SECURE ZERO TRUST ACCESS FOR CORPORATE NETWORKS

Today, security professionals need an architecture that protects assets wherever they are by securing authorized user access from wherever they are.

Introduction

Most organizations use a mix of products to secure user access and face challenges aligning remote versus on-premises user requirements. At the same time, as workloads migrate to the cloud, decisions must be made regarding how to secure both cloud and on-premises resources.

Challenges

Hybrid environments include corporate, campus or branch networks that typically require different architectures, resulting in complicated administration across multiple policy engines, incompatible management consoles with limited integration and delayed response when incidents arise. And users have varied connection experiences between working remotely and in an office.

To provide secure access for all users and resources, including the corporate network, security professionals need a singular agile and scalable solution that:

- Provides least privilege access
- Reduces complexity
- Secures all workloads, including containers
- Supports comprehensive monitoring

Solution

Most organizations employ a hybrid infrastructure: a complex mix of multi-cloud, data centers and corporate or campus networks, plus IoT/OT devices, that supports on-premises and remote workforces. Adopting a robust Zero Trust Network Access (ZTNA) solution that features unified security policy management improves your security posture and user satisfaction. The result is increased operational efficiency.

Appgate SDP, an industry-leading ZTNA solution, was built to go beyond safeguarding remote and cloud access to secure the complete corporate network, including on-premises users, resources, IoT and other network enabled devices.

APPGATE SDP BENEFITS

SUPPORT A HYBRID WORKFORCE

Consistent policy enforcement for users located anywhere in the enterprise

SIMPLIFY POLICY THROUGHOUT THE ENTERPRISE

Any mix of on-premises, cloud or hybrid workloads are protected

IMPROVE USER EXPERIENCE

Users securely access all resources in the same manner regardless of location, boosting productivity

REDUCE ADMINISTRATIVE COMPLEXITY

A unified security policy model for all connections–remote, on-premises and IoT–with one solution

INCREASE OPERATIONAL EFFICIENCY

Replace or reduce reliance on traditional controls like firewalls, VPNs and NAC

> ***"When we saw the Appgate SDP demo, we were very surprised at what it could do. The least privilege access and entitlements were exactly what we needed, and the SPA feature caught our attention because it provided an extra level of security. It was easy to set up, and Appgate was there to help. The leadership team and users praised how seamless it is to use."***
>
> ***- Damian Zavala, lead systems engineer, Jellyvision***

Appgate SDP secures access for the hybrid enterprise

Hybrid workforce. Dynamic, unified policies are consistently enforced for local, remote and third-party users.

Local devices. LAN devices, including IT and IoT devices such as IP-based printers, VoIP phones, physical access control systems, IP-based cameras and surveillance systems, can all be secured with one ZTNA solution.

Corporate network resources. Secure workloads wherever they are, on the corporate or campus network, in the data center or in the cloud. Appgate SDP protects your entire portfolio of resources, from legacy apps to modern containers under one unified, enterprise-wide security policy model.

Heterogenous networks. Appgate SDP can secure access to any of your networks: local, campus-wide, at a branch office, or any other LAN/WAN combination, your security policies are uniformly enforced.

Cloud, multi-cloud, and hybrid cloud. Seamless security policies applicable to all cloud providers ensure that privileges are enforced regardless of where the resource is hosted.

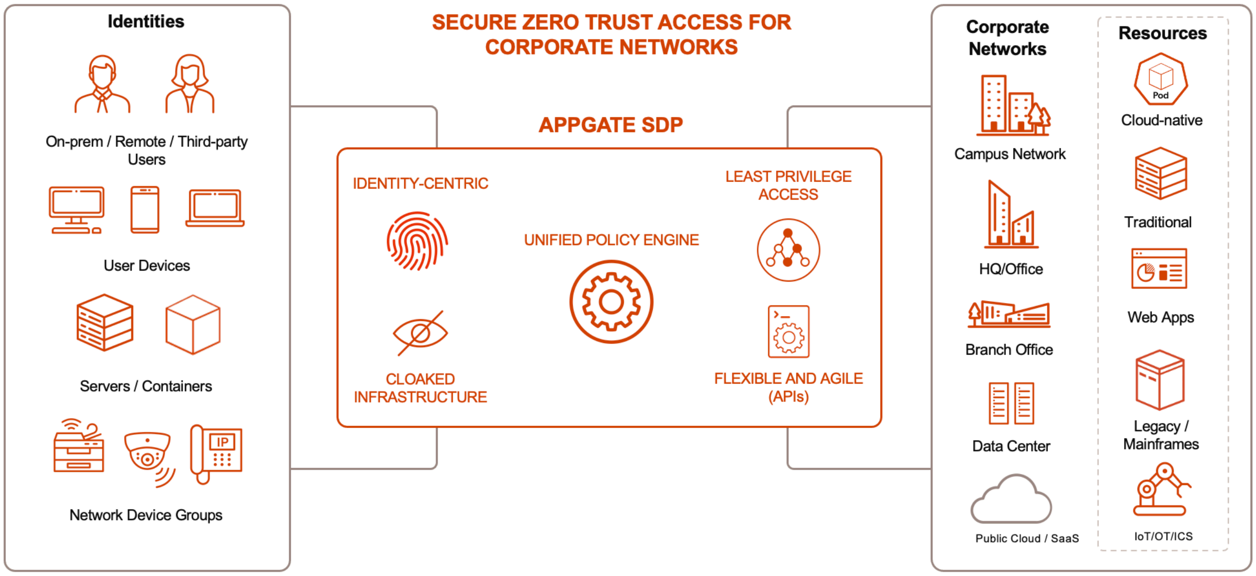
Benefits of adopting Appgate SDP for the hybrid enterprise

Fine-grained access. While traditional security solutions “connect first and validate later,” Appgate SDP enforces access at the service or network level, which counters the risk of lateral movement by cybercriminals or malware across the hybrid enterprise.

Improved user and admin experience. By reducing the number of tools needed, you can improve the user experience and reduce administrative complexity with a unified policy engine that controls access no matter where the connection originates. Appgate SDP can act as the policy decision point, ensuring consistent, dynamic policy enforcement and management for all users connecting to all resources. This solution is far less complicated than administering policies on multiple firewalls and legacy systems such as Network Access Control (NAC) and VPNs.

Reduced friction between security and network teams. These equally important teams share responsibility for addressing the necessary processes for returning to the office or campus. The networking team must provide connectivity for any scenario, while the security team can overlay a robust, API-driven ZTNA solution that delivers least privilege access without interfering with the network. This simplifies the ecosystem and creates a hardened security posture across the board.

Simplified network device and IoT security. Users and their devices aren’t the only network connections; IoT, OT and SCADA/ICS devices are connecting to network resources as well. With Appgate SDP all connections are managed under a unified policy framework, so you don’t need to manage multiple consoles for different devices connecting to your network.



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. Learn more at appgate.com