

ZERO TRUST NETWORK SECURITY PURPOSE-BUILT FOR FEDERAL AGENCY CRITICAL INFRASTRUCTURE

Appgate SDP quickly and comprehensively secures your critical infrastructure no matter where it resides, how your network is configured or what legacy dependencies exist

In the vulnerable world of critical infrastructure, there's critical and then there's **a disaster, waiting-to-happen critical**. Think infected grid sensors that could imperil the lives of millions. Or compromised defense communications in war zones. Or ransomware planted on in-air flight systems.

As federal CISOs strive to protect their agencies' critical infrastructure, they face twin risks:

1. Unprecedented remote access by users and intensely connected, yet scattered, legacy, cloud and IoT environments.
2. Increasingly sophisticated, hostile cyberthreats that, if successful, can result in ruined environments, exposed privileged data, privacy invasion, damaged national defense, devastated finances and even potential lives lost.

"... We're in a state now where our critical infrastructure is much more vulnerable than it should be. And frankly, that's what I worry about most every day."

--Jen Easterly, Director , CISA

Source: Center for Strategic & International Studies

How Appgate SDP Secures Your Critical Infrastructure

Appgate SDP, an industry-leading Zero Trust Network Access (ZTNA) solution, was built to comprehensively protect your critical infrastructure from intrusion, exploitation and exfiltration. Requiring no inbound connections, in just days it can be deployed **as-is** behind your edge firewall to deliver fast, secure and simple connections for your work-from-anywhere users to your distributed, critical infrastructure resources and workloads.

Appgate SDP is flexible and agile Zero Trust security built on five core design principles:

- **Cloaked infrastructure:** uses a sophisticated form of single packet authorization (SPA) to make your network invisible with no exposed ports
- **People-centric:** adapts access based on user, device, application and contextual risk, building a multi-dimensional identity profile before access is granted
- **Dynamic and continuous:** live entitlements that automatically modify access in near real-time based on changes in context and risk, so security risks are automatically blocked
- **Microperimeters:** using patented multi-tunneling technology that microsegments users, workloads and resources providing least privilege access to limit lateral movement inside the network
- **Programmable and adaptable:** extensible 100% API-first technology that enhances and integrates with your tech stack and builds security directly into the fabric of business processes and workflows



Appgate SDP Features and Benefits:

1. **Any environment:** can be deployed wherever resources need to be secured, delivered as self-managed or as-a-service, in any environment: hybrid or multi-cloud, containerized environments, on-premises or virtualized ... and it supports legacy networks and infrastructure
2. **Centralized policies:** unified policy engine simplifies configuration and management, administering policies for all devices, all IT, all network configurations, and employees, vendors, partners and other third parties
3. **Onboarding:** offers multiple options for easy, secure onboarding and a seamless user experience
4. **Automated access:** programmable and extensible capabilities enable highly automated just-in-time policies; environmental metadata and APIs automate access with Appgate SDP to enable security-as-code and mature DevOps practices

"We could do things other ways, but it would be harder and more expensive compared to what Appgate delivers out of the box."

-CIO, Government Systems Integrator

Source: Nemertes Real Economic Value report

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
- Federal contract vehicles: GSA Schedule, SEWP, DHS CDM APL

In order to keep pace with federal mandates and the WHEO, 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 is purpose-built to secure the government's most critical infrastructure, 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.