OPSWAT

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:

- Focus on Secure File Upload and Transfer of this data through OPSWAT solutions
    - K3001 Kiosk
        - 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.
    - MetaAccess Network Access Control (NAC)
        - Devices can be profiled using rich heuristics and quarantined until they are explicitly known
        - The captive portal allows different authorization and access levels based upon user groups, including guests
        - Deep endpoint compliance and real-time posture check
        - Leverage device information, including user ID, IP and MAC addresses, role, location, time and ownership of the device