SOLUTION BRIEF

Government Supply Chain Cyber Risk Management

Innovative Services That Identify and Mitigate Cyber Risk Within Your Supply Chain

The U.S. Government (USG) relies on a network of over 200,000 direct vendors to meet its needs and requirements, each posing a unique supply chain risk. The recent SolarWinds breach further demonstrates vulnerabilities in USG supply chains to cyberattack vectors.

The USG currently lacks a comprehensive and verifiable tool to assess the cyber vulnerabilities of its supply chains. While standards and certifications like NIST, CMMC, FedRamp etc., can be helpful in reducing cyber risk, they only provide a snapshot of a vendor's cyber health at the time of implementation and during periodic reviews.

Traditional physical supply chain risk can be traced with a simple upstream to downstream pattern. Cyber risk to supply chains, however, has endless permutations including through software suppliers and third-party vendors with which a company is in regular communication. Even onshoring or re-shoring supply chains does little to reduce cyber risks.

Overview

- Provides an unblinking eye on the supply/partner chain and proactive cyber defense
- Developed by former US Government personnel, a globally scaled, continuously updating, external target reconnaissance system (like an advanced adversary) – operationalized for rapid defensive remediations

Operational Options

- BlueVoyant Risk Operations Center curates findings, guides supplier remediation, escalates when not responsive, and provides client with real time visibility of the portfolio including remediation status.
- Alternatively, can deliver findings and remediation monitoring to US Government for follow up.
- BlueVoyant covers many, delivers findings/status on critical subset that USG prefers to cover directly.

What Makes Us Different

- SOC approach to 3rd Party Risk - continuous updating
- We go beyond alerting, working with your supply chain to fix problems
- Largest exclusive outside-in data sets and analytics
- Founded by highly credentialed former private sector and government cybersecurity experts

Core Capabilities

✓ **ACCURATE**
Extensive proprietary and commercial data sets, detection playbooks, findings prioritization and quality control

✓ **GLOBAL CAPABILITY**
Operational in 6 Continents

✓ **QUICKLY AND EASILY DEPLOYED**
Need only supplier company names and main internet address. Then external data and detection algorithms – no installation needed at supplier. Quickly covers thousands of suppliers/partners.

✓ **SCALABLE**
Data continuously generated on 16.5 Million Suppliers/Partners

✓ **RAPIDLY ADAPTABLE TO NEW THREATS**
Responds to New Externally Visible 0 Days Within 24 Hours

✓ **NOT JUST ANOTHER DATA SET**
Risk Reduction Service that continuously interacts with suppliers to eliminate cyber risks, with full visibility to US Government clients.

CYBER RISK TO U.S. GOVERNMENT SUPPLY CHAINS, BY BLUEVOYANT

- The U.S. Government (USG) relies on a network of over 200,000 direct vendors to meet its needs and requirements, each posing a unique supply chain risk. The recent SolarWinds breach further demonstrates vulnerabilities in USG supply chains to cyberattack vectors.
- The USG currently lacks a comprehensive and verifiable tool to assess the cyber vulnerabilities of its supply chains. While standards and certifications like NIST, CMMC, FedRamp etc., can be helpful in reducing cyber risk, they only provide a snapshot of a vendor's cyber health at the time of implementation and during periodic reviews.
- Traditional physical supply chain risk can be traced with a simple upstream to downstream pattern. Cyber risk to supply chains, however, has endless permutations including through software suppliers and third-party vendors with which a company is in regular communication. Even onshoring or re-shoring supply chains does little to reduce cyber risks.
- According to a September 2018 Department of Defense (DoD) report, DoD "supply chain operations rely on an infinite number of touch points where information flows through a network."
- Even large companies with formidable cyber defensive capabilities are vulnerable through a reliance on small and medium-sized US manufacturers, over 50% of which lack basic cyber controls according to the Bureau of Industry and Security.
- The USG needs real-time and scalable insights into its supplier network so that it can drive down cyber vulnerabilities, enhance national security, and protect key processes.

About BlueVoyant

BlueVoyant is an expert-driven cyber security services company whose mission is to proactively defend organizations of all sizes against today's constant, sophisticated attackers and advanced threats.

Led by CEO Jim Rosenthal, BlueVoyant's highly skilled team includes former government cyber officials with extensive frontline experience in responding to advanced cyber threats on behalf of the National Security Agency, Federal Bureau of Investigation, Unit 8200 and GCHQ, together with private sector experts. BlueVoyant services utilize large real-time datasets with industry-leading analytics and technologies.

Founded in 2017 by Fortune 500 executives and former Government cyber officials and headquartered in New York City, BlueVoyant has offices in Maryland, Tel Aviv, San Francisco, London, and Latin America.

BlueVoyant®

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**