appgate

SUPPORTING THE DEPARTMENT OF DEFENSE ZERO TRUST STRATEGY

Appgate SDP identity-centric Zero Trust Network Access strengthens and simplifies network access controls across global hybrid agency infrastructures

Accelerated Zero Trust implementation at the highest levels

The stakes have never been higher in the fight against malicious threat actors and well-organized nation states seeking to infiltrate the Department of Defense Information Network (DoDIN). In October 2022, the Department of Defense CIO Zero Trust Portfolio Management Office published its DoD Zero Trust Strategy to align with executive-level calls-to-action, including the May 2021 Executive Order on Improving the Nation's Cybersecurity and the January 2022 Federal Zero Trust Architecture Strategy. The impetus for speedy Zero Trust adoption is clearly stated in the DoD strategy document:

> *"Defending DoD networks with high-powered and ever-more sophisticated perimeter defenses is no longer sufficient for achieving cyber resiliency and securing our information enterprise that spans geographic borders, interfaces with external partners, and supports millions of authorized users, many of which now require access to DoD networks outside traditional boundaries, such as work from home. To meet these challenges, the DoD requires an enhanced cybersecurity framework built upon Zero Trust principles that must be adopted across the Department, enterprise-wide, as quickly, as possible ..."*

Appgate SDP: Zero Trust access purpose-built for mission critical networks

Appgate SDP, the first and only Zero Trust Network (ZTNA) solution to achieve Common Criteria Certification, strengthens and simplifies access controls to and across federal agency hybrid infrastructures. With robust enhanced automation and adaptable, diverse deployment options, Appgate SDP hardens overall security postures while minimizing administration duties for IT and security teams with flexible Zero Trust architecture.

- Cloaked infrastructure: Makes your network invisible using single packet authorization (SPA)
- Identity-centric: Evaluates each users' identity, device and contextual risk as criteria for secure access
- Dynamic and continuous: Constantly monitors and modifies access automatically based on changes in context and risk
- Microperimeters: Enforces the principle of least privilege by only granting access to micro-segmented resources
- Programmable and adaptable: 100% API-first technology easily integrates and enhances existing architecture

APPGATE SDP BENEFITS

Authorized DoD Enterprise Software Initiative (ESI) Cybersecurity Blanket Purchase Agreement vendor for cost-effective federal procurement (www.esi.mil)

Supported agency use cases include secure access to SaaS, DevSecOps, GitOps, comply-to-connect, bring your own approved device (BYOAD) and secure hybrid cloud or secure remote access

Simplified, unified resource access for anything; government-furbished equipment (GFE), non-GFE, bring your own approved device (BYOAD) and mobile connecting to on-premises or cloud services

Direct-routed network topology model that supports all protocols (web, non-web, TCP, UDP and ICMP) and connection types

Unburdens existing JRSS/IAP/CAP infrastructure, while enhancing overall user experience

Connects users directly to cloud-hosted or on-premises resources as the enabling Zero Trust Network Access (ZTNA) technology of the DoD CNAP architecture

Appgate is a uniquely qualified, Zero Trust market leader serving the federal sector with designations including:

- Common Criteria Certified
- FIPS 140-2 validated
- DoD Approval to Operate (ATO) in IL5 environments, certified for SC2S [secret IL6]
- Contract vehicles: DoD ESI BPA, GSA Schedule, SEWP, DHS CDM APL

To keep pace with federal mandates and the White House Executive Order, Appgate is tightly aligned with:

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

The power of comprehensive Zero Trust Access and Appgate SDP

CAPABILITY	APPGATE SDP	VPNS AND OTHER ZTNA SOLUTIONS
Mitigate stolen credentials and access tokens	✓ Uses single packet authorization (SPA) to make the enterprise edge undiscoverable to an adversary … even with stolen credentials	✗ VPNs and most ZTNA solutions expose listening ports that will accept compromised credentials or tokens
Simplify security using data-centric concepts like tags and labels (metadata) to create policies; not thousands of IP address-based ACLS	✓ Fully open bi-directional APIs allows use of tags and labels to create security policies dynamically	✗ Not capable of using tags or labels to drive security policy
Standardize access to any on-premises or cloud platform or service	✓ An agnostic solution able to support disconnected operations	✗ VPNs create one tunnel to one location and can't directly connect users to multiple sites
Standardize access across multiple devices and use cases	✓ Supports nearly all operating systems (including mobile) and can be delivered as clientless; supports the entire network stack	✗ Some can't support all DoD use cases and have limited support for all network protocols; e.g. VOiP, ICMP, etc.
Simplify security by enabling "security as code"	✓ Can be completely delivered as code for security policy components and virtual infrastructure (Rest API, YAML, JSON)	✗ Cannot be completely delivered as code
Increase performance and user experience	✓ A single virtual Gateway can support up to 10 Gbps and can be clustered to support 100+ Gbps	✗ Most VPNs cannot scale past 2 Gbps. Other ZTNA solutions are limited to 500 Mbps per appliance creating a large infrastructure footprint
Apply context aware, conditional-based access controls in a Zero Trust model	✓ Policies run within the DoD security boundary, not routed through a cloud-based proxy solution	✗ Cloud-routed secure access solutions are NOT Zero Trust. DoD security policies, configurations, certificates, and encryption do not run within the DoD boundary

About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Learn more at appgate.com.