REPORT REPRINT

Cyxtera spins off security business as AppGate, with a focus on SDP and zero trust

JANUARY 6 2020

By Garrett Bekker

The company recently announced plans to spin off its security businesses under the AppGate brand. Updates to AppGate SDP include Common Criteria certification, a new 'light' client that does not require admin privileges to install and broader support for Google Cloud Platform.

451 Research®

Introduction

We have chronicled the rise of the 'zero trust' phenomenon in a series of reports on vendors that specifically incorporate zero trust principles in their products, particularly software-defined perimeter (SDP) startups that provide remote access to applications and resources without a traditional VPN (Odo Security, Banyan, Centrify, Luminate, Meta Networks, Vidder, Pulse Secure). Our latest report in the series focuses on Cyxtera, whose AppGate SDP product is among the earliest entries in the SDP category.

Recent updates to AppGate SDP include Common Criteria certification, a new 'light' client that does not require admin privileges to install and broader support for Google Cloud Platform. However, one of the most notable changes is that Cyxtera will be spinning off its security businesses under the AppGate brand, while its colocation and datacenter businesses will remain with Cyxtera.

451 TAKE

Although some SDP products are designed mainly for web and cloud-based applications, AppGate SDP has a flexible architecture that works with nearly any application and supports both on-premises and cloud deployments as well as a wide variety of use cases. As such, we see AppGate SDP as better suited to large, established enterprises with complex, hybrid networks for both strategic Zero Trust initiatives as well as more focused security products compared with many SDP startups. The VPN replacement stakes are high, however, and we expect incumbent vendors across multiple IT segments to continue to target the opportunity and place pressure on all independent SDP vendors, including AppGate. Although as initial M&A activity suggests, established IT vendors could serve as both a competitive threat as well as a potential buyer.

Context

Miami-based AppGate has a unique and storied history. Parent company Cyxtera was created via a joint venture formed in 2016 between private equity firms Medina Capital, BC Partners and Longview Asset Management, which spent $2.8bn to simultaneously purchase 57 datacenters owned by CenturyLink, along with several of Medina's portfolio investments: Easy Solutions (fraud prevention), Cryptzone (DLP/SDP), Brainspace (machine-learning and analytics) and Catbird (micro-segmentation). Medina Capital's founder, Manual Medina, founded Terremark, which was sold to Verizon for $2.1bn in 2011.

Cryptzone itself had acquired five companies between 2009 and 2014, including AppGate Network Security, ControlGuard (endpoint-based access controls), NETconsent (security policy management), SE46 AB (app whitelisting) and HiSoftware (DLP, data access governance). Most recently, Cyxtera acquired fellow Miami-based security assessment and pen testing vendor Immunity early in 2018.

Prior to the announced split, Cyxtera had roughly 1,500 full-time employees, 500 of whom are focused on cybersecurity. Once the split is finalized on January 1, AppGate will operate as a separate legal entity, but still be owned by Medina Capital and BC Partners. Mike Aiello will operate as the new CEO, after serving as head of cloud security at Google and as CISO at Goldman Sachs.

Products

The new AppGate entity will house all of Cyxtera's former security software and services businesses, including AppGate SDP, digital threat protection, pen testing, incident response, advanced threat analytics and also some offensive and defensive security (from the Immunity acquisition), as well as ML/AI analytics from the Brainspace acquisition.

Cyxtera's entry in the zero trust/SDP fray is AppGate SDP. AppGate SDP was initially positioned as role-based access control for large networks, and several years ago developed a new distributed architecture that took an identity-centric approach to access controls that were enforced at the network level and would prevent TCP connections from being established until after the user was authenticated.

Architecturally, AppGate SDP follows the guidelines established by the Cloud Security Alliance (CSA), and includes three main pieces: client software for end-user devices, controllers and gateways (AppGate offers an AppGate appliance that can be deployed as a VM, on-premises server or cloud-based server and can be configured to function as either a controller or gateway).

The client is responsible for checking device attributes and connecting to the controllers (via a mutually authenticated TLS connection to eliminate man-in-the-middle attacks). The client is also responsible for receiving, interpreting and sending authentication tokens that contain the user's entitlements to the various gateways in order to permit access to the resources to which the client is entitled, such as network subnets and hostnames. During the authentication process, they are contained in a token and sent to the client device.

The controllers are the 'brains' or central nervous system of an SDP deployment and determine who has access to what resources by connecting to an external identity provider (IDP) such as Microsoft Active Directory (AD) or Okta. The controller pulls user attributes, roles and permissions from the IDP, validates authentication requests, and if all goes well, sends a token to the client that contains entitlements to certain resources. The controllers also serve as a policy store.

AppGate SDP gateways are in-line physical or virtual appliances that are in front of the applications they are protecting – either on-premises or at an ingress point into AWS, Azure or GCP – and are responsible for enforcing access decisions. Gateways, for example, can require the client to 'step up' to a stronger form of authentication in order to access certain resources that may be more sensitive or higher risk. The AppGate SDP gateways can also make API calls to external services such as ServiceNow so that support tickets can be used to trigger policy responses, such as to enable temporary access to a router for routine maintenance.

SDP's controllers and gateways have no open ports for attackers to scan or probe and won't respond to any network connections from unauthorized users or devices. The AppGate SDP client is set up to be dynamic and can automatically reevaluate policies and update user access as the environment changes, for example, if the gateway discovers new applications.

Strategy

AppGate SDP is offered as a subscription, and priced on a per-user, per-year basis.

AppGate SDP's primary use case is as a VPN replacement, for remote users looking to access internal applications, particularly legacy applications that don't support modern standards like SAML.

Competition

AppGate SDP competes with a variety of zero trust and SDP vendors that come from a variety of backgrounds and tackle access control from different perspectives. Architecturally, we view AppGate SDP as most similar to early SDP vendors like Vidder (acquired by Verizon), Juniper spinoff Pulse Secure and open source toolkit Waverly Labs. The latter follow an architecture that follows the SDP guidelines laid out by the Cloud Security Alliance, with full agents and on-premises hardware to address hybrid use cases. The latter can be more 'heavy' to deploy but can also offer some benefits in terms of flexibility, breadth of use cases and in some cases, performance.

Cyxtera sees its approach as distinct from 'cloud-based' SDP vendors including those with a CDN-like distributed architecture such as Zscaler (Zscaler Private Access), Akamai (via the Soha acquisition), Cloudflare (Cloudflare Access) and Netskope Private Access. Other vendors that could be loosely grouped within this camp include Okta (via the purchase of ScaleFT), Luminate (acquired by Symantec) Meta Networks (acquired by Proofpoint), Banyan, Odo Security, Perimeter81, Strongdm, Zentera and Safe-T. Identity management vendors specifically addressing the zero-trust concept include Cisco (Duo Security), Microsoft (Conditional Access) and Centrify.

SWOT Analysis

STRENGTHS

Flexible architecture, support for a wide variety of apps and protocols (such as HTTP, TCP, UDP, ICMP, SSH, RDP), both on-premises and in the cloud. Direct connections to gateways can help with performance and latency concerns, and API connections can help connect to external services.

WEAKNESSES

AppGate SDP does not yet have an agentless client to support unmanaged devices or non-employees, although it is on the company's roadmap.

OPPORTUNITIES

Larger enterprises running complex, hybrid networks with substantial on-premises resources as well as a growing range of cloud-based assets and applications seem to be the best fit for AppGate SDP.

THREATS

The VPN replacement stakes are high, and we expect incumbent vendors across multiple IT segments to continue to target the opportunity and place pressure on all independent SDP vendors, including AppGate.