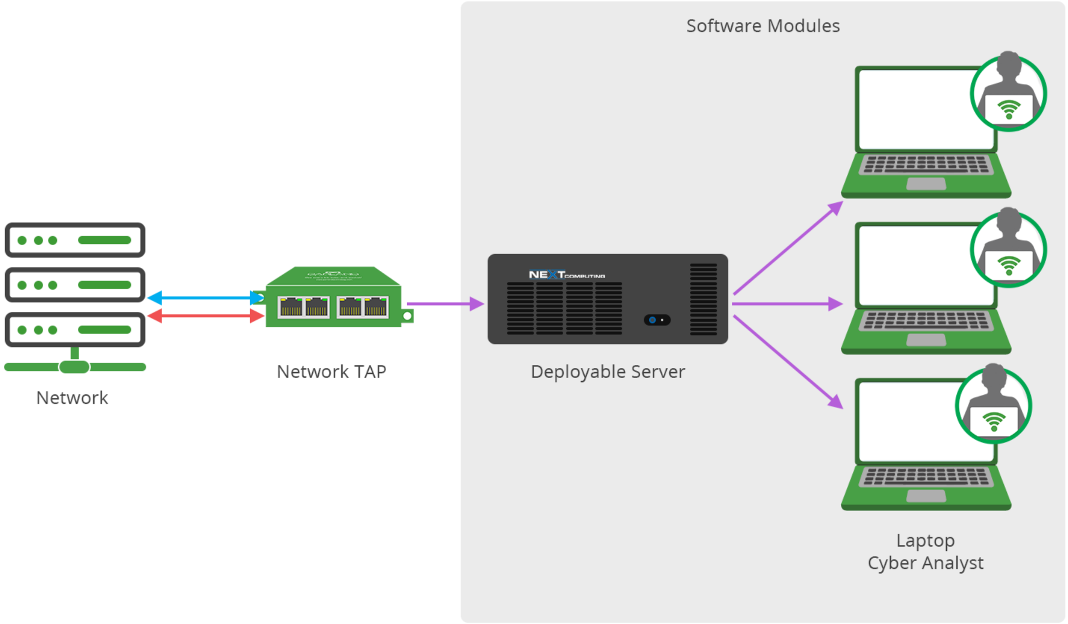
SOLUTION GUIDE

Monitoring: Fly-Away Kits

Tactical Gear for Rapid Response Teams

A Fly-away Kit (FAK) or Expeditionary Kit is a self-contained suite of equipment the Department of Defense (DoD) and federal civilian Cyber Protection Teams (CPTs) deploy to operate in both tactical (field) and back-office environments. The FAK suite of cyber tools or cloud/server applications include tools to conduct vulnerability analysis, incident response, and other cyber-analytic functions, and are suitable for operation on both classified and unclassified networks.



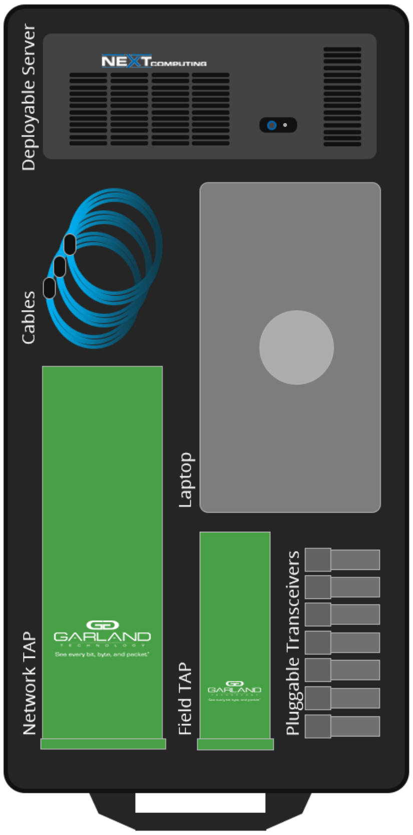
In order to determine the state of the critical networks or to run a deployable network, cyber teams, IT infrastructure teams, and data analytics teams require:

- Packet visibility and access into the network
- Network data from sensors from deployable servers
- Analytic capability from the hardware and software
- A user interface typically via their laptops

Fly-away Kit Objectives

A Fly-away kit must enable agile rapid response by CPT teams. These kits need to easily scale up and scale down while traveling to meet the mission and be able to respond at a moment’s notice, and not have to carefully schedule additional travel assets. Fly-away kits must:

- Be “carry-on” accessible for commercial aircraft, staying close to the analyst
- Lifted by a single person
- Easily transported by rental car, sedan, or SUV vehicles
- Make travel less conspicuous by carrying smaller items
- Reduce operation costs, by simplifying procurement
- Reduce travel costs by leveraging commercial travel options
- Reduce setup time & tear down time
- Reduce size, so less space used on the site/location, expanding the potential sites where space is a constraint



Fly-away Kit Pain Points

Legacy FAK tools have typically been too large, consist of too many components and peripherals, and are vulnerable to shock damage. In addition, the lack of modularity of legacy tools do not allow the flexibility to support various missions and subordinate commands simultaneously. Legacy tools have been costly and complex to use, which sometimes include large rack servers and 1U network TAPs, making transportation difficult:

- Not agile — transport has to be carefully planned and scheduled, subject to delays
- Expensive to transport
- Subject to damage
- Subject to separation of critical data & equipment from the CPT teams
- 3-4+ person lift
- Large, bulky, takes up a lot of space — cannot go to certain locations based on size/weight
- Cannot easily transport on commercial airline, or via car or standard vehicles
- Complex to setup & complex to tear down
- Not easily configurable

Pay-off Points: There is a critical need for less expensive tools where personnel can engage quickly with minimal training. The ideal cyber Fly-away Kit provides a lighter, smaller, shock-tolerant, faster and more capable suite than the current legacy tools in use today.

Fly-away Kit Requirements

Access Visibility with Network TAP

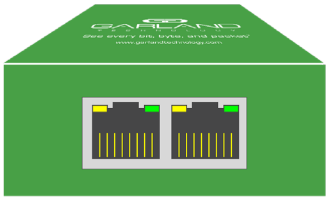
- Duplicate 100% packet traffic (not replication), eg. passing physical errors
- Support various media type, including copper, fiber, and SFP/+ interfaces
- Supports network speeds from 1Gbps and 10Gbps, sometimes up to 40/100Gbps for fiber
- 100% secure and invisible (no IP or MAC addresses)
- Portable, Plug & Play design

GARLAND
TECHNOLOGY
See every bit, byte, and packet®
www.garlandtechnology.com

XtraTAP: Portable Packet Broker

Portable fully configurable and inter-changeable

- Provide full-duplex traffic visibility
- Four port SFP+ design
- Advanced filtering for Layer 2, Layer 3 and Layer 4
- Set utilization alerts to avoid oversubscription
- Media Conversion
- Supports tap filtering, 'breakout,' aggregation, and regeneration/SPAN modes



FieldTAP

Provide pocket size USB network access

- Provide full-duplex traffic visibility
- Monitoring on USB 3.0
- Passes PoE (Power over Ethernet)
- Passes physical layer error
- Link failure propagation (LFP) and Link speed synchronization
- Supports Jumbo frame

Deployable Server

- Fits into overhead storage bin of commercial airlines (TSA-compliant):
  -Physical dimensions: 22" long, 9" tall, 14" wide
  -Under 40 pounds (single-man lift, hand-carried and in a roll-away cases)
- Deployable server hardware is physically modular, with other components capable of being added to increase storage and/or performance capabilities
- Deployable server hardware is also rack-mountable front or back (or both), with removable "ears"

- Systems are capable of meeting all operational requirements in temperatures ranging from 40 °F to 95°F
- Deployable server hardware, in its transport configuration, withstands typical-use vibration tests and drop-tests

Deployable Server – Performance and Modularity

- Intel or AMD processors (single or dual), up to 64 cores / 128 hyperthreads
- No-tools removable storage includes up to (2) NVME, (8) SAS/SATA SSDs, and (2) SATA 6G SSDs
- Up to 512GB of RAM
- Multiple USB 3.1 or better Type-A ports
- PCI Express 3.0 expansion slots
- Both 110-220v AC 50/60Hz power
- Secure Boot UEFI compliant BIOS, Boot Guard, TPM2.0
- Certified for CentOS, Red Hat Enterprise Linux, VMware vSphere, Windows 2019 server, Windows 10

Supports virtualization

Software Components

- Deployable servers and laptops all support virtualized software modules
- These software capabilities are often utilized for cyber protection operations:

  -Network Mapping Software

  -Incident Response Software to include

    • Full disk image capture

    • Memory capture

    • Forensic analysis

-Network traffic ingestion and analysis capabilities that takes advantage of

  • full packet capture

  • offloading and analysis

  •metadata creation for use by other tools

- Host agent and log collection for collection of data from remotely installed agents.
- Vulnerability scanners
- Malware analysis sandbox capability

Transit Pelican Cases

- Deployable server hardware and transit cases may be customized with markings:

  - Private-label logos

  - Labels that identify the weight and number of persons required to lift the object

  - Marked in accordance with MIL-STD-130N (Identification Markings of US Military Property)

- Transit cases include custom cutouts for optional components, as needed.

  - Laptops - multiple laptops will be required per Deployable server

  - Cables, power strips, tools, etc

  - Battery backup module

  - Quick-start documentation

Looking to add network TAP visibility to your troubleshooting or fly-away kit, but not sure where to start? Join us for a brief network Design-IT consultation or demo. No obligation - it's what we love to do.