REPORT REPRINT

Newcomer Banyan tackles zero trust with a mesh-based approach to multi-cloud security

MAY 17 2019

By Garrett Bekker

The startup focuses on unifying the authorization layer of a zero-trust platform with a two-pronged approach: a service mesh-based architecture to protect apps down to the API and micro-service level, and trust scoring to make continuous contextual access decisions.

Introduction

We have recently authored a series of reports (Centrify, Luminate, Meta Networks, Vidder, Pulse Secure) that have addressed what has been variously referred to as zero trust, software-defined perimeter (SDP), Beyond Corp or, 451 Research's preference, 'Unified Access Control (UAC)' – in which the ability to access corporate resources is no longer based mainly on where you are but more on who you are and what you are allowed to do based on your role and other contextual attributes.

Startup Banyan is one of a handful of vendors that have emerged to specifically address the zero-trust concept, with a new offering that focuses on the authorization layer of a zero-trust platform, or what it calls a 'zero trust continuous authorization framework.' The latter uses a service mesh-based architecture and trust scoring to make contextual access decisions for every single access request, down to the API and micro-service level.

451 TAKE

In some sense, zero trust represents a convergence between network- and identity-based access controls, and from that perspective, Banyan is looking to provide the 'glue' that binds separate camps of the broader zero-trust ecosystem. Since many companies already have MFA and IDaaS/SSO, as well as policy enforcement points via their NGFWs and microsegmentation offerings, it's arguable that authorization is the missing link in a full zero-trust network strategy – or as Banyan sees it, 'the brains of zero trust.' Banyan's argument is twofold: 1) that a dynamic workforce requires continuous authorization as opposed to just static one-time authentication and 2) that data breaches from cloud-hosted applications, servers and APIs that are exposed to the internet need a more scalable access enforcement point than a standard VPN to 'cloak' these resources from attack.

Context

San Francisco-based Banyan was founded by Yoshio Turner, Jayanth Gummaraju and Tarun Desikan, veterans of HP, VMware and CDN/XDN platform provider Moovweb. Banyan has recently emerged from stealth and has nearly 20 full-time employees, most of whom are based in the Bay Area other than a small development team in India.

Banyan is backed with seed funding by Unusual Ventures, a new VC firm led by John Vrionis (ex-Lightspeed) and AppDynamics (sold to Cisco for $3.7bn) founder Jyoti Bansal. Banyan is currently targeting customers in technology, health care and financial services, and is very active in the open source community.

Products

The company's core offering is the Banyan Continuous Zero Trust Platform. Like other vendors in the SDP segment of the broader 'zero trust' ecosystem, Banyan's focus is to provide employees, contractors and partners with access to applications and resources without a VPN.

However, Banyan differs from others in the SDP category in two primary ways. First, rather than focusing on user and device authentication and SSO, Banyan is more focused on the arguably more challenging issue of authorization – determining what those users (and devices, applications or processes) should have access to after they have been authenticated. The latter may sound trivial

in theory, but in reality can be surprisingly complex. As we noted in our recent report on PlainID, authorization policies in large organizations can spawn thousands of difficult-to-maintain policies based on roles or attributes and can be scattered across many repositories and applications.

Second, while most SDP vendors either approach remote access control using either an on-premises, hardware-based architecture (like Vidder or Cyxtera), or a cloud-based proxy (Luminate, Meta Networks, Akamai, Zscaler), Banyan is to our knowledge the first vendor to apply a service mesh-based architecture to the problem. Banyan's contention is that in a world where containers and cloud instances and even entire network segments are spun up and down rapidly, relying on a perimeter-based architecture – whether appliance or cloud-based – quickly becomes unmanageable.

Behind the scenes, Banyan's architecture is what it calls a 'cloud command center' – a centralized management plane and a 'multi-cloud access hub' – a service mesh that is a network of distributed software-defined enforcement points. Every node in the mesh is assigned a cryptographic identity – laptops and mobile devices, applications – which allows for direct, mediated control over access to applications and resources. Banyan uses machine learning to develop a trust score for each access request to allow for automated decision-making.

Since Banyan's network is highly distributed, it is very resilient to failure anywhere in the mesh – there is no single point of failure, unlike some cloud-based systems. Banyan also doesn't require any appliances to be installed and notably doesn't require any modifications to applications or network resources. Banyan does require an app that can be downloaded from an app store.

Strategy

Banyan is focused on authorization and is content to leave user and device authentication and verification to native integration partners like Okta or Airwatch (VMware). Like many SDP vendors, Banyan's use cases include VPN replacement, although since it's independent of existing network infrastructure, Banyan can be rolled out in conjunction with existing VPNs and then gradually migrated off them over time. In terms of user populations and application types, Banyan is currently focused on employee access to apps in the cloud.

Competition

As noted in our recent TBI report 'Beyond the Perimeter: From 'Zero Trust' to 'Unified Access Control,' there is an emerging and growing list of vendors that could arguably be placed under the zero-trust umbrella. We break down zero trust further into several camps, including both SDP and those that focus on microsegmentation of east-west traffic.

The former generally provide remote access to applications without a VPN, and includes vendors like Zscaler (Zscaler Private Access), Akamai (via the Soha acquisition), Cloudflare (Cloudflare Access), Pulse Secure and Okta (via the ScaleFT purchase), newcomers like Luminate (a 451 Firestarter award recipient recently acquired by Symantec) and Meta Networks, and SDP 'veterans' such as Cyxtera and Vidder (recently acquired by Verizon). Google is arguably the 'grandfather' of the zero-trust concept with its' BeyondCorp reference architecture built for Google's internal networks, parts of which are publicly available from Google under the Identity Aware Proxy and Context Aware Access monikers.

Identity management vendors specifically addressing the zero-trust concept include Duo Security (acquired by Cisco for $2.4bn), Microsoft (Conditional Access) and Centrify.

The microsegmentation camp includes vendors such as vArmour, Illumio, Unisys (Stealth), Guardicore, Palo Alto Networks and newcomer Edgewise Networks.

We place Banyan more squarely in the SDP category, which itself can be further broken down based on architectural approach. Early SDP vendors like Cyxtera and Vidder generally rely on on-premises hardware, while the remaining vendors rely to some degree on a cloud-based approach.

Banyan could also compete with traditional VPN vendors such as Check Point Software, Cisco, Juniper, Palo Alto Networks, Fortinet, SonicWALL and WatchGuard.

SWOT Analysis

STRENGTHS

Bayan focuses on authorization and service mesh-based architecture that provides resiliency and eliminates need for hardware deployments.

WEAKNESSES

Banyan is still in early stages and is trying to find its way in terms of marketing positioning and where to stake its claim in a crowded field.

OPPORTUNITIES

Banyan has a chance to fill in white space in the zero trust/SDP ecosystem and serve as an orchestration layer to tie together disparate pieces such as MFA, MDM, SSO and microsegmentation offerings. SDP vendors have been prime M&A targets of late, and Banyan could draw interest from larger vendors.

THREATS

The stakes are high in the access control game, and it's no great surprise that IT heavyweights like Cisco, Google, Microsoft and others have thrown their hats in the ring. What role remains for independent startups is still unclear.