Digital Visibility and Protection for Public Sector

Gain visibility, achieve compliance, extend protection across social media and external assets
The Challenge for Public Sector

The government has a massive footprint and attack surface on social media & external digital platforms — all of which is ungoverned, unmonitored and unprotected by the existing security perimeter — exposing agencies to targeted cyber attacks, data loss, employee scams, compliance violations and account takeovers. Employees post sensitive data and bypass information barriers, relatives post travel and deployment plans, foreign actors distribute misinformation campaigns, and targeted cyber attacks are distributed across your organization at scale.

The Challenge for Public Sector

ZeroFOX provides government organizations with critical visibility, compliance reporting & automated protection necessary to secure external social media and digital platforms. Using diverse data sources, artificial intelligence-based analysis and automated remediation, the ZeroFOX Platform reduces fraud, takes down spoofed accounts, protects against targeted cyber attacks and identifies non-compliant content.

Who We Work With

- Civilian Agencies
- Department of Defense
- Intelligence Community

Top Risks to Public Sector

- Impersonations of agencies and departments
- Executive spoofing and romance scams
- Targeted phishing/malware
- Dissemination of misinformation
- Compromised credentials
- Data leakage
- Insider threats
- Account hijacking
- Physical security threats

Top Benefits to Public Sector

Gain Visibility and Control

Immediately see beyond your perimeter to catch more risks and targeted attacks faster, before they impact your agency, customers, partners & employees.

Automatically Distill Risks from the Noise

Don't waste time scouring trillions of potentially malicious accounts and posts; leverage artificial intelligence and automation to reduce time-intensive collection, analysis and remediation.

Obtain Attack Indicators and Find Leaked Data

Attackers use social media to bypass traditional security perimeter controls and execute targeted attacks at scale. Indicators of attacks being planned or leaked data after an attack are broadcast on social media.

Identify and Remove Misinformation Campaigns

People endorse & engage on social media, all of which can be exploited by cybercriminals and scammers. Protect public engagement by finding and taking down fraudsters and financial crime at scale.

Ensure Compliance

Highly-public organizations, like government agencies, deal with the public nature of social media and external digital communication platforms by enforcing policy compliance for all employees and executives.

Safeguard Leadership and Identify Fraudulent Accounts

Executives and other high-value employees are prime targets for attackers building spoofed accounts. ZeroFOX automatically identifies and remediates fraudulent accounts.

Protect Agencies and Departments from Impersonations & Account Takeovers

Stop attackers from hijacking accounts by locking down accounts in the event of takeover, automatically hide or remove sensitive or offensive content posted to owned pages and block offending perpetrators.
About ZeroFOX

ZeroFOX, the market leader in social media & digital protection, safeguards modern organizations from dynamic security, brand and physical risks across social, mobile, web 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 & dark web, domains and more.