# THE ZEROFOX PLATFORM

## Public Attack Surface Protection

## // PROBLEM OVERVIEW

Organizations today increasingly rely on digital platforms to engage customers, interact with employees, and grow business. Public platforms, including surface, deep and dark web, social media, mobile apps and email, provide a critical business conduit while simultaneously providing bad actors a new attack surface with which to target organizations: their public attack surface. Attackers leverage the scale, trusted nature, lack of security visibility and anonymity of these public platforms to launch a new breed of highly-effective attacks, all of which occur outside the firewall. With a fundamental lack of visibility and control, organizations struggle to identify and remediate digital risks and protect themselves across this public attack surface.

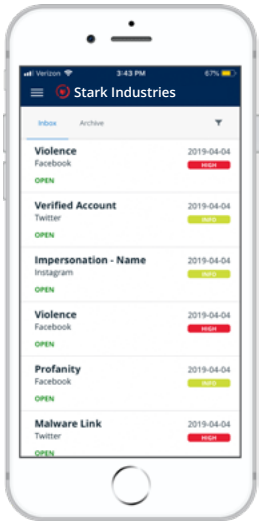
## // SOLUTION OVERVIEW

ZeroFOX, the global leader in Public Attack Surface Protection, constantly monitors all publicly available platforms in existence to discover hidden threats and all types of malicious cyber activity targeting your organization, and coordinates with network providers and hosts to take threats down before they go public. Using diverse data sources and artificial intelligence-based analysis, the ZeroFOX Platform identifies and remediates targeted phishing attacks, credential compromise, data theft, impersonations, brand hijacking, executive and location threats that abound on public platforms. ZeroFOX continuously monitors for emerging threats, instantly alerts security teams and authorities upon attack initiation, and automatically takes swift corrective actions ranging from offending content moderation to attacker infrastructure take down.

# The ZeroFOX Platform

The ZeroFOX Platform is an easy to deploy, always-on, cloud-based solution giving organizations critical visibility and protection across their public attack surface.

The ZeroFOX Platform delivers automated threat detection and remediation across a broad, ever-expanding set of digital platforms. ZeroFOX identifies organizational risks and security threats targeting both businesses and employees. 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 entities. It also provides a summary of takedown metrics and recent advisories from Alpha Team research.




## The ZeroFOX Platform enables:

### Omnichannel Visibility

Safeguard your enterprise from dynamic security risks across the industry's broadest range of public platforms including surface, deep and dark web, social media, mobile apps, code share repositories, email and collaboration platforms and much more. Have confidence that if a new threat is out there, you'll see it first.

### Actionable Threat Intelligence

Enrich traditional security programs with intelligence uniquely focused on social media and digital threats across surface, deep and dark web. Integrate IOCs into your larger threat intelligence tech stack with pre-existing integrations to leading SIEM, TIP, and SOAR platforms.

### Advanced Threat Discovery

Using machine learning techniques and artificial intelligence-based analysis achieved at unprecedented scale, the ZeroFOX Platform automatically identifies hidden threats that evade detection within objects, images and videos, and remediates targeted phishing attacks, credential compromise, data theft, impersonations, brand hijacking, executive and location threats and more.

### Rapid, Automated Remediation

ZeroFOX continuously monitors for emerging threats, instantly alerts security teams and authorities upon attack initiation, and automatically takes swift corrective actions ranging from offending or malicious content moderation to attacker infrastructure takedown.

Using targeted data collection and artificial intelligence-driven analysis engines, the ZeroFOX Platform automatically identifies and remediates fraudulent accounts, phishing attacks, customer scams, exposed PII, insider threats and more. Accessible in the office or on your phone through the ZeroFOX mobile app, never miss a critical threat. The ZeroFOX Platform provides the visibility, analysis, protection and remediation your organization needs to effectively protect your growing public attack surface.

# Visibility

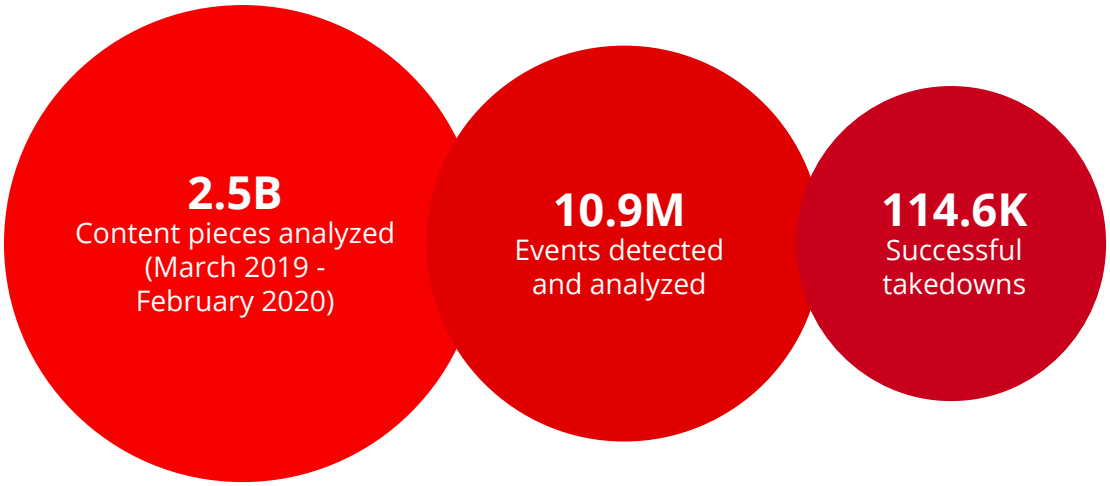
ZeroFOX provides comprehensive coverage outside the firewall, on the platforms you rely on for business. Complete Public Attack Surface Protection requires coverage of a broad range of data sources, from social networks and domain registrations, email, to surface, deep and dark websites. As new threats emerge, ZeroFOX continually expands coverage and capabilities to meet the needs of the market.

ZeroFOX is committed to full transparency surrounding data source coverage. The ZeroFOX data collection framework digests 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 the cleanest and most accurate data possible.

## // DATA SOURCE COVERAGE

ZeroFOX's data source coverage includes but is not limited to:

- Social media networks
- Deep and dark web
- Paste sites
- Web domains
- Email
- Surface web sites and searches
- Web marketplaces
- Forums, blogs, news and review sites
- Mobile app stores
- Vulnerabilities
- Breaches
- Code sharing sites
- Collaboration platforms
- Video conferencing tools
- Network scanning of IPs and hostnames



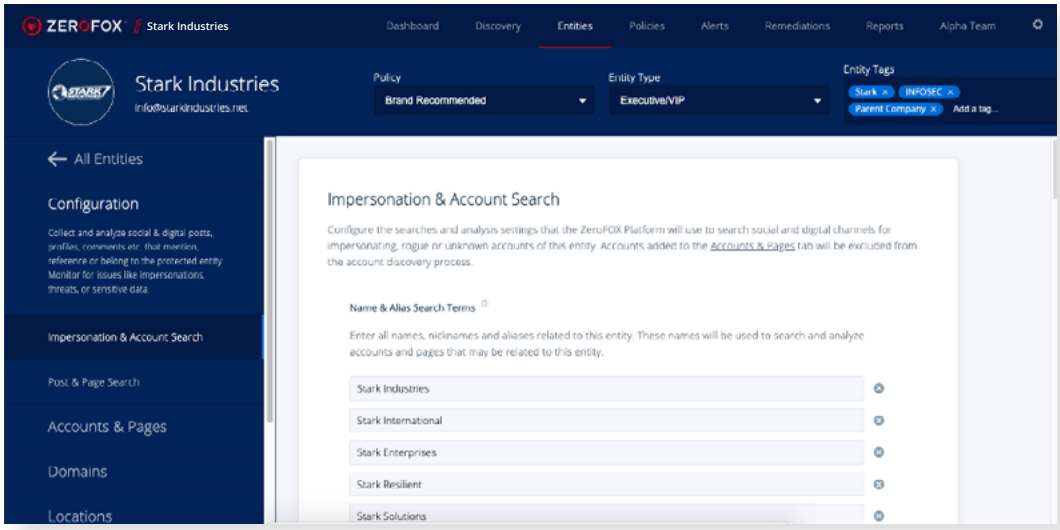

ZeroFOX Platform and ZeroFOX Alpha Team 12 Month Activity

# Protection

Modern businesses have a massive footprint on social and digital channels—all of which is ungoverned, unmonitored and unprotected by the existing security perimeter—exposing them to continuous cyberattacks, physical threats and brand risk.

## // ENTITIES

Entities are anything that matters to your organization—brands, employees, executives and VIPs, products, locations and corporate pages—and are composed of a variety of different "objects"—profiles, names, keywords, images, domains, hashtags and more. Entities govern where and how ZeroFOX gathers data, ensuring what is ingested is only the data that is relevant to your organization. During the launch phase of onboarding, our team of launch specialists help correctly configure your entities.




### Brand Protection

Your brand encompasses any and all external representation of your organization. Protect your digital presence, owned assets and accounts, logos and trademarks against account hacking, impersonations, malicious content and reputation damage.

### Account Protection

Owned social media accounts allow an organization to engage directly with followers, prospects and customers. Protect brand and executive accounts against account hacking attempts and offensive content published to your pages and profiles. Quickly freeze accounts at early warning signs of hijacking.

### Executive Protection

Executives, VIPs, and high profile clients have a large digital presence, some of which is owned and some of which is outside their control. Protect executives against spear-phishing attacks, impersonations, account hacking, physical threats and more.

### Employee Protection

Employees are the number one target for cyberattacks on an organization. Keep your employees up to date on the latest social media security best practices and enable them to protect their social accounts against account hacking in a unique instance of the ZeroFOX Platform.

### Location & Event Protection

With bad actors posting attack plans and threats online, the line between physical and digital threats is increasingly blurred. Protect your locations, including headquarters, stadiums, facilities, and residences, and events against threats of violence and targeted attacks. Gain situational awareness and early warning of attack planning or nearby threats to your locations and events.

### Web Domain Protection

Your owned websites often serve as the first form of engagement a customer, prospect, candidate or employee uses to connect with your organization. Bad actors know this, and create fraudulent, spoofed, and impersonating domains that trick your customers into providing information and damage your brand. Protect your owned domains through identification and remediation of impersonating domains, trademark infringement, and spoofing.

### Email Abuse & Phishing Protection

The Email Abuse and Phishing Detection service enhances organizational protection and detects brand abuses leveraging existing information such as DMARC failure reports and forwarded 'abuse@.....' emails. Combined with ZeroFOX capabilities for analyzing and remediating malicious domains, brand impersonations and offensive content, the service uniquely provides the ability to identify and take down attacker infrastructure to disrupt attackers and prevent future attacks. The service works in concert with standard anti-spam, anti-virus and mail filtering gateways intended to protect users and message content.

### Business Email Compromise (BEC) Protection

ZeroFOX Business Email Compromise enhances organizational email security, detecting email impersonations and alerting targeted employees. It complements current email protection solutions, extending protection to address one of the toughest digital threats facing organizations today. ZeroFOX analyzes inboxes to identify malicious emails stemming from BEC attacks, flagging malicious emails through banner warnings and remediating malicious domains hosting attacker email addresses to keep your employees and customers protected.

### Remote Workforce Protection

Secure Zoom meetings and stop Zoombombing with automated protection. Identify stolen credentials and malicious Zoom meeting links. Monitor chats and attendee lists for signs of malicious or inappropriate activity to ensure secure video conferencing for employees, customers and partners. ZeroFOX for Slack protects your internal and external collaboration teams by identifying and remediating malicious, inappropriate or confidential content posted in your Slack channels. ZeroFOX for Slack is set up in seconds, identifies attacks and compromising content in real-time, and provides in-line automated content removal with in-channel alerts.

## // USE CASES

ZeroFOX provides information security, corporate security and brand protection teams with the critical visibility and automated controls necessary to safeguard against external social and digital threats, and address the following:

| | |
|---|---|
| Compromised Credentials | Fraud, Piracy & Scams |
| Identity Theft & PII | Violence |
| Inappropriate Use | Insider Threats |
| Emerging Threats | Spoofed Accounts |
| Executive Impersonations | Brand Impersonations |
| Account Takeover | Physical Threats |
| Data Loss | Travel Threats |
| Compliance Violations | Threat Intelligence |
| Phishing/Smishing & Malware | Custom Rules & Policies |

## Advanced Phishing Detection

Comprehensive detection of phishing attacks, wherever they occur: on social media, email, domains and more. ZeroFOX identifies known and new phishing URLs, regardless of whether they are hosted on domains or subdomains that include relevant terms to your organization. Through the collection of hosted content, ZeroFOX alerts you if your logo or brand terms are included as part of any hosted phishing content. ZeroFOX's Advance Phishing Detection enables your organization to:

- Monitor for new domain and subdomain registrations that use your organization's brand names and associated terms
- Monitor phishing data feeds for new phishing URLs that reference your organization's brands
- Utilize Certificate Transparency Logs for new certificates that reference your brand names
- Search for URLs that mention relevant terms associated with your organization in page content

## 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. ZeroFOX identifies malicious URLs in your social media environment.

## Account Compromise

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

## Fraudulent Brand & Executive Accounts

Fraudulent and spoofed accounts leverage the implied trust on social media, email and legitimate websites to launch phishing attacks, perpetrate scams, and damage brands. ZeroFOX identifies and removes accounts, email addresses and domains impersonating your brand or people.

## Customer Fraud & Scams

Whether financial fraud, billing scams or fake offers, social media and digital platforms expose your customers and brand reputation to exploitation. ZeroFOX identifies this malicious activity, mitigating the costs around remediation, customer support and lost business.

## Physical & Cyber Situational Awareness

Adversaries, both physical and digital, frequently telegraph their intentions on the internet. ZeroFOX monitors for organization-specific keyphrases and terms, alerting you to malicious chatter about your organization or posts within a specific geography.

## 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 scans these channels to identify where this data or other sensitive company IP has been exposed.

## Insider Threat

The risk of an insider threat ranges from disgruntled employees absconding with sensitive data to staff posting non-compliant content on social media or on collaboration tools to threats both physical and cyber. ZeroFOX identifies damaging activity unique to your organization, both inside and out.

## 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. ZeroFOX automatically identifies proprietary content, posted intentionally or not, circulating on social media.

## Domain Spoofing & Typo Phishing

Attackers squat on domains similar to your organization's, either relying on user typos or leveraging them in social engineering attacks targeting your customers. ZeroFOX identifies and removes domains similar to yours across gTLDs, ccTLDs and impersonating subdomains.

## Executive & Corporate Threats

Executives and corporate assets are exposed to risks on the dark web and even on social media, such as doxxing, lost PII, physical threats and exposed travel details. ZeroFOX monitors executive & corporate accounts and the digital world for malicious activity, threats or sensitive content.

## Offensive Content & Corporate Page Risks

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

## // DISCOVERY

Using the Discovery capability, you can search across social networks and the social web (forums and paste sites), all from a single console. From the Discovery page, analysts can map their organization's social media footprint, find new profiles for protection, look for rogue accounts, identify adversary profiles, search for stolen information or investigate attacks being planned.

# AI Analysis

## // 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 you exposed. ZeroFOX's AI toolkit consists of machine learning and computer vision capabilities to detect threats in text, image and video beyond traditional security solutions.

## // FOXSCRIPTS

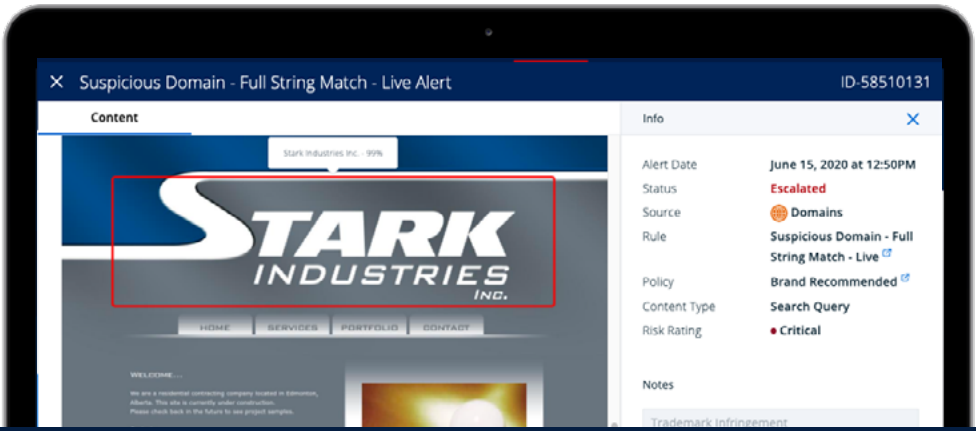
FoxScript, a part of the ZeroFOX Platform, is a JavaScript-based language that opens the power of ZeroFOX's data collection and analysis engines to virtually any use case. This fine-tuning capability means each organization can regulate the volume of their alerts, ensure only the most critical information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

## // RULES AND POLICIES

Once entities have been configured, you can determine what analyses to perform for each entity, 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 policies are turned on, and which policies apply to which entities. ZeroFOX comes out of the box with hundreds of default rules for the most prevalent challenges on social media, including malicious links, impersonations accounts, violence, offensive content, compromised accounts, compliance violations (PCI, FFIEC, HIPAA, GDPR, etc), scams, PII and much more.

## // ALERTS

Once entities 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 entity, type of threat, timestamp, social network and much more. Each alert contains the content of the offending post or profile, threat metadata, perpetrator intelligence, alert logs and the ability to take action on the alert, including assigning the alert, emailing the alert, whitelisting the perpetrator 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.



# Remediation

## // ZEROFOX TAKEDOWN-AS-A-SERVICE

ZeroFOX's Takedown-as-a-Service™ provides comprehensive remediation capabilities to directly address threats, including hiding, blocking and removing malicious or offending content, removing fake accounts and sites, and enforcing service terms.

ZeroFOX saves you from the manual, costly and arduous process of finding and taking down malicious profiles and dangerous posts, working on your behalf to package and report directly to the source provider for removal. ZeroFOX maintains the most effective and broadest automated takedown capabilities of any security vendor across a wide range of data sources including social media, web, deep and dark, domains and more, saving you time and resources.

Whether the culprit is a malicious profile or a dangerous post, ZeroFOX saves you from the manual, costly and arduous process of finding and taking down unwanted content, working on your behalf to automate the process of packaging and directly reporting it to the data source provider for removal. ZeroFOX maintains the most effective and broadest takedown capabilities of any security vendor across a wide range of data sources including social media, surface web, deep web, paste sites, marketplaces, mobile app stores, domains and more, saving you time and resources.

# Intelligence

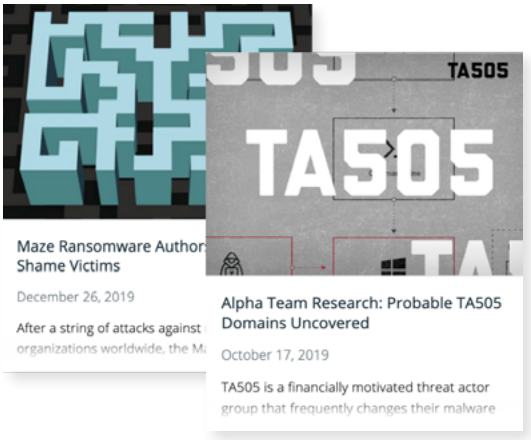
Enrich traditional security programs with intelligence uniquely focused on social media and digital threats across surface, deep and dark web. ZeroFOX's Global Threat Intelligence offering provides finished intelligence including advisories, threat actor and campaign research, vulnerability and breach notifications, and breaking news. Combined with a threat feed of social media and digital threat indicators, such as malicious domains/IPs, impersonating user profiles, and phishing email addresses that integrate directly into major threat intelligence platform providers. ZeroFOX Global Threat Intelligence enhances threat intelligence programs with a unique focus on social media and digital platforms that traditional threat intelligence providers lack.

## // BREAKING NEWS

ZeroFOX's Alpha Team curates and contextualizes relevant breaking news stories, delivering them to users directly within the ZeroFOX Platform as well as to your email inbox through the Alpha Team Daily Digest.

## // 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 attacks, research reports and more.



## // VULNERABILITY INTELLIGENCE

ZeroFOX Vulnerability Intelligence allows security teams to reduce time spent on vulnerability research with automatic alerts about the vendors and products that actually matter to your organization. Gain access to vulnerability intelligence through AI and human-driven identification and enrichment of vulnerabilities daily. Search and filter through a full repository of vulnerabilities and export relevant vulnerability intelligence. Receive relevant alerts, understand associated risk and take appropriate action. Each vulnerability includes key contextual details such as severity, impact and recommendations.

# Managed Services

## // ONWATCH™ SERVICES

Your ZeroFOX coverage and protection are fully managed and supported by our team of experts. ZeroFOX OnWatch™ provides initial configuration, continuous optimization, and 24/7 support including alert triage, validation, analysis and response with tailored workflows to meet unique use cases.

ZeroFOX OnWatch™ extends AI-driven analysis performed by the ZeroFOX Platform to help customers gain peace of mind and comprehensive digital risk protection. Let our team manage the entire process of validation, analysis and escalation so you can focus on your business. ZeroFOX OnWatch™ extends the value of the ZeroFOX Platform, saving you valuable time and resources.

### ZeroFOX OnWatch™ includes:

- Initial onboard configuration and setup
- 24x7 platform support
- 24x7 managed service alert validation, triage and investigation, escalation, and response services
- Customer workflow design
- Expert ongoing configuration, tuning, and consultation
- Continuous platform optimization services
- Online access to ZeroFOX University

## // CUSTOM THREAT ANALYSIS

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 investigation requests and/or persistent issues.

# Integrations

Built entirely on REST APIs, the ZeroFOX Platform is extensible to a wide variety of existing security and analytics tools, extending social and digital protection seamlessly into the existing SOC. In addition, ZeroFOX offers an array of custom-built apps and integrations, including Splunk, ArcSight, FireEye, Maltego, Anomali, ThreatConnect, ThreatQuotient and more.

# 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 & 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, configure platform settings and enhance your platform experience.

## // ZEROFOX UNIVERSITY

ZeroFOX offers training programs, both technical and non-technical, 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.

# Get Started With ZeroFOX

### 1 Decide what's important

Tune the platform to collect data relevant to your organization by configuring your entities, or investigate what's important using the platform's real-time, cross-network Discovery capability.

### 2 Define your policies

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 Receive alerts on risks

Automatically receive real-time alerts as the platform identifies risks. Each alert comes packaged with threat intelligence, alert logs, perpetrator intelligence and remediation actions.

### 4 Remediate malicious content

Issue takedown requests from within the platform, and ZeroFOX works on your behalf to package and send violating content directly to the social network.

### 5 Integrate data in your environment

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

# About ZeroFOX

ZeroFOX, the market leader in public attack surface protection, safeguards modern organizations from dynamic security, brand and physical risks across surface, deep and dark web, social, mobile, email and collaboration platforms. Using diverse data sources and artificial intelligence-based analysis, the ZeroFOX Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more. The patented ZeroFOX SaaS technology processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Twitter, Instagram, Pastebin, YouTube, mobile app stores, the deep and dark web, domains and more.

ZEROFOX®

CONTACT US: (855) 736-1400 | SALES@ZEROFOX.COM | ZEROFOX.COM