

SOLUTION BRIEF

Secure Remote Access for Engineering Teams

The Banyan Security Platform

The Challenge

The majority of employees are now working remotely, often having to use decades-old Virtual Private Network (VPN) technology to get by. The exploding dependency on VPN infrastructure only exacerbates its numerous security, performance, manageability, and user experience challenges, and nowhere are they more pronounced than with software development organizations.

Engineers need to use SSH and RDP to connect, access, and control data and resources on remote hosts as if they were doing it locally. Secure, transparent access to hosts, servers, and apps whether on-premises, privately hosted, private- and public-cloud, or SaaS-based is a baseline requirement. But, the collection of VPNs, bastion hosts, firewalls, and authentication agents used to manage such access makes for a complicated user and admin environment that causes productivity problems.

A well-architected solution that supports enterprise-scale distributed work, performed from a myriad of managed and unmanaged devices, in uncontrolled environments, with rock-solid security and high performance is required.

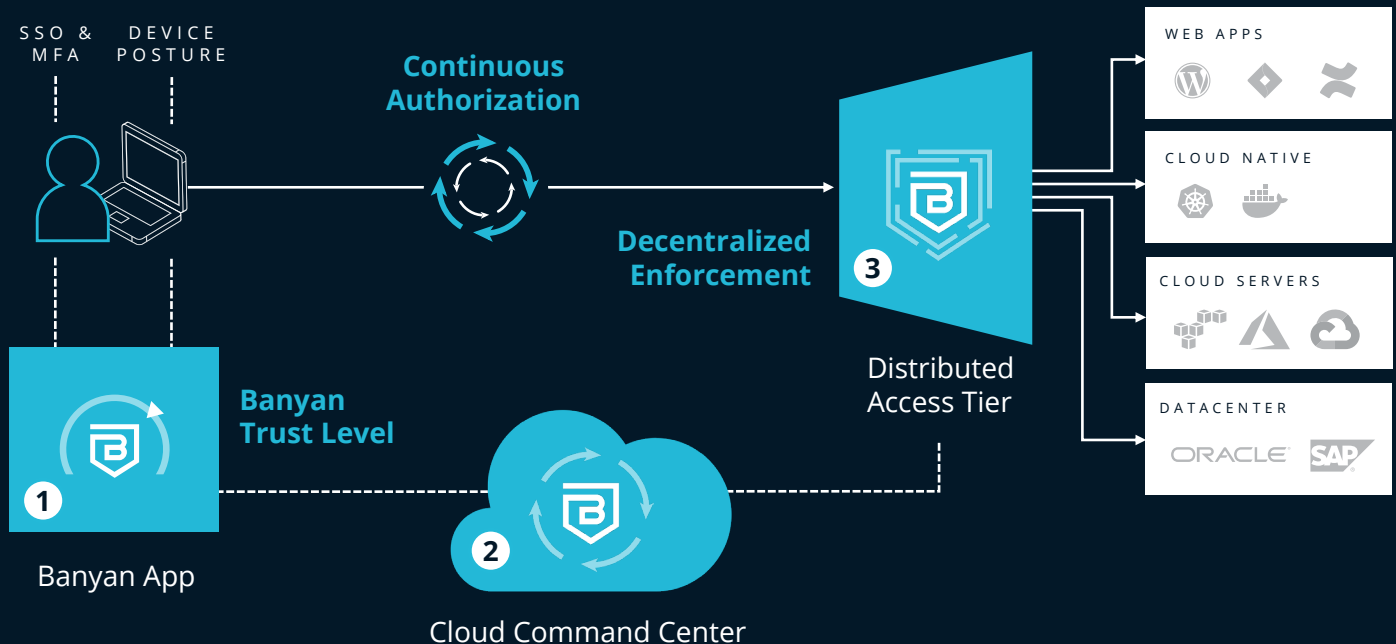
Banyan Security provides a modern approach to server access that is fundamentally more secure and easier to manage than today's typical setups. Following a zero trust security model, the user and device are explicitly authenticated with access only granted to a specific resource (without broad network access). By leveraging the organization's existing identity provider for authentication and issuing short-lived certificates with user entitlements, Banyan sets up connectivity on-demand and eliminates the risk associated with static passwords and credential leakage. Best of all, Banyan's real-time Trust Level enforcement allows for dynamic security policies that can be customized based on resource sensitivity.

Banyan's Key Benefits

- ✓ No more choosing between security and productivity – the Banyan Security Platform delivers both at scale
- ✓ Consistent, easy connection to resources across complex software engineering environments, including one-click Zero Trust SSH, RDP, and Kubernetes access
- ✓ Replaces complex VPNs, bastion hosts, firewalls, and authentication agents
- ✓ Integrates with existing security stack investments, maximizing value and tightening security
- ✓ Granular security with Role-Based Access Controls (RBAC) and automatically-provisioned short-lived certificates

Banyan Security Zero Trust Remote Access

How It Works



1

Banyan App

The Banyan Security trust score measures user and device security posture similar to how credit scores reflect creditworthiness. When a user's Trust Level drops below a policy-specified level, access is denied or terminated if already connected. App also provides a list of accessible hosts and services.

2

Cloud Command Center

A SaaS platform that lets you write simple but granular policies and generates trust tokens and short-lived certificates for continuous authorization.

3

Distributed Access Tier

Simply deployed, cloud-integrated, smart reverse proxies running alongside applications enabling end-to-end security and direct access, bypassing third-party clouds.

Problems Solved



One-Click Access to Heterogeneous Resources

- > Secure remote access to on-premises, hybrid, and multi-cloud hosts, servers, and applications without the need for VPNs and bastion hosts
- > One-click Zero Trust SSH, RDP, and Kubernetes access
- > No choke point traffic routing, removing latency and geographic POP issues, improving performance for all



Reduce Administrative Costs

- > Easily add and manage users, policies, hosts, servers, and apps in your remote access environment
- > Contractors, consultants, and third-parties are easily accommodated, either as members of a group or handled individually for a particular role
- > Users receive guidance to self-remediate security issues that cause TrustScore changes – no helpdesk tickets, unproductive waiting, or increase in IT workload
- > APIs bring Infrastructure as Code (IaC) benefits for fast, consistent, and accountable infrastructure management



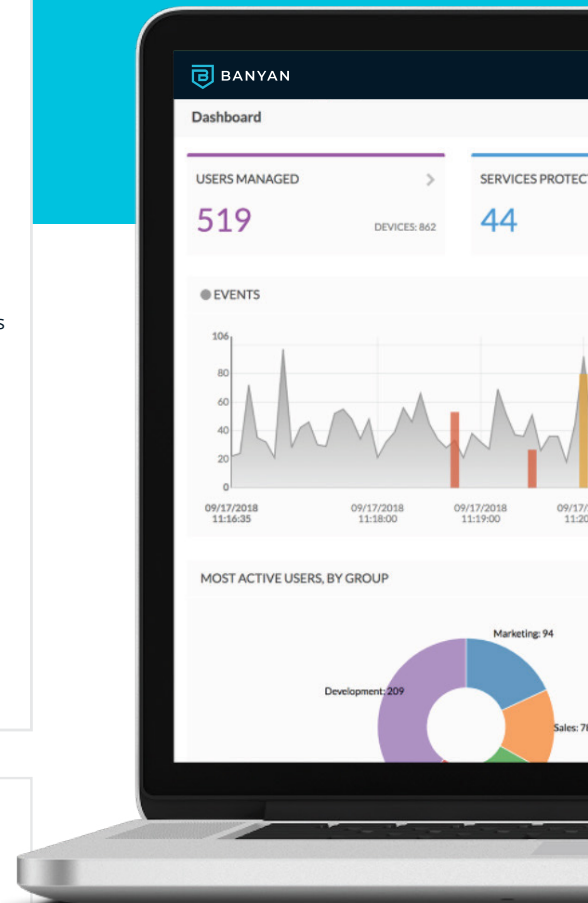
Granular, Continuous Management of Security Risk

- > Access requests are continuously evaluated in the context of user, device, and resource – access can be automatically withdrawn when a user's security posture worsens
- > Banyan applies a least-privilege strategy, strictly enforcing policy-based access to all hosts, servers, and apps
- > Integration with identity providers, device managers, and endpoint detection and response tools leverages existing security investments



Easily Audit Resource Access and Demonstrate Compliance

- > Banyan provides comprehensive user, device, and access logs, satisfying internal audit, regulatory, and compliance needs
- > Demonstrably control and limit access to sensitive information
- > Identity provider integration and device trust enforcement eliminates “shadow IT”



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](https://twitter.com/BanyanSecurity).