Solution Showcase

Securing the Shifting Network Perimeter with Cryptzone AppGate

Date: January 2017 **Author:** Doug Cahill, Senior Analyst; and Leah Matuson, Research Analyst

Abstract: In today's dynamic business landscape, CISOs and security practitioners are charged with securing an increasingly multidimensional infrastructure against a variety of threat actors. Broad adoption of cloud services, knowledge worker mobility, and increased inter-organization collaboration has created an amorphous network perimeter. To keep pace, there is a need to align how infrastructure is managed with the security controls to protect them from compromise.

Using a software-defined perimeter (SDP) is an approach that provides the right combination of threat prevention efficacy because it is based on the least privilege security model and provides the operational efficiency to move at the speed of DevOps. Cryptzone's AppGate delivers on the must-have requirements of an SDP solution for today's and tomorrow's compute environments.

Modern Data Center Security Challenges

There are multiple aspects that make securing today's data center challenging—from how infrastructure is provisioned and managed, through the flexibility end-users require in accessing business applications and data, to the ever-evolving threat landscape.

Multi-dimensional Infrastructure

The movement of workloads to the public cloud is resulting in many organizations having to secure a combination of on-premises resources as well as those that are cloud resident. Recent ESG research highlights the heterogeneous makeup of today's data center with 44% of respondents stating they are already running workloads simultaneously in both private and public clouds, while another 32% are currently testing this configuration.[1]

As more of that footprint moves to the cloud, the role of traditional network security controls is beginning to change with certain controls, such as firewalls, getting pushed to the edge. Manually updating IP-based rules can be operationally misaligned with modern dynamic, software-defined environments and thus in conflict with DevOps methodology employed to continuously integrate, deliver, and monitor applications. As a result the speed at which organizations must move for competitive considerations often relegates security to an afterthought.

While cybersecurity initiatives are typically funded, the acute shortage of cybersecurity skills makes resourcing those initiatives problematic. In fact, according to ESG research, 46% of organizations have a problematic shortage of

[1] Source: ESG Research Report, *The State of Cloud Security in the Enterprise*, October 2016.

cybersecurity skills.[2] As such, forward-thinking organizations are strategically changing their security technologies, processes, and tools in order to benefit from automation of an increasingly API-driven infrastructure.

The Any-to-any Matrix of Knowledge Worker Mobility

Part of the new normal of today's compute environment is multi-device end-users who are often mobile—creating a need to secure any device accessing any application at anytime from anywhere. Securing these innumerable combinations requires an approach that goes beyond simple authentication and considers factors such as device integrity. In addition, certain business-critical applications warrant additional levels of control including multi-factor authentication (MFA).

Diversified Threat Types and Vectors

Models such as Lockheed Martin's cybersecurity kill chain, which depicts the stages and behaviors employed by a wide variety of attacks, are highly applicable to the characteristics of the modern data center. The entry point for most attacks exploits a vulnerability on an endpoint—be it software or human gullibility that makes techniques, such as spear phishing, effective. Another entry point arises from port scanning externally facing resources, which can identify easily exploitable vulnerabilities and enable lateral movement across a network to a target. The any-to-any nature of end-user computing, and the proliferation of cloud-resident workloads has greatly expanded the attack surface area. As such, organizations need security controls that span endpoints, networks, and servers.

These aspects of the modern data center, coupled with end-user mobility, raise the question of whether there is a perimeter and, if so, how to best secure it. Perimeters are now amorphous in that they are less defined by physical markers and more defined by the end-users, their devices, and the assets they are accessing.

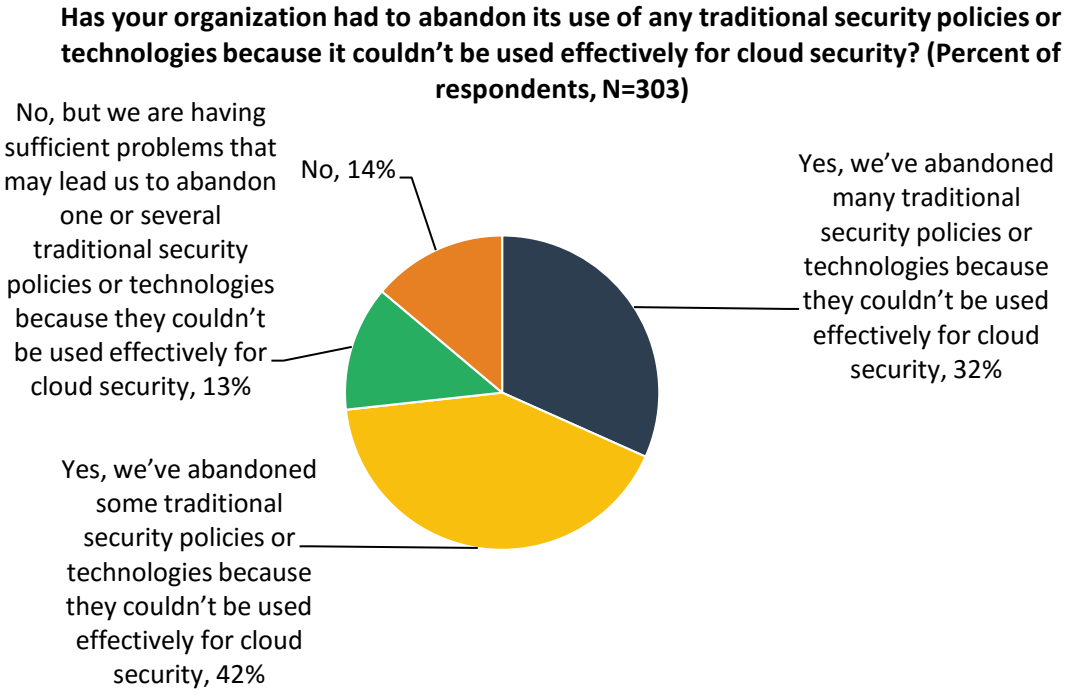
Perimeters are now amorphous in that they are less defined by physical markers and more defined by the end-users, their devices, and the assets they are accessing.

Applying Least Privileged Access with Software-defined Perimeters (SDPs)

Due to the changes in the complexion of the data center, the rapid adoption of cloud services, and employee mobility, organizations are abandoning existing controls and retooling. In fact, according to ESG research, 74% of survey participants stated that they have had to abandon some or many of their traditional security policies or technologies because they couldn't be used effectively in the cloud (see Figure 1).[3]

[2] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.
[3] Source: ESG Research Report, *The State of Cloud Security in the Enterprise*, October 2016.

Figure 1. Abandonment of Traditional Security Policies or Technologies Due to Cloud Security Concerns



Source: Enterprise Strategy Group, 2017

In response, purposeful security solutions are required. Developed by members of the Cloud Security Alliance, software-defined perimeters (SDPs) are based on the Defense Information Systems Agency (DISA) "Black Cloud" security model whereby network resources are invisible unless (and until) access is authorized. SDPs represent a highly appropriate approach for securing the attributes of today's compute environments, as well as those on the near-term horizon with the following capabilities.

Identity-based Least Privileged Application Workload Access

The cornerstone concept of SDPs is as follows: Providing access to the least amount of network-based resources for the least number of individuals, who are then granted the lowest level of privileges required to perform their job. Access privileges are set, defined, and updated by user-centric policies which leverage multiple aspects of server and user context, such as via integration with identity and access management (IAM) systems. This approach eliminates the need to try to keep up with an ever-changing environment through traditional firewall "ports and protocol" settings. Because this identity-based approach means policy travels with the user, and many users access corporate assets from multiple devices, an SDP solution should profile device integrity as part of the authentication process. That policy lexicon should also include the ability to require MFA for access to more critical applications when conditions require it.

Cloaking via Separation of Control and Data Paths

While you can't secure what you can't see, the converse is also true—*you can't hack what you can't see*. SDPs cloak those resources to which one does not have access, making them invisible to unauthorized users. This is achieved by separating the control and data paths via which access is authenticated before hand-off to an application gateway to set up a secure connection between the user and application. These session-based connections are temporal—they are provisioned when needed, and then torn down to prevent unauthorized access. An SDP should also obfuscate communication over these connections with strong encryption inclusive of robust key management capabilities.

If an authorized endpoint device *does* get infected, and a threat moves laterally to a server workload to which the user is authorized to access, it *will not be able to then traverse more of the network* since other resources (including ports and protocols) are abstracted and invisible—effectively reducing the attack surface area. This containment to a single segment prevents the ability of such threats to communicate with a remote command and control (C&C) server.

Coverage Across Devices, Workloads, and Location Dimensions

To support hybrid cloud environments, an SDP offering should be server-location-agnostic and support bare metal Unix servers, virtualized Linux and Windows machines, and dynamically provisioned cloud-resident workloads. End-user device coverage should include Windows, MacOS, iOS, and Android.

Enables Automation

The DevOps methodology of continuous delivery represents an opportunity to realize similar efficiencies via automation in security. An SDP solution should support policies that leverage server workload metadata, such as the name:value pair tags used as the naming convention for dynamically provisioned cloud workloads, so that access to those workloads can be secured based on those tags. Tags extend the identity-based construct of an SDP, further eliminating the need to instrument firewalls.

Future-ready Extensibility

An SDP solution should also be extensible for future architectures. Securing east-west traffic between workloads will become more of a security imperative when workloads in a multi-tier application span infrastructures such as an on-premises database server communicating to the load balancing and web application tiers deployed in the public cloud for scale and access to a content delivery network (CDN). As more connected devices come online, Internet of Things (IoT) represents another expansion of the attack surface area well suited for cloaked and identity-based micro-segmentation. These architectures require a user-centric, device-agnostic, context-aware security model that is policy-driven for the modern, software-defined data center.

Introducing Cryptzone AppGate

Cryptzone's AppGate offering is a software-defined perimeter solution that implements the software-defined perimeter architecture by applying an identity-based approach to secure end-user access to network resources with the following functional capabilities.

Context-based User-centric Access Control

AppGate's policy engine considers context beyond user identity before granting access to applications. When access is being requested, AppGate employs a virtual network adapter to profile the device and location from which the request came, as well as other attributes such as whether or not appropriate endpoint security controls are present. The richness of this policy lexicon mitigates the use of stolen credentials to access corporate applications—e.g., an authorized user requesting off-hours access to an application from a remote location and new device. Policy settings are streamlined via integration with existing IAM services, including those that are Security Assertion Markup Language (SAML)-compliant.

Invitation-only, Segments of One

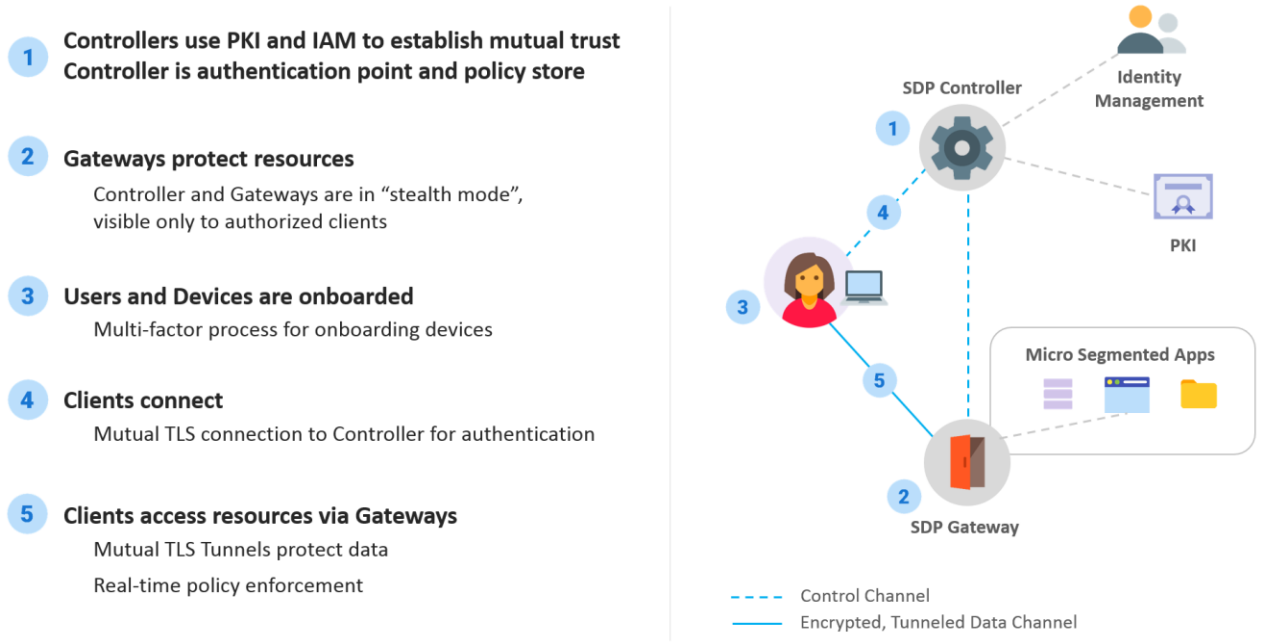
Once access is authorized, the AppGate controller instructs the AppGate gateway to enable the provisioning of a session-specific connection from the authorized user to the application through the gateway. The connection is an individualized "segment of one" for each user (see Figure 2). The resources behind the gateway are invisible and, therefore, inaccessible

by unauthorized individuals. The connections are also encrypted for further protection, including those that cross public networks. All user activity is logged, establishing an audit trail for compliance purposes.

Coverage across Hybrid Clouds and User Devices

AppGate supports both on-premises and cloud-resident workloads with connectors for Amazon Web Services, Microsoft Azure, and Google Compute Platform. The AppGate virtual network adapter also supports a wide variety of endpoint operating systems including Windows, MacOS, iOS, and Android, as well as a number of Linux distributions.

Figure 2. SDP Architecture



Source: Enterprise Strategy Group, 2017

The Bigger Truth

Aligning security with the infrastructure it is intended to protect requires the use of purposeful controls. The move to software-defined infrastructure coupled with employee mobility is resulting in a shifting perimeter, necessitating software-defined security in the form of software-defined perimeters so that security can move at the speed of business. Such a model is adaptive to change, and thus designed for the dynamic nature of today's compute environments inclusive of DevOps methodologies. SDP gives organizations the flexibility to apply least privilege access controls to individual user-application connections, effectively reducing the attack surface by making servers invisible to bad actors. Cryptzone's AppGate product allows organizations to leverage an SDP to protect users and the applications they access with an architecture well-suited for today's hybrid environments, and is designed to support future use cases and technologies.