SECURING CLOUD ACCESS

Zero Trust Network Access access to, from and between any cloud architecture

Cloud Adoption Escalates Digital Transformation

For every industry, the cloud and cloud-native adoption ushers in workload scale, performance and agility and accelerates digital transformation. Organizations use the cloud for infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Embracing these popular services, along with heterogeneous environments like public and private cloud and multi-cloud architectures, present different challenges when it comes to securing connections to, from and between users and workloads.

Cloud Security Challenges

- **Outdated network security tools:** Perimeter-based VPNs, next-gen firewalls and NACs are difficult to administer and can't secure distributed, hybrid infrastructure due to their "default allow" access approach that weakens overall security posture.
- **Fragmented security architecture:** Maintaining policies with traditional access solutions across hybrid infrastructures is hard without a centralized console that can seamlessly apply rules across all endpoints and workloads.
- **Broader attack surface:** Distributed workloads located in multiple heterogeneous environments make it easier for malicious actors to infiltrate corporate networks.
- **DevOps vulnerabilities:** The potential to introduce vulnerabilities and cyber risk goes up as development teams are pressured to quicken the pace of software releases.
- **Limited visibility and control:** A lack of a single pane-of-glass policy view across user, endpoints and workloads makes it difficult for IT and security teams to discern a true security posture.

ZERO TRUST ACCESS FOR CLOUD:
SECURITY AND OPERATIONAL BENEFITS

Zero Trust secure cloud access for users and workloads

Unified policy model to, from and between users, devices, workloads and microservices

Reduce attack surface and administrative complexity

Improve business agility and user experience

The Solution: Secure Zero Trust Access for Cloud

Cloud deployments are about speed and agility, so complicated security controls that impede users and developers are antithetical to cloud benefits. Organizations with a robust cloud strategy need a Zero Trust secure access platform with a single policy framework to dynamically protect people and workloads, while keeping pace with cloud agility.

The Power of Appgate SDP

Appgate SDP, an industry-leading Zero Trust Network Access (ZTNA) solution, streamlines secure user-to-workload and workload-to-workload access within a single system and unified policy model.

Unified Platform

Build a Zero Trust café-style network and apply least privilege access to, from, and between users, devices, workloads and microservices. Acting as a network overlay and integrating with existing identity tools, security and business systems, Appgate SDP architecture supports a heterogeneous network and delivers a unified policy model across your entire IT ecosystem.

Any Cloud

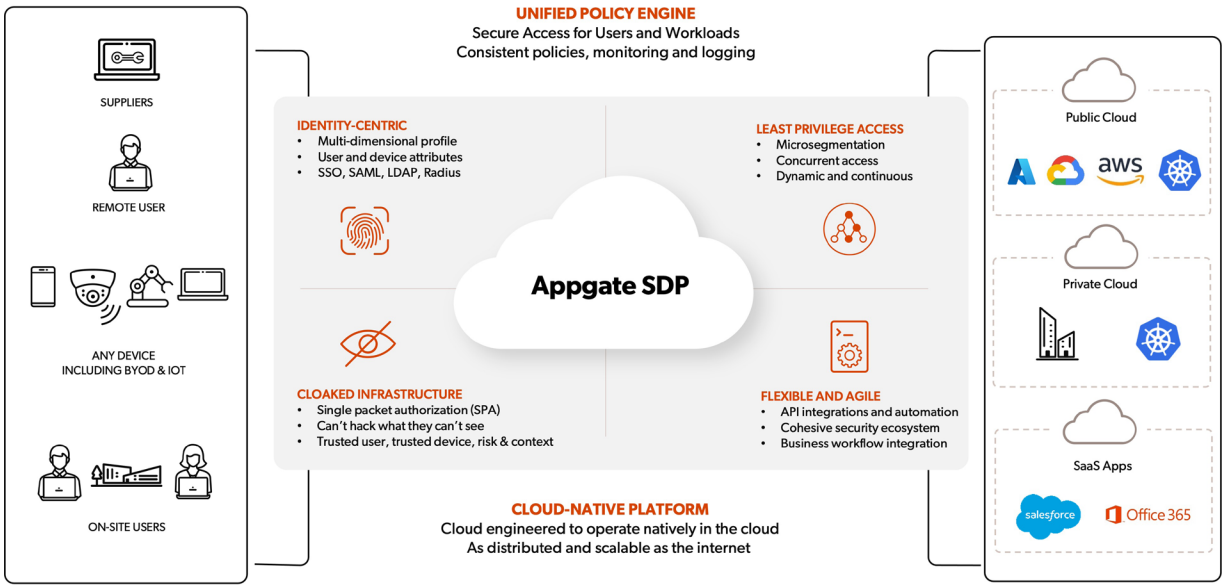
Appgate SDP is proven to provide secure dynamic Zero Trust access to solve complex hybrid enterprise security problems. It secures all types of cloud workloads, as well as cloud-native microservices by enforcing granular, secure access to and from Kubernetes environments and building security into CI/CD pipelines.

Logs

Appgate SDP collects a rich set of detailed logs that provides the who, what, when and where behind every access request and session. This data can be presented using Kibana and a built-in ELK stack or be fed to a SIEM to enrich SOC and incident investigation and response. These logs also support compliance efforts and reduce audit scope.

Flexible and Agile

The API-first, extensible and programmable capabilities of Appgate SDP integrate with technology stacks so you can build security directly into business processes and workflows. It also has built-in scripting to extend functionality and adapt to future or unforeseen security challenges. This powerful combination supports secure access-as-code deployments and matures DevSecOps practices.



Business Outcomes

Appgate SDP delivers industry-leading Zero Trust access to anything from anywhere by anyone. Gain better security for your users, devices, resources and containers with continuous risk and context verification before and during each access session. And reduce your organization's attack surface by cloaking your infrastructure, microsegmenting resources and granting least privilege access to only explicitly approved sessions.

SECURE ACCESS FOR USERS	SECURE ACCESS FOR WORKLOADS
Secures authorized employees and third parties accessing resources using any device to workloads, regardless of location.	Secures workloads and microservices running in a public or private cloud with secure granular resource-to-resource or resource-to-component connections.
Least privilege access: Provide access to resources, not the network, to limit risk, minimize attack surface and improve the user experience. **Better user experience:** Deliver a secure, consistent, and seamless user experience from wherever they are, on any device to the resources they need. **Reduced complexity:** Dynamically allow secure remote access when moving or adding cloud resources. **Protect against credential compromise:** Verify your users' identities with multi-factor authentication (MFA) and single packet authorization (SPA). **Gain visibility into applications access activities:** Get visibility into access activity across all locations, devices and users. Control cloud application access and prevent malicious connections. **Enforce device compliance:** Identify risky devices, enforce contextual access policies and ensure device health directly or by integrating with device management tools. **Concurrent connections:** Patented multi-tunnel technology delivers fast, secure and concurrent connections from any user to multiple cloud locations.	**Least privilege access:** Applied to, from and between workloads and services to reduce unsanctioned lateral movement between resources. **Simplified security stack:** Automatically deploy, configure cloud-to-cloud and cloud-to-datacenter connectivity without overhead and cost of managing transit gateways, virtual firewalls and VPNs. **Segment applications:** Enforce least privilege access to minimize lateral movement for any cloud and on-premises environment. **Real-time security built on identity and context:** Controls, such as service certificates, iidentify what workloads can access what, based on business-level policies. Metadata attributes like tags, location and role also feed policy decisions. **Remediate threats quickly:** Dynamically contain threats, reduce splash damage by quarantining workloads or servers that display anomalous processes and behaviors. **Detailed logs:** Correlate connections with matching policy and service attributes to support compliance and reduce audit scope. **Software-driven approach:** Runs on the OS and/or at the container level to secure connections between clouds and resources.

Appgate SDP in Action

Zero Trust for cloud protects all users, resources and environments with a unified policy model so you can rapidly and confidently secure access to, from and between cloud environments. The proven benefits of Appgate SDP can be applied to a variety of scenarios:

1. **Cloud-native workloads:** Automate and easily secure Kubernetes workloads at scale using metadata to provide just-in-time fine-grained access to and from containers
2. **Cloud migration:** Maintain a single set of security policies—before, during and after the migration— ensuring a smooth transition while maintaining security throughout the process
3. **Multi-cloud user access:** Enable employee and third-party access to cloud systems from any device, anywhere, secured by granular control per workload or resource
4. **DevOps:** Provide secure, seamless and direct access to multiple cloud accounts simultaneously to improve the speed and productivity of developer teams
5. **Traditional cloud workloads:** Proactively interrogate the environment for changes to dynamically grant, restrict or limit access to critical services and prevent lateral movement
6. **Secure Access-as-Code:** Build security based on Zero Trust principles into your CI/CD pipeline for DevSecOps to deploy and configure access as code

"Appgate SDP is one of the few security tools that both developers and security teams get benefits from and enjoy using. It's not often you roll out a new security tool and people love it while at the same time making your environment much more secure."
— Ben Collen, Director, IT and security, Vertex

Appgate SDP has a proven track record in providing secure dynamic Zero Trust access to solve complex enterprise security problems. It delivers Zero Trust user-to-resource and resource-to-resource access for traditional and cloud-native workloads, regardless of location. Learn More

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. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at appgate.com

appgate