



SOFTWARE-DEFINED PERIMETER

AppGate SDP by Cyxtera

Adaptive, Identity-Centric Security for Hybrid IT

WHY ADAPTIVE, IDENTITY-CENTRIC SECURITY IS NEEDED

In the new world of consistent and pervasive internal and external threats, distributed organizations and global ecosystems, it's become clear that the network perimeter has dissolved. Today's IT is software-defined, distributed, and interconnected.

Traditional network security isn't designed for today's IT reality. We need to move from perimeter-centric, firewall, VLAN and IP-focused security to a model that focuses on securing the entire path from user to application, user to server and server to server, on a one-to-one basis. Traditional security tools like VPNs, firewalls, and NAC enable users to connect first and authenticate second, the equivalent of letting a stranger into your house to snoop around before knowing who they are.

AppGate SDP is a new approach to security. It secures the network with a Software-Defined Perimeter – a network security model that dynamically creates one-to-one network connections between the user and the resources they access.

Everything else is invisible, including the system itself.

WHAT IS APPGATE SDP?

AppGate SDP is a Software-Defined Perimeter solution that is:

- Designed around the individual: authentication and authorization are based on the person, environment and infrastructure. It's context-aware, dynamically adapting access based on environmental, infrastructure or organizational changes.
- Built for the cloud: it's distributed and stateless, built for hyper scale, with a microservices architecture.



Features

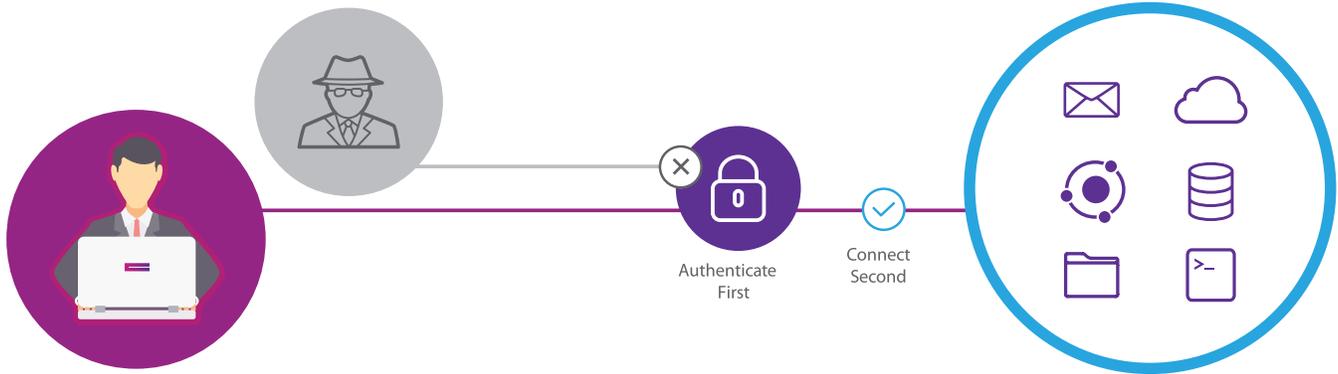
- Access based on context sensitive identity
- Secure, encrypted connection between user and approved system
- Makes entire network completely invisible
- Eliminates lateral movement on internal networks
- Built like cloud – massively scalable, distributed & resilient

"By 2021, 60% of enterprises will phase-out network VPNs for digital business communication in favor of software-defined perimeters"
- GARTNER



ZERO TRUST. AUTHENTICATE, THEN CONNECT

Based on the zero trust model: AppGate takes an “authenticate first, connect second” approach, ensuring that only authorized users can connect over an encrypted connection to network resources. This reduces the attack surface and significantly improves security.



WHY DEPLOY APPGATE SDP?

Secure high-risk users and assets



- Crown jewels
- Third-party access
- Privileged user access

Secure and compliant cloud deployments



- Extend to AWS and Azure
- Manage users, not IP addresses
- Improved compliance reporting

Eliminate complex corporate firewalls and VPNs



- Simplify management
- Reduce firewall rules
- Eliminate NACs, VPNs, Firewalls



For more information regarding SageNet’s AppGate SDP by Cyxtera, call 1-866-480-2263 or visit www.sagenet.com/cyber.

AppGate_DS090218

Tulsa | Washington, D.C. | Atlanta | Chicago | Philadelphia
866.480.2263 | www.sagenet.com/cyber