APPGATE®

Reduce Over-Privileged Risk with AppGate SDP

AppGate SDP enforces least-privilege network access in real time: any user, any device, from anywhere, to any application on any platform.

Over-privileged, remote and third-party users need access to your critical systems. But VPN technology simply doesn't work. It treats allusers the same: an IP address allowed to connect to your network – or not. This all or nothing approach results in over-privileged users and heightened risk of a data breach. Consequences can be far reaching – data breaches, stolen intellectual property, financial loses or fines. And most companies never fullyrecover from catastrophic data breaches – apart from the regulatory fines and financial impact, the organization's reputation in the free market is almost unrepairable.

AppGate SDP, a secure access solution, implements the zero-trust principles of software defined perimeter providing a unified, enterprisegrade solution to protect against over-privileged or super users. AppGate SDP creates encrypted, one-to-one connections between users and resources and dynamically enforces identity centric access policies at the network level. Policies dynamically adapt to changes in the environment; granting access to server instances based on a combination of user attributes, server metadata, and overall system context.

LIVE ENTITLEMENTS: DYNAMIC, CONTEXT

Privileged users are dynamic – they need to work anywhere at any time. 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 ensures individual users access only what they need to do their jobs. Benefit from consistent, automated security and remove the human error factor.

FINE-GRAINED, INDIVIDUALIZED NETWORK ACCESS

Traditional network security like VPNs or firewalls connect various roles or groups to a network segment and then rely on application level permissions for authorization. AppGate SDP is fundamentally different. It uses a real-time understanding of policy to create individualized perimeters for each user. 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.

BENEFITS

- Unauthorized resources are completely invisible
- Connections are secure, encrypted 1:1 between user and resource
- Built like the cloud—massively scalable, distributed & resilient
- Consistent access control across cloud native and hybrid environments
- Better network security than legacy VPNs, NACs and firewalls
- Remote and third-party access is identity and context sensitive
- Eliminates lateral movements on the network

COMPLETELY CLOAKED FROM PRYING EYES

Single-Packet Authorization technology cloaks infrastructure so that only verified users can communicate with the system. This significantly reduces the network attack surface by preventing network reconnaissance and limiting lateral movement on the network.

HOW IT WORKS

A Software-Defined Perimeter (SDP) architecture is made up of three primary components: a client, controller and gateway. The controller is where the brains of the system resides, acting

as a trust broker for the system. The Controller checks context and grants entitlements. The controller and gateway are completely cloaked.

1. Using Single-Packet Authorization (SPA), Client device makes access request to and authenticates to the Controller. Controller evaluates credentials, and applies access policies based on the user, environment and infrastructure.
2. Controller checks context, passes live entitlement to Client. The Controller returns a cryptographically signed token back to the Client, which contains the authorized set of network resources.
3. Using SPA, Client uploads live entitlement, which the Gateway uses to discover applications matching the user's context. When the user attempts to access a resource – for example by opening a web page on a protected server – the network driver forwards the token to the appropriate. cloaked Gateway. The Gateway then applies additional policies in real time – network location, device attributes, time of day and more. It may permit or deny access, or require an additional action from the user, such as prompting for a one-time password.
4. A dynamic Segment of One network is built for this session. Once granted, all access to the resource travels from the Client across a secure, encrypted network tunnel, and through the Gateway to the server. Access is logged through the LogServer, ensuring there's a permanent, auditable record of user access.
5. Controller continuously monitors for any context changes, adapts Segment of One accordingly.