HELPING FEDERAL AGENCIES ACHIEVE C2C COMPLIANCE

Appgate SDP Supports Cloud Native Access Point (CNAP) Comply-to Connect (C2C) and Zero Trust Security for the U.S. Air Force

The Challenge

As the DoD's Information Network (DoDIN) has expanded, so has its attack surface. Widespread digitalization, combined with endpoints numbering in the tens of millions, means adversaries have more opportunities to attack federal networks. The list of adversaries ranges from terrorists and criminals to advanced persistent threats by coordinated, well-funded, highly trained nation state hackers.

The stakes could not be higher: Cyber-attacks on DoDIN have the potential to destroy critical infrastructure, hobble government and military activity, compromise operations, steal technology, undermine the economy, and endanger the lives of military and civilian personnel.

DoD Response to Cyberthreats

To ensure clear visibility and full situational awareness into DoDIN, DoD developed the Comply-to-Connect (C2C) platform. C2C is designed to authenticate devices and users accessing the network, determine if they meet security requirements and monitor for ongoing compliance. C2C also automates security tasks and remediation, and coordinates responses to noncompliant devices and incidents.

U.S. Air Force Leverages Appgate SDP as CNAP

The U.S. Air Force (USAF) chose to leverage Appgate SDP for Zero Trust Network Access, deployed as Cloud Native Access Point (CNAP). CNAP provides the USAF with the ability to protect cloud and on-premises operating environments with a more dynamic architecture that is easily adaptable and scalable … one that securely connects users from anywhere at any time on any device and is agnostic to underlying infrastructure or platforms.

By leveraging a Zero Trust architecture, CNAP provides security capabilities and systems monitoring to protect, respond and recover from cyberattacks. Its benefits include:

- Determining device configuration
- Automating ticket generation
- Quarantining vulnerable devices and at-risk users
- Isolating and denying access to unauthorized and noncompliant devices
- Integrating with identity credential and access management (ICAM) solutions
- Enforcing least privilege network segmentation
- Continuously monitoring devices and user activities
- Continually rechecking and enforcing policies and compliance
- Providing device fingerprinting, remediation steps and automated ticket generation.
- ATARC Zero Trust Lab Performer

Accordingly, CNAP directly aligns with requirements outlined in the DOD CIO C2C memorandum, while increasing USAF dominance in the cyber battlespace.

CNAP Side-by-Side Comparison with Traditional C2C

The table illustrates how CNAP provides superior services and security capabilities compared to traditional C2C compliance, by augmenting or replacing traditional C2C elements and combining user, device, and environmental context to strengthen the DoDIN's security posture.

CAPABILITY	TRADITIONAL C2C	CNAP CAPABILITY
Device Discovery & Identification	✔ Area of strength on Managed Networks	✔ Area of Strength: All Assets "Untrusted"
Device Inventory	✔ Area of Strength	– Limited: Requires Log aggregation and correlation
Determine Asset Configuration	✔ Area of Strength	✔ Area of Strength
Automated Remediation and Reporting	✔ Area of Strength	– Limited: Requires Integration
Continuous Device Posture Monitoring	✔ Area of Strength	✔ Area of Strength
Fully Integrate with ICAM - Attribute based access controls	– Limited: Attributes do not drive Micro-segmentation	✔ Area of Strength
Extend Zero Trust Capability Anywhere, Any Network	– Limited	✔ Area of Strength
Displace the need for Trusted on Managed Switches	– Limited	✔ Area of Strength
Does not Requires 801.1x Port Access Control (Managed Network)	– Limited	✔ Area of Strength
Enforce Least Privilege per Application Segmentation	✘ Not Supported	✔ Area of Strength
Micro-segmented access control	✘ Not Supported	✔ Area of Strength
Conditional Access Policies - Time, Location, Risk Score, MFA Provided	✘ Not Supported	✔ Area of Strength
Next Generation Firewall (IDS, WAF, Reverse Web Proxy)	✘ Not Supported	✔ Area of Strength
Base Boundary Replacement- SWAN & SDP	✘ Not Supported	✔ Area of Strength
Single Sign-on	✘ Not Supported	✔ Area of Strength
Connection Compliance - Access to CSP or C/B/P/S	✘ Not Supported	✔ Area of Strength
Delivered "as code" Virtual Infrastructure and Configuration	✘ Not Supported	✔ Area of Strength
Fully Integrated into DevSecOps - CI/CD	✘ Not Supported	✔ Area of Strength

Proven Zero Trust for Federal Agencies

Appgate is a uniquely qualified, Zero Trust market leader serving the federal government sector and was recently named a Leader in the 2021 Forrester ZTNA New Wave report.

Federal designations include:

- Common Criteria Certified
- FIPS 140-2 Validated
- DoD Approval to Operate (ATO) in IL5 environments, certified for SC2S [secret IL6]
- FedRAMP via Rackspace Government Cloud
- Contract vehicles: GSA Schedule, SEWP, DHS CDM APL

In order to keep pace with federal mandates and the White House Executive Order, Appgate maintains tight alignment with the following:

- DoD ZTRA March 2021
- NIST 800-207 NCCoE Collaborator
- OMB Zero Trust Memo 12 May 2021
- CISA ZT Maturity Model July 2021
- DoD CIO Memo Cloud Native Access Point (CNAP) Reference Design July 2021
- ATARC Zero Trust Lab Performer

To learn more about how Appgate SDP can help your organization achieve C2C compliance, visit www.appgate.com/federal-division, visit www.appgate.com/federal-division.

About Appgate

Appgate is the secure access company that provides cybersecurity solutions for people, devices and systems based on the principles of Zero Trust security. Through a set of differentiated cloud and hybrid security products, Appgate enables global enterprises and governments to easily and effectively shield against cyber threats. Learn more at appgate.com/federal-division.

appgate