Forcepoint

Solution Brief

Multilevel Zero Trust Protection for Government

Enable Zero Trust management, edge protection, data protection and risk profiles across all security domains and networks in your organization.

Challenge

- **Zero Trust for government environments is unique:** Government agencies must manage the increasing risk of protecting sensitive data across all security domains and networks.
- **Gaining comprehensive visibility and dynamic response:** Agencies must discover and inventory critical data and intellectual property across environments.

Solution

- Enable Zero Trust management, edge protection, data protection and risk profiles across security domains and networks.
- Securely share user risk levels across multiple networks for adaptive and consistent enforcement from end to end.
- Consolidate log and monitoring information to a Defensive Cyber Operations (DCO) enclave.

Outcome

- **Greater visibility:** Combine analytics and threat intelligence sharing for users and systems across security domains into a single dashboard.
- **Strengthened security and faster incident response:** Ensure high-assurance controls and conditional access across environments to enable rapid delivery of Zero Trust access.

The NIST Zero Trust data flow tenets suggest that fundamentally Zero Trust must ensure:

I. All communication is secured regardless of network location

II. Access to individual enterprise resources is granted on a per-session basis

III. Access to resources is determined by dynamic policy—including the observable states of client identity, application/service and the requesting asset—and may include other behavioral and environmental attributes

IV. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses that information to improve its security posture.

Zero Trust for government is different:

Federal entities face the challenge of adapting Zero Trust principles to meet unique operational requirements and risk factors. Segregation of agency networks into multiple classified and unclassified security domains introduces additional complexity across government environments, where a user may operate using multiple identities when their activities span multiple security domains. For example, a user who operates in the unclassified domain (e.g. NIPRNET) and the classified domain (e.g. SIPRNET) generates activity information that is collected and stored separately within each domain. This information needs to be consolidated and analyzed as part of the User Entity and Behavioral Analytics (UEBA) capability, which derives user risk levels that drive critical ZT security functions inside the control plane

NSA has clarified: Zero Trust Frameworks shall not be used as an alternative to Cross Domain Solutions.
From a multilevel cyberspace perspective, there is only one user; a user's risk level could vary significantly between security domains. It is important that organizations take a holistic view of user and entity behavior when applying Zero Trust policy.

> Zero Trust mechanisms do not remove requirements for cross-domain solutions, especially when information sensitivity differences create excessive risk or when maturity levels vary widely."

National Security Agency Cybersecurity Information Sheet: Advancing Zero Trust Maturity Throughout the User Pillar
U/OO/127344-23 | PP-23-0208 | MAR 2023 Ver. 1.0

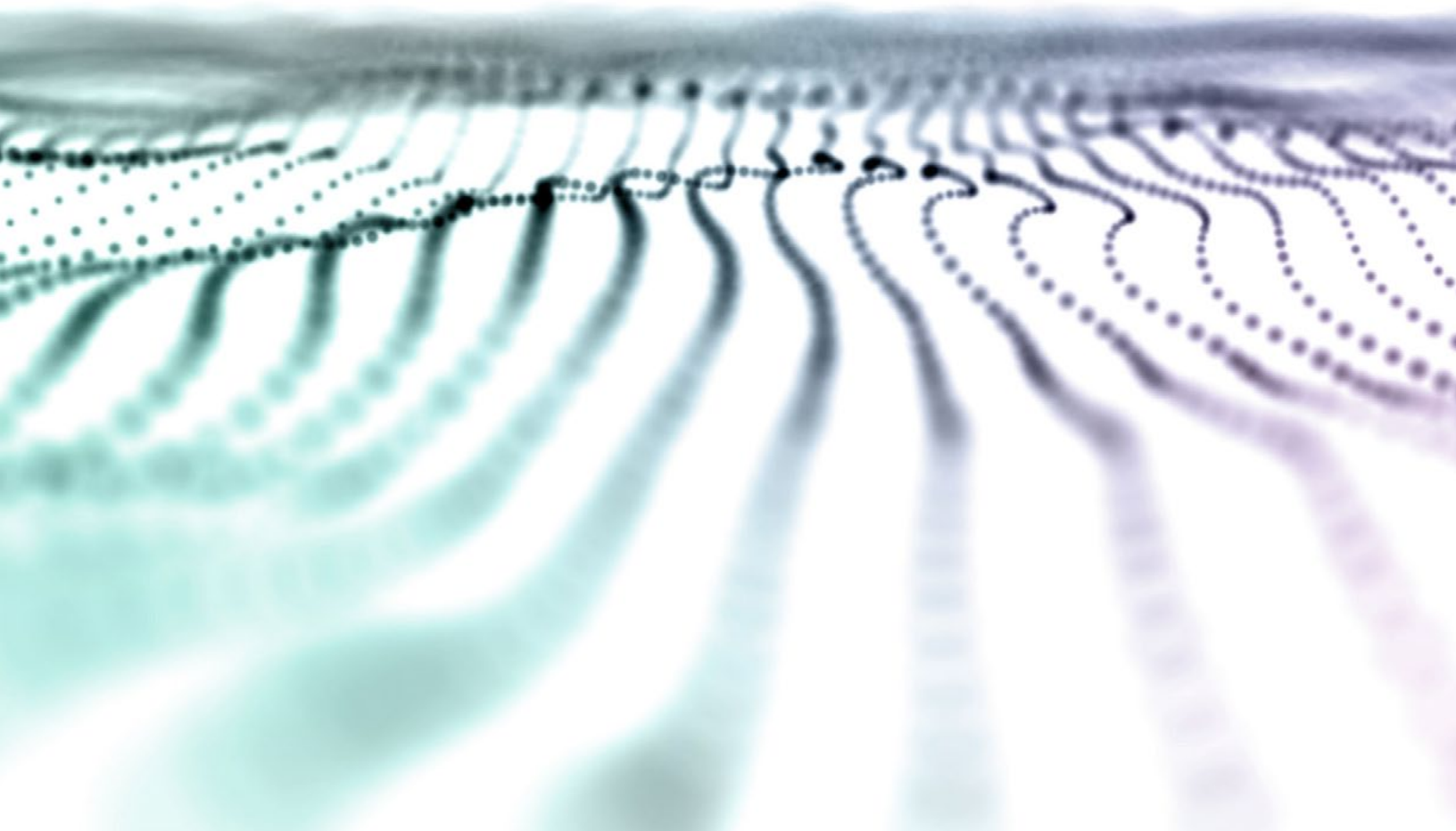
Enable Zero Trust protections across environments with multilevel protection from Forcepoint

Forcepoint brings more than 20 years of expertise supporting the unique and complex missions and objectives undertaken by the people who protect national security and mission-critical information. Forcepoint solutions bring together data security, network, web and cloud security; threat protection; advanced monitoring; Cross Domain protection and Zero Trust control to empower agencies to use data where and how your people need it safely. The cybersecurity solutions within the Forcepoint portfolio are designed to meet the most stringent security requirements and mission objectives. Our mission is to simplify security and protect data wherever it resides.

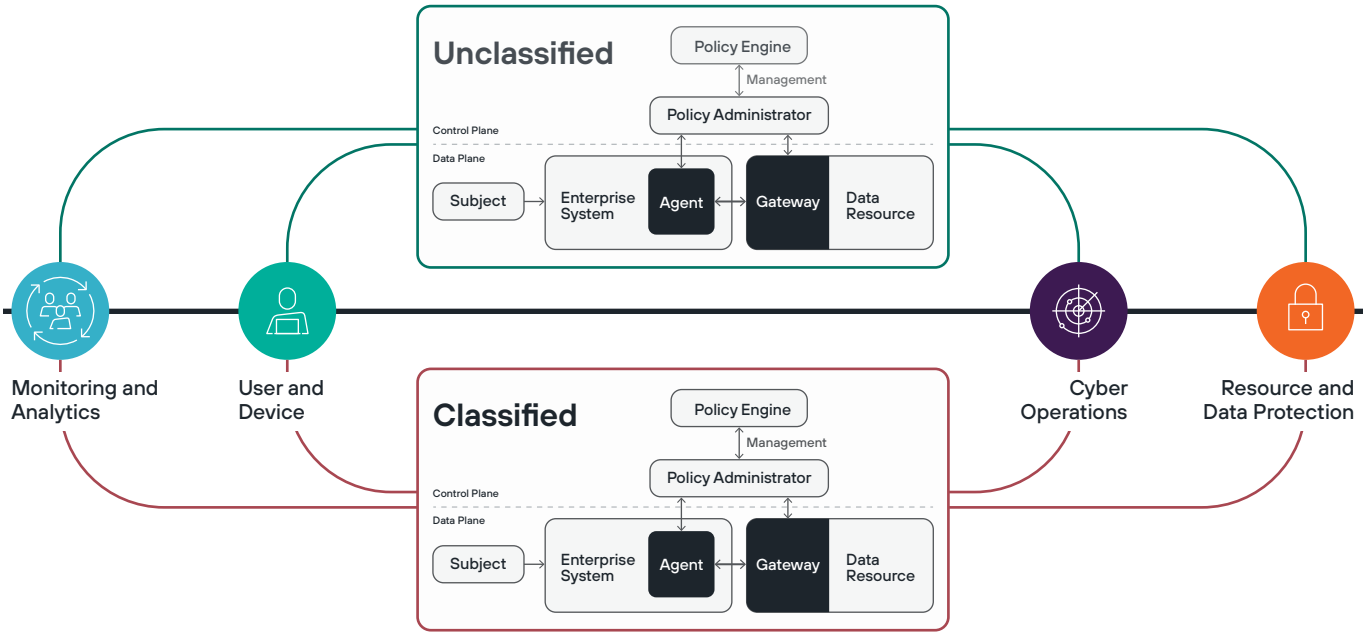
Government agencies around the world depend upon Forcepoint to connect and protect their highly sensitive environments. Forcepoint Cross Domain Solutions help to consolidate information about user and device behaviors across multiple security domains. Forcepoint's Cross Domain Solutions are included on the US NCDSMO baseline list for TSABI and SABI and meet NSA's Raise The Bar guidelines; developer with Access and Transfer solutions recognized by the US NCDSMO.

Forcepoint Cross Domain capabilities—coupled with our extensive portfolio of data security, network, web, and cloud security; threat protection; advanced monitoring; and Zero Trust control—come together to empower agencies to protect data where and how people need it safely, even across physically separated networks.

Forcepoint Multilevel Zero Trust protection solution enables monitoring and enforcement of Zero Trust controls to protect users and systems across security domains. Combining Forcepoint's Cross Domain capabilities with Forcepoint Behavioral Analytics provides holistic visibility of data from broad sources to proactively identify and monitor high-risk behavior, in turn driving better policy enforcement and automatically adjusting risk levels based on changes in behavior. The combined expertise enables Forcepoint to deliver a multilevel Zero Trust solution that continuously monitors risk and enables unrivaled visibility into user behaviors across security domains.



Multilevel Zero Trust Architecture



Forcepoint helps agencies enable Zero Trust management, edge protection, data protection and risk profilesacross security domains and networks. Enabling:

MONITORING AND ANALYTICS

- → Consolidation of log data across multiple security domains
- → Single-device access to dashboards from all security domains
- → Combined analytics for users and systems across security domains

USER AND DEVICE PROTECTION

- → Enforces conditional access controls and segments user traffic based on workload
- → High assurance controls that prevent user device exploits
- → Rapid delivery of Zero Trust access across enterprise

CYBER OPERATIONS

- → Perform activities across multiple monitoring and control planes
- → Automated threat intelligence sharing across domains

RESOURCE AND DATA PROTECTION

- → Automated DevSecOps between security domains
- → Ensures integrity of data labels and other metadata when moving information between security domains

forcepoint.com/contact