BANYAN SECURITY

SOLUTION BRIEF

SaaS Application Security

The Banyan Security Platform

Achieve robust, consistent SaaS application security with Banyan's Cloud Access Security Broker (CASB) functionality

Today, organizations have moved most, if not all, of their applications and data to the cloud, largely through the use of SaaS applications, leading to numerous access and security compromises. On their own, SaaS applications offer a limited set of authentication and authorization options. Many of the SaaS application vendors believe they are providing "good enough" security but far too often we see news headlines spotlighting breaches revealing end user credentials and private data. Solutions that don't allow for advanced authentication and device trust are less likely to stand up to today's advanced threats and cyber criminals.

Banyan's CASB (Cloud Access Security Broker) functionality delivers excellent SaaS application security providing consistent security and access policies, along with unified visibility regardless of where the application or resource lives.

The Obstacles

So many SaaS applications

- There are consumer and enterprise SaaS applications for every job function imaginable, literally thousands available globally.
- Not all SaaS applications are created equally, and switching is easy. While an application might be chosen based on vendor reputation, location, price, etc., if it doesn't work out, the business can easily switch.

Basic authentication/authorization methods

- Authentication is often limited to a simple username and password. Unfortunately, passwords are often reused so when a breach occurs in one SaaS application, passwords for other SaaS applications are exposed.
- Authorization is very binary in SaaS applications. Most applications allow for full access once authenticated. Advanced authentication, using technology like continuous authorization and device identity and posture, is often not even an option.

Limited visibility

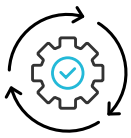
- End-user traffic flows directly to a SaaS application keeping most organizations in the dark as to what applications their workers are using.
- Obtaining visibility into who is accessing which applications and what they are doing once inside often results in organizations building separate siloed tools for each SaaS application.

Getting started with SaaS Application Security

Getting started is simple:

- Enable multi-factor authentication (MFA) for all resources and services.
- Enable device identity and device trust policy for all resources and services.
- Create Access Policy for the SaaS applications that are used by employees and third parties.
- Enable Source IP validation to ensure that only devices coming from the configured source are attempting to access the SaaS application.
- Enable Service Tunnel Discovery to find "shadow IT applications" that shouldn't be used or to discover ways to further secure applications your workers are authorized to use.

Banyan SaaS Application Security Benefits



Consistent authentication/ authorization

- End users don't have to remember which log in is required for each SaaS application
- No surprises when it comes to the how Device Trust affects authorization

Layered security and controls

- Enable Source IP validation and restrictions to ensure only users from known IPs attempt access
- Protect communications by leveraging Service Tunnels and ensure safe devices with EDR

Enhanced Visibility

- Single view of all SaaS application access
- Insights into user, device identity and posture, and time for all SaaS application activity

Key CASB features for Advanced SaaS Application Security

- Control access to SaaS applications while enhancing authentication and authorization
- Enable SAML and OIDC with other Identity Providers (IdPs), device identity and posture for authorization
- Enable Source IP validation using domain-aware Service Tunnels
- Enable/disable, step-up/step-down access to SaaS applications based on chosen parameters

About Banyan Security

Banyan Security provides secure, zero trust "work from anywhere" access to applications and resources for employees and third parties while protecting them from being phished, straying onto malicious web sites, or being exposed to ransomware. A Flexible Edge architecture enables rapid, incremental deployment on-premises or in the cloud without compromising privacy or data sovereignty. A unique device-centric approach intelligently routes traffic for optimal performance and security delivering a great end user experience. Banyan Security protects workers across multiple industries, including finance, healthcare, manufacturing, and technology. To learn more, visit www.banyansecurity.io or follow us on Twitter at @BanyanSecurity.

BANYAN SECURITY

Banyan Security, Inc. | +1 415-289-9414 | www.banyansecurity.io