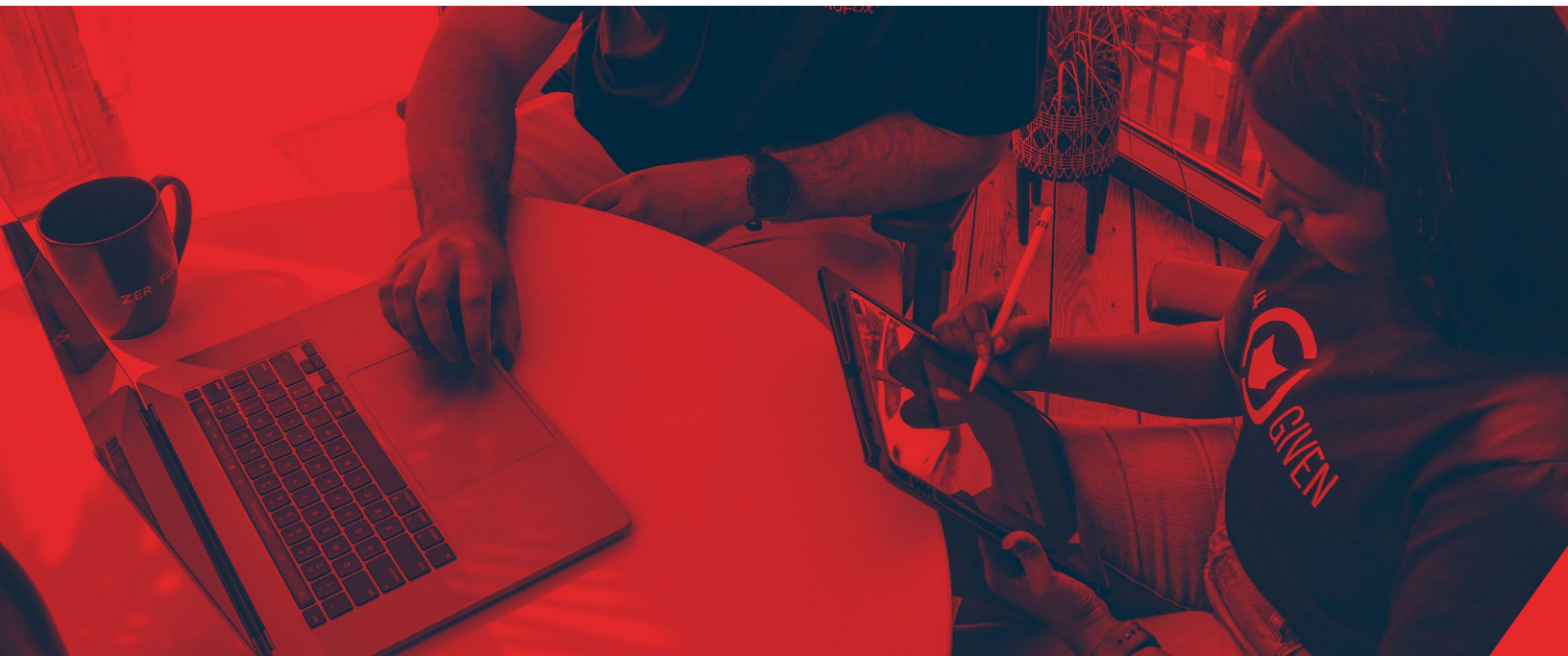
## ZeroFox University

ZeroFox offers training programs, both technical and nontechnical, to ensure you and your team get the most out of your ZeroFox Platform investment. Users can tap into this professional-grade certification to better protect their organization and grow their career.



*The ZeroFox platform is so intuitive and easy to use. Integrating it into my workflow was seamless.*

**AGENCY PRIVACY ANALYST**  
US FEDERAL AGENCY



# I Get Started With ZeroFox

## 1. Decide What's Important

Work with the ZeroFox Launch team to tune the platform and collect data relevant to your organization by configuring your assets, or go deeper to investigate what's important by tapping into ZeroFox's massive and historically complete threat intelligence data lake.

## 2. Define Your Policies

Work with the ZeroFox Launch team to tweak which out-of-the-box rules and policies are enabled for the things you want to protect. In addition, ZeroFox gives you full access to write your own custom FoxScript rules, enabling organization-specific use cases.

## 3. Extend Your Team

Maximize team resources by leveraging an elite global threat intelligence service team for research, investigations, analysis, reports, dark ops engagement, etc.

## 4. Receive Alerts on Risks

Focus on what matters while the ZeroFox OnWatch™ team delivers relevant, actionable alerts as the platform identifies risks. Each alert comes packaged with contextualized threat intelligence, alert logs, perpetrator intelligence and remediation actions.




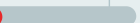









## 5. Remediate Malicious Content & Disrupt Attacks

Issue and track takedown requests from within the platform. ZeroFox works on your behalf to remove threatening content while also automating distribution of malicious URLs and indicators to Third party providers for the purposes of blocking and dismantling attacker infrastructure.

## 6. Integrate Data in Your Environment

Leverage one of ZeroFox's hundreds of existing integrations or tap into ZeroFox's RESTful APIs to pull in alert data into your existing security environment and push remediation actions back through the platform.

## ZeroFox Launch Timeline

Actions	Week 1	Week 2	Week 3	Week 4+	Description
Pre-Kickoff					Sales Handoff Asset Discovery Pre-Configuration
Kickoff					Introductions & Overview of launch process: Review attack surface discovery findings, disruption, workflow and reporting distribution.
Consult 1: Assets & Policies Review					Live review of configured assets and policies.
Configuration & OnWatch					Launch Consultant will update the platform based on your feedback. Once the initial scan is completed, OnWatch Alert Management will be enabled.
Consult 2: Alerts & Disruption					Live walkthrough of your alerts. Introduction to disruption and ZeroFox takedown request process.
Consult 3: Reports & Intelligence					Live walkthrough of reporting capabilities and the intelligence tab.
Consults 4+: Tuning (optional)					Optional additional consultation calls. Feel free to discuss any topic
Platform Overview					High level overview of ZeroFox Platform: Dashboard, Alerts & Disruption, Reporting, Intelligence (60-min). Preparation for post-launch experience.
Wrap Up Call					Review Launch Summary Report and confirm completion of success criteria.



# I About ZeroFox

## The leader in External Cybersecurity

ZeroFox (Nasdaq: ZFOX), an enterprise software-as-a-service leader in external cybersecurity, has redefined security outside the corporate perimeter on the internet, where businesses operate, and threat actors thrive. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers, including some of the largest public sector organizations as well as finance, media, technology and retail companies to stay ahead of adversaries and address the entire lifecycle of external cyber risks. ZeroFox and the ZeroFox logo are trademarks or registered trademarks of ZeroFox, Inc. and/or its affiliates in the U.S. and other countries.

**See ZeroFox in action**  
[zerofox.com/demo](https://zerofox.com/demo) | [zerofox.com](https://zerofox.com)

**Get in touch with us today**  
[sales@zerofox.com](mailto:sales@zerofox.com) | 855.736.1400

