Updates in Cyber Tools

- Cloud Based Internet Isolation
- Comply to Connect
- Enterprise Email Security Gateway

The information provided in this briefing is provided for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

Cloud Based Internet Isolation (CBII)

Improved DODIN Perimeter Security

CBII

CLOUD BASED INTERNET ISOLATION

Laurel Lashley
Cyber Security and Analytics Directorate

Apr. 28, 2022

About this Brief

This brief provides:

- Overview of the capability
- Steps to Consume the Service
- Benefits of Using CBII

Cloud Based Internet Isolation

CBII
CLOUD BASED INTERNET ISOLATION

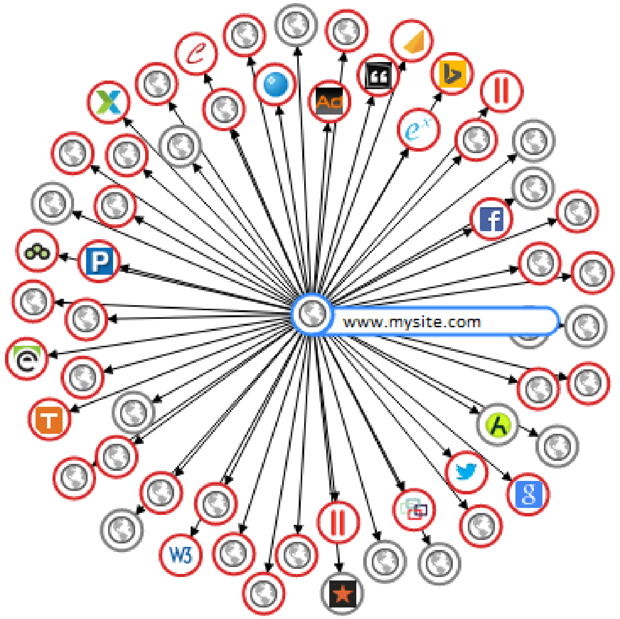
- Reduce the risk and attack surface of the Department of Defense Information Network (DODIN) and relieve internet access point (IAP) congestion
- Moves non-mission internet browsing off the endpoint to a trusted, external cloud environment

Capabilities

- Native modern browser integration
- Moves browsing off the endpoint to trusted cloud
- Strongly attributes browsing to user
- Eliminates 3rd party plugins (e.g., Flash)
- Remote document viewing (safe document creation)
- File antivirus scanning/detonation/hash comparison
- Bandwidth optimization
- Bandwidth monitoring/reporting
- Video optimization
- Browser recording

Enhancements

- Integrated Data Loss Prevention toolset baseline
- Mobile integration



Modern websites:

- *May contain 6,000+ lines of code.*
- *Connect to >60 other domains (ad networks, content delivery networks, trackers, etc…).*

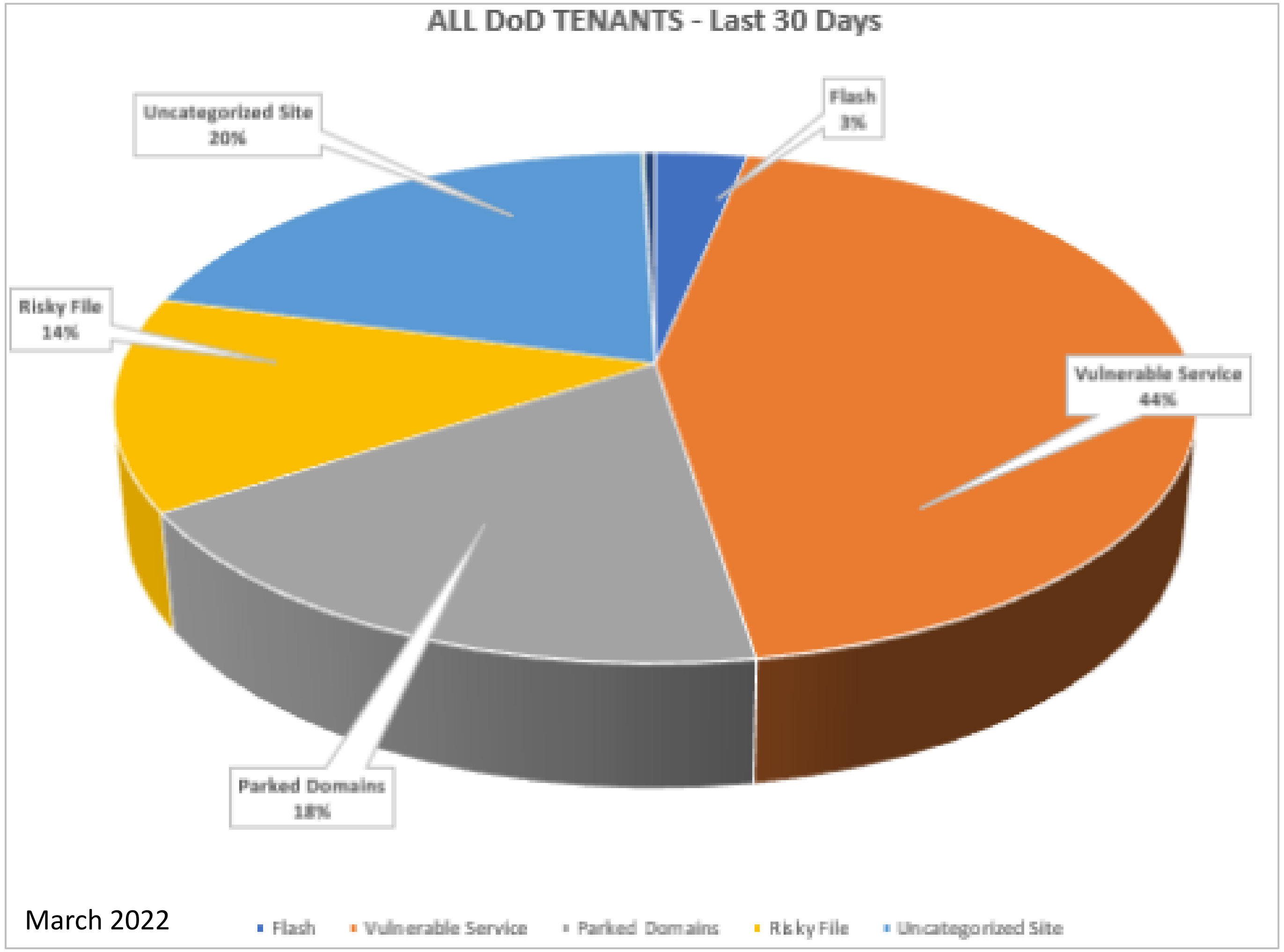
Migrating to CBII

1. **Configure and Test Connectivity**
    - Manual Configuration
    - Active Directory Automation Guide - Outlines the group policy object setup
    - Global Federated User Directory integration
2. **Test and Troubleshoot the Final Configuration**
3. **Deployment**

Complete DoD-Wide Migrations NLT September 2024

Threat Mitigation & Bandwidth Utilization Snapshot

CBII
CLOUD BASED INTERNET ISOLATION



ALL DoD TENANTS - Last 30 Days

March 2022

All DoD Tenants

March 2022

THREAT	EVENTS
Flash	1,552,241
Vulnerable Service	21,184,517
Parked Domains	8,765,923
Risky File	6,483,712
Uncategorized Site	9,669,317
Malware	43,468
Phishing	177,820
Plugin Risk	3,349
Spam	3,814
Botnet	33
DoD Threats Mitigated	**47,884,194**

Aggregated Bandwidth Utilization

Downloads	Uploads
2478.61 TB	**36.64 TB**

PROTECT THE DODIN AGAINST BROWSER-BASED THREATS

CLOUD BASED INTERNET ISOLATION

CBII
CLOUD BASED INTERNET ISOLATION

Adopt or Expand CBII in your organization.

47.8M
THREATS MITIGATED

1.96M
USERS ENGAGED

>2,515TB
NON-MISSION ESSENTIAL
TRAFFIC OFFLOADED

March 2022

Email **DISA.CBII-M@MAIL.MIL** to get started today!

DISA

Back-up Slides

CBII – Threat Type Definitions

Vulnerable Service	Menlo Security analyzes the software packages (WordPress, vBulletin, VanillaForum, Squid, Python, PHP, Perl, nginx, Microsoft-IIS, MediaWiki, Joomla!, Drupal, Apache) used to serve the web page being requested. If the packages are versions which have known CVE's/Vulnerabilities, the request is marked as *Vulnerable Service*. There are policy controls on the individual services (via the Central Manager *Web Policy -> Threat Rules -> Detailed* screen).
Uncategorized Site	Any site which has not been categorized (sports, news, etc.). Sites which are uncategorized generally represent a significant source of malware or phishing, as hackers are constantly trying to create new sources to serve malicious software.
Flash Site	Sites which leverage Flash to serve content (games, videos, ads, etc.). Note that this is not listed on the *Threats* pane but is available as an exception.
Spam	URLs contained in SPAM.
Phishing	Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personal information from a user.
Malware	Malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, and code. Spyware or Adware sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, the end user or the organization. Also unsolicited advertising popups and programs that may be installed on a user's computer. Downloads and discussion of software agents that track a user's keystrokes or monitor their web surfing habits. Includes subcategory names: *Key Loggers and Monitoring*, *Dead Sites*, *Spyware and Addware*.
Malvertising	Malware delivered via ad networks. Often classified generically in the *Malware* category.
Compromised Host	System observed operating as a Tor exit node or performing scans of ranges of internet addresses.
Command and Control	System observed either hosting malware command and control communications or connecting to a command and control server.
Botnet	These are URLs, typically IP addresses, which are determined to be part of a Bot network, from which network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contacts.
Parked Domains	Registered internet domain name that is not associated with any services such as e-mail or a website.

CBII – Threat Type Definitions (cont.)

Risky Files

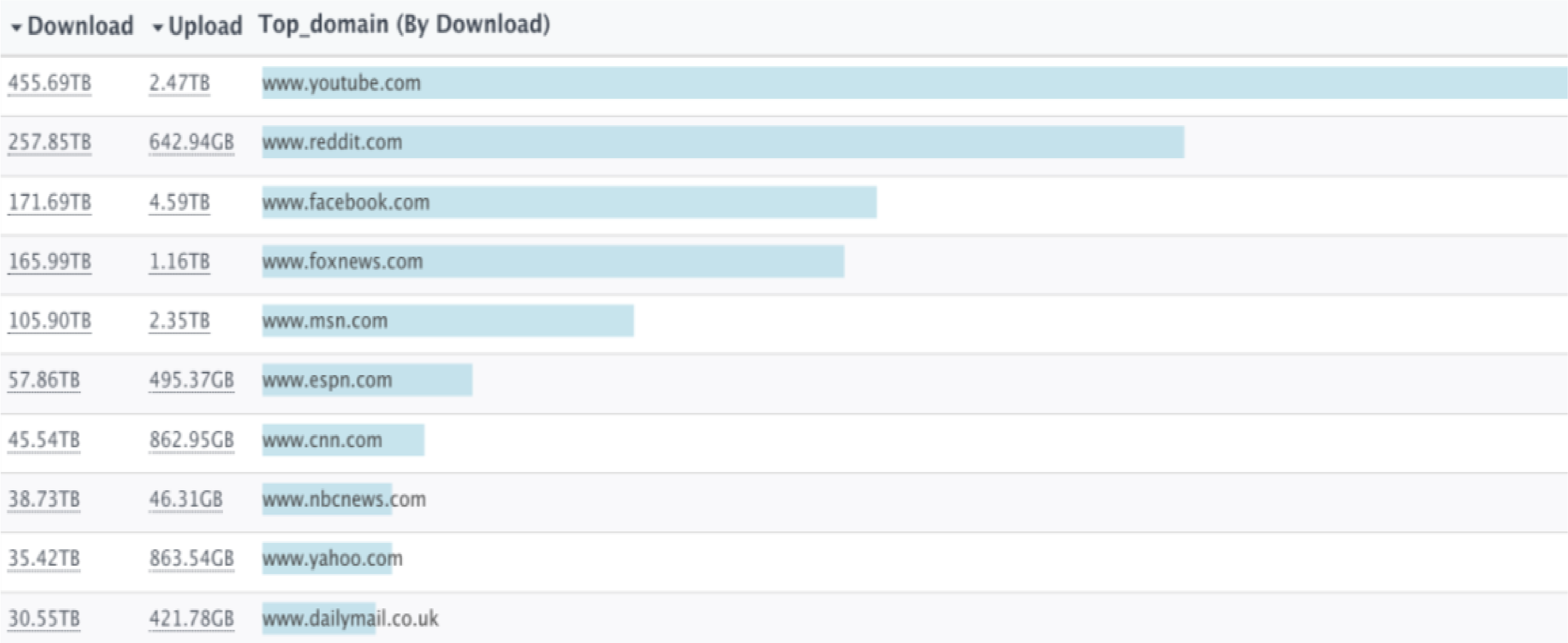
File are marked as risky if:

- Files found to be marked as Infected by any of the Content Inspection engines.
- Files not known to the hash database for File Hash Check is disabled.
- Content Inspection Exceptions to mark a file as Infected.
- If AV(Anti-Virus) scanning had to be skipped because the file was encrypted and Skip password prompting of encrypted files was enabled.

Plugin Risk

Browser plug-ins have proven to be more insecure than browsers themselves, and Flash and Java are some of the biggest attack vectors on the web. During an isolated browsing session, the CBII surrogate browser executes all active content (scripts, Java, ActiveX, etc.) on behalf of the end-user, delivering only safe rendering instructions and ultimately mitigating native-browsing vulnerabilities associated with the use of plugins.

Top 10 Aggregated Download/Upload –Sites – March (All DoD tenants)



▾Download	▾Upload	Top_domain (By Download)
455.69TB	2.47TB	www.youtube.com
257.85TB	642.94GB	www.reddit.com
171.69TB	4.59TB	www.facebook.com
165.99TB	1.16TB	www.foxnews.com
105.90TB	2.35TB	www.msn.com
57.86TB	495.37GB	www.espn.com
45.54TB	862.95GB	www.cnn.com
38.73TB	46.31GB	www.nbcnews.com
35.42TB	863.54GB	www.yahoo.com
30.55TB	421.78GB	www.dailymail.co.uk

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Comply to Connect (C2C)

Foundational Capability for Zero Trust Environments

Mr. Donald Cook

Cyber Security and Analytics Directorate

27 April 2022

C2C Overview (Why C2C)

- The National Defense Authorization Act (NDAA) for FY17, Section 1653, requires implementation of Comply-to-Connect (C2C) and Information System Continuous Monitoring (ISCM) capability

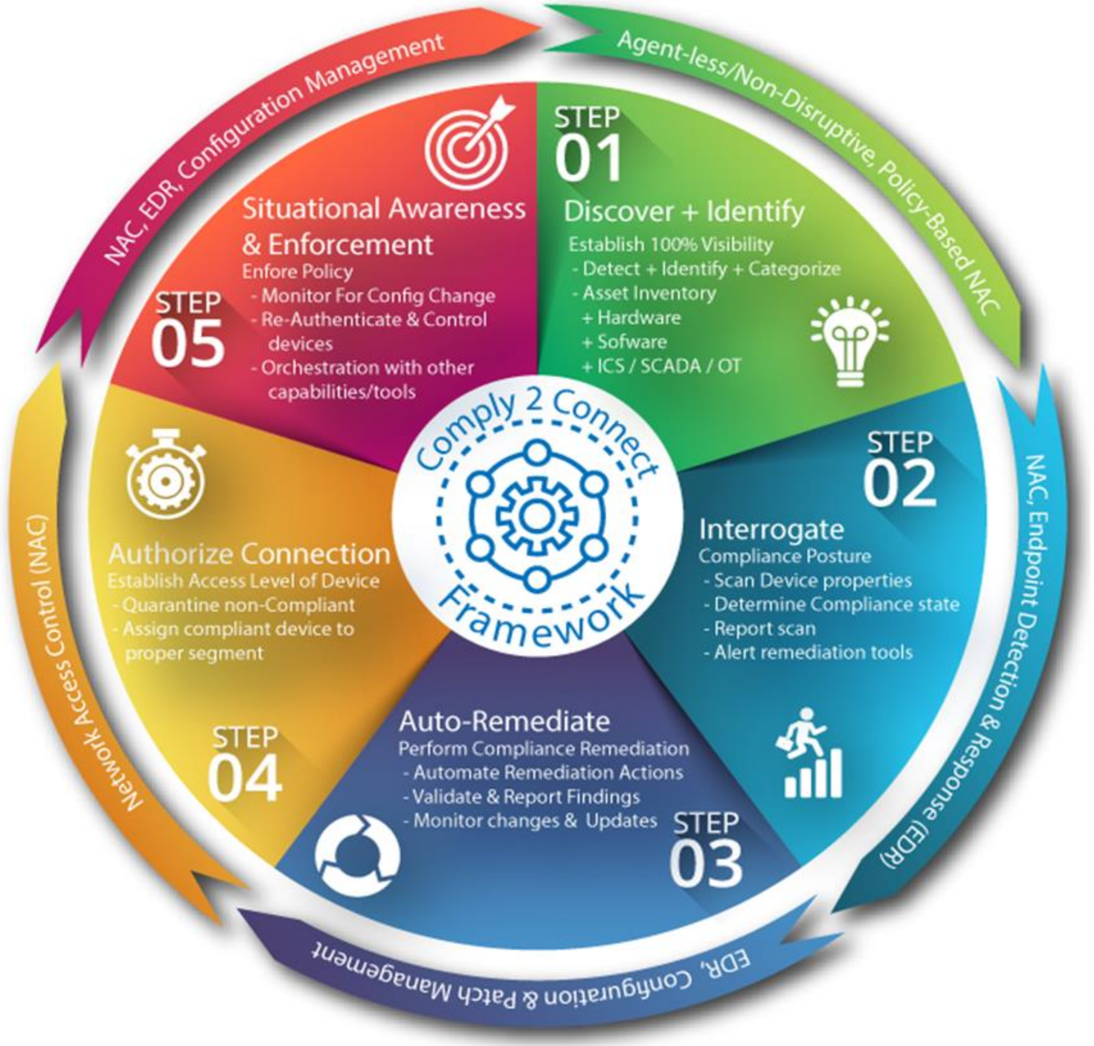
- The Federal Information Security Modernization Act FY 2018 Annual Report to Congress
    - Office of Management and Budget identified five common security shortfalls across the federal agencies high value assets
        - Lack of data protection
        - Lack of network segmentation
        - Inconsistent patch management
        - Lack of strong authentication
        - Lack of continuous monitoring

- Presidential Executive Order (EO) 14028, *Improving the Nation's Cybersecurity,* May 2021
    - Government-wide effort to ensure that baseline security practices are in place to migrate the DoD to a zero-trust architecture

Comply to Connect is An Enabler for Zero Trust

Unified, extensible, interoperable platform that offers:

- Continuous Discovery & Identification
- Live Interrogation
- Auto-remediation
- Authorizing Connection / "Segmentation"
- Full Situational Awareness



Agent-less/Non-Disruptive, Policy-Based NAC

STEP 01
Discover + Identify
Establish 100% Visibility
- Detect + Identify + Categorize
- Asset Inventory
+ Hardware
+ Sofware
+ ICS / SCADA / OT

NAC, Endpoint Detection & Response (EDR)

STEP 02
Interrogate
Compliance Posture
- Scan Device properties
- Determine Compliance state
- Report scan
- Alert remediation tools

EDR, Configuration & Patch Management

STEP 03
Auto-Remediate
Perform Compliance Remediation
- Automate Remediation Actions
- Validate & Report Findings
- Monitor changes & Updates

Network Access Control (NAC)

STEP 04
Authorize Connection
Establish Access Level of Device
- Quarantine non-Compliant
- Assign compliant device to proper segment

NAC, EDR, Configuration Management

STEP 05
Situational Awareness & Enforcement
Enfore Policy
- Monitor For Config Change
- Re-Authenticate & Control devices
- Orchestration with other capabilities/tools

Comply 2 Connect Framework

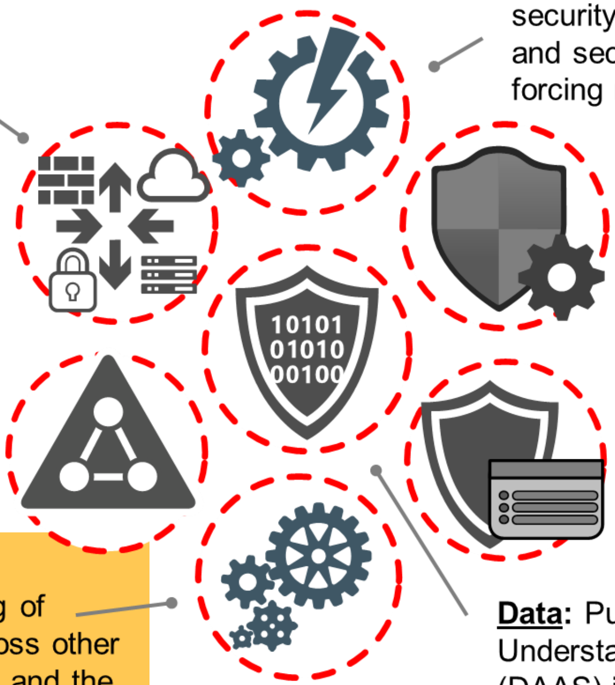
Zero Trust and Comply-to-Connect

Principles:

1. **Never Trust, Always Verify** – All users and devices are treated as untrusted. Every device, user, application/workload and data flow is authenticated and explicitly authorized to the ***least privilege*** required using dynamic security policies.
2. **Assume Breach** – Consciously operate and defend resources with the assumption that an adversary has presence within your environment. Deny by default, heavily scrutinize requests for access, users, devices and data flows. All traffic is logged and inspected.
3. **Verify Explicitly** – All resources are ***consistently*** accessed in a secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access to resources.

Definition: "A data-centric security model that eliminates the idea of trusted or untrusted networks, devices, personas or processes and shifts to ***multi-attribute based confidence levels that enable authentication and authorization policies*** under the concept of least privileged access."

DoD Digital Modernization Strategy
Jul 12, 2019



Network/Infrastructure: Segment (logically and physically), isolate and control network environment with granular access and policy restrictions.

Automation/Orchestration: Automated security response based on defined processes and security policy, i.e. blocking access, or forcing remediation

User: Continuously authenticate, authorize and monitor user activity patterns to govern users' access and privileges, while protecting and securing all interactions.

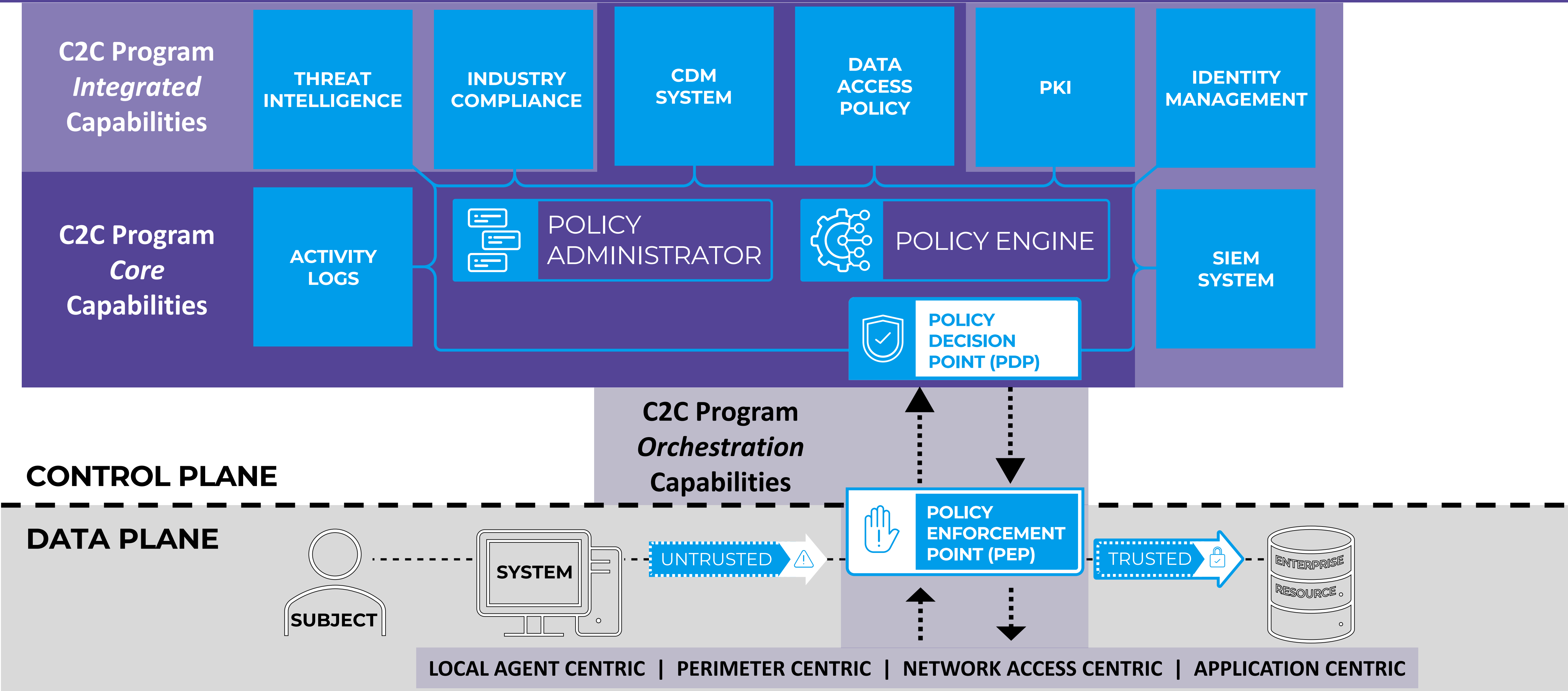
End Devices: Understanding network health and status informs risk decisions. Realtime inspection, assessment and patching informs every access request.

Applications/Workload: Controlling access and further controlling what resources applications can access is central to ZT.

Visibility & Analytics: Provides vital, contextual data to derive understanding of performance, behavior and activity across other ZT pillars. Improves detection, reaction and the ability to make real-time access decisions.

Data: Purpose of Zero Trust is to protect data. Understanding data, application, assets and services (DAAS) is critical. A data management strategy is part of the approach to Zero Trust.

C2C Orchestration Capabilities


C2C Program *Integrated* Capabilities
THREAT INTELLIGENCE
INDUSTRY COMPLIANCE
CDM SYSTEM
DATA ACCESS POLICY
PKI
IDENTITY MANAGEMENT
C2C Program *Core* Capabilities
ACTIVITY LOGS
POLICY ADMINISTRATOR
POLICY ENGINE
SIEM SYSTEM
POLICY DECISION POINT (PDP)
C2C Program *Orchestration* Capabilities
CONTROL PLANE
DATA PLANE
SUBJECT
SYSTEM
UNTRUSTED
POLICY ENFORCEMENT POINT (PEP)
TRUSTED
ENTERPRISE RESOURCE
LOCAL AGENT CENTRIC | PERIMETER CENTRIC | NETWORK ACCESS CENTRIC | APPLICATION CENTRIC

Conclusion

Objective: "When fully implemented, DoD Components will have control over what endpoints are allowed to connect to DoD networks, comprehensive and continuous network visibility of the diverse endpoints connected to their networks along with understanding of endpoint security compliance."

NDAA, Fiscal Year 2017, Section 1653
Dec 23, 2016

Please send your questions or inquiries to:

Contact:
DISA C2C Project Management Office (PMO)
disa.meade.id.mbx.id31-comply-to-connect-c2c-program-management-@mail.mil

Closing Slide

DISA

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

/DISA **@USDISA** **/USDISA** **DISA.mil**

Enterprise Email Security Gateway

AFCEA Technet Cyber 2022

Thuy Che

Cyber Security and Analytics Directorate – EEMSG Program Manager

EEMSG Overview

Mail continues to be a top threat vector – EEMSG receives over **1.2** billion Internet-sourced emails per month from **1,000**s of source IPs

Improves the ability to detect, diagnose, and react to email-borne cyber attacks

Provides enterprise-level email protection at the boundary to act as the DODIN's first line of defense for SMTP traffic

Manages Inbound and Outbound traffic flows

Evolves as we transition from on prem email servers to SaaS

Capabilities Provided by EEMSG

Filters emails based on custom signatures

Develops and implements new filters and signatures based on intelligence reports and world events

Validates IP/domain and URL reputation

- Over 85% of Inbound email is dropped due to sender reputation
- Delivers improved user experience, neutering URLs only if they have a poor reputation score

Applies DoD enterprise security policy based on commercial standards

(SPF, DKIM, DMARC)

- Reduces inbound email spoofing
- Validates emails were not modified
- Identifies attempts to hijack DoD domains

Integrates with Zero-day Network Defense and other tools to provide advanced threat detection

Modernization Activities

Support direct delivery to multiple Microsoft (MS) Office 365 (O365) tenants

- Direct delivery will allow MS O365 customers to decommission their on-premise mail servers and **reduce costs**
- IOC Summer 2022

Pilot an MS Azure-based enclave to enhance MS O365 tenant security

- Neuter untrusted and unknown URLs to **make them unclickable**
- Enforce DoD enterprise security policies on tenant-to-tenant email
- Start Summer 2022

Secure email for Impact Level (IL)2 domains - Internet-hosted commercial cloud .mil

- Currently in investigation phase
- Recommend cloud .mil domains migrate to IL4/5 to gain automatic Inbound and Outbound EEMSG protections

Conclusion

- **EEMSG provides an effective service enforcing DoD email security policies**
  - Centrally funded
  - Domain-specific polices are enforced within the customer enclaves
  - Capability is evolving with SaaS
- **DoD Customer/Sponsor Service Requests (DISA Enterprise Service Desk)**
  - NOT for Internet customer use
  - DoD Enterprise Services Service Desk
    - COM: (844) 347-2457; Select Option 1, then 5, then 1
    - DSN: 850-0032; Select Option 1, then 5, then 1
    - disa.tinker.eis.mbx.dod-enterprise-services-service-desk@mail.mil
- **PMO Contact Info**
  - disa.meade.ma.list.emsgtieriii@mail.mil

Closing Slide

DISA

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

/DISA **@USDISA** **/USDISA** **DISA.mil**