National Bank of Moldova.

Brand Protection & Digital Risk Protection Proposal

PREPARED BY:
Gabrielle McManus
Enterprise Account Manager
gmcmanus@zerofox.com

PRESENTED: 30th March 2025

Digitally signed by Vicol Irina
Date: 2026.04.07 15:43:15 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Executive Summary

Dear National Bank of Moldova.

ZeroFox would like to thank you for the opportunity to respond to your requirements around Brand, Domain and Executive Protection. The proposal set forth includes all the information discussed and validated during our initial engagement. As well as the indicative commercial proposal detailing the solution required to meet and exceed National Bank of Moldova's requirements. We look forward to reviewing the proposal in detail and ZeroFox's suitability as a partner.

We are committed to developing a successful partnership with National Bank of Moldova and to providing industry acknowledged thought leadership in combination with our comprehensive holistic Threat Intelligence and DRP Services. This partnership would be built on a foundation of trust and communication as we mutually create and implement a robust security program together for the entire organization.

Scope (not limited to):

Utilising the services detailed within this proposal ZeroFox, will be able to meet and exceed requirements in relation to the below scope as identified by National Bank of Moldova:

- VIP / Executive Impersonation
- Social Media monitoring
- Domain protection / monitoring
- Mobile application monitoring
- Dark web monitoring
- Brand protection

Bank of Moldova Requirements

We are happy to discuss the details and our pricing model to ensure full transparency and understanding. ZeroFox offers a bundled licensing model and with that we have outlined both the core requirements and what is included beyond that.

Core Requirements

1. Threat Mitigation	
Service/Solution Description	**ZeroFox Response**
Ability to block and remove fraudulent, malicious and illegal accounts, websites and content.	ZeroFox offers a fully managed takedown service, supported by in-house expertise, that addresses the removal of malicious domains, impersonating social media accounts, fraudulent mobile apps, marketplace listings, and other violating content.
Support for social networks, mobile app stores, cloned sites, domains and other platforms.	The platform continuously scans for newly registered or active domains and subdomains that may misuse organisational brand names, typosquats, homoglyphs, associated terms, or stolen website code. For social media, ZeroFox covers major global platforms, including Facebook, Instagram, Twitter (X), LinkedIn, YouTube, TikTok, Snapchat, BlueSky, and Telegram, detecting and addressing malicious activities in real time, such as phishing campaigns, scam promotions, and brand abuse. We also have access to Mobile Apps
Automation of takedown requests through a global network of content blocking partners.	ZeroFox provides automated takedown request processing with distribution of indicators of attack to approximately one hundred of the world's largest digital providers. Customers can automate takedown requests directly from the platform for malicious or spoofed domains, impersonating social media accounts, fraudulent mobile apps and marketplace listings, content that infringes copyright or IP, and content that violates hosting provider terms of service. The Global Disruption Network (GDN) enables automated submission to 50+ partners with collective intelligence from 80+ partners including ISPs, DNS and Cloud providers, domain hosts and registrars and web security blocklists. Submissions are automatically tagged for takedown and sent to the Global Disruption Network, triggering blocking actions in significantly less time than traditional takedowns (minutes/hours vs. days/weeks).
Ability to track the status of requests through a centralized platform.	ZeroFox tracks takedown submissions through a dedicated in-platform dashboard, providing analysts with real-time status visibility and eliminating the need for updates via email or vendor calls. The platform consolidates alerts and metrics in a centralised dashboard, offering a near real-time visual overview of the organisation's risk landscape. The disruption module allows users to access information related to the takedown process for domains and other threats, track the status of takedowns, view disruption actions performed, and review additional evidence requirements.
Support from an incident management team available 24/7.	ZeroFox provides dedicated analyst support for alert investigations through its Security Operations Center (SOC), with certified analysts available 24/7/365.

Universal takedowns: minimum 12 takedowns included in the offered license.	Included, ZeroFox will support up to 250 takedowns within the current proposal.

2. Management and Key Personnel Protection	
Service/Solution Description	**ZeroFox Response**
Minimum 5 employees or managers included in the offered license.	ZeroFox allows unlimited platform access for users.
Monitoring for impersonation of accounts, unofficial accounts on social networks.	ZeroFox provides active monitoring and protection across major global social media platforms, including Facebook, Instagram, X (Twitter), LinkedIn, YouTube, TikTok, Snapchat, BlueSky, and Telegram. Monitoring also extends to domains and subdomains, covering threats to brands, executives, and key digital assets. ZeroFox uses advanced machine learning and AI-based analysis to examine text, images, and video content, detecting threats such as impersonation and fraudulent accounts. The ZeroFox Platform delivers comprehensive detection and takedown services for fake profiles and accounts that impersonate identities across social media platforms. Upon identification of impersonating accounts, ZeroFox manages the complete takedown process through automated and manual methods. The service includes unlimited removal of fraudulent and impersonating accounts through a fully managed takedown process.
Monitoring for possible compromised credentials including deep web and dark web.	The platform detects data compromise incidents and attacks by collecting breach data from multiple sources, including third-party breaches, the deep and dark web, and botnet data. It monitors for keywords and accounts associated with the organisation, its staff, and its customers, and provides notifications when access to accounts is identified for sale.
Doxxing Monitoring – detecting unauthorized publication of private information by searching public databases, social networks and using hacking and social engineering techniques to identify malicious intent.	ZeroFox's platform uses 24/7 automated crawlers and APIs to discover doxxing content across social media, the open web, deep and dark web, data brokers, and marketplaces. The platform continuously monitors dark web marketplaces, forums, and messaging platforms—including Telegram, Discord, and covert communication channels—to detect and analyse doxxing attempts, personal data exposure, and information leaks related to VIP personnel. When doxxing content or threats are identified, the ZeroFox SOC prioritises alerts and supports risk-based prioritisation of discovered content.
Continuous detection and automatic removal of personal data exposed on data brokerage sites.	ZeroFox scans more than 150 data broker sites to identify personally identifiable information (PII) related to assigned executives and employees. When PII is found, the PII Removal service automates its removal from data broker websites and associated Google search results. The service includes ongoing monitoring to detect if PII reappears, triggering automated removal as needed.

3. Brand and Company Protection	
Service/Solution Description	**ZeroFox Response**
Brand and NBM threat monitoring for one (1) brand, covering all data sources (open, deep and dark web). Includes protection against:	ZeroFox Brand Protection allows security teams to proactively address external threats to revenue, reputation, and customer engagement. The platform monitors for risks targeting brands, sub-brands, products, and intellectual property across the surface, deep, and dark web. Threats include

	brand impersonation, fraud, scams, abuse, piracy, counterfeiting, attack chatter, breach evidence related to branded terms, compromised account credentials, BIN number exposures, rogue mobile apps, doxxing, data exposure, and mentions or breach evidence on OSINT and non-OSINT channels.
Brand impersonation	ZeroFox Brand Protection allows security teams to proactively address external threats to revenue, reputation, and customer engagement. The platform monitors for risks targeting brands, sub-brands, products, and intellectual property across the surface, deep, and dark web. Threats include brand impersonation, fraud, scams, abuse, piracy, counterfeiting, attack chatter, breach evidence related to branded terms, compromised account credentials, BIN number exposures, rogue mobile apps, doxxing, data exposure, and mentions or breach evidence on OSINT and non-OSINT channels.
Negative brand mentions	We can support negative sentiment
Evidence of security breaches in non-OSINT sources (data exfiltration, compromised credentials, credit cards and other personal or proprietary data)	ZeroFox Brand Protection allows security teams to proactively address external threats to revenue, reputation, and customer engagement. The platform monitors for risks targeting brands, sub-brands, products, and intellectual property across the surface, deep, and dark web. Threats include brand impersonation, fraud, scams, abuse, piracy, counterfeiting, attack chatter, breach evidence related to branded terms, compromised account credentials, BIN number exposures, rogue mobile apps, doxxing, data exposure, and mentions or breach evidence on OSINT and non-OSINT channels.
Includes protection for: – 1 domain and all its subdomains – 1 corporate social media account – 1 mobile application	This is included.
Threat monitoring across all available sources (open, deep and dark web).	Yes, the ZeroFox platform supports data collection from all the specified sources. ZeroFox monitors digital channels—including the surface, deep, and dark web—to protect executives, VIPs, and brands from a wide range of threats. The platform provides real-time, continuous monitoring across supported data sources such as domains, web searches, blogs, forums, news, paste sites, and social media platforms (including Facebook, Instagram, LinkedIn, Twitter, TikTok, Telegram, and YouTube).
Detection of impersonations, negative mentions, data leaks and credential compromise.	These can all be supported.
Support for protecting the domain, corporate social media accounts, mobile applications and financial assets.	These can all be supported.
Monitoring of data leaks, credential compromises and other sensitive information.	ZeroFox provides comprehensive data leak exposure monitoring to detect the exposure of sensitive information and credentials across the surface web, deep web, and dark web. The platform monitors for a wide range of leaked data, including compromised account credentials, employee Personally Identifiable Information (PII), payment cards, technical and commercial documents, marked documents, sensitive code, and intellectual property. Monitoring extends to unsecured S3 buckets, web repositories, and numerous online sources, including surface web platforms, well-known deep

	and dark web forums, marketplaces, and messaging channels such as Pastebin, Telegram, Discord, and IRC. Additional coverage includes covert communication channels and social media platforms like GitHub, GitLab, Bitbucket, Instagram, Twitter, and YouTube.

4. Threat Intelligence and Search	
Service/Solution Description	**ZeroFox Response**
Access to a database of cyber threat intelligence, including attacks, vulnerabilities, and indicators of compromise. Includes at a minimum:	ZeroFox maintains an expansive threat intelligence data graph with over 12 billion interconnected data points covering attacks, vulnerabilities, and indicators of compromise. The Intelligence Search module provides unlimited access to petabytes of curated data and intelligence, including both finished intelligence and raw data spanning over 20 years of historical threat intelligence. Users can 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, and other threat indicators. The platform enables correlation of alerts with known malicious network IoCs like Command and Control domains, compromised account credentials, "zombie" IP addresses found in information stealer logs, and ransomware and malware hashes. The platform provides threat feeds with indicators of compromise (IOCs) delivered via REST API, including timely, contextualised, and actionable intelligence with analytic standards and contextual descriptions.
– License for one user of the intelligence platform	This is included.
– Enterprise API key for access to the intelligence database	ZeroFox offers access via the Intel Search. ZeroFox can look to support the bank with Threat feeds separately.
– Unlimited threat searches	Unlimited
– Strategic intelligence reports	ZeroFox's Global Threat Intelligence offering provides finished intelligence including: • Advisories and threat actor research • Campaign research and vulnerability notifications • Weekly Threat Intelligence bulletins • Industry-specific threat landscape reports • Threat forecast reports • Geo-political event analysis • Dark web incidents tracking (ransomware, data leaks, fraud, malware)
– 24/7 technical support	ZeroFox offers 24x7x365 global technical and operational support
Rapid correlation of alerts with known indicators of compromise (IOCs), such as:	ZeroFox rapidly correlates alerts with known malicious network IOCs including Command and Control (C2) domains, compromised account credentials, "zombie" IP addresses found in information stealer logs, and ransomware and malware hashes.
– Command and Control (C2) domains	ZeroFox Intelligence Search enables rapid correlation of alerts with known Command and Control (C2) domains using a massive intelligence graph of over 12 billion interconnected data points delivering actionable intelligence across the surface, deep, and dark web in real time. SOC analysts can quickly

	correlate alerts with known malicious network IOCs like Command and Control (C2) domains. ZeroFox correlates detected C2 infrastructure against comprehensive threat intelligence sources including commercial threat intelligence feeds with known C2 domains and IPs with malware family attribution, open source threat intelligence (OSINT) with community-contributed C2 indicators from malware analysis, malware analysis platforms with C2 infrastructure extracted from dynamic malware sandbox analysis, and ZeroFox internal research with C2 infrastructure discovered through ZeroFox threat research and proprietary C2 intelligence from active campaign monitoring. The platform performs active analysis of detected C2 candidate infrastructure including C2 panel detection using HTTP response analysis to identify C2 administration panel interfaces, SSL/TLS fingerprinting (JA3/JA3S) with TLS handshake fingerprinting to identify characteristic malware communication patterns, and HTTP/S beaconing pattern detection using URI pattern analysis and request interval analysis to identify C2 communication patterns in HTTP/S traffic.
– Compromised credentials	ZeroFox Intelligence Search enables rapid correlation of alerts with known Command and Control (C2) domains using a massive intelligence graph of over 12 billion interconnected data points delivering actionable intelligence across the surface, deep, and dark web in real time. SOC analysts can quickly correlate alerts with known malicious network IOCs like Command and Control (C2) domains. ZeroFox correlates detected C2 infrastructure against comprehensive threat intelligence sources including commercial threat intelligence feeds with known C2 domains and IPs with malware family attribution, open source threat intelligence (OSINT) with community-contributed C2 indicators from malware analysis, malware analysis platforms with C2 infrastructure extracted from dynamic malware sandbox analysis, and ZeroFox internal research with C2 infrastructure discovered through ZeroFox threat research and proprietary C2 intelligence from active campaign monitoring. The platform performs active analysis of detected C2 candidate infrastructure including C2 panel detection using HTTP response analysis to identify C2 administration panel interfaces, SSL/TLS fingerprinting (JA3/JA3S) with TLS handshake fingerprinting to identify characteristic malware communication patterns, and HTTP/S beaconing pattern detection using URI pattern analysis and request interval analysis to identify C2 communication patterns in HTTP/S traffic.
– Zombie IPs from Botnet logs	Our platform automatically correlates alerts with compromised account credentials and other known malicious network IOCs. ZeroFox continuously monitors for compromised credentials across dark web sources, breach databases, and underground marketplaces and delivers real-time alerts.
– Ransomware and malware hashes	Users can 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, and other threat indicators. The platform enables correlation of alerts with

	known malicious network IoCs like Command and Control domains, compromised account credentials, "zombie" IP addresses found in information stealer logs, and ransomware and malware hashes.
Detailed analyses of threat actors targeting the banking industry and the surrounding region, including TTPs per MITRE and MISP frameworks.	ZeroFox provides external threat intelligence services through its proprietary platform. Within the Intelligence tab, users can access a dataset profiling over 300 prominent threat actors, including information on tactics, techniques, and procedures (TTPs), MITRE ATT&CK and MISP IDs, and descriptions of threat actor activities. Intelligence on these threat actors and their associated TTPs, aligned with the MITRE ATT&CK framework, is also accessible via the Threat Actors API endpoint.
Investigations to collect IOA, IOC, and Dark Web chatter to improve defensive strategy.	ZeroFox builds investigations to compile relevant IOAs, IOCs, and Dark Web chatter to inform your defensive strategy. The platform provides detailed analyses of threat actors targeting your industry and region, including TTPs mapped to MITRE ATT&CK. ZeroFox DarkOps continuously monitors the dark web for the latest trends in cyber-attacks, tracking threat actors and performing security investigations. ZeroFox delivers external threat intelligence utilising both automated and human intelligence collection methods, gathering information from a wide range of OSINT (Surface) and Deep/Dark Web sources, including social networks, domain registrations, email, surface, deep and dark web sites, forums, and marketplaces.
Analysis of critical vulnerabilities and exploits to prioritize and recommend mitigation measures.	These can all be supported - License dependent The ZeroFox Platform and attack surface discovery continuously identifies and monitors exposed services and systems to detect shadow IT assets, risky services, and associated vulnerabilities. Each discovered vulnerability is mapped to standardised CVE identifiers, enabling precise tracking and remediation across environments. To assess threat relevance, the platform cross-references CVEs against CISA's Known Exploited Vulnerabilities (KEV) Catalog, flagging vulnerabilities that are actively being exploited. Vulnerabilities are also evaluated using the Exploit Prediction Scoring System (EPSS), which estimates the likelihood that a given CVE will be exploited within the next 30 days. By correlating CVEs with KEVs and applying EPSS scoring, security teams can prioritise remediation efforts based on asset criticality and real-world exploitability. We also can support providing information via our intelligence tool
Automated reports and analysis, including strategic summaries and IoC.	ZeroFox offers both out-of-the-box self-service reporting and analyst-derived custom reporting. The platform delivers information in formats tailored to stakeholder needs and provides real-time monitoring and alerting across all supported data sources, operating continuously. Dashboards present threat status, trends, KPIs, and contextual threat intelligence, including alert logs, perpetrator information, and remediation actions.

	Intelligence output formats include IOCs, TTPs mapped to MITRE ATT&CK, threat actor profiles, campaign tracking reports, on-demand investigation briefs, and real-time feeds consumable by SIEM, TIP, and SOAR platforms via REST API and over 700 pre-built connectors.

5. Managed Platform	
Service/Solution Description	**ZeroFox Response**
24/7 threat monitoring by SOC specialists.	ZeroFox's global SOC and OnWatch teams, staffed by security-certified experts, provide managed security services 24x7x365.
Automated and manual collection of intelligence from OSINT, deep and dark web sources.	ZeroFox uses a multi-layered approach to collect and analyse data from a wide range of digital channels. The platform monitors closed forums and unindexed digital spaces to identify information on the dark web. Data collection covers sources including hacker forums, illicit marketplaces, leak sites, Telegram channels, Discord servers, IRC networks, OSINT (surface), deep and dark web sites, social networks, domain registrations, email, blogs, news, paste sites, and other covert channels. Collection methods include automated bots and scrapers, API integrations with various platforms, proprietary techniques, and manual threat analyst infiltration of closed forums. Data is collected daily through both automated and manual processes.
Support for AI-based threat analysis.	ZeroFox uses AI-driven analytics and custom rules to automate threat detection, remediation, and reduce risk exposure. The platform applies a range of AI techniques, including natural language processing (NLP), sentiment analysis, optical character recognition (OCR), computer vision, anti-cloaking, logo, weapon, and credit card detection, as well as facial matching models. Generative AI, such as FoxGPT, is being incorporated to accelerate intelligence analysis across large datasets and enhance the identification of malicious accounts and attacks.
Access to vulnerability reports and cyber threat analysis.	ZeroFox delivers vulnerability intelligence by automatically collecting and analysing data from multiple authoritative sources, including CVE databases, the National Vulnerability Database (NVD), vendor security advisories, and proprietary research. The platform correlates identified vulnerabilities with specific infrastructure and assets, supporting risk-based prioritisation to focus remediation efforts on the most critical exposures. Real-time alerts are provided for newly disclosed vulnerabilities affecting the environment, along with exploit availability tracking and integration of vulnerability context with broader threat intelligence to assess active exploitation risks. The platform offers dedicated threat intelligence advisories and contextual intelligence reports covering cyber-attacks, incidents, breaches, threat actor groups, and major cyber events. The Global Threat Intelligence offering includes advisories, research on threat actors and campaigns, notifications of vulnerabilities and breaches, and Weekly Threat Intelligence bulletins.
Inclusion of training materials and user support.	ZeroFox provides comprehensive support for onboarding and ongoing use of its platform, including initial configuration and setup, customer workflow design, expert configuration, tuning and consultation, platform optimisation,

	and health checks. Users have online access to ZeroFox University, which offers training and education programs with two courses: Certified Security Analyst and Certified Security Engineer. The ZeroFox Platform features a library of support articles, documentation, and troubleshooting guides accessible through the support portal. Training resources cover platform navigation, alert triage and management, takedown submission and tracking, API configuration, integration setup, and solution-specific guidance across Brand and Domain Protection, Attack Surface Intelligence, CTI, Executive Protection, and Physical Security Intelligence. User guides and technical documentation provide reference material for platform configuration, API documentation, connector setup, and evidence package management.
OnWatch Alert: 24x7x365 threat management by SOC experts.	ZeroFox OnWatch™ Alert extends digital visibility and protection by providing 24x7x365 managed services through a global SOC staffed by security-certified experts. The OnWatch team reviews, triages, and escalates incidents, prioritises threats, and processes takedown requests on behalf of your organisation.
Global Intelligence Collection (GIC): data collection from OSINT (open), Deep and Dark Web, including social networks, hidden forums, code repositories and vulnerability databases.	ZeroFox provides external threat intelligence for digital business platforms, utilising both automated and human intelligence collection methods. Information on protected assets is gathered from a wide range of sources, including OSINT (Surface), Deep, and Dark Web data. These sources encompass social networks, domain registrations, email, surface, deep and dark web sites, forums, and marketplaces.
Engine AI analysis: automated threat analysis using artificial intelligence.	The ZeroFox Platform utilises machine learning and artificial intelligence-based analysis at global scale to identify hidden threats that evade traditional detection methods within objects, images, and video. This accelerates remediation for targeted phishing attacks, credential compromise, impersonations, brand hijacking, executive and location threats, among others.
Finite Information & Vulnerability Alerts: strategic reports and insights on current vulnerabilities and threats.	Vulnerability intelligence is delivered by automatically collecting and analysing data from multiple authoritative sources, such as CVE databases, the National Vulnerability Database (NVD), vendor security advisories, and proprietary research. The platform correlates identified vulnerabilities with specific infrastructure and assets, supporting risk-based prioritisation to focus remediation efforts on the most critical exposures. Real-time alerts are provided for newly disclosed vulnerabilities affecting the environment, along with exploit availability tracking and integration of vulnerability context with broader threat intelligence to assess active exploitation risks.

Included

Service/Solution	Description	Quantity
Foundation Bundle	he ZeroFox Foundation Bundle offers AI-enabled Brand Protection, Domain Protection, and Takedown services to help security teams mitigate external threats to an organization's revenue and reputation. What's Included: ● Brand Protection (2) ● Domain Protection (10) ● Takedown (250/yr.) ● Platform Alerts & Takedown API Connector (1) ● OnWatch Alert (Managed Service) Brand Protection (2) Monitoring for brand and organizational threats for brands, sub-brands or product line/family across all data sources of surface, deep and dark web. This includes brand impersonation, mentions or breach evidence on non-OSINT channels. Includes monitoring for corporate social accounts for a given brand or product. Domain Protection (10) Protection for company owned domains/sub-domains through continuous identification and remediation of impersonating domains, trademark infringement, and spoofing against bad actors that trick your customers into providing information and damage your brand. Includes protection for the primary domain for a given brand or product. Each domain protected asset covers all derivative sub-domains for the same primary domain. Takedown (250/yr.) Takedown and/or disruption actions of any and all applicable impersonating or malicious account/site/content and other terms of service violations from social networks, mobile app stores, paste sites, domains, code shares, and other data sources (excluding deep and dark web). Rapidly Identify and automate the request submission process to remove or block malicious sites and content with end-to-end visibility. ● Takedown malicious & illegal content across social media platforms ● Takedown malicious & illegal domains ● Automated requests to our Global Disruption Network partners for content blocking and attacker campaign disruption ● Full-transparency of takedown status via in-platform experience and managed service team support Platform Alerts & Takedown API Connector (1) Connect alerts from the ZeroFox platform with your other internal tools and applications to streamline your security programs. Also request takedowns through the API from your application. Customers are entitled	1

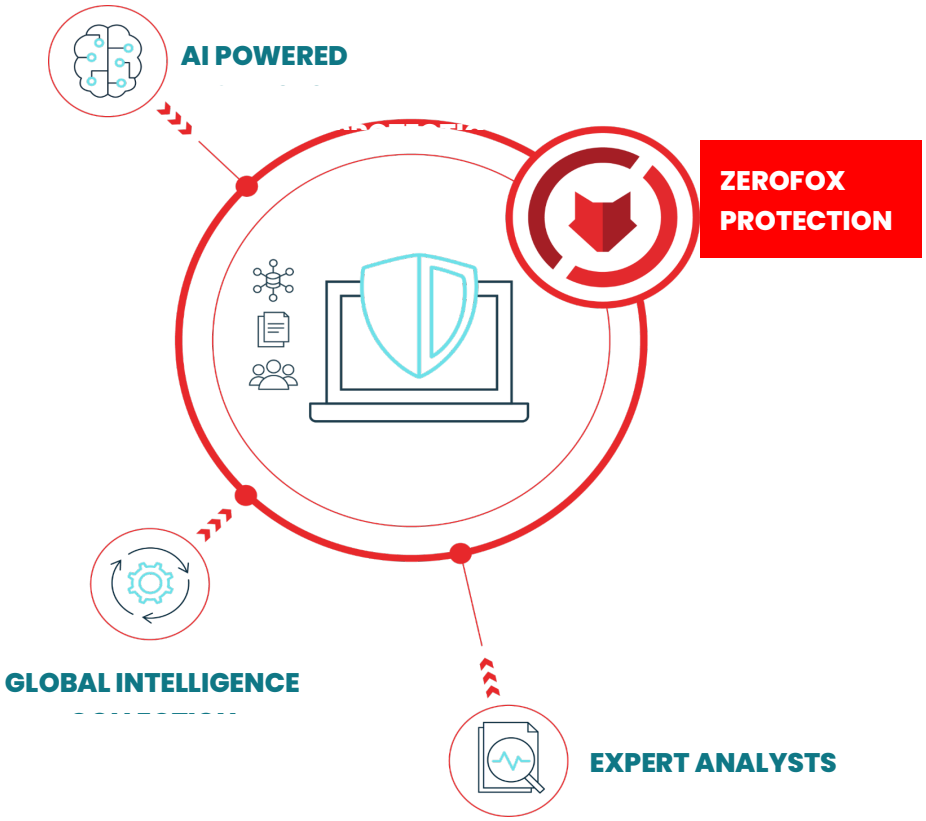
	to support for integration enablement and ongoing Platform API support and maintenance. OnWatch Alert Platform support for the ZeroFox platform: ● 24x7 Alert Review, Validation and Escalation ● Global SOCs, SOC 2 Type 2 Certified ● Standard Launch and 24x7 Support ● Access to Global Intelligence Collection (GIC) ● Advanced AI Analysis Including Computer Vision, NLP, Image Analysis, Machine Learning, and more	
Executive Protection	Protect VIPs against account takeovers (ATOs), impersonations, sensitive information leakage, doxxing, credential compromise and cyber-threats. Executive Protection comes with PII Removal*, which scans a multitude of data broker sites to look for assigned executives' and your employees' personal information. Once the PII is identified, PII Removal automates the request to remove this information from data broker websites and related Google search results. Executive Protection Use Cases: The ZeroFox platform provides executive protection coverage for the following use cases: ● Executive Impersonation Monitors for impersonations, unofficial, or unsanctioned accounts of executives across social media. ● Compromised Credentials Continuously monitors the surface, deep and dark web for any mentions of possible compromised credentials of protected VIPs and executives. ● Doxxing Monitoring Monitor for instances of doxxing for executives and other VIPs – doxxing is a technique in which data about an individual is shared online often with the intent to harass or embarrass. Methods employed to acquire this information include searching publicly available databases and social media websites, hacking, and social engineering. What's Included: ● Protection for one (1) high profile executive, employee, and VIP, and their associated individual social accounts. ● PII Removal (1)	5
Corporate Social Accounts	Automate remediation of offensive or inappropriate content for corporate or organizational Social Media accounts across Facebook, Instagram, LinkedIn, YouTube and Twitter (X). Corporate Social Accounts are those owned social accounts and pages for which you have administrative control. Authenticated accounts within the Platform receive inline content moderation for offensive or inappropriate content postings on supported social networks.	1

	Corporate Social Account Content Remediation Use Cases: The ZeroFox platform provides corporate social account content remediation for the following use cases: ● Social Media Content Moderation Monitors for individuals identifying themselves or identified by others as employees, partners, vendors, or associates engaged in objectionable behaviour or posting objectionable content on owned social networks and forums. What's Included: ● Automated Remediation for up to 1 owned social accounts and pages	
Mobile App Protection	Mobile App Protection discovers fraudulent, rogue, or malicious mobile applications impersonating a brand or organization across mobile app stores available on Android or IOS. A Mobile App is an application designed to run on a mobile device, whether that is a smartphone or tablet. What's Included: Protection for one (1) Mobile Application includes monitoring for any fraudulent, rogue, or malicious mobile applications impersonating a brand or organization.	1
Intelligence Search	Provides access to ZeroFox's Threat Intelligence Graph. Search across Threat Actors, Indicators, Malware and Dark Web Activity.	1 seat

ZeroFox Overview

The ZeroFox mission is clear - We protect customers - their data, their assets and their people - across the internet.

Through AI-powered technology, global intelligence collection, and services provided by a team of expert analysts and threat hunters, we give customers the protection and intelligence needed to disrupt a new era of attacks on the surface, deep, and dark web.



ZeroFox Platform

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 delivers:

- **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.

ZeroFox Global Intelligence Collection provides comprehensive coverage outside the firewall on the platforms you rely on for business. We offer automated and human intelligence collections for protected assets from all relevant open-source intelligence (OSINT) and Deep/Dark Web data sources.

ZeroFox covers a broad range of data sources, from social networks and domain registrations, email, to 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 the market.

Data Source Coverage
The ZeroFox Platform provides API-level access to hundreds of data sources across:

- Regional and international social media networks
- Deep and dark web sites and communities
- Paste and code share sites
- Covert communication channels
- Web domains
- Email
- Surface web sites and advanced web searches
- Web marketplaces
- Forums, blogs, and review sites
- RSS Feeds
- Breaking News
- Mobile app stores
- Vulnerabilities
- Breaches (including botnet compromised data)
- Collaboration platforms
- Network scanning of IPs, hostnames and CIDRs

Advanced Domain and Phishing Detection
Provide comprehensive detection and analysis of phishing attacks, wherever they occur: on social media, email, domains and more. ZeroFox continuously monitors and processes hundreds of millions of websites across the web and 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 advanced domain and phishing protection enables your organization to:

- Continuously monitor for newly registered or active domains and subdomains that use or abuse your organization's brand names, typosquats/homoglyphs, associated terms, and stolen website code

- Continuously monitor phishing data feeds, web beacons, and abuse@/DMARC emails 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
- Leverage AI-driven facial comparison capabilities to detect impersonating executive social accounts used in phishing campaigns

- **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 & 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.