



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

September 30, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EDT) on September 27, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 This Week's ZeroFox Intelligence Reports	2
ZeroFox Intelligence Flash Report: Dark Web Actors Seek to Avoid Russian Military Conscription	2
ZeroFox Intelligence October 2024 Geopolitical Brief	2
 Cyber and Dark Web Intelligence Key Findings	4
Ukrainian Government Restricts Telegram Use amid Russian Spy Fears	4
Biden Administration Proposes to Ban Russia and China-Made Vehicle Technology	4
Critical Infrastructure: A Lucrative Target	5
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2024-7593	8
CVE-2024-7481	9
 Ransomware and Breach Intelligence Key Findings	11
Evolving Ransomware Threats and Tactics	11
Large-Scale Data Breaches Target Various Sectors	12
 Physical and Geopolitical Intelligence Key Findings	15
Physical Security Intelligence: Global	15
Physical Security Intelligence: United States	16
 Appendix A: Traffic Light Protocol for Information Dissemination	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – Dark Web Actors Seek to Avoid Russian Military Conscription

On September 18, 2024, well-regarded actor “Monashka” posted in the Russian-speaking dark web community Rutor, bringing attention to the launch of a government web portal designed to overhaul the method by which military draft notices are served to Russian citizens. The post prompted discussion from several other actors centered around potential deep and dark web (DDW) services offering different methods of avoiding conscription in Russia. Since the February 2022 Russian invasion of Ukraine, ZeroFox has observed numerous discussions in DDW forums involving actors seeking ways to avoid being drafted. As the war continues and eligibility requirements widen, it is likely that an array of DDW services will emerge to meet the growing demand from those seeking to avoid military service.

ZeroFox Intelligence October 2024 Geopolitical Brief

Russia will likely deploy a range of hybrid war tactics to discourage Western states from allowing Ukraine to use longer-range weapons against Russia. This will include threats to use nuclear weapons, changes in military strategy, cyber influence operations, sabotage, and arming U.S. adversaries like the Houthis in Yemen. The military successes Israel is experiencing as it approaches the October 7 anniversary of Hamas’ attack against it contrast with the military and intelligence failures of a year earlier. French left-wing protests have subsided but are likely to resume when the new government starts pursuing conservative policy positions. Smaller European states are holding elections in October 2024, where support for Russia and reducing immigration are leading opposition demands. The EU released its long-awaited competition report, which will dictate how most EU funds will be spent in the coming years while giving threat actors a list of targets.

| **Cyber and Dark Web Intelligence** |

| Cyber and Dark Web Intelligence Key Findings



Ukrainian Government Restricts Telegram Use amid Russian Spy Fears

What happened: Ukraine has implemented a ban on the use of the Telegram messaging app on official devices for government officials, military personnel, and critical workers. This decision stems from concerns raised by the head of Ukraine's GUR military intelligence agency, who presented evidence suggesting that Russian special services have the capability to spy on Telegram users and their communications. The restrictions are aimed at safeguarding sensitive information from potential interception by Russian operatives.

- > **What this means:** The ban is significant in the context of the ongoing conflict between Ukraine and Russia, as Telegram has emerged as a vital communication tool for both countries. While the app is widely used for disseminating information and coordinating activities, Ukrainian security officials have expressed worries regarding its security vulnerabilities. Protecting sensitive information is crucial for national security, especially given the reported capability of Russian special services to access private data on the platform and disseminate disinformation. The head of the security council's center clarified that the restrictions apply only to official devices, allowing personal use while emphasizing the need to safeguard official communications. Meanwhile, in a significant policy shift, the messaging app Telegram has [declared](#) that it will share users' IP addresses and phone numbers with authorities when valid legal requests are made. This move aims to combat criminal activity on the platform.



Biden Administration Proposes to Ban Russia and China-Made Vehicle Technology

What happened: The Biden-Harris administration proposed new rules to mitigate national security threats from connected vehicle technologies associated with China and Russia. The Department of Commerce has issued a notice of proposed rulemaking (NPRM) to ban the import or sale of connected vehicles and related components, such as vehicle connectivity systems (VCS) and automated driving systems (ADS), designed or developed by entities linked to these countries. The proposal is the next step in investigating Chinese smart cars, which [began](#) in February. It follows

concerns over misusing smart technologies for espionage, sabotage, or disrupting critical infrastructure. The rule would prohibit the import of VCS and ADS software by 2027 and hardware by 2030, with some exemptions for small producers.

- > **What this means:** State cyber actors are known for targeting U.S. entities to gather intelligence, steal intellectual property, and disrupt critical infrastructure. Technologies like Bluetooth, cellular, and ADS collect sensitive data—such as location tracking, sensitive driver data, and detailed infrastructure mapping—making users potential targets for cyberattacks and espionage by foreign adversaries like China and Russia. Hackers could also likely sabotage critical transportation systems, disrupt supply chains, or gain strategic insights into U.S. operations. The United States aims to safeguard its digital networks and critical infrastructure from foreign manipulation by restricting imports of connected vehicle technologies from these nations. However, it will be crucial to maintain a balance between national security and the industrial need for innovation and supply chain resilience because overregulation could hinder the automotive sector, especially small players. Moreover, the upcoming U.S. elections present an additional concern. Connected vehicle technologies could be leveraged in state-sponsored operations to target political figures, track their movements, threaten their physical security, or disrupt campaign operations.



Critical Infrastructure: A Lucrative Target

What happened: Several vulnerabilities have been identified in automatic tank gauge (ATG) systems that threaten critical infrastructure. Some of these are critical-severity bugs, and some are even unpatched. The 11 bugs observed can allow threat actors to have full control of an ATG system as an administrator, posing serious environmental risks. Recently, a water treatment facility at Arkansas City in Kansas was also the [target](#) of a cyberattack, forcing the facility to switch to a manual process to contain the cyberattack.

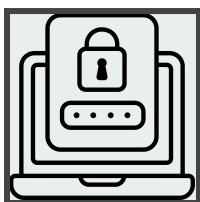
- > **What this means:** ATGs are essential for monitoring fuel levels and ensuring proper storage at critical infrastructure facilities like gas stations, airports, and industrial sites. The discovered vulnerabilities, which also include unpatched ones, could allow attackers to gain full administrative control over these systems. Attackers could manipulate ATG systems to disrupt fuel distribution, cause fuel shortages, or even lead to physical damage and environmental harm, such as fuel leaks or spills. If these vulnerabilities are left unpatched, the consequences of an attack could escalate, affecting fuel availability and even causing widespread environmental issues. A more dangerous manipulation likely

involves changing the reported size of the tanks. By altering the tank's capacity, hackers can trick operators into believing that the tank can hold more fuel than it actually can. This could lead to overfilling, risking an environmental spill or leak. Additionally, modifying alarm thresholds to trigger at higher fuel levels could prevent early warnings, worsening the consequences of overfilling. CISA has recently [addressed](#) better securing U.S critical infrastructure like water treatment facilities against continuous cyber activities. Exposed and vulnerable operational technology (OT) and industrial control systems (ICS) systems may allow cyber threat actors to use default credentials, conduct brute force attacks, or use other sophisticated and unsophisticated methods to access these devices and cause harm.

| **Exploit and Vulnerability Intelligence** |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in software solutions, industrial control systems (ICS), government, and network and security. Several vulnerabilities have been [identified](#) in automatic tank gauge (ATG) systems that threaten critical infrastructure. Some of these are critical-severity bugs, and some are even unpatched. An improper input validation vulnerability in Microchip Technology Advanced Software Framework can [cause](#) remote code execution through a buffer overflow. The software is reportedly no longer supported by the company, which means that the vulnerability is likely to be exploited in the wild, according to the CERT/CC. Ivanti [released](#) an advisory, which includes CVE-2024-8963—a path traversal bug in the Ivanti CSA (before 4.6 Patch 519) that allows a remote unauthenticated attacker to access restricted functionality. GitLab has [issued](#) critical patches for a high-severity vulnerability affecting both its Community Edition (CE) and Enterprise Edition (EE). The vulnerability, CVE-2024-45409, can potentially allow attackers to bypass authentication controls and log in as arbitrary users within the vulnerable system. Versa Networks released an advisory to address [CVE-2024-45229](#), a vulnerability in Versa Director. The Versa Director offers REST APIs for orchestration and management. By design, certain APIs, such as the login screen, banner display, and device registration, do not require authentication. [CISA](#) urges organizations to apply necessary updates. Atlassian has released patches for several high-severity [vulnerabilities](#) across its products, including Bamboo, Bitbucket, Confluence, and Crowd. The September 2024 security bulletin includes four security flaws, all of which can be exploited to create denial-of-service (DoS) conditions.



CRITICAL

CVE-2024-7593

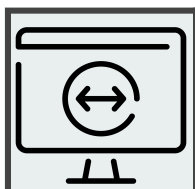
What happened: This vulnerability is a critical authentication bypass flaw with a CVSS score of 9.8, resulting from a flawed implementation of the authentication algorithm. It enables remote, unauthenticated attackers to circumvent authentication on vTM admin panels that are exposed to the internet. CISA has added this Ivanti vTM vulnerability to its Known Exploited Vulnerabilities (KEV) catalog, indicating that it is currently being actively exploited.

- **What this means:** This vulnerability poses a significant risk as it allows remote attackers to bypass authentication on Ivanti vTM admin panels, which are accessible over the internet. Threat actors can exploit this flaw to gain unauthorized access, potentially compromising sensitive systems and data. The impact could include data breaches, system

manipulation, and unauthorized administrative control, making it critical for affected organizations to address the issue promptly to safeguard their assets.

➤ **Affected products:**

- Ivanti Virtual Traffic Manager versions 22.2, 22.3, 22.3R2, 22.5R1, 22.6R1, and 22.7R1



HIGH

CVE-2024-7481

What happened: This vulnerability allows local attackers to escalate privileges on affected installations of TeamViewer. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

- **What this means:** The specific flaw exists within the TeamViewer service, which listens on TCP port 5939 by default. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM.

➤ **Affected products:**

- TeamViewer Full Client (Windows) versions < 12.0.259312
- TeamViewer Full Client (Windows) versions < 11.0.259311
- TeamViewer Host (Windows) versions < 15.58.4
- TeamViewer Host (Windows) versions < 14.7.48796
- TeamViewer Host (Windows) versions < 13.2.36225
- TeamViewer Host (Windows) versions < 12.0.259312
- TeamViewer Host (Windows) versions < 11.0.259311

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

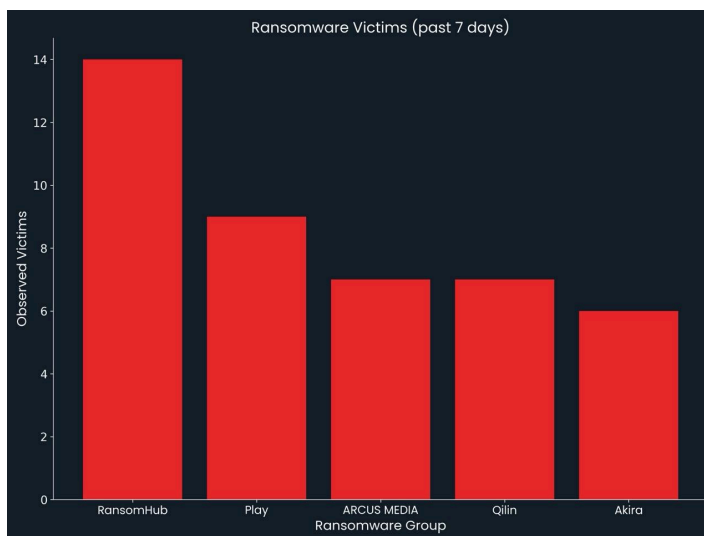


Evolving Ransomware Threats and Tactics

What happened: In the past seven days,

ZeroFox has observed over 90 ransomware attacks, mostly on the manufacturing sector primarily conducted by the RansomHub ransomware group. Over 60 percent of these targeted industries were from North America. In recent developments within the cybersecurity landscape, the RansomHub ransomware group has [announced](#) that they have stolen 56 GB of data, including financial documents, in a recent attack on Delaware Libraries.

The organization acknowledged an ongoing system and internet outage that has impacted library services at several public libraries, resulting in some closures. However, the Delaware Library Catalog and eMedia services remain operational. Meanwhile, AutoCanada has [issued](#) a warning that employee data may have been compromised in a cyberattack attributed to the Hunters International ransomware group that occurred in August. In another concerning turn, an affiliate of the Mallox ransomware operation, also referred to as TargetCompany, has been [detected](#) using a slightly altered version of the Kryptina ransomware to target Linux systems. Amid these alarming trends, the DragonForce ransomware has been observed [broadening](#) its Ransomware-as-a-Service (RaaS) operation, positioning itself as a significant global cybersecurity threat to businesses.



Source: ZeroFox Internal Collections

- **What this means:** The surge in ransomware attacks poses a significant challenge for organizations across both public and private sectors, revealing critical vulnerabilities in their infrastructure and sensitive data handling. As organizations like Delaware Libraries and AutoCanada grapple with cyberattacks, the implications extend beyond immediate operational disruptions; they can lead to long-term reputational damage, fraud, and financial repercussions. The targeting of specific systems, such as Linux by the Mallox affiliate, reflects an evolving landscape where cybercriminals continuously adapt their

tactics. Moreover, the expansion of RaaS operations, particularly with groups like DragonForce, makes these advanced threats more accessible to a wider range of cyber criminals, complicating the efforts of businesses to safeguard their assets and maintain the trust of customers and stakeholders.



Large-Scale Data Breaches Target Various Sectors

What happened: Over the past week, threat actors have exposed personal and sensitive information from a federal agency and a background check company. Dell has [experienced](#) a series of data breaches. The Centers for Medicare & Medicaid (CMS) [reported](#) data of over 3 million health plan beneficiaries was exposed in the 2023 MOVEit ransomware attacks [orchestrated](#) by the Clop ransomware group. The threat actor infiltrated the Wisconsin Physicians Service (WPS)—which provides Medicare administrative services—and compromised sensitive data. MC2 Data, a background check firm, [experienced](#) a data breach that exposed sensitive information of approximately 100 million U.S. citizens. The breach targeted an unsecured 2.2 TB database—comprising 106,316,633 records—and leaked private data, including names, birthdates, encrypted passwords, legal documents, and partial payment information. Additionally, over 2.3 million MC2 subscribers had their details compromised. Meanwhile, threat actor “grop” allegedly [targeted](#) Dell thrice, each time, revealing data sets and records, including videos, models, MFA data, access vectors, and Chinese infrastructure.

- **What this means:** The breaches targeting CMS and MC2 Data exposed personal data, including names, email addresses, and phone numbers, which can subject affected individuals to further targeted attacks like extortion, spear phishing, and blackmail. The scale of both breaches also indicates a large volume of affected individuals, potentially exposing gaps in the security of the two organizations. Furthermore, the stolen data from such breaches can be readily shared or sold on the dark web, increasing the likelihood of further attacks and leaving affected individuals vulnerable to identity theft and fraud. Besides, the CMS breach also exposed sensitive medical information, compromising the privacy of the beneficiaries and making them susceptible to financial scams and medical fraud schemes. Meanwhile, the data leaked from MC2 Data has exposed encrypted passwords and partial payment information, which threat actors will likely leverage to access sensitive information. On the other hand, the exposed data from Dell supposedly [comprises](#) confidential data, including database tables, schema migrations, and employee details—like employee ID, full name, and employee internal ID. If verified, the

breach is likely to subject Dell to further cybersecurity threats by exposing critical system configurations and security vulnerabilities. Moreover, threat actors will likely engage compromised Dell employees in targeted malicious attacks, such as spear-phishing, extortion, and blackmail.

| Physical and Geopolitical Intelligence |

| Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

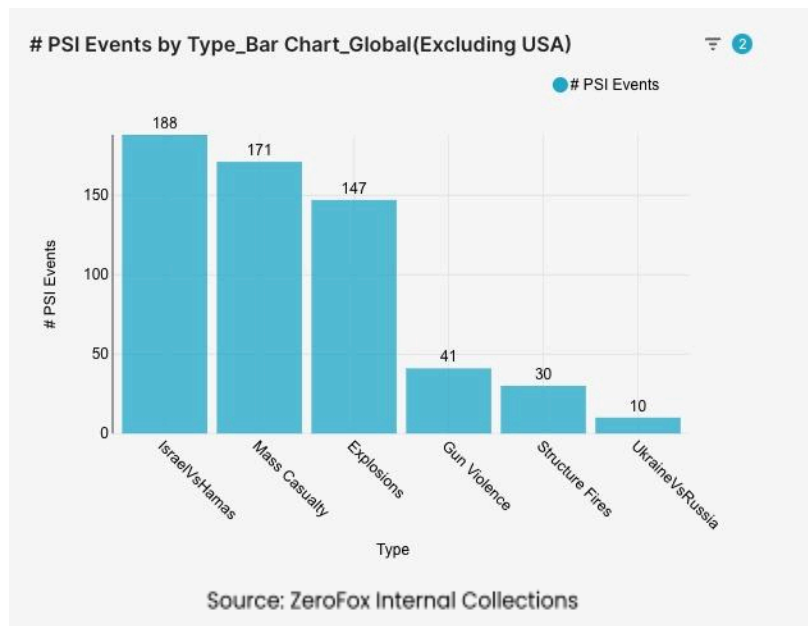
What happened: Excluding the United States, there was an 8 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Israel, and Lebanon. Approximately 86 percent of these events were explosions, and the three aforementioned countries accounted for about 64 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by 54 percent from the previous week.

However, events related to Russia's war

in Ukraine did not increase or decrease from the week

prior. The top three most-alerted subtypes were explosions, which saw a 24 percent increase from the previous week; gun violence, which also increased by 24 percent; and structure fires, which did not increase or decrease from the week prior. Notably, global protest activity increased by 12 percent.

- **What this means:** The most drastic increases this week were seen with the Israeli conflict as well as with explosions, which is in accordance with the fact that almost two-thirds of all mass casualty events alerted this week came from three of the countries involved. Hezbollah and Israel's altercation has amplified quite significantly this week, with Hezbollah launching an intercepted missile towards [Tel Aviv](#), resulting in Israeli Defense Forces carrying out a strike on the central headquarters of Hezbollah in [Beirut](#), Lebanon. The latter attack was meant to target Hezbollah leader Hassan Nasrallah, whose body has reportedly been [recovered](#) from the site. Hezbollah confirmed Nasrallah's death on Saturday. This comes after the United States attempted to implement a 21-day ceasefire between the two organizations, which was not successful. As a result of the heightened intensity of the conflict, global protest activity has also increased somewhat, with larger-scale protests seen in [Canada](#) and [Australia](#).

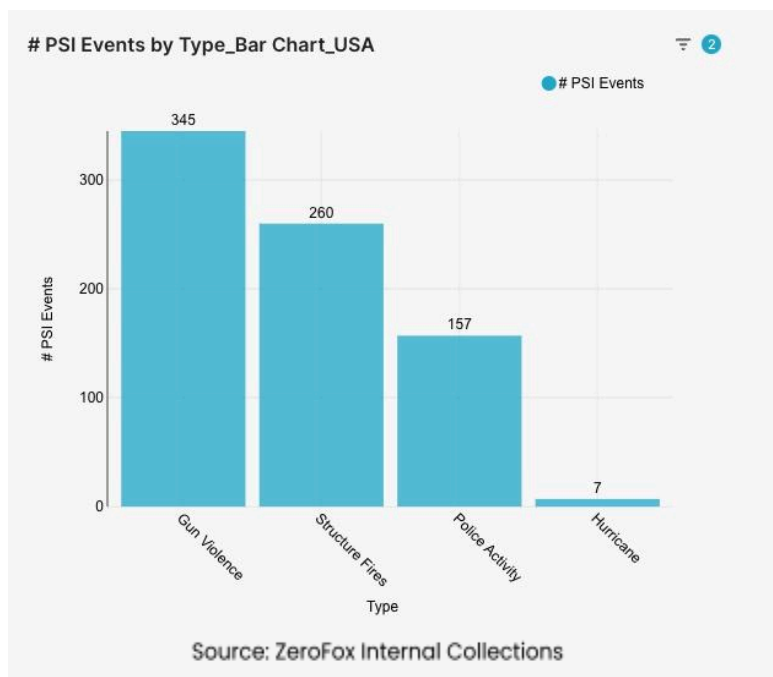


Physical Security Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, and police activity. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, police activity involves law enforcement presence for generalized threats or for unknown reasons, and structure fires are fires that affect man-made buildings. The top two states that had the most gun violence alerts were Illinois and California, which together made up 26 percent of this week's nationwide total. Gun violence across the United States overall decreased by 16 percent from the week prior. Police activity alerts decreased by 34 percent, and the top contributing

states were California and Georgia. Structure fires decreased by 14 percent, and the top two states for this subtype were California and Illinois. Notably, alerts with the subtype of Hurricane appeared seven times in the last week and zero times in the week prior to that.

- **What this means:** Hurricane [Helene](#) made landfall as a Category 4 shortly after 11 p.m. ET on Thursday in Florida and has since killed at least 22 people and left millions without power across the southeast part of the country. Now a tropical storm, Helene is expected to bring damaging wind gusts and catastrophic flooding as it heads north across the Southeast. In all three of the top subtypes, California made the top two, with many instances coming out of Los Angeles; for example, on Wednesday, there was a mass [shooting](#) that wounded six people in the city. Additionally, on September 21st in Birmingham, Alabama, 21 people were shot. This stemmed from an isolated incident where multiple victims were caught in the crossfire. Overall, it is evident that although the total amount of events across all top subtypes decreased from the previous week, the severity of the individual events remained notable.



| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%