UNIVERSAL ZERO TRUST NETWORK ACCESS OVERVIEW

Introduction

Universal Zero Trust Network Access (ZTNA) ensures the consistent application of Zero Trust principles for all users regardless of their device or location—whether on-campus or remote—through a unified policy model. The adoption of universal ZTNA simplifies secure access management by consolidating and replacing traditional technologies such as VPNs, MPLS and NAC across diverse network infrastructures and environments. This enables organizations to maintain network security without introducing complexity for end users and realize administrative efficiencies while reducing operational and capital expenditures.

Appgate SDP Universal ZTNA

Appgate SDP dynamically creates individualized, secure connections between users and resources based on verified identity and context. Utilizing a direct-routed architecture, the solution provides optimal performance, minimal latency and centralized access controls for all user-to-resource and resource-to-resource connections. This approach provides organizations with the versatility and control required to secure diverse environments spanning remote and on-premises locations, multi-cloud scenarios and legacy infrastructures.

Appgate SDP leverages multi-layer authorization to provide context-aware control over all user access attempts:

- **Single Packet Authorization (SPA):** This layer cloaks the infrastructure and ensures complete invisibility with no exposed ports, enabling communication channel access only to users that are cryptographically validated with a single packet.
- **Multi-Factor Authentication (MFA) at Sign-In:** Registering a user's device serves as a second authentication factor, enhancing security by blocking unauthorized access attempts with stolen credentials.
- **Authentication:** This layer validates user and device credentials against defined trusted sources such as SAML and OIDC.
- **Authorization:** Policy assignment criteria evaluates user/device attributes, enabling a specific set of entitlements to be assigned to each user/device.
- **Access Controls:** This layer compares user traffic to entitlements, enforces access policy, verifies conditions for access and prompts user for action (e.g., MFA) when required. Appgate SDP dynamically manages the access for each user/device based on the host, port and protocol of the protected resource defined in entitlements.
- **Alert Actions:** This layer acts as a triggering system that blocks and logs with an alert for high-risk behaviors, such as unauthorized port scans, to proactively address potential threats.

USE CASES

- Full VPN replacement
- Third-party access
- Transition traffic off MPLS to the internet
- Eliminate software-defined wide area network (SD-WAN)
- Network access control (NAC) replacement
- Branch connectivity to corporate resources

CRITICAL CAPABILITIES

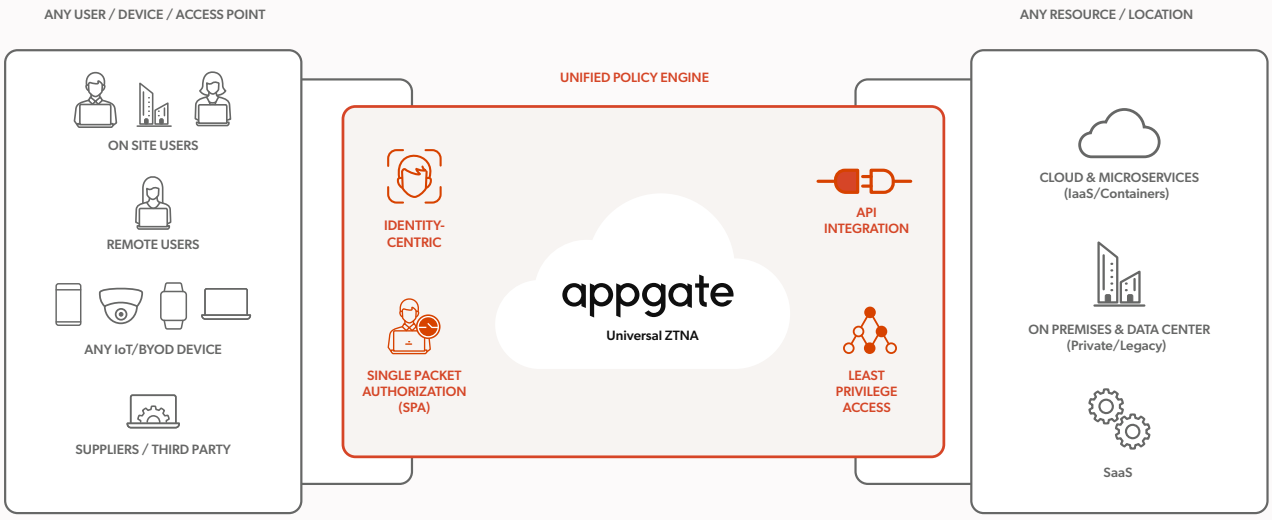
Identity-centric security: Guaranteeing that only authorized and authenticated entities can access specified network resources

Application layer access control: Ensuring users have the minimum necessary access required to perform their task

Dynamic access policies: Granting access based on the specific context of the user and device

Adaptive authentication: Responding to changes in user behavior or contextual factors to ensure access privileges are appropriate for the current security posture

Scalability and high performance: Dynamic scalability to accommodate a growing number of users and devices, while maintaining optimal performance



Appgate SDP delivers a unified policy engine to support universal ZTNA for all users, resources including legacy and custom apps, and locations across hybrid IT, multi-cloud, HQ, branch offices and data centers.

How It Works

Appgate SDP has three essential components that facilitate secure, dynamic access to authorized resources:

Controller:

- Acts as a trust broker and policy decision point
- Authenticates users, checks context, and generates live entitlement tokens
- Sends digitally signed tokens to the Client

Gateway:

- Functions as the policy enforcement point
- Validates entitlement tokens from the Client and establishes a dynamic session-specific micro firewall network for accessing protected resources

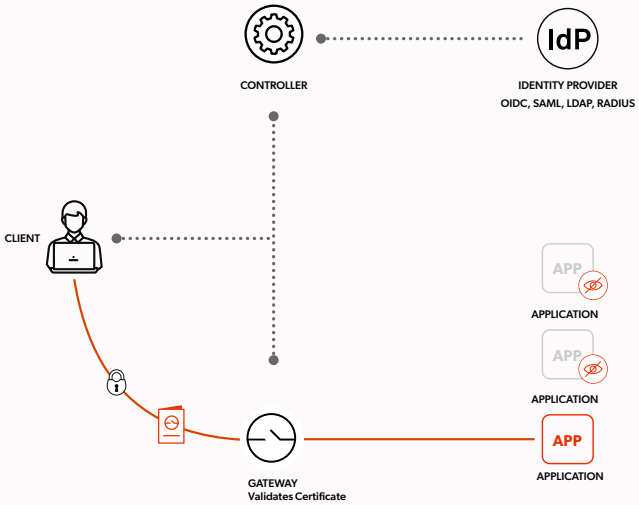
Client:

- Connects users/devices to authorized resources
- Sends SPA entitlement token to Controller and Gateway to initiate communication
- Requests access from the Controller and sends the entitlement token to the Gateway for validation

The Client makes an access request to the SPA-cloaked Controller. The Controller validates the SPA packet, authenticates the user, checks the context, generates a live entitlement token, and sends it to the Client.

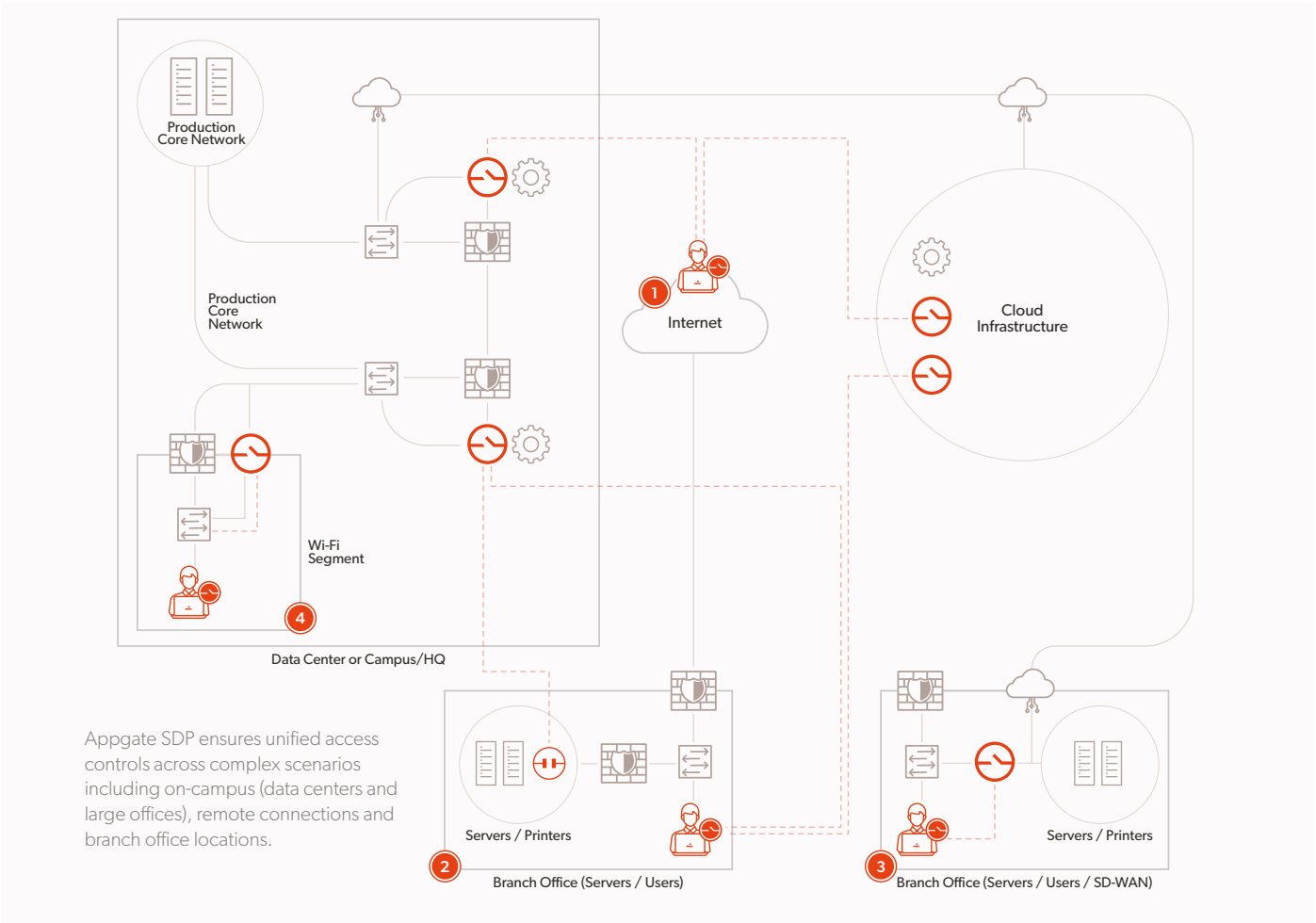
Using SPA, the Client sends the entitlement to the Gateway and when validated, establishes a dynamic session-based micro firewall network for access to the protected resource. Appgate SDP continuously monitors the system, adapting or revoking access in response to changes in context.

The LogForwarder distributes authentication, authorization, access and blocked events to security information and event management (SIEM) tools for correlation and centralized management of events. Appgate SDP can be cloud-hosted, self-hosted or isolated to meet diverse security and compliance needs across varied network topologies.



Appgate SDP has three key components: the Controller, acting as a trust broker and policy decision points; the Gateway, functioning as the policy enforcement point; and the Client, connecting users to authorized resources.

Sample Appgate SDP Enterprise Architecture for Universal ZTNA



There are four scenarios in the above image that include: (1) an on-campus user connected to a Wi-Fi segment; (2) a remotely connected internet user; (3) a non-WAN connected branch office with users and devices (i.e.. servers, IoT devices, printers, etc.); and (4) a WAN/SD-WAN-connected branch office with a combination of similar devices. With Appgate SDP, dynamic access controls can be uniformly applied consistently across each scenario. Users are free to move between different office locations and environments, while maintaining a consistent user experience that requires no operational changes.

Appgate SDP seamlessly integrates with existing security controls and components. For example in scenario (4) above, the traffic from a branch office will be enforced by the existing SD-WAN quality of service (i.e., filter traffic, performance enhancements, etc.) and security policies without negatively impacting performance. In scenario (3), SD-WAN has been eliminated from this branch and replaced by Appgate SDP for branch to data center connectivity. The user in this scenario has direct access to data center resources and cloud resources without impacting bandwidth on either side, bypassing any potential hairpinning through Appgate SDP's direct-routed ZTNA architecture.

Appgate SDP Universal ZTNA Benefits

1. **Unified access for all users and devices:** Eliminate the friction of managing multiple solutions; achieve consistent and uniform access controls for all users and devices.
2. **Adaptive and scalable security:** Dynamically adapt access policies to accommodate diverse users and devices, ensure suitability for a wide range of use cases and security requirements.
3. **Increased productivity:** Reduce trouble tickets and expedite access to resources for authorized users for a more agile and productive environment.
4. **Simplified compliance:** Apply consistent access controls to reduce the reporting scope and ensure compliance with industry regulations.
5. **Cost efficiency and return on investment (ROI):** Enhance operational efficiency and achieve a significant ROI by consolidating multiple access control tools.

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

appgate