

# Zero Trust Remote Access Platform

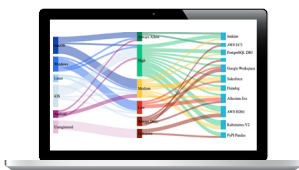
**Provide secure work from anywhere capabilities for employees, developers, and contractors**

Banyan Security's Zero Trust Remote Access platform is a Zero Trust Network Access (ZTNA) solution that protects company resources by enabling least-privilege access to hosted applications and infrastructure based on real-time contextual factors including user and device trust scoring and resource sensitivity. In short, Banyan is safely and securely enabling "Work From Anywhere" for the modern and, now largely remote, enterprise.

Infrastructures grow ever more complex, with applications spread across on-premises, hybrid, and multi-cloud environments. Traditional network-centric solutions like VPNs have been put to the test and revealed significant performance, usability, and systemic security issues that band-aids cannot fix. To keep up with these realities, a scalable and comprehensive approach to secure remote access is required.

The Banyan Zero Trust Remote Access platform leverages a robust Trust Scoring methodology during initial authentication and continuously re-authorizes access based on real-time contextual information. The Banyan Distributed Access Tier cloaks all corporate assets and provides granular or global, secure access within policy guidelines. The Cloud Command Center provides clear visibility and audit capabilities for IT teams to set and monitor those policies and respond in real-time to changing trust scores.

## Why Banyan



### Trust-Based Access Control

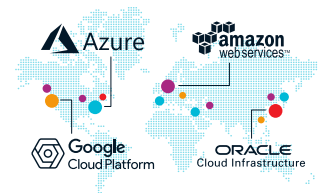
Fine-grained controls use Banyan's TrustScore-powered policy engine, enabling continuous authorization based on user and device trust, device security posture, and resource sensitivity.

Banyan aligns the risk of the request with the sensitivity of the resource, revoking access mid-session if warranted.



### One-Click Infrastructure Access

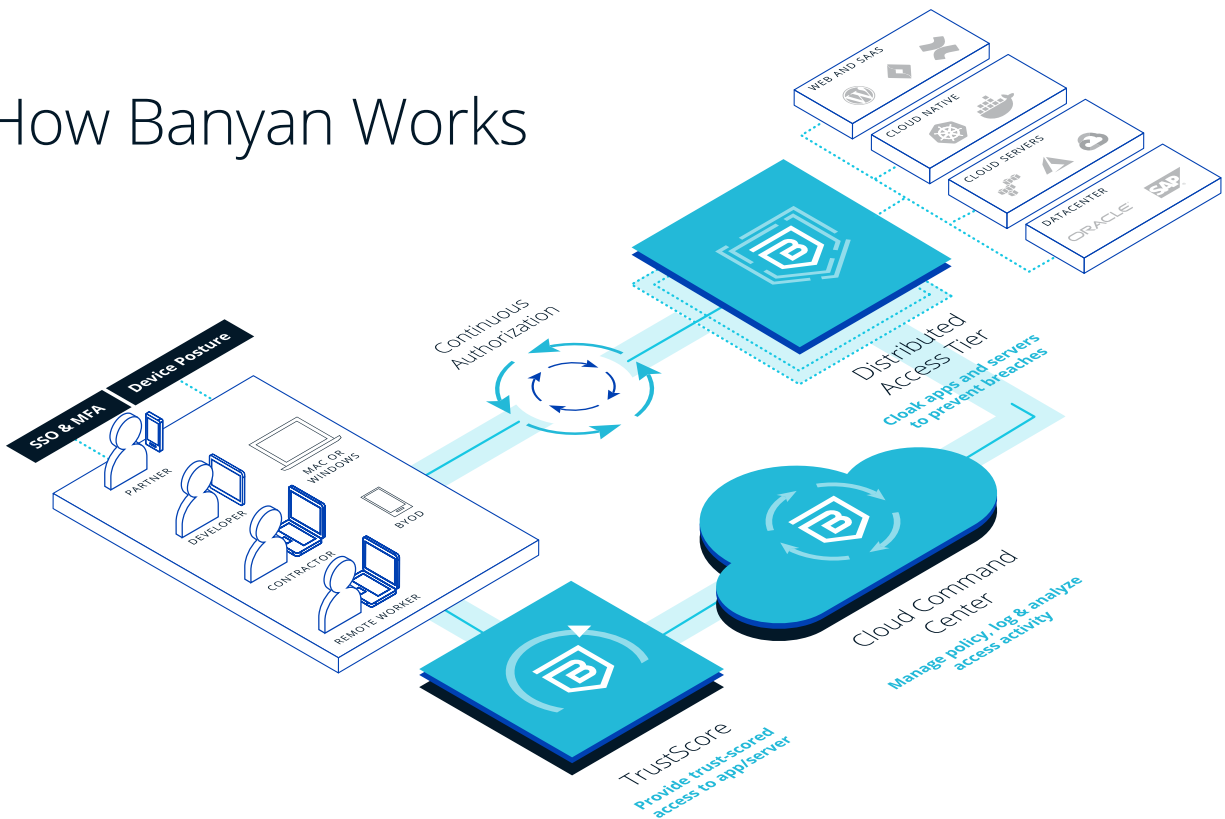
Banyan integrates with IaaS and PaaS environments providing one-click access to developer resources such as SSH/RDP servers, Kubernetes, databases, and more. Least privilege access allows differentiated access for FTEs and third parties alike that is a snap to deploy, administer, and audit.



### The Enterprise Edge

Banyan's mesh architecture extends security controls to distributed assets, spanning all environments and protocols. The cloud-native approach leverages the public internet without network tunnels or MITM clouds resulting in a highly performant, yet scalable solution that doesn't risk data privacy.

# How Banyan Works



## Zero Trust Access Use Cases

### Replace Legacy VPN

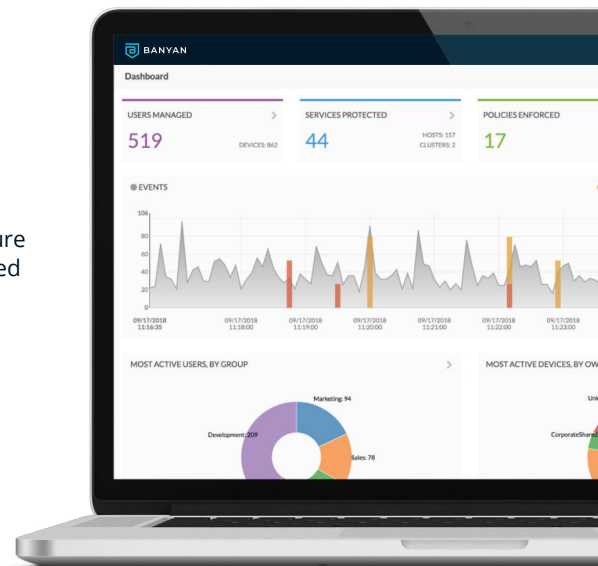
Protect company resources by enabling least-privilege access to specific applications and servers based on combined real-time contextual factors including user and device trust scoring and resource sensitivity.

### Provide Consistent, Easy Access for Engineering Teams

Provide user-friendly, VPN-free, least-privilege access to key DevOps infrastructure with one-click access to SSH/RDP and Kubernetes environments, as well as hosted applications like GitLab, Jenkins, and Jira whether on premise or in the cloud.

### Support BYOD and Third-Party Access

Enable BYOD without needing Mobile Device Management (MDM) or Unified Endpoint Management (UEM) installed on each device. Corporate assets are continually protected while delivering an enhanced user experience that doesn't require control of their preferred devices.



## About Banyan Security

Banyan Security provides secure, zero trust "work from anywhere" access to infrastructure and applications for employees, developers, and third parties without relying on network-centric solutions like VPNs. User and device trust scoring along with continuous authorization and least privilege access delivers the highest level of protection without sacrificing end user productivity. Banyan Security currently protects tens of thousands of employees across multiple industries, including finance, healthcare, manufacturing, and technology. To learn more, visit [www.banyansecurity.io](http://www.banyansecurity.io) or follow us on Twitter at [@BanyanSecurity](https://twitter.com/BanyanSecurity).