**OPSWAT**

*Trust no file. Trust no device.*

*OPSWAT protects critical infrastructure (CIP). Our goal is to eliminate malware and zero-day attacks. Our products focus on threat prevention and process creation for secure data transfer and safe device access. 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.*

**Key Contacts & Contracts (if applicable):**

Currently implemented in National Security Sector across the majority of intelligence components to help protect against advanced cybersecurity threats.

**Company Overview**

OPSWAT was founded in 2002 with a focus in addressing the need for cybersecurity in the critical infrastructure space. Throughout the past 20 years, OPSWAT has developed multiple cybersecurity solutions surrounding our Zero Trust Philosophy. We believe that every file and every device pose a threat. Trust no file. Trust no device.

In addition to protecting several government sectors, OPSWAT is:

* Trusted by the DoD, Law Enforcement, and Critical Infrastructure
* Listed on GSA, NASPO, and many other contract vehicles
* Common criteria, FedRamp (in progress), and VPAT 508 authorized
* Collaborates with more than 300 technology partners, highlighted by: F5, Citrix, VMware, and McAfee

**Brief Summary:**

*Geospatial mapping data from satellites to secure networks*

* Focus on Secure File Transfer of this data through OPSWAT solutions
  + K3001 Kiosk (demonstration)
    - Prevent unverified media from accessing your environment.
    - Create and audit secure processes for data transfer via removable media.
    - Detect and prevent advanced threat and targeted attacks.
    - Support multiple media formats like USB, CD/DVD, mobile phones.
    - Maintain compliance with regulations like NERC CIP.
  + Secure Vault
    - Files are scanned for malware and vulnerabilities by 35+ of the cyber industry’s best malware and heuristics engines.
    - Files are re-scanned and evaluated continuously as virus definitions are updated in order to avoid Zero Day incidents
    - Suspicious files are sanitized.
  + Other solutions include Unidirectional Gateway and USB Firewall

**Visit us during GEOINT 2021**

Booth #