APPGATE SDP
UNIVERSAL ZERO TRUST NETWORK ACCESS (ZTNA)

Solution Overview

Appgate SDP is an industry leading universal Zero Trust Network Access (ZTNA) solution that addresses the security challenges of modern distributed workforces. It provides granular, context-aware access control for cloud and hybrid infrastructures, ensuring robust security without compromising flexibility. Appgate SDP uses a software-defined perimeter model, creating dynamic 1:1 network connections between users/devices and the specific resources they need. This approach delivers a scalable, distributed and highly available architecture with direct routing, optimized for both security and performance in hybrid and cloud environments, enabling granular "segment-of-one" network resource access.

Key Components

1. **Controller:** Policy decision point
2. **Gateway:** Policy enforcement point
3. **Client:** End-user device software
4. **Connector:** Multi-client appliance for local resource traffic handling

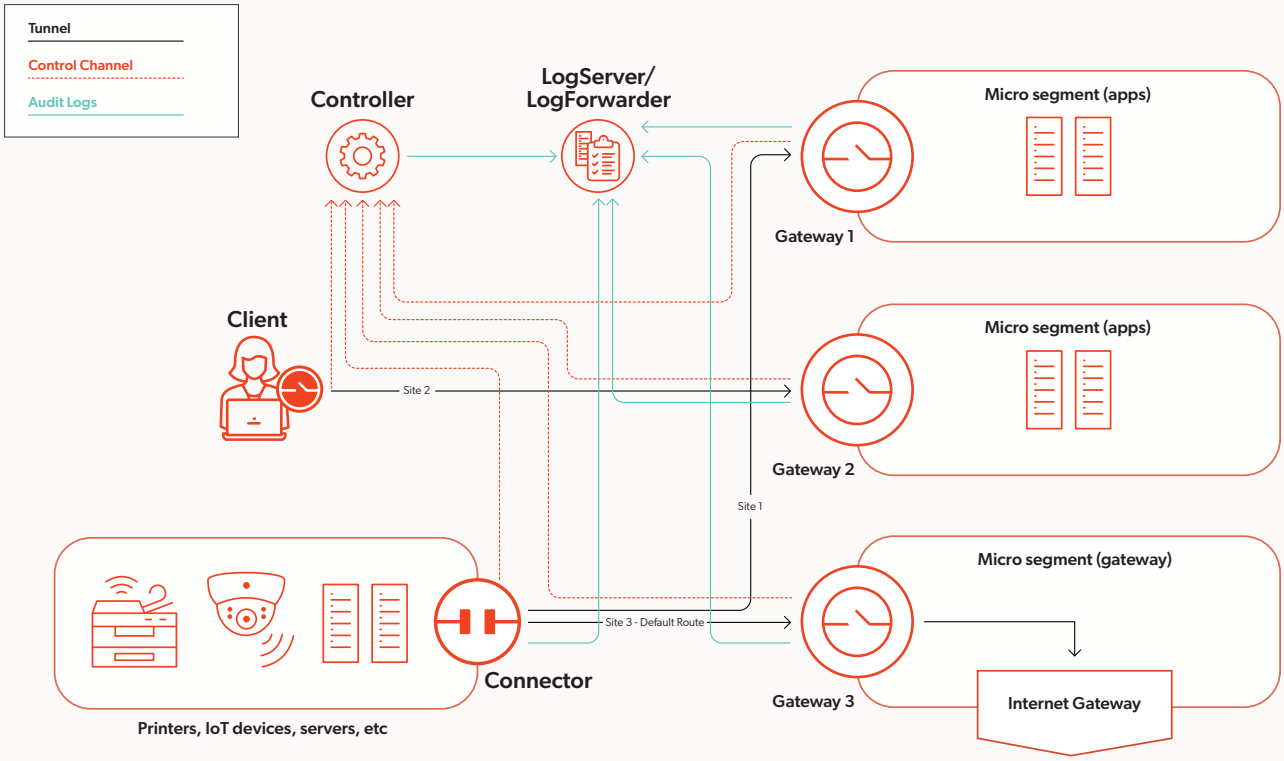
Technical Specifications

- **Authentication:** PKI-based algorithms for inter-component trust relationships
- **Access Control:** Real-time policy evaluation based on user, environment and infrastructure attributes
- **Network Security:** Secure tunnels established via client network driver
- **Compatibility:**
  - **Identity Providers (IdPs):** Appgate SDP is IdP-agnostic, and supports authentication through external LDAP (AD), LDAP certificates, OIDC, RADIUS and SAML IdPs
  - **OS Support:** All major desktop, server and mobile operating systems
  - **Infrastructure:** All major cloud and virtualization platforms

Appgate SDP provides universal ZTNA to all users regardless of device or location—whether on-campus or remote—through a unified policy model. The solution dynamically creates individualized, secure connections between users and resources based on verified identity and context. Single packet authorization (SPA) renders the network invisible where no ports are exposed, permitting communication channel access only to users that are cryptographically validated with a single packet. Appgate SDP enforces the principle of least privilege by establishing just-in-time, session-based micro firewalls to microsegment users, workloads and resources. Dynamic live entitlements then modify access in near real-time based on context and risk. With Appgate SDP, organizations have complete control over how data travels across their network infrastructure.

KEY FEATURES:

1. **Advanced Trust Model:** Implements a unique six-layer trust model, extending security beyond initial authentication to verify access at the point of resource connection.
2. **Intelligent Access Control:** Utilizes a controller system to authenticate users and devices based on multiple factors, issuing entitlement tokens for precise access management.
3. **Browser-Based Access:** Offers a portal for clientless access via web browsers, maintaining the same level of security as the full client.
4. **IoT and Legacy Device Integration:** Features a connector component to securely onboard and manage access for various devices, from sensors to servers.
5. **Dynamic Micro-Firewalls:** Creates individual firewall instances for each session, ensuring granular control and invisibility of protected resources.
6. **Simplified Remote Resource Access:** Enables easy integration of distributed resources through connectors, requiring only an outbound connection on port 443.
7. **Comprehensive Auditing:** Includes a LogForwarder for flexible and powerful audit logging, supporting compliance and security monitoring needs.
8. **Flexible Deployment:** Operates independently of traditional network perimeters, leveraging software virtualization for seamless integration across cloud and hybrid environments.



Appgate SDP's distributed architecture offers the flexibility to deploy appliances wherever needed; each appliance is a stateless machine and can be configured to deliver different functions: Controller, Gateway, LogServer, LogForwarder, Metrics Aggregator, Portal or Connector.

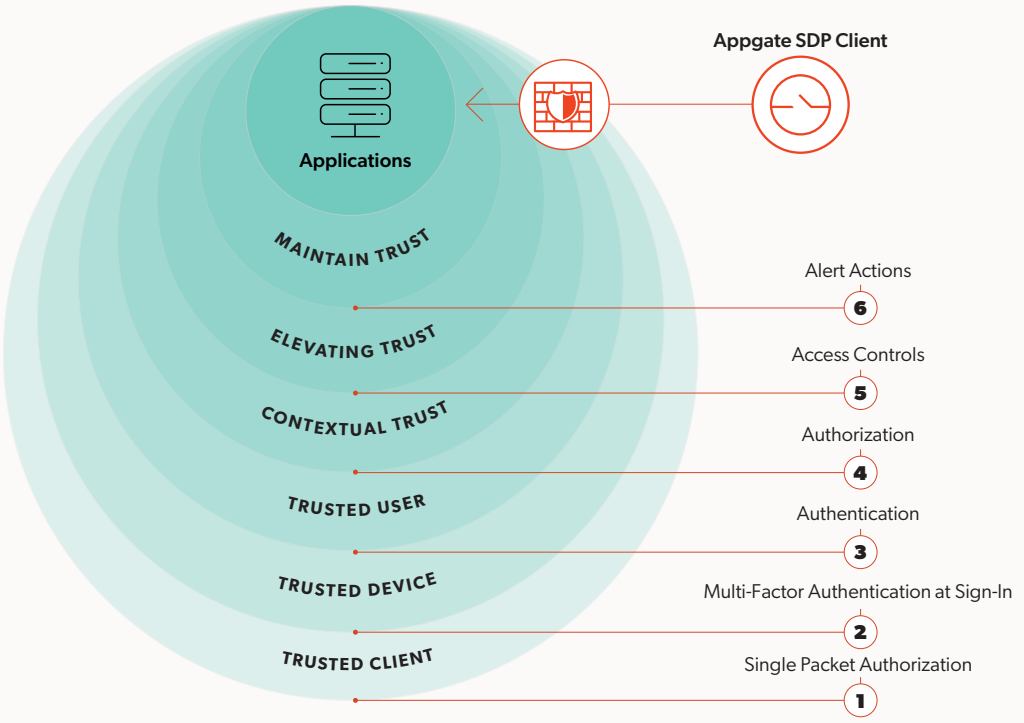
Operational Flow

1. Client authentication is sent to the controller.
2. Controller issues a cryptographically signed token with authorized resources.
3. Client establishes secure tunnels and routing rules.
4. Gateway applies real-time conditional access checks.
5. Access is granted via secure tunnel: Client ~~-~~Gateway ~~-~~Server.
6. LogServer records all access events.
7. Optional: LogForwarder integrates with SIEM/IDS systems.

Establishing Trust: The Six Layer Model

Appgate SDP uses a multi-layer authorization model to provide real-time, context-aware control over all user access attempts. The numbers below correspond to the process layers in the diagram that follows.

1. **Single Packet Authorization (SPA):** SPA renders the Appgate SDP system (i.e. components/infrastructure) invisible to unauthorized users, only allowing clients with the pre-shared key to open a communications channel. Appgate SDP will accept one or more SPA keys, included in the profile used by the Client.
2. **Multi-Factor Authentication (MFA) at Sign-in:** Registering a user's device serves as a second (trusted) authentication factor, enhancing security by blocking unauthorized access attempts with stolen credentials. Any configured MFA can be used and once a device (or browser) is registered, removes the need for users to perform MFA at every sign-in.
3. **Authentication:** This layer validates user and device credentials against defined trusted sources such as SAML and OIDC.
4. **Authorization:** Policy assignment criteria evaluate the user's/device's attributes, enabling a specific set of entitlements to be assigned to each user/device.
5. **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.
6. **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.



Appgate's six-layer trust model extends security beyond initial authentication, continuously verifying access at the point of resource connection.

Security Specifications

- **SPA:** Utilizes AES-256-GCM cipher for enhanced security.
- **Appliance Certificate:** Generated by the Controller using SHA512 with RSA encryption, key size 4096. It acts as a Certificate Authority with strict constraints to ensure secure controller-client communication.
- **Claims and Entitlement Token Encryption:** Employs AES-256-CTR cipher for securing tokens.
- **Database Encryption:** Uses AES-256-CTR cipher to protect stored data.
- **Backup File Encryption:** Secured with GPG symmetric encryption (AES-256-CFB) to ensure data integrity and confidentiality.
- **FIPS Compliance:** For desktop clients, Appgate SDP complies with FIPS 140-3 standards, leveraging the wolfCrypt module.

Communication Protocols and Encryption

- **TLSv1.3:** Default protocol for all communications, with TLSv1.2 as a fallback when necessary.
- **Appliance to Appliance Communication:** Secured using TLS13-AES256-GCM-SHA384 and ECDHE-RSA-AES256-GCM-SHA384 ciphers, with mutual certificate-based authentication and DN checking.
- **Client and Admin to Appliance Communication:** Defaults to using TLS13-AES256-GCM-SHA384 and ECDHE-RSA-AES-256-GCM-SHA384 ciphers.
- **SSH to Appliance:** Supports AES-256-CTR, AES-192-CTR, and AES-128-CTR ciphers.
- **Client to Gateway Tunnel:** Utilizes TLS13-AES256-GCM-SHA384 and ECDHE-RSA-AES256-GCM-SHA384 ciphers with mutual certificate-based authentication.

CRITICAL CAPABILITIES

- **MDM Support:** For managing mobile devices securely.
- **Multi-Tunnel VPN:** Allows multiple simultaneous VPN connections.
- **IPv6 Support:** Ensures compatibility with IPv6 networks.
- **Health Check Probe Service:** For monitoring and maintaining the health of the system.
- **Metrics Aggregator and Prometheus Exporter:** For collecting and exporting system metrics.
- **Proxy Protocol Support:** Enhances compatibility with proxy servers.
- **SPA:** Adds an additional layer of security by cloaking the underlying network infrastructure.
- **High Availability:** Ensures system reliability and uptime.
- **Multi-Site Support:** Enables the deployment of Appgate SDP across multiple geographical locations.
- **Per User Firewalling:** Provides granular access control based on individual user profiles.
- **Load Balancing:** Distributes traffic across multiple servers to ensure optimal performance.
- **External REST Calls in Criteria Scripts:** Allows for dynamic access control decisions based on external data.

Technology Integrations

- **Endpoint Detection and Response (EDR):** CrowdStrike and SentinelOne
- **IT Service Management (ITSM):** ServiceNow
- **Microsegmentation:** Illumio and ColorTokens
- **Security Incident and Event Management (SIEM):** Splunk, Sumo Logic, Falcon LogScale, Elasticsearch, OpenSearch, DataDog, Coralogix, Azure Monitoring, AWS Kinesis, as well as any SIEM tool that accepts TCP forwarding

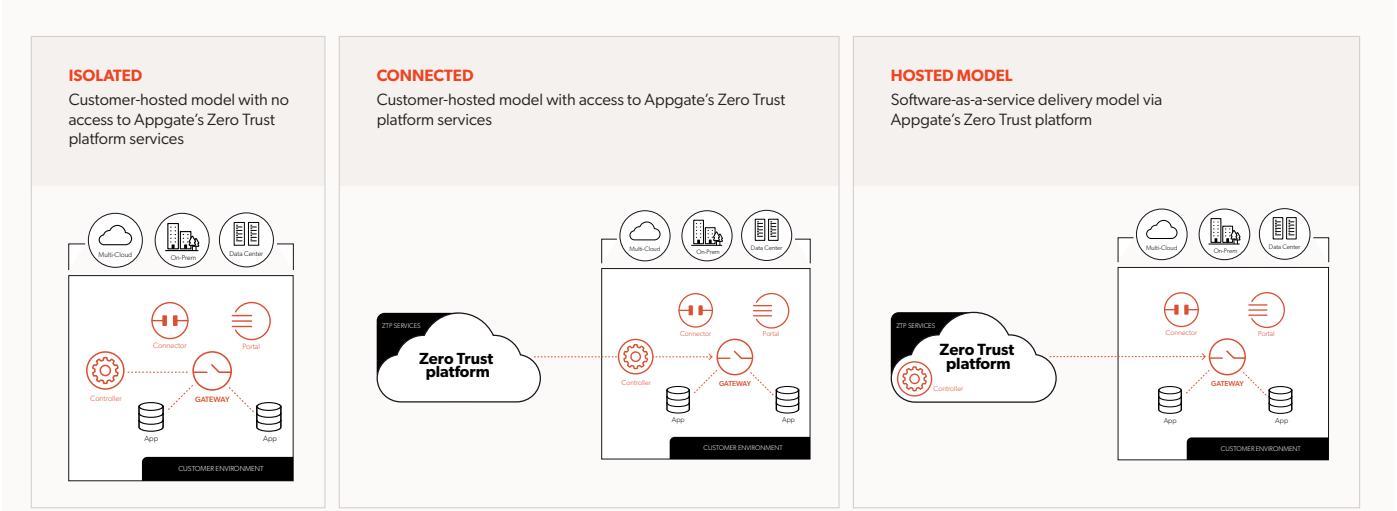
Value-Added Cloud Services

Appgate's Zero Trust platform (ZTP) is a cloud-native solution that enhances Appgate SDP's capabilities, offering a robust framework for implementing ZTNA across diverse IT environments. It features flexible deployment models, a unified policy engine with identity-centric access control, and dynamic network segmentation that enforces least privilege access. ZTP provides continuous multi-factor authentication and authorization, adapting to user behavior and device posture in real-time. With universal resource coverage, it offers consistent Zero Trust policies across hybrid and multi-cloud environments, significantly improving security posture while enhancing operational efficiency.

- **Application Discovery:** Application Discovery offers a unique opportunity for organizations to quickly transition from VPN-based remote access to a modern and secure ZTNA model. This feature employs an advanced machine learning (ML) system to observe user behavior and access patterns over time. By analyzing this data, Application Discovery generates actionable insights that empower administrators to define and fine-tune access policies, ensuring that only authorized users can access specific resources aligned with the organization's security objectives. As organizations adopt hosted or connected deployments, leveraging Application Discovery can significantly enhance their ability to respond to evolving security threats while preserving a seamless user experience.
- **Risk Engine:** The Risk Engine enhances access policies with security posture insights gathered by third-party IT, security and business solutions. Built-in integrations with leading security tools and a click-to-configure interface eliminates the cost and complexity of custom API scripting.
- **Risk Alerts:** The Risk Alert service enables Appgate SDP's dynamic policy engine to respond to information from third-party services that indicate changes in device or user security posture.
- **Policy Analyzer:** The Policy Analyzer is a powerful tool designed to streamline the policy creation and management process. It helps administrators reduce their organization's attack surface, while simplifying operations. By leveraging real-time data and analytics, the Policy Analyzer enables organizations to identify policies and entitlements that can be safely retired, uncovers entitlements with overlapping resources and highlights configurations that might otherwise be missed. This proactive approach enhances security and simplifies regulatory compliance, making it a vital asset for organizations transitioning to a hosted or connected deployment. **Note:** Policy Analyzer will be Generally Available Q2 of 2025.

Deployment Flexibility

Appgate SDP can be deployed across cloud, on-premises, and hybrid environments, offering a versatile solution that adapts to the specific needs of an organization. Its software-defined nature allows for rapid deployment and scalability without the constraints of traditional hardware-based solutions.



Appgate SDP provides choice and flexibility with various deployment models, including isolated, connected, or hosted options.

Instance Sizing

Appgate SDP employs a fundamentally different architectural approach. Its distributed design allows discrete functional components to operate as stand-alone appliances, each optimized for specific tasks. Utilizing a patented method, the Appgate SDP Gateway establishes a secure tunnel service and deploys a micro-firewall instance for each client, with each connected client handled by a dedicated thread.

All system functions are delivered through a highly performant, hardened Ubuntu-based appliance. These appliances can be deployed as cloud instances, virtual machines, or physical hardware. The software architecture has been fine-tuned to leverage multi-core processors and integrated features such as AES-NI, allowing Gateway throughput in the range of 20Gb/s to 40Gb/s even in virtual environments. Appgate SDP provides the flexibility to scale both vertically and horizontally, including the use of AutoScaling capabilities on the IaaS platforms, accommodating the evolving demands and infrastructure of modern enterprise environments.

Appgate SDP Benefits

Handles Complex Environments and High Security Requirements: Tailors architecture for unique network challenges; maintains control without relying on vendor clouds; and leverages extensibility to build a unified, interoperable security ecosystem.

Hardens Your Security Posture: Cloaks all resources to render attack surfaces invisible; halts lateral movement through risk-informed Zero Trust least privilege access; achieves comprehensive network visibility; and builds robust Zero Trust foundation.

Revolutionizes Your Network: Overlays secure universal access experience across full topology; revolutionizes network with secure café-style connectivity; and decreases OpEx by eliminating redundant connectivity costs.

Improves User Experience: Delivers consistent connectivity experience for any employee or authorized third party with simultaneous direct multi-tunnel connections providing automatic Gateway and site failover.

Minimizes IT and Security Admin Time: Decreases hands-on time with a unified policy engine; automates access provisioning; and minimizes trouble tickets.

Enhances Technology Investments: Seamlessly integrates with a range of industry-standard monitoring and reporting tools to centrally correlate access-related security risks and events; enables security posture insights by third-party services such as endpoint detection and response (EDR); and enhances dynamic access control policies based on context and risk.

Conclusion

Appgate SDP significantly benefits organizations by implementing a ZTNA model that dynamically authenticates and authorizes users based on identity and context, minimizing the risk of unauthorized access. Its software-defined architecture reduces the attack surface, while granular access controls enhance network segmentation and limit lateral movement within the network. Flexible deployment options across hybrid environments, seamless integration with existing security tools, and robust end-to-end encryption further strengthen security and simplify management, aligning with modern Zero Trust security strategies.

About Appgate

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at appgate.com.

For more information, please review the Appgate SDP Admin Guide.

appgate