appgate

APPGATE **FEDERAL DIVISION**

FEDERAL AGENCIES: SECURE YOUR HYBRID WORKFORCE, ENABLE BYOD POLICIES

Appgate SDP fully aligns with **TIC 3.0** and **CLAW**

Federal agencies have never faced greater cybersecurity threats than they do today.

Hackers have been emboldened by the rapid shift to work-from-home, an explosion of bring your own device (BYOD) policies and expanded attack surfaces. In fact, agency breaches are driving headline news:

- US agencies hacked in monthslong global cyberspying campaing
- SolarWinds hack 'compromised' 9 fed agencies
- Multiple agencies breached by hackers using Pulse Secure vulnerabilities

Additionally, compliance with urgent federal security mandates has never been more essential to the effective functioning of federal agencies. The dynamic response by the Department of Homeland Security (DHS) and its cybersecurity arm, the Cybersecurity and Infrastructure Security Agency (CISA), demands that agencies adopt technology and practices to deter and respond to cyberthreats. That response includes:

- **TIC 3.0:** the Trusted Internet Connection initiative requires that all federal internet traffic be routed through an agency that is TIC-approved. TIC 3.0 allows agency employees to access cloud services and work securely off premises.
- **CLAW:** the Cloud Log Aggregation Warehouse assists the National Cybersecurity Protection System (NCPS) in capturing security information as agencies migrate to the cloud. CISA analysts can examine the information and provide situational awareness and support to the agencies.

The Solution

Appgate SDP, an industry-leading Zero Trust Network Access (ZTNA) solution, is purpose-built for today's federal cybersecurity challenges and designed to meet the requirements of TIC 3.0 and CLAW.

Meeting TIC 3.0 and CLAW requirements with Appgate SDP

One key feature of TIC 3.0 is how it divides remote access into different logical zones, representing varying levels of trust, and describes real-world "security patterns" (or use cases); the intersection of these zones and patterns demands a fine-grained access and enforcement policy matrix. This complex, user-driven remote access model is solved with a Zero Trust architecture, controlling access to resources aligned to these security patterns. Appgate SDP delivers on this and integrates disparate systems to make data-driven conditional access decisions.

With DHS's CLAW mandate, the ability to query and take advantage of analytics can be an integral part of the data-driven decision-making process within Appgate SDP. By centralizing all respective logs that an end user took part in generating, a thorough baseline for any User & Entity Behavioral Analytics (UEBA) tool can be established. This baseline, utilized with Appgate SDP extensive APIs that support inbound and outbound calls, can be continuously queried for deviations or anomalies to dynamically update policies based on risk at enterprise scale. This combination is a major leap forward towards modernizing agency security and achieving compliance with the DHS mandates for CLAW and TIC 3.0 and its Zero Trust architecture strategy.

Hybrid workforce

If your agency has a hybrid workforce, you know that your attack surface has been drastically expanded and opportunistic bad actors might be probing for vulnerabilities. If you are prioritizing employee access to the network over stringent security, then you need a security model more effective than traditional legacy secure access. You need to implement the principle of least privilege, which limits worker access strictly to the data and applications essential to their job. Least privilege is a core aspect of Zero Trust security, which assumes no one seeking access is who they say they are without stringent authentication and verification measures.

Appgate SDP offers these capabilities -- and more -- to significantly shrink the attack surface and reduce the vectors for compromise. The need to enforce Zero Trust across the permutations of government-furnished equipment (GFE), third-party contractors, on-premises workers, and employees working from home, is simplified and made more secure with Appgate SDP. As a scalable Zero Trust Network Access (ZTNA) solution, Appgate SDP provides seamless, fast and secure access to only the resources users need and only under pre-configured conditions based on context and risk.

Bring Your Own Device (BYOD) policies

If you want to minimize BYOD policy restrictions, especially for work-from-home employees, but are concerned about compromising security, Appgate SDP has the answer by protecting resources from the assets – remote or otherwise. Employees' personal devices, by definition, operate outside of a professional IT organization and are thus at higher risk when updates, anti-virus signatures, and acceptable use policies might not be applied.

TIC and CLAW create clear federal agency mandates for securing today's technological challenges, specifically regarding remote access and cloud migration. Appgate SDP helps federal agencies meet these mandates, by providing the necessary security: Enabling the required access by natively and seamlessly tying security tools together through continuous device posture checking and robust API integrations. Policies that govern users are automated using risk, context, and data-driven entitlements. As a result, overall risk is reduced, and seamless BYOD policies become increasingly feasible.

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 secure your hybrid workforce and meet the needs of TIC 3.0, CLAW and BYOD, 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