G-Cloud 15 Service Definition

Cyber Threat Intelligence & Digital Risk Prevention Service

ZeroFox (via [Partner])

Lot 2a Infrastructure Software (I-SaaS)

Contents

1. Introduction

Company Overview

ZeroFox is a trusted cybersecurity leader, protecting brands, digital assets, and high-profile leaders at global scale. Our AI-powered platform, combined with expert human intelligence, detects and disrupts threats before they impact your people, organisation, or even national security. Delivering our services through **[Partner],** specialising in securing external digital footprints across social media, surface web, and deep/dark web environments.

ZeroFox serves thousands of customers globally, including FTSE 100, Fortune 10 and Global 2000 companies, as well as many public sector organisations.

[Partner to add company overview]

Value Proposition

Senior leaders within Central and Local Government face growing digital and physical threats, from impersonation to targeted influence campaigns to protests or acts of violence. As adversaries exploit public platforms and personal data, traditional defenses fall short, putting agency operations and public trust at risk.

The service protects against:

- Impersonation attacks and scams - Fake accounts pretending to be elected officials, politicians, or government agencies
- Disinformation campaigns - False information targeting public trust and policy
- Phishing and credential compromise - Targeted attacks on government personnel
- Data leakage - Unauthorised exposure of sensitive government information
- Brand hijacking and domain scams - Fraudulent websites impersonating government services

Executive protection as an example, now requires proactive threat disruption. That means identifying risks across the surface, deep, and dark web—and even the physical landscape—before they compromise local or central government or prove to be a threat to national security. ZeroFox addresses these critical challenges by providing visibility and automated protection beyond the traditional security perimeter.

ZeroFox delivers proven results at scale: protecting over 21,000 leaders and executives globally, with 350,000 successful executive impersonation takedowns in 2024 alone. The platform validates 105,000 physical security alerts annually and takes 800,000 disruption actions weekly. With over 75% of executives' credentials exposed online, this comprehensive approach enables public sector organisations to secure their external digital footprint, protect key personnel, and maintain public trust.

What the Service Provides

The Cyber Threat Intelligence & Digital Risk Prevention service secures your external digital footprint, detecting and mitigating disinformation and risks across social media, the surface web, and the deep/dark web. Powered by advanced AI, extensive data sources, and expert threat researchers, the service identifies and counters phishing, credential theft, data leaks, impersonations, and brand hijacking.

Social Value

[PARTNER TO COLLABORATE ON ANSWER]

The following 4 Social Value areas have been identified from the PPN002 Social Value Model as relevant to this agreement:

- Kickstart economic growth
- Make Britain a clean energy superpower
- Break down barriers to opportunity
- Build an NHS fit for the future

Overview of the G-Cloud Service

The service delivers AI-enabled threat detection and remediation across multiple digital channels with 24x7x365 managed security operations. The platform aggregates over 100 intelligence sources, processing over 1 trillion rows of data and incorporating 70+ threat intelligence feeds with 35+ million Indicators of Compromise (IOCs) per month. Key capabilities include:

- Brand Protection: Monitoring for brand and organisational threats across surface, deep and dark web
- Domain Protection: Continuous identification and remediation of impersonating domains and spoofing
- Executive Protection: Monitoring for high-profile individuals against account takeover, doxxing, and credential compromise (already protecting 1,000+ protectees and monitoring 2,000+ physical locations for public sector customers)
- Takedown Services: Universal takedown capabilities for malicious content across social media, domains, and other platforms
- Intelligence Search: Access to comprehensive threat intelligence data lake with continuous enrichment through machine learning
- Managed Security Operations: 24x7x365 SOC services with alert review, validation, and escalation

The service is delivered through ZeroFox's global Security Operations Centers (SOCs), which are SOC 2 Type 2 certified, with optional foreign language support available in 20+ languages.

Core Service Bundles

Customers must select one of the following bundle types:

ZeroFox Foundation Bundle

The Foundation Bundle offers AI-enabled Brand Protection, Domain Protection, and Takedown services to help security teams mitigate external threats to an organisation'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)

ZeroFox Core Bundle

The Core Bundle elevates your organisation's security by combining advanced, AI-enabled Brand, Domain, and Executive Protection with expanded Takedown services, along with self- and full-service Intelligence capabilities.

What's Included:

- Brand Protection (5)
- Domain Protection (50)
- Executive Protection (10)
- Takedown (500/yr.)
- Intelligence Search (5 seats)
- ODI Credits (5/yr.)
- Platform Alerts & Takedown API Connector (1)
- OnWatch Alert (Managed Service)

ZeroFox Premium Bundle

The Premium Bundle provides comprehensive security combining advanced, AI-enabled Brand, Domain, and Executive Protection with expanded Takedown services, and self- and full-service Intelligence capabilities.

What's Included:

- Brand Protection (50)
- Domain Protection (100)
- Executive Protection (100)
- Takedown (1,000/yr.)
- Intelligence Search (5 seats)
- ODI Credits (20/yr.)
- Platform Alerts & Takedown API Connector (1)
- OnWatch Alert (Managed Service)

ZeroFox Executive Bundle

The Executive Bundle delivers comprehensive digital risk protection for high-profile executives, combining AI-powered monitoring, managed services, and automated disruption capabilities.

What's Included:

- Executive Protection Essentials (10)
- Executive Protection Premium (5)
- Takedown (100/yr.)
- CEO Executive Threat Assessment (12 ODI/yr.)
- Platform Alerts & Takedown API Connector (1)

Bundle Feature Explanations

Brand Protection (quantity): Protection includes monitoring for brand and organizational threats for the specified number of Brands or product lines/families 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 (5) Corporate Social Accounts for a given brand or product. The Brand may not be reused or reallocated to a different Brand after it has been provisioned.

Domain Protection (quantity): Provides Protection for your 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. Each domain protected asset covers all derivative sub-domains for the same primary domain. Domain protection is shared across brands rather than allocated per brand.

Executive Protection (quantity): Executive Protection includes monitoring for the specified number of high-profile executives, employees, or VIPs against account takeover impersonations, sensitive information leakage, doxxing, credential compromise, PII exposure, and cyber-threats. Executive Protection includes PII Removal for the executive. The executive may not be reused or reallocated to a different executive after it has been provisioned.

Executive Protection Premium (quantity): Protection includes monitoring for the specified number of executives and up to five (5) immediate family members per executive across all data sources of surface, deep and dark web. This covers use cases for individual impersonations, sensitive information leakage, doxxing, credential compromise, account takeovers, and cyber-threats. Includes:

- PII Removal for the executive and up to 5 immediate family members
- Location-based alerting for 5 locations

Takedowns (quantity/yr): Universal takedowns can be purchased at discrete quantities to meet organizational needs to block and remove any applicable impersonating or malicious account/site/content and other terms of service violations including from social networks, mobile app stores, paste sites, domains, code shares, and others. Includes:

- Takedowns of malicious and illegal content across social media platforms
- Takedowns of malicious and 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

Intelligence Search (seats): Intelligence Search provides threat intelligence analysts with unlimited search access into the complete threat intelligence data lake from the ZeroFox platform. Provides the ability to search ZeroFox's extensive Data Lake and retrieve all threat intelligence related to search terms. Includes Threat Actors, Indicators, Malware, Dark Web Forum & Marketplace posts, Breaking News, and Finished Intelligence. What is included:

- Single User Licenses for ZeroFox Platform
- Unlimited Searches
- Export Search Results

ODI Credits (quantity/yr): On Demand Investigation credits, which include incident support and RFI response and a variety of assessments and investigations, including Executive Threat Assessments, Persons of Interest Investigations, Background Checks, Third-Party Assessments, Travel Assessments, Geopolitical and Strategic Assessments, or Digital Asset Inquiry, Transaction, & Recovery.

OnWatch Alert (Managed Service): Our team of global SOC first-line threat experts provides 24x7x365 managed services to review, validate, and escalate incidents and prioritize threats on your behalf. Includes:

- 24x7 managed alert service and customer support
- Global Intelligence Collection (GIC): Automated and human intelligence collection for protected assets from all relevant OSINT (Surface) and Deep/Dark Web data sources including major and regional social networks, surface, deep and dark web, covert communication channels, paste sites, e-marketplaces, mobile app stores, blogs, news, job and review sites and forums, code shares, vulnerability databases and more.

Associated Services

Included in all bundles:

- 24x7x365 managed security operations via OnWatch
- Platform Alerts & Takedown API Connector
- Access to Global Intelligence Collection
- Advanced AI Analysis including Computer Vision, NLP, Image Analysis, Machine Learning
- SOC 2 Type 2 certified global SOCs

Not included (available as optional services):

- Extended support services beyond standard bundle
- Additional domain, brand, or executive protection quantities beyond bundle limits

Optional Service Elements

The following optional services are available for additional charges:

External Attack Surface Discovery (EASD)

This solution defines and maps your organisation's internet-exposed attack surface, identifying known and unknown assets. Utilise passive discovery to build an accurate inventory of your digital assets including domains, IP addresses, CIDR blocks, open ports, risky services, security certificates, shadow IT, code repositories, and more. Ongoing discoveries monitor for new exposures and changes to existing assets.

Extended Support Services

OnWatch Expert: Named Threat Intelligence Analyst, 20 hours/week to perform as an extension of your security operations team.

OnWatch Expert Advanced: Named Threat Intelligence Analyst, 40 hours/week Premium. Dedicated Security Expertise: Enhance your security operations by adding a dedicated analyst who provides expert threat hunting, contextual analysis, routine threat reporting, and executive briefings, strengthening your team's capabilities.

Dark Ops Managed Service: Dark Ops Specialist, 20 hours/week (US or UK based). Includes monthly briefing (oral), monthly allowance for DDW purchases, 8 monthly reach-backs. Dedicated Dark Web Intelligence Expertise: enhance your visibility into exposure of your brand and executives on the dark web by adding a dark ops analyst who provides expert threat hunting, contextual analysis, routine threat reporting and executive briefings.

Technical Account Manager: Dedicated TAM for Configuration Optimisations, Tuning and Support. Enhanced Technical Support: Dedicated Technical Account Manager (TAM) for continuous configuration management platform monitoring, tuning, and swift technical escalations, ensuring optimal performance and rapid issue resolution.

2. Data Protection

Information Assurance

ZeroFox maintains SOC 2 Type 2 certification for its global Security Operations Centers. The service follows industry-standard security practices for information management and complies with relevant data protection regulations.

[PARTNER TO ADD: Additional security accreditations/certificates, e.g., ISO 27001, Cyber Essentials]

Data Back-Up and Restoration

The ZeroFox platform includes automated backup processes to protect against data loss. Platform data is backed up regularly with redundancy across multiple geographic locations. Specific backup schedules and restoration procedures can be discussed with customers prior to order placement and documented in the Order Form.

Business Continuity Statement

ZeroFox maintains comprehensive business continuity planning covering its global SOC operations, platform infrastructure, and intelligence collection capabilities. The plan includes:

- Scope: All critical service delivery functions including platform availability, SOC operations, and intelligence collection
- Key business areas: Platform operations, managed security services, threat intelligence, takedown operations

- Critical functions: 24x7x365 alert monitoring, threat detection and validation, platform availability
- Dependencies: Cloud infrastructure providers, intelligence data sources, disruption network partners
- Acceptable downtime: Platform availability target of 99.0% per month
- Operational continuity: Geographically distributed SOC operations ensure service continuity

A more detailed plan can be provided to buyer on request.

Privacy by Design

The ZeroFox service is designed with GDPR compliance as a core principle. Data protection considerations are integrated throughout the service architecture, including data minimization, purpose limitation, and data subject rights management. The service processes only the data necessary for threat detection and mitigation purposes.

3. Using the Service

Ordering and Invoicing

To order the service, customers should contact **[Partner]'s** G-Cloud team at the contact details provided in Section 5. The process includes:

1. Initial consultation to discuss requirements and appropriate bundle selection
2. Completion of Order Form documenting selected bundle and any optional services
3. Agreement of Commercial Terms
4. Service provisioning upon order confirmation

Invoicing will be conducted according to the terms specified in the Commercial Terms and Order Form.

Availability of Trial Service

Trial services may be available on a discretionary basis. Please contact the G-Cloud team to discuss trial opportunities and conditions.

Trial services include: 2 week POV evaluating, Threat Intelligence Search Capabilities, Dark & Surface Web Exposure, Executive Protection, Social Media Monitoring, Domain Protection, Brand Impersonation, AI & Human based advanced collection & Analysis, Takedown Process & Prioritisation and remediation of threats from outside of your network.

On-Boarding Process

Service on-boarding includes:

- Kick-off meeting with key stakeholders
- Assignment of dedicated Customer Success Manager for initial 90 days
- Configuration of protected assets (brands, domains, executives)
- Integration of Platform Alerts & Takedown API Connector if required
- Access provisioning for authorized users
- Training on platform usage and alert management
- Documentation package including user guides and API documentation

[PARTNER ADDITION OPTIONAL]

Off-Boarding Process

Service termination process includes:

- Notice of termination as specified in contract terms
- Engagement with customer to formulate exit plan
- Agreed timeframe for service wind-down
- Data export capabilities for customer records
- Removal of platform access upon contract conclusion

[PARTNER ADDITION OPTIONAL]

Training

Training services include:

- Initial on-boarding training sessions
- Online documentation and help resources
- Access to customer support team for ongoing assistance
- Platform user guides and best practice documentation

Implementation Plan

A detailed implementation plan can be provided to the buyer on request, customized to the specific bundle and optional services selected.

[PARTNER ADDITION OPTIONAL]

Service Management

The service follows IT Service Management (ITSM) best practices with SOC 2 Type 2 certified operations. Service management includes:

- 24x7x365 SOC monitoring and operations
- Defined support classification and response procedures
- Regular service performance monitoring
- Customer communication protocols
- Change management processes

Service Constraints

- Service availability target: 99.0% platform availability per calendar month
- Support hours: 24x7x365 for SOC operations and platform support
- Maintenance windows: Scheduled maintenance communicated in advance
- Asset provisioning: Protected assets (brands, domains, executives) cannot be reallocated once provisioned
- Customization: Service delivered as standardized bundles with optional add-ons

Service Levels

Platform Availability

ZeroFox commits to make the Platform Available, as measured by ZeroFox over the course of each calendar month during the term of an Order, at least 99.0% of the time, exclusive of any time the Platform is not Available as a result of one or more Availability Exceptions (the "Availability Requirement"). "Available" means the Platform is available for access and use by Customer and its Authorized Users over the internet.

Takedown Processing

While formal service level agreements (SLAs) are not currently defined for takedown processing, our team follows clear internal guidelines to ensure consistent turnaround. Different types of threats have varying complexities and require different takedown approaches, so takedown speed depends on type of threat.

Support Services

Contact Support: You can request support online (ask.ZeroFox.com), by phone (1-855-ZFOXSPT) and by email (ask@zerofox.com). ZeroFox OnWatch™ will be provided 24 x 7 x 365.

Support Classification: ZeroFox classifies support requests according to the following priority levels:

- P1: The Platform is totally or substantially disrupted, or a broad class of Authorized Users are deprived of essential features or functions of the Platform.
- P2: One or more of the Platform's key features are partially or moderately disrupted, or a small class of Authorized Users are materially impacted from utilizing one or more key features of the Platform.
- P3: Any other case where the Platform is not operating in accordance with the Documentation or the MCA.
- P4: Requests for new features or functionality with respect to the Platform.

Although response and resolution times are not guaranteed, ZeroFox endeavors to handle support requests as follows:

Priority	**Initial response and acknowledgment**	**Target fix or workaround date**	**ZeroFox-internal escalation**	**Email status updates to Customer**
P1	4 hours	1 business day	Manager / VP: Immediately	Every 8 hours
P2	8 hours	2 business days	Manager: 1 business day / VP: 2 business days	Daily
P3	2 business days	5 business days	VP Product Management reviews bugs weekly	Weekly
P4	2 business days	At ZeroFox discretion	VP Product Management reviews feature requests weekly	None

Service Support Coverage

The Customer shall be provided with the following Support Service for the Core Service Elements and Optional Service Elements. The Support Service shall be delivered from South America, India and the US.

Support Service	**Service Cover Period**
Alert Review, Validation and Escalation	24x7 365 days a year
Global SOCs, SOC 2 Type 2 Certified	24x7 365 days a year
Standard Launch	24x7 365 days a year
Access to Global Intelligence Collection (GIC)	24x7 365 days a year
Advanced AI Analysis including Computer Vision, NLP, Image Analysis, Machine Learning	24x7 365 days a year

Outage and Maintenance Management

ZeroFox employs proactive monitoring and maintenance practices to minimize service disruptions:

- Continuous platform monitoring for performance and availability
- Scheduled maintenance communicated to customers in advance
- Redundant infrastructure to support service continuity
- Incident response procedures for service disruptions
- Post-incident reviews and corrective actions

Financial Recompense Model for not Meeting Service Levels

Service Credits and financial recompense for not meeting service levels are defined in the Commercial Terms and can be discussed prior to order placement.

4. Provision of the Service

Customer Responsibilities

Customers are responsible for:

- Providing accurate information about assets to be protected (brands, domains, executives)
- Designating authorized users for platform access
- Responding to escalated threat alerts in a timely manner
- Maintaining appropriate internal security controls
- Complying with the ZeroFox Acceptable Use Policy
- Providing feedback on false positives to improve threat detection accuracy

Technical Requirements and Client-Side Requirements

Minimum technical requirements:

- Internet connectivity for platform access
- Modern web browser (Chrome, Firefox, Safari, Edge - current or previous version)
- Email capability for alert notifications
- For API integration: technical resources familiar with RESTful APIs

Specific technical requirements will be documented in the Order Form based on selected services.

Outcomes/Deliverables

Customers will receive:

- Access to ZeroFox platform with configured monitoring
- 24x7x365 managed security operations via OnWatch
- Threat alerts and notifications for protected assets
- Takedown services for identified threats (per bundle allocation)
- Threat intelligence reports and data
- Platform analytics and reporting capabilities
- API access for integration with customer systems

Development Life Cycle of the Solution

ZeroFox follows an Agile development methodology for platform enhancements and new features:

- Identify: Customer feedback, threat landscape analysis, market requirements
- Plan: Feature prioritization, sprint planning, resource allocation
- Design: Technical design, user experience design, security review
- Build: Iterative development in sprints
- Test: Automated testing, security testing, quality assurance
- Deploy: Staged rollout, monitoring, validation
- Maintain: Ongoing support, bug fixes, performance optimization

Platform updates and enhancements are released regularly with minimal disruption to service.

After-sales Account Management

ZeroFox and **[Partner]** provide comprehensive account management:

- Dedicated Customer Success Manager during on-boarding period
- Regular business reviews and service optimization discussions
- Technical support available 24x7x365
- Access to product updates and roadmap information
- Customer feedback channels for service improvement

- Escalation procedures for critical issues

Termination Process

Service termination follows the process defined in the Commercial Terms:

- Notice period as specified in contract
- Continued service delivery during notice period
- Data export capabilities for customer records
- Orderly wind-down of monitoring services
- Final reporting and closeout documentation
- No early termination fees unless specified in Commercial Terms

[PARTNER TO ENSURE THIS ALIGNS WITH THEIR TERMS AND GCLOUD TERMS]

5. Our Experience

Case Studies

Case Study: UK Big Four Bank - Comprehensive Digital Channel Visibility

Problem: The bank faced limited visibility into digital channels beyond major social networks, unreliable threat alerting, and manual, time-consuming alert review and takedown processes. The organization struggled to measure its threat landscape and risk exposure effectively.

Action: The bank implemented the ZeroFox platform for comprehensive digital channel monitoring, gaining full coverage across multiple data sources. Working directly with ZeroFox, they created custom rules and leveraged ZeroFox's Global Customer Operations for alert triage and takedowns.

Outcomes:

- 40 hours saved per week on takedown investigation
- 7x more successful takedowns per month compared to previous solution
- Enhanced ability to identify previously unseen digital threats
- Improved strategic decision-making through trend and contextual analysis
- Analysts could be reallocated from manual tasks to strategic threat analysis

Quote: "With ZeroFox, we have a much better understanding of our digital footprint and a full view of our digital risk." - Bank Cyber Security Manager

Public Sector Relevance: This case study demonstrates how ZeroFox can help even the largest public sector organisations gain comprehensive visibility across digital channels, automate threat detection and takedown processes, and free up security teams to focus on strategic threat analysis - all critical capabilities for government agencies facing sophisticated digital threats and resource constraints.

Additional Case Studies

ZeroFox has successfully delivered digital risk protection solutions across multiple sectors including:

- Civil Aviation Authority - Tackled hundreds of web domain scams
- Ivy League University - Social media brand security
- Luxury Goods, Travel, Insurance, Technology, Sports, and Retail sectors - Various digital risk protection use cases

Detailed case studies available upon request.

Clients

ZeroFox serves thousands of customers globally across multiple sectors:

Public Sector:

- Federal, state, and local government agencies
- Civil Aviation Authority
- Educational institutions including Ivy League universities

Private Sector:

- Fortune 10 companies
- Global 2000 enterprises
- Financial services institutions (including UK Big Four banks)
- Technology companies (Nokia)
- Luxury goods manufacturers
- Travel and tourism companies
- Insurance providers
- Sports organizations
- Retail chains

Key Statistics:

- 21,000 leaders and executives protected globally
- 350,000 successful executive impersonation takedowns in 2024
- 105,000 physical security alerts validated in 2024
- 800,000 disruption actions taken weekly
- 1,000+ protectees and 2,000+ physical locations monitored (public sector)
- Over 100 intelligence sources with 1+ trillion rows of data
- 70+ threat intelligence feeds with 35+ million IOCs per month
- Platform supports 20+ languages for foreign language intelligence requirements

There are publicly available case studies but due the secure nature of our work additional logos and references may be available under a mutual NDA.

Contact Details

For G-Cloud inquiries regarding the ZeroFox Digital Risk Prevention service:

[PARTNER TO PROVIDE CONTACT DETAILS]

Email: [Partner email address]

Phone: [Partner phone number]

For technical support after service activation:

- Online: ask.ZeroFox.com
- Phone: 1-855-ZFOXSPT
- Email: ask@zerofox.com

Additional Information

Additional information about ZeroFox services and terms:
https://www.zerofox.com/terms-and-transparency/

Document Version: 1.0

Last Updated: [Date to be inserted]

Prepared for: G-Cloud15 Framework Submission