APPGATE

Bridging the Gap: Consistent Secure Access for On-Premises and Cloud

AppGate SDP delivers the industry's most comprehensive Software-Defined Perimeter solution, offering secure access regardless of infrastructure or migration destination.

As enterprise organizations adopt cloud, there are decisions made on what needs to stay on-premises and what can move. These hybrid environments are often architected differently and support many different use cases and legacy applications. In this hybrid world, the perimeter can be anywhere and needs to be consistently secured everywhere. Organizations undertaking cloud migration need to consider how they'll deliver consistent, secure access across all their environments.

Traditional perimeter-based security solutions such as VPNs, next-gen firewalls, and NACs are ineffective at securing distributed, hybrid IT infrastructure. There are multiple ways people are managing polices and permissions for cloud vs. on-premises workloads. It's complicated, difficult, expensive, and dangerous.

APPGATE SDP: SECURE ANY APPLICATION, ON ANY PLATFORM, ANYWHERE

AppGate SDP is a powerful network security platform capable of securing any application, on any platform, in any location. While many Software-Defined Perimeter solutions are built primarily to secure web and cloud-based applications, AppGate SDP is purpose-built for hybrid environments.

AppGate SDP dynamically controls access across hybrid networks based on identity-centric policies. It works by creating one-to-one connections between users and the network they need to access – a segment of one. AppGate SDP is resilient and massively scalable to support enterprise-grade, mission-critical, and global environments.

BENEFITS

- Consistent access control across cloud-native and hybrid environments
- Built like the cloud—massively scalable, distributed, and resilient
- Better network security than legacy VPNs, NACs, and firewalls
- Remote and third-party access is identity and context sensitive
- Unauthorized resources are completely invisible
- Secure, encrypted connection between

LIVE ENTITLEMENTS: DYNAMIC, CONTEXT-SENSITIVE ACCESS POLICES

AppGate SDP replaces static Access rules with Live Entitlements – dynamic, context-sensitive access policies. Live Entitlements dynamically change security based on what users are doing, where, and when. This fine-grained Access control for cloud and on-premises ensures individual users access only what they need to do their jobs. It delivers consistent, automated security and removes the human error factor.

FINE-GRAINED, INDIVIDUALIZED NETWORK ACCESS

AppGate SDP uses a real-time understanding of policy to créate individualized perimeters for each user. It ensures that all endpoints attempting to access a given infrastructure are authenticated and authorized prior to being able to access any resources. Once authorized, AppGate SDP creates an encrypted tunnel – a 'segment of one' – allowing traffic to flow only from the user device to the protected resource.

PROTECTS END-USER DEVICES FROM UNAUTHORIZED ACCESS

AppGate SDP's Ringfence™ feature isolates and protects both the protected resource and the user device from all inbound connections by securing the latter from inbound connections. Access to internal resources can be granted without concern about malicious users on the local network. Local outbound traffic (DNS, etc.) is untouched.

SAFE FROM PRYING EYES

Single-Packet Authorization technology cloaks infrastructure so that only verified users can communicate with the system. It is invisible to port scans and cryptographically hashed as a further defense. Gateways and controllers are completely cloaked so they cannot be probed, scanned, or attacked. This significantly reduces the network attack surface by preventing network reconnaissance and limiting lateral movement.

ENTERPRISE-GRADE, CLOUD NATIVE, CLOUD SCALE

AppGate SDP is engineered to opérate natively in cloud networks, with a completely decentralized, distributed, stateless network architecture. Native integration with cloud-specific security features secures public cloud work-loads and provides consistent access controls across hybrid environments at scale. Users can leverage patented multi-tunnel capabilities to seamlessly connect users to applications - wherever they run.