BANYAN

WHITEPAPER | AUGUST 2019

Zero Trust Remote Access Platform

Secure Remote Access to Applications and Servers Hosted in Hybrid and Multi Cloud Environments

TABLE OF CONTENTS

OVERVIEW

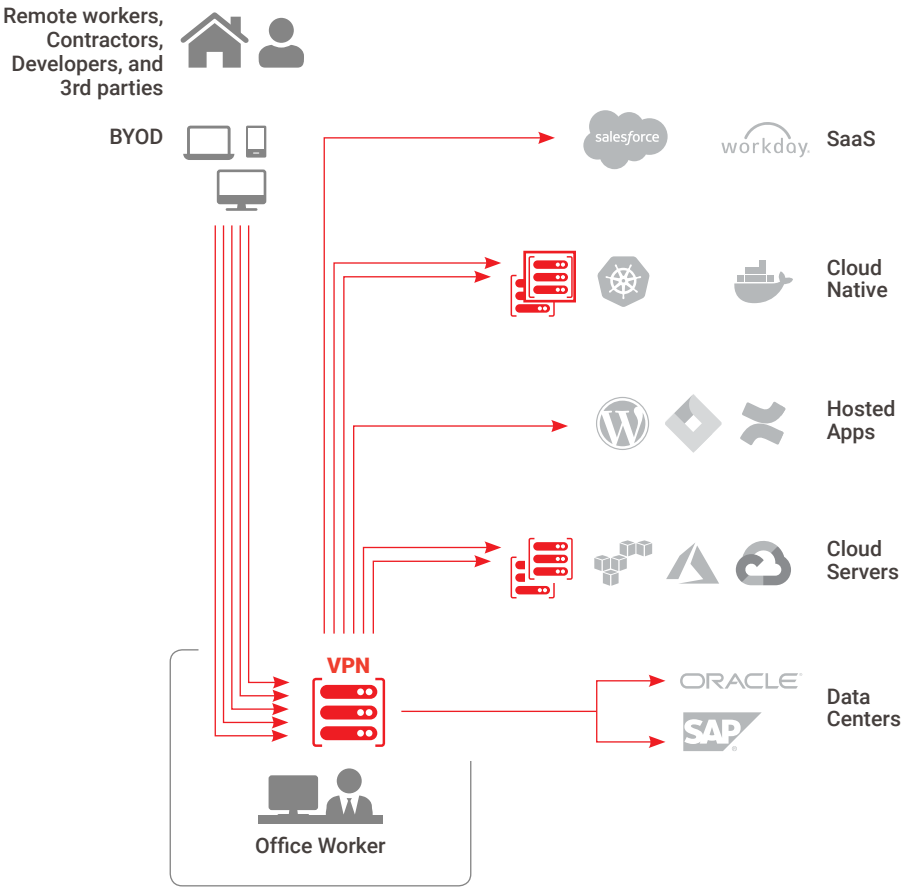
As applications and infrastructure migrate to the cloud, the traditional VPN and DMZ based perimeter security model for remote access breaks down, placing critical limits and risks on a company. The Banyan Continuous Zero Trust Platform has been designed from the ground up for today's hybrid- and multi- cloud environments, delivering the seamless access experience that users want and the enhanced security that enterprises need.

Banyan delivers Zero Trust Network Access by shifting control away from the network perimeter and network layer to the application layer. Banyan uses a sophisticated trust scoring framework, based on user, device, and application context, so that access to corporate resources can be continuously authorized via a contextual policy engine regardless of the user's network location. A cutting-edge access mesh architecture enables the solution to scale almost infinitely across any infrastructure —on-premises, hybrid-cloud or multi-cloud. Organizations deploy Banyan today to accelerate cloud adoption, reduce security risk and exposure, regulate contractor access and to secure developer access to hybrid-cloud infrastructure.

THE CHALLENGE

VPN-based Security Poses Unbounded Access Control, Costs, and Risks

Providing secure remote access is a core requirement for all businesses. Organizations have traditionally solved this problem by deploying Virtual Private Network (VPN) technology, where users launch a VPN client to join a trusted network in which applications run. Now, as internal applications and infrastructure move to IaaS clouds like AWS and Azure, and SaaS clouds like Salesforce and Workday, and remote users access them from their favorite cafes and multiple devices, traditional VPNs place critical limitations and introduce risks to secure network access.



Traditional VPN-based Security

Security teams **lack visibility, control, and auditability** on the broad network access that VPNs grant

Operations teams struggle to roll out, automate, and maintain **complex network architectures**

Users suffer from **slow connections** due to long routes with extra hops

BANYAN ZERO TRUST AUTHORIZATION

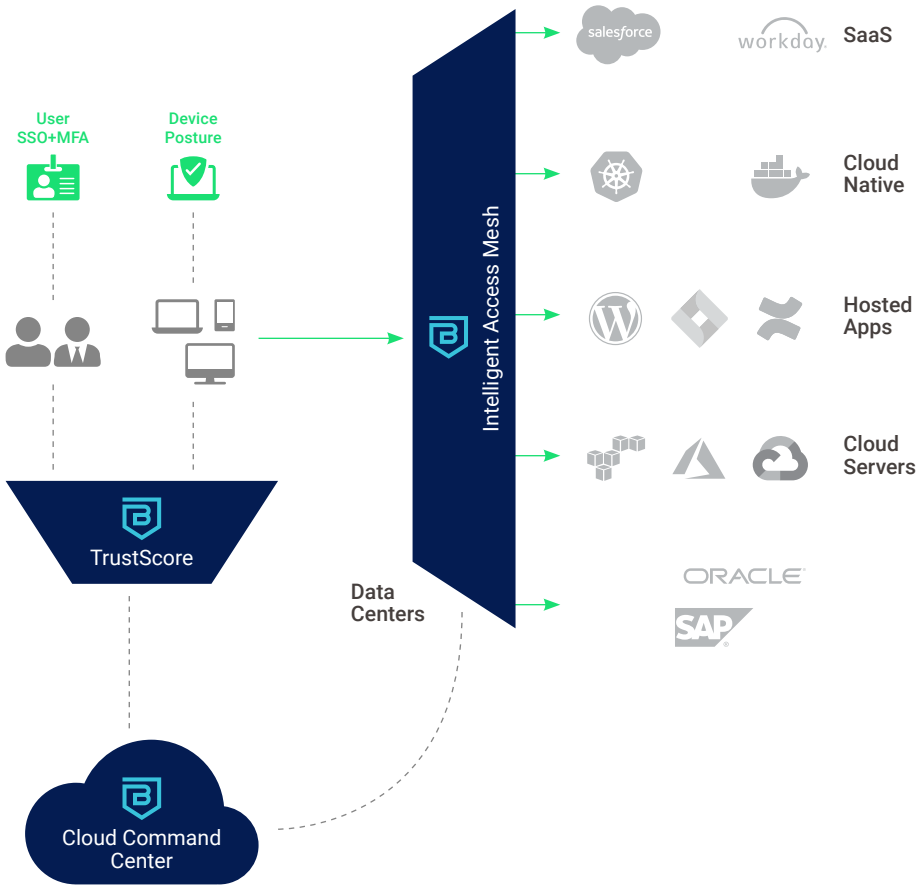
Protect Applications and Infrastructure with Continuous, Least-Privileged Access

Inspired by the Google BeyondCorp enterprise security model, Banyan shifts access controls from the network perimeter to individual users and devices, and the services and hosts they access. Banyan uses sophisticated trust scoring based on user, device, and application context, so IT and Security administrators can create simple yet powerful contextual access policies. All access to enterprise resources is then fully authenticated, fully authorized, and fully encrypted, regardless of network location - be it a cloud cluster, an enterprise location, a home network, or a coffee shop.

Centralized command center enables fine-grained **security policies** and reporting

Operations teams use automation to manage the software-based **access mesh**, designed for today's **hybrid clouds**

Users get secure, performant, and **direct connectivity** based on **device and user trust scoring**



Banyan Zero Trust Network Access Security

THE BANYAN DIFFERENCE

3 Core Principles of Zero Trust

Banyan's unique implementation of 3 core principles – Distributed Enforcement, Quantified Trust, Continuous Authorization —delivers best-in-class Zero Trust Network Access for the modern enterprise.

Distributed Enforcement

Enforce policies in close proximity to applications for better security, scalability, and performance

Quantified Trust

Compute real-time risk profiles for every entity requesting access, regardless of network location

Continous Authorization

Apply granular policies to ensure least-privileged access to all sensitive corporate resources

BANYAN CAPABILITY	CUSTOMER BENEFIT
Deploys a distributed trust model in any enterprise environment	**Tighter security for critical internal assets** → Applications are invisible to untrusted devices → Users do not have broad access to the network → Unified controls for HTTP, SSH, RDP and inter-service communications
Employs a Trust Score based framework for Continuous Authorization	**Manage controls based on user context and behavior** → Users get fast, direct access to applications → Quickly create policies using pre-built templates → Imbibe signals from UEBA and EDR tools
Architected for Multi- and Hybrid- Cloud environments	**Simplified network operations** → Employ automation and clouds' native capabilities → App segmentation without network segmentation
Enables Customers to Retain Ownership of their Data Plane	**Maintain security and compliance across hybrid clouds** → Consistent policies across IaaS, SaaS and on-prem → Don't hand over crypto keys or admin rights to 3rd parties
Utilizes standard security protocols – Mutual-auth TLS and OpenID Connect	**Accelerate enterprise-wide adoption** → Avoid vendor lock-in → Future proofed for Kubernetes and microservices

USE CASES

Enterprises deploy Banyan to reap the benefits of a highly dynamic workforce and distributed cloud applications while still delivering the high level of security they require.

Accelerate Cloud Adoption With Zero Trust Access for Web Applications

- → Deliver security along with a great user experience; get rid of fragile device clients
- → Single console for policy management, no matter which cloud, application, or user
- → Utilize Trust Scoring and apply fine grained access policies to ensure least-privileged access to all sensitive corporate applications

Secure Development Tools and SSH/RDP Server Administration

- → Seamlessly add controls to resources used by DevOps and Engineering teams like development sites, self-hosted tools and SSH/RDP access
- → Reduce reliance on insecure static credentials; instead, use short-lived X509 and SSH client certificates or JWT tokens with a specific scope and context tied to the user's entitlements

Deliver Secure, VPN-free Access to On-premises Resources

- → On-premises resources are invisible to unauthorized users and devices, and users are never placed on the network
- → Enable contractors to use enterprise resources from unmanaged devices without exposing your internal networks
- → Drastically reduce the complexity of network and security architectures

Transparent TLS Encryption and Access Controls for Service-to-Service Traffic

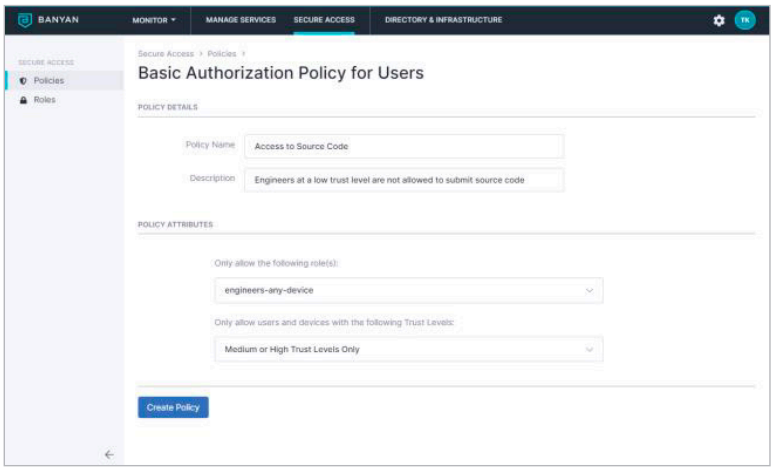
- → Extend Zero Trust security principles to "east-west" communications and microservice deployments
- → Leverage native integrations with infrastructure orchestrators (AWS/ Azure, Kubernetes/Docker, etc.,) to insert security controls without impacting developer productivity

ARCHITECTURE

3 Core Components

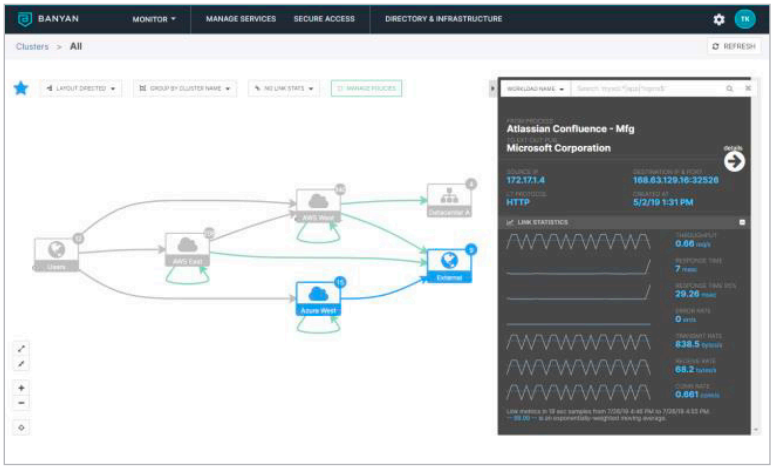
1. Cloud Command Center

Centralized dashboard and policy engine to provide least-privileged access to sensitive corporate resources



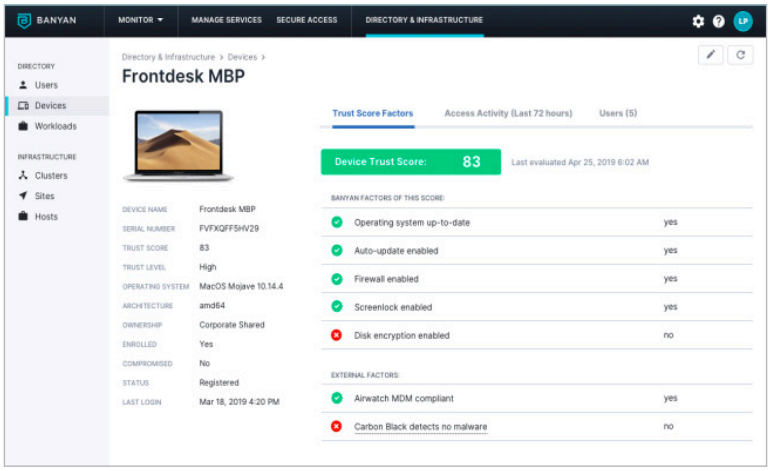
2. Intelligent Access Mesh

A multi-cloud identity-aware access proxy that securely cloaks applications and servers from malicious attacks or inadvertent exposure and also provides real-time enforcement of accessibility due to policy infractions



3. Trust Score

Real-time risk metric computation algorithms, continuously updated to capture user/device context and behavior



Cloud Command Center

The Cloud Command Center provides IT Admins and Security teams a central dashboard and policy engine from which to manage access to all their internal applications and services.

Command Center functionality falls into 4 major categories:

- **User & Device Inventory** - Meta-inventory that normalizes user and device information from multiple enterprise sources
- **Service & Host Registry** - Meta-inventory that normalizes service and host information from multiple clouds
- **Trust Provider** - OpenID Connect (OIDC) and Public Key Infrastructure (PKI) workflows for streamlined authentication of users, devices and services
- **Policy Engine** - Access control management that provides service-level authorization to enterprise applications

Banyan Cloud Command Center empowers administrators to write authorization policies in easy-to-understand terms using Roles and Trust Levels.

Policies can be as fine-grained as needed:

- Global rules are coarse-grained affecting all services and resources; e.g., “Devices at a low trust level are not allowed to submit source code”
- Service-specific rules apply to a given service or host and typically involve assertions about the user; e.g., “Access to a finance application is restricted to full-time and part-time employees in the finance group using managed devices”
- Resource-specific rules manage access at the API level, typically for sensitive development services; e.g., “Admin APIs are restricted to IT operations team members using managed devices at a high trust level”

The Command Center provides sophisticated API-level analytics capabilities for visibility into who has access to what, when, and where as well as GDPR, HIPAA, and PCI compliance. These logs and reports can be automatically streamed to your SIEM tools. The Cloud Command Center can be delivered as a Banyan managed SaaS offering or deployed on-premises.

Intelligent Access Mesh

Security policy enforcement is fully distributed to the Intelligent Access Mesh, a set of lightweight network-transparent reverse proxies deployed in the customer datacenter and cloud environments. Banyan's mesh architecture ensures all traffic is encrypted end-to-end, and that no man-in-the-middle networks can ever decrypt your data or monitor connections.

Every node of the Intelligent Access Mesh is identity-aware, using standard Mutual-auth TLS and OpenID Connect authentication protocols, so that access is granted only to requests from authorized entities. Sensitive corporate resources are securely cloaked from prying eyes.

The enforcement layer can be deployed in multiple form factors:

- → Host agent, deployed on Linux and Windows hosts
- → Sidecar container, deployed within a Kubernetes pod
- → Elastic access tier, deployed as managed appliances in your cloud or on-prem clusters
- → Authentication interceptor, managed by Banyan in the cloud, to enforce policies on federated authentication requests

Banyan's Intelligent Access Mesh has been designed to leverage Public Cloud platform's perimeter services (such as AWS Load Balancers) wherever available. Each node of the mesh is capable of elastically scaling based on load and securely bootstrapping itself into the global Intelligent Access Mesh, making it perfect for enterprise environments that require both convenient management as well as high security.

Because Banyan's Intelligent Access Mesh provides enforcement for all TCP/IP protocols and uses the same controls for workload entities as well as user entities, it can be used to transparently encrypt service-to-service traffic and for microsegmentation.

Trust Score

Banyan gives every organization the ability to configure a custom Trust Scoring framework based on how trust is distributed from the network perimeter to individual devices/users and hosts/ services.

Banyan ingests and processes 100s of device, user, and access activity factors for its Trust Score computations. Some examples of factors collected include:

- **Users** – whether and how a user was authenticated, what groups the user belongs to, what APIs were being accessed, etc.,
- **Devices** – apps running, patch level of the operating system, screen lock settings, the use of disk encryption and firewalls, etc.,

Banyan's internal algorithms then use a variety of machine learning and statistical techniques —clustering, change-point detection, regression, and classification and Bayesian inference– to synthesize factors related to users, devices, and their access activities in order to compute user and device Trust Scores.

Banyan provides a native App for desktop platforms (MacOS, Windows) and mobile platforms (iOS, Android) that display the user's Trust Score and provides remediation instructions. Organizations use the Banyan App to empower their employees to maintain a strong security posture across all their devices.

In addition, Banyan provides well-documented APIs and pre-built integrations so organizations can leverage their existing systems of record for Trust Scoring:

- **Users** – Single Sign-On Providers (e.g., Okta, Active Directory) and User Entity Behavior Analyzers
- **Devices** – Enterprise Endpoint Managers (e.g., Airwatch, Zenprise) and Endpoint Detection & Response tools (e.g., CrowdStrike, CarbonBlack)
- **Services** – Orchestrators (e.g., Chef, Ansible, Docker, Kubernetes) and Cloud Platforms (e.g., AWS, Azure, GCP, VMware)

Conclusion

Banyan Security has created a platform comprised of three components: the Intelligent Access Mesh which provides distributed enforcement, securing applications on premises, IaaS or SaaS; Trust Scoring, which integrates with security tools to calculate and assign a quantifiable trust metric to any entity (users, devices, or other applications) that require access to corporate resources; and finally a Cloud Command Center which provides IT and Security teams with a single pane of glass to write continuous authorization security policies to provide complete visibility to all access events. Together these three elements combine to create a comprehensive Zero Trust security framework for all enterprise environments.

The Banyan Security Zero Trust Network Access platform uniquely allows for flexibility, control and security because it allows teams to customize the policies to best suit the needs of the organization today and tomorrow.

ZERO TRUST HERO

Visit www.banyansecurity.io

BANYAN

Banyan helps secure the modern enterprise by delivering continuous Zero Trust Access for hybrid and multi-cloud environments. Modeled after the BeyondCorp architectural framework, Banyan's Continuous Zero Trust Platform replaces legacy remote access VPNs with a least privilege, network independent, contextual remote access solution. Utilizing innovative Trust Scoring powered by machine learning, Banyan ensures both users and devices are authenticated and trusted before authorizing granular access to sensitive corporate resources. Banyan's distributed, highly scalable platform is currently used by enterprises across verticals including Adobe, SAP, Veeva, BlueVoyant and Byton.

To learn more, visit www.banyansecurity.io.

www.banyansecurity.io | 415.498.0635 | info@banyansecurity.io | 300 Brannan St., Suite 309, San Francisco, CA 94107