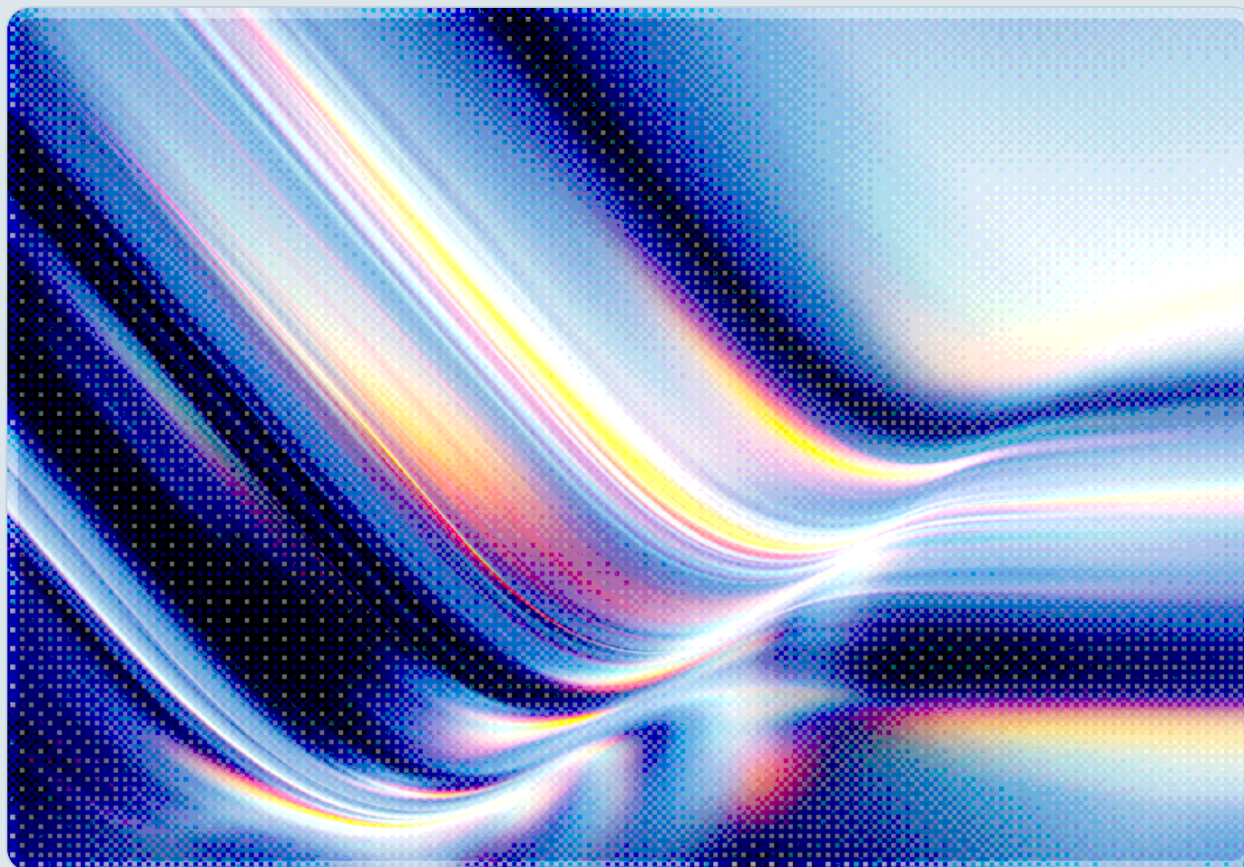


# When a Security Vendor Is Named as Adversary Infrastructure

Integrity Technology Group and Vendor-Trust Concentration:  
Security Implications and Guidance

2026-10-17

 AI-assisted Rapid Research



CSAI

cloud  
security  
alliance®

**© 2026 Cloud Security Alliance. Some rights reserved.**

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

*This document was generated with AI assistance and has not undergone official CSA review and approval processes.*

---

## Key Takeaways

On October 8, 2026, the FBI, CISA, the NSA and partner agencies from several countries published joint advisory AA26-281A, which describes Integrity Technology Group as a China-based, profit-driven company with government ties that supplies cyber tools, hosts infrastructure and facilitates network compromise on behalf of actors tracked as Flax Typhoon, Ethereal Panda and Red Juliett [1]. The same company markets itself as a network security vendor, is listed on the Shanghai Stock Exchange, and has been the subject of U.S. sanctions since January 2025 [3][5]. The case is the second U.S. law enforcement disruption of infrastructure tied to the company in roughly two years [2].

The technical lessons of the advisory are conventional: the eight exploited vulnerabilities date from 2014 to 2023, and the core mitigations are patching, multifactor authentication and segmentation [1][8]. The governance lesson receives less attention. A commercial entity can sell security-adjacent products, appear on vendor lists and in market research, and simultaneously operate offensive infrastructure for a state. Vendor risk programs built mainly around control questionnaires are unlikely to surface that condition unless they also ask about ownership and government obligations. Organizations that have concentrated trust in a small number of security suppliers also have less room to remove one quickly.

This note separates what the public record establishes from what it does not. It then offers guidance for security and procurement teams on screening vendors for state-nexus and sanctions exposure, on limiting the blast radius of any single security supplier, and on what to do if a product from a designated entity is already present in the environment. The advisory, as summarized by one policy commentary, cautions that commercial labels are not one-to-one mappings to threat actors and that indicator matches are investigative leads rather than proof of compromise [1][7]. We follow that caution throughout.

## Background

Integrity Technology Group, also known as Yongxin Zhicheng Technology Group, is a Beijing-based network security company founded in 2010 and listed on the Shanghai Stock Exchange [4][3]. Public descriptions of its commercial business include network simulation, security training and security

competition products [5]. In a statement to the exchange, the company has said that U.S. accusations have no factual basis [3]. That denial should be recorded alongside the government findings, which are allegations by the issuing agencies and not adjudicated outcomes.

The U.S. government's published actions against the company have accumulated over two years. In September 2024, a court-authorized operation disrupted the Raptor Train botnet, which the FBI said had infected more than 200,000 consumer and small-business devices worldwide, and which the FBI associated with Flax Typhoon and a company later identified as Integrity Tech [2][6]. On January 3, 2025, the Treasury Department's Office of Foreign Assets Control designated Integrity Tech under Executive Order 13694, as amended, stating that Flax Typhoon actors used infrastructure tied to the company between summer 2022 and fall 2023 and routinely exchanged information with it [5]. One secondary report states that the United Kingdom imposed cyber financial sanctions in December 2025 and that the European Union listed the company in March 2026 [4]. We have not confirmed those listings against the issuing governments' primary notices, so the remainder of this note relies on the U.S. designation alone.

The October 2026 actions extend the picture. The Justice Department and FBI announced court-authorized seizure of two tools, MicroScan, a vulnerability-scanning application, and FishHub, a spear-phishing and malware-delivery tool, along with five domains used to deliver malware, several of which imitated well-known brand names [2]. Victims identified in the Justice Department announcement included a South Carolina power company, airports in Japan and Poland, Taiwanese universities and natural gas and power entities, and a multinational non-governmental organization [2].

The same day, the joint advisory consolidated evidence of activity going back to at least January 2021, targeting government, critical manufacturing, healthcare, IT, law enforcement, education and religious organizations [1][7]. It describes MicroScan as a custom Python application containing over 1,300 penetration testing scripts, the use of open-source scanners, password spraying against Microsoft Exchange interfaces using the open-source EBurst tool, and persistence through legitimately licensed SoftEther VPN software [1]. It lists eight exploited vulnerabilities in Bash, ProFTPD, BIND, Apache Struts, Pulse Secure (Ivanti Connect Secure), GitLab, ONLYOFFICE and Strapi [1][8]. The Hacker News and Tech Times report that the actors operated a web application providing third-party access to stolen email content; the reporting does not identify those third parties [3][4].

# Security Analysis

## What the record supports

The public record supports three statements with reasonable confidence. First, U.S. and allied agencies attribute to a single commercial entity the supply of offensive tooling, infrastructure hosting and intrusion services used by state-aligned actors [1]. Second, the entity's commercial identity is that of a security vendor, which means that, if the agencies' attribution is accurate, both the "vendor" and "adversary infrastructure" labels would apply to the same legal person [4][5]. Third, the activity has continued after a botnet takedown in 2024 and sanctions in 2025, which suggests that designation alone did not end the operation, although the public record does not show whether the level of activity changed [1][2][5][6].

The record does not establish how many organizations were breached, which of the company's commercial products, if any, were present in Western enterprise environments, or who the portal's third-party users were. According to one policy commentary, the advisory is a defensive package and not evidence of a single new intrusion, and it does not provide a complete victim list [1][7]. It also notes that three advisory indicators remained active into May 2026 against vulnerabilities different from those originally listed, which an analyst summary reads as possible infrastructure repurposing or compromise [8]. Readers should treat that interpretation as an inference.

## Why the vendor-trust framing matters

Most vendor risk programs ask whether a supplier will protect the customer's data. This case asks a different question: whether the supplier's business model is the attack. In a conventional supply chain compromise, a legitimate vendor is breached and its customers inherit the exposure. Here the reported relationship runs the other way, with a company that sells cyber tools and hosts infrastructure for use against third parties [1]. In the authors' assessment, standard due diligence artifacts such as SOC reports, penetration test summaries and security questionnaires speak to the first problem and say little about the second.

The offensive and defensive halves of the cybersecurity industry also share skills, tooling and customers. Penetration testing scripts, scanning frameworks and cyber range products are dual-use by design, and the 1,300-script MicroScan application described in the advisory is, in functional terms, a large collection of assessment scripts [1]. This overlap makes a vendor's stated product category a weak signal of its

allegiance. It also means an organization that buys training, simulation or assessment products from a state-linked supplier may provide that supplier with telemetry, personnel information or network detail without any breach occurring.

### Concentration and replaceability

Security tooling sits at privileged points in the architecture: endpoint agents run with administrative rights, scanners hold credentials, and management consoles reach every managed asset. When a single supplier occupies several of those positions, removal after a designation or advisory becomes an operational project with a long tail. CSA's earlier work on AI stack concentration argues that shared control points create blast radius beyond what any one organization's vulnerability management program is designed to absorb [9][10]. The same logic applies to the security stack. A sanctions designation, an advisory or a supplier compromise converts a quiet dependency into an urgent migration.

Sanctions add a compliance dimension to the technical one. Because OFAC designation blocks property and generally prohibits U.S. persons from engaging in transactions with the designated person, an enterprise that discovers a designated entity's product, license or service in its estate faces a legal question alongside the security one [5]. Entities owned or controlled by designated parties can also create exposure that does not appear under the parent's name, so screening on the vendor's trade name alone is inadequate. Counsel should interpret the scope of any prohibition, including how OFAC's ownership rules apply.

### Exposure paths in practice

The table below summarizes the ways in which a state-nexus vendor can reach an enterprise, together with the signals that may reveal each path. The classification is the authors' analytical framing and is not drawn from the advisory.

| Exposure path   | How it may arise                                                                    | Detection signal                                                                   |
|-----------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Direct purchase | Training, simulation, assessment or security products bought from the entity        | Vendor master data, license records, procurement screening against sanctions lists |
| Indirect resale | OEM, white-label or subcontractor components embedded in another supplier's product | Software bills of materials, contract flow-down clauses, supplier disclosures      |

| Exposure path                    | How it may arise                                                                                 | Detection signal                                           |
|----------------------------------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| Adversary infrastructure contact | Internal hosts communicating with indicators the advisory associates with the actors             | Network telemetry matched against published indicators [1] |
| Initial-access exposure          | Unpatched internet-facing systems among the eight vulnerabilities, or Exchange password spraying | Vulnerability scans, authentication logs [1]               |
| Third-party data resale          | Stolen mailbox content made available to unnamed parties through a query portal                  | Breach notification, law enforcement contact [3][4]        |

The first two rows concern vendor governance, and the last three concern conventional detection and response. In the authors' experience, enterprise programs tend to invest more in the second group than in the first.

## Recommendations

### Immediate Actions

Security teams should compare the indicators in AA26-281A against network and endpoint telemetry, treating matches as leads for investigation and not as confirmation of compromise, consistent with the advisory's own framing [1][7]. Teams should confirm that internet-facing systems are patched against the eight listed vulnerabilities, with particular attention to Ivanti Connect Secure and Pulse Secure remote access, which sit directly on the perimeter [1][8]. They should also review Microsoft Exchange authentication logs for sustained password-spraying patterns and confirm that multifactor authentication covers every Exchange interface the advisory lists [1].

Procurement and legal teams should screen the vendor master file, software inventory and subcontractor lists for Integrity Technology Group and its known aliases, including Yongxin Zhicheng, against the OFAC Specially Designated Nationals list [5], and against the UK and EU consolidated sanctions lists, on which this note could not confirm current listings (see Background) [4]. Any match should be escalated to counsel before further payments or renewals, because the compliance consequences differ from the technical ones.

## Short-Term Mitigations

As a suggested target of the next quarter, organizations should extend vendor intake to ask ownership, government-contract and state-affiliation questions of any supplier that sells security, assessment or training products, and to require disclosure of material subcontractors and OEM components. The goal is to identify a vendor's relationship to a government, which a security questionnaire does not normally capture. Continuous monitoring of sanctions and advisory feeds should replace annual re-screening, since this one entity was the subject of a botnet disruption (2024), a U.S. sanctions designation (2025) and a seizure of operational tools (2026) within about two years [2][5][6].

Teams should also restrict what security tools can see and reach. Scanners, agents and training environments from suppliers whose provenance is uncertain should run with least privilege, segmented from production credentials, and with outbound traffic constrained to documented destinations. Examples include separate service accounts for scanners and egress allowlists for management consoles. Software bills of materials should be requested for commercial security products so that embedded components from a designated entity can be located.

## Strategic Considerations

Over the longer term, organizations should assess how many privileged control points depend on a single supplier and document an exit path for each, including data export, credential rotation and a tested replacement. A security supplier that cannot be removed within a defined period is a concentration risk whether or not any adversary is involved. Boards and risk committees should receive this analysis as part of third-party risk reporting.

Industry bodies and assurance schemes also have a role. The AICM and STAR, as currently published, focus on the controls a provider operates and do not evaluate ownership or state affiliation as a stand-alone criterion. Assurance programs could add transparent ownership, government-obligation and sanctions-status disclosures as structured fields, so buyers receive consistent data rather than collecting it bilaterally.

## CSA Resource Alignment

CSA's research on AI stack concentration risk is the closest prior work to this note's central argument. It describes how shared control points across the development stack create systemic exposure that exceeds what individual vulnerability management programs are designed to handle [9]. CSA's paper on AI developer ecosystem monoculture risk examines the same dynamic in the open-source ecosystem

[10], and its AI infrastructure monoculture whitepaper extends the analysis to foundation-layer providers [13]. Those papers focus on AI toolchains, but the structural point carries over: when privileged tooling is concentrated, a single trust failure, whether a compromise, a designation or a state-nexus disclosure, propagates widely. Security teams can reuse their analytical approach by inventorying privileged control points in the security stack and asking, for each, how quickly it could be replaced.

The AI Controls Matrix (AICM) v1.1 provides the control vocabulary for the vendor governance measures recommended above, in particular its supply chain management, transparency and accountability domain, which addresses supplier assessment and the flow-down of requirements to subcontractors [11]. For the assurance gap discussed in the Strategic Considerations section, CSA's Security, Trust, Assurance and Risk (STAR) program is the natural venue for structured supplier disclosures, since it already publishes provider self-assessments and third-party attestations that buyers can consult [12]. Neither artifact currently evaluates ownership or state affiliation as a stand-alone criterion; the extension is a proposal of this note and not a feature of the existing programs.

# References

- [1] CISA, FBI, NSA and partner agencies. "[Chinese Government-linked Cyber Threat Actors Combine Automated and Hands-on Hacking Tools \(AA26-281A\)](#)." CISA, October 8, 2026.
- [2] U.S. Department of Justice. "[Justice Department and FBI Seize Vulnerability Scanning and Spear Phishing Tools Operated by Integrity Technology Group](#)." Office of Public Affairs, October 8, 2026.
- [3] The Hacker News. "[FBI Says China-Linked Hackers Ran Portal Giving Third Parties Access to Stolen Emails](#)." October 2026.
- [4] Tech Times. "[Beijing Firm Integrity Technology Group Hacked Government Email, Built Third-Party Portal](#)." October 9, 2026.
- [5] SecurityWeek. "[US Sanctions Chinese Firm Linked to Flax Typhoon Attacks on Critical Infrastructure](#)." January 2025.
- [6] Dark Reading. "[FBI Leads Takedown of Chinese Botnet Impacting 200K Devices](#)." September 2024.
- [7] Cyber Policy Review. "[Integrity Tech-enabled campaigns: a new joint advisory, not a new single breach](#)." October 2026.
- [8] VulnCheck. "[Expanding Visibility Into Chinese Government-linked Cyber Threat Actors](#)." October 2026.
- [9] Cloud Security Alliance. "[AI Development Stack Concentration Risk](#)." CSA Labs, May 2026.
- [10] Cloud Security Alliance. "[AI Stack Monoculture: Systemic Risk in the Open-Source Ecosystem](#)." CSA Labs, May 2026.
- [11] Cloud Security Alliance. "[AI Controls Matrix \(AICM\) v1.1](#)." CSA, 2026.
- [12] Cloud Security Alliance. "[STAR Program Overview](#)." CSA, last updated March 13, 2026.
- [13] Cloud Security Alliance. "[AI Infrastructure Monoculture: Foundation-Layer Concentration Risk](#)." CSA Labs, April 2026.