SECURE THIRD-PARTY ACCESS

Provision secure access for third parties without introducing friction or complexity.

Introduction

To maintain their focus on core competencies, today’s organizations depend on a third-party ecosystem of vendors, contractors and other outsourced service providers for a wide range of enabling and ancillary functions.

To fulfill their obligations, users within these third parties often need access to resources within your IT environment. For example:

• Contractors need access to internal systems and resources
• Vendors need access to internally deployed products and applications
• Outsourced IT providers need access to helpdesk ticketing systems and infrastructure components

Appgate SDP, an industry-leading Zero Trust Network Access (ZTNA) solution, allows enterprises to enable this third-party access—securely, seamlessly, and simply.

Challenges

Safeguarding third-party access requires overcoming a number of challenges, including:

• **Enforcing least privilege access**: Ensuring each third-party user can only access the resources needed to perform the particular function or task at hand

• **Keeping pace with ever-changing access needs**: The specific access needs of each third party (and even of each user within a particular third-party) are unique to the function being performed and may change dynamically

• **A heterogenous set of users**: The third-party ecosystem includes a diverse collection of users, devices and locations, rendering simple access control rules unsuitable

• **Satisfying compliance requirements**: To recognize risks, enhance auditability and support compliance programs, organizations need granular visibility into what resources are accessed by whom

Unfortunately, traditional remote access technologies, such as VPNs, treat all incoming connections equally, validating access only after the connection is made. This all-or-nothing approach results in third-party users having excessive privileges, which is why threat actors have increasingly targeted VPN solutions as access vectors.

**BENEFITS**

**WORRY-FREE THIRD-PARTY ACCESS**

Live entitlements—dynamic and context-sensitive access policies—continually evaluate and enforce least privilege access, ensuring each third-party user can only access the resources they need for the task at hand.

**FRICIONLESS PROTECTION**

Easy-to-use browser-based access for contractors, vendors and other trusted third parties with no clients or plug-ins required.

**STRONGER SECURITY POSTURE**

Resources are never exposed to the internet, as Appgate SDP cloaks infrastructure while traffic travels through mutual TLS-based microtunnels on a per-user basis.

**SIMPLIFIED POLICY MANAGEMENT**

A central, unified policy engine controls access and reduces administrative overhead—even for the diverse mix of users, devices and locations that make up the third-party ecosystem.

**ENHANCED VISIBILITY INTO EVERY ACCESS**

Support compliance programs, on-demand audits and ongoing risk assessments with detailed logging.

**IMPROVED OPERATIONAL EFFICIENCY**

Replace time-consuming and error-prone processes with automated provisioning that keeps up with your changing operational needs.

“The Appgate system is relatively easy to use, but the key issue is that it is very powerful. It is possible to define so many different profiles for different people with very different needs. We couldn’t find any other system that allows us to define such a variety of different profiles for all our different users.”

- Tomaz Szudejko, Deputy Director Operator Services, PSE S.A.
**Solution**

Appgate SDP is a proven way to provision secure access for third parties without introducing friction or complexity. Enforcing the principles of Zero Trust, Appgate SDP establishes a software-defined perimeter that satisfies the complex requirements of third-party access by:

- Providing flexible access options, including broad protocol and app support, as well as choices for user access (clientless for web-based resources or via an installed client for the highest level of security)
- Authenticating using context and identity before controlled access is permitted, while keeping all other resources completely invisible
- Providing each third-party user with precise and granular access to only the resources they need for the task at hand
- Dynamically adapting to contextual changes, granting access based upon a combination of user attributes, risk posture, metadata and other factors
- Generating a rich set of access logs that can easily be integrated into existing security event management for visibility and compliance

Additionally, Appgate SDP’s unified policy engine reduces administrative complexity, allowing you to keep pace with changing needs and scalable architecture. And Appgate SDP’s straightforward deployment ensures any organization can get up and running quickly and effectively.

**How Appgate SDP Enables Secure, Frictionless Third-Party Access**

With Appgate SDP, you won’t have to worry about third-party vendors and partners accessing your entire network or that their devices are unsecured or contain a virus. With Appgate SDP, authorized users only have access to the resources you allow versus the entire network, making lateral movement impossible and reducing the risk and impact of a breach. And a single set of unified policy controls gives granular and dynamic control of all user and application activity, while access to apps is made seamless for third parties through browser-based access.

**How it works**

- Admin creates third-party user entitlements
- Third party utilizes Appgate SDP client or clients via web browser
- User is directed to enterprise identity provider (IdP) for authentication.
- Before accessing the IdP, the client makes an access request to the controller using single packet authorization (SPA)
- Controller checks context, passes live entitlements to client
- Using SPA, client uploads live entitlements, which gateway uses to discover applications matching the user’s context
- Dynamic segment of one between user and resource is built for this session and continuously monitors for any context changes, and adapts accordingly
Key Capabilities for Third-Party Access

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

Browser-based clientless access
Third-party users need secure access to hybrid enterprise applications but often do not want to install another company’s client to access their network. With Appgate SDP, anyone can easily and securely access protected resources with clientless, browser-based access.

Hybrid cloud, cloud-native and cloud agnostic
Appgate SDP is proven to provide secure dynamic Zero Trust access to solve complex hybrid enterprise security problems. It secures all types of on-premises and 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.

Cloaked infrastructure
Single packet authorization (SPA) technology cloaks infrastructure so that only verified users and workloads can communicate with the systems. It is invisible to port scans, protecting against DDoS attacks and is cryptographically hashed as a further defense. Gateways and controllers are completely cloaked so they cannot be probed, scanned or attacked—significantly reducing the network attack surface and limiting lateral movement by preventing network reconnaissance.

Comprehensive visibility and control
Appgate SDP provides rich visibility into all user and application activity, not just IP address and port data, and user activity logs are automatically captured or delivered to an enterprise SIEM – reducing security loopholes for attackers.

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