appgate

SECURE ZERO TRUST NETWORK ACCESS FOR AZURE PUBLIC CLOUDS

Many organizations presume security and compliance responsibilities rest solely with their cloud service providers. Yet, security in IaaS environments is a shared responsibility. Microsoft says, "For IaaS solutions, the elements such as buildings, server, networking hardware and the hypervisor should be managed by the platform vendor. The customer is responsible or has a shared responsibility for securing and managing the operating system, network configuration, applications, identity, clients and data."

Security is a Shared Responsibility

Customers are responsible for their portion of Azure security, in particular for three areas:

1. Azure's native security model is based on Active Directory (AD) supported by Role-Based Access Control (RBAC). This is used to authenticate users into any IaaS instances in Azure. The drawback is that using only Azure Active Directory, authentication happens only at login and doesn't provide network level security.
2. While configurable, Microsoft only offers a static assignment of user to role. When considering the dynamic nature of cloud environments, this is problematic.
3. Traditional security tools like VPNs, firewalls and NACs are not well-suited to controlling user access to the Azure environment because:
   - Azure is located outside the company perimeter and may be accessible without user being present on the corporate network
   - Cloud environments are highly dynamic, with server instances being created and terminated on an ongoing basis. Traditional security tools cannot keep up with these ever-changing environments and typically result in users being granted access to all services running on all instances within the cloud environment, which creates security and compliance risks

APPGATE SDP BENEFITS:

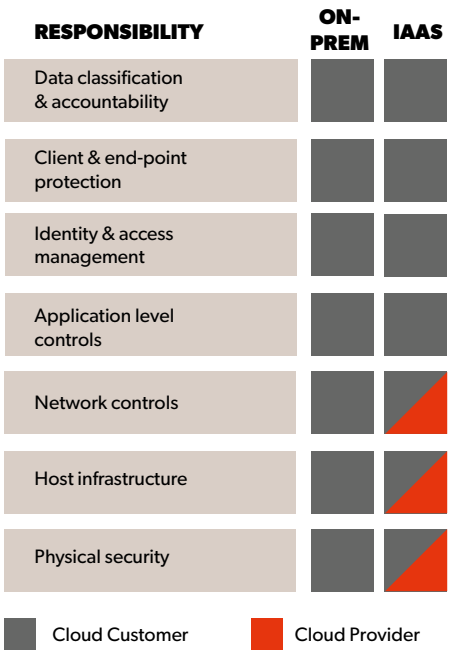
Access based on identity

Secure, encrypted connection between user and approved Azure workloads

Makes the Azure environment completely invisible

Perfect for DevOps – easy to deploy and adapts to added or removed instances in real-time

Built like the cloud and for the cloud – massively scalable, distributed and resilient

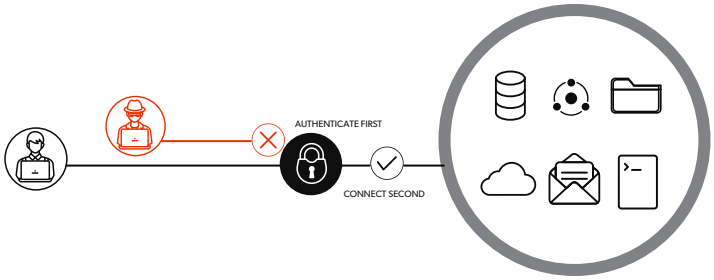


Adaptive, Identity-Centric Security Is Needed

Appgate SDP dynamically creates a secure, encrypted network segment of one that's tailored to each user session. It simplifies the cloud resource user access problem and eliminates over-entitled network access. In Azure environments, Appgate SDP:

- Integrates with AD to provide initial user authentication and assignment of access rights. It attaches conditions to these rights, so that at the time of actual access, claims are checked again to ensure the user still complies with the security policy.
- Provides an identity-centric VPN service with simultaneous connections directly from the device to any number of sites. Each Gateway is built to accept many thousands of secure Client (TLS) connections simultaneously and can be clustered for high availability and scale.
- Allocates policies (roles) to users based on rules that include any number of dynamically measured claims. Appgate SDP sets access rights based on current status

Appgate SDP architecture is distributed, highly resilient and massively scalable. It allows enterprises to implement a global, secure access system in any hybrid environment with greater control and improved economics.



How Appgate SDP Works With Azure

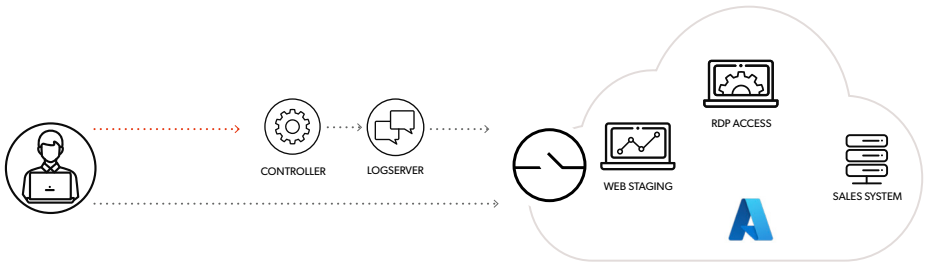
Client devices authenticate to the Controller, which evaluates credentials and applies access policies (based the person, environment and infrastructure). The Controller returns a cryptographically signed token back to the Client, which contains the authorized set of network resources.

For example, when the user attempts to access a resource by opening a web page on a protected server, the network driver forwards the token to the appropriate cloaked Gateway, which then applies additional policies in real time to control access based on network location, device attributes or time of day. The Gateway may permit access, deny access or require an additional action from the user, such as prompting for a one-time password.

Once granted, all access to the resource travels from the Client across a secure, encrypted network tunnel and through the Gateway to the cloud infrastructure.

Access is logged through the LogServer, ensuring that there's a permanent, auditable record of user access. Appgate SDP also feeds alerts into a SIEM or IDS for analysis and response. Appgate SDP supports all major operating systems (desktop and mobile) and all major cloud and virtualization platforms.

Appgate SDP delivers fine-grained access control, adjusting automatically based on changes in context while hiding all Azure resources.



What is Appgate SDP?

Appgate SDP is an industry-leading Zero Trust Network Access solution that dynamically creates one-to-one network connections between the user and the instances and services they access. Appgate SDP for Azure is:

- **Designed around the individual:** Authentication is based on the person, environment and infrastructure. It's context-aware, dynamically adapting policy based on environmental, infrastructure or organizational changes.
- **Built for the cloud:** It's distributed and stateless, built for hyper scale, via a microservices architecture and API-driven entitlements.
- **Based on the Zero Trust model**: It takes an "authenticate first, connect second" approach, ensuring that only authorized users can connect over an encrypted connection to cloud instances and resources. This reduces the attack surface and significantly improves security.

Appgate SDP delivers fine-grained access control by dynamically creating a network segment of one that's tailored to each user session. It adjusts access automatically based on changes in context while hiding all network resources, except those that the user is authorized to see. By making the rest of the network invisible, enterprises can simplify their security infrastructure, while granting access with confidence.

Appgate SDP policies make access decisions based on attributes from the person – user, device, anti-virus, department, group membership, app permissions; the environment – location, time, security posture; and the infrastructure – network analytics, security groups, tags, hostnames. It's dynamic and scriptable and encrypts one-to-one connections between the user and application or service.

Superior integrations with SIEM and IDS systems build bridges among security tools. The result is improved security and more efficient compliance reporting.

Built like the cloud

- Hyper-scalable
- Decentralized and distributed
- Resilient and highly available

Adaptative & individualized

- Simple user experience
- Policy-based network access
- Dynamic segment of one

Hidden from prying eyes

- Unauthorized resources are invisible
- Cloaked gateways and controllers protect system itself
- End-to-end encrypted connections

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