

ZERO TRUST NETWORK ACCESS

7 Considerations for Implementing ZTNA



INSTALLATION

Quick ROI
Simple 15 minute deployment



INTEGRATION

Integrates easily with existing security tools



IAM

{okta}



Azure Active Directory

MOBILE DEVICE MANAGER

mobileiron

airwatch

EDR TOOLS

Carbon Black.

CROWDSTRIKE

UEBA

elastic

splunk>



ACCESS CONTROLS

Granular policy engine,
TrustScored least
privileged access
control / Real-time event
monitoring, alerting
and policy enforcement



ARCHITECTURE

Organizations own their data
plane, no a man-in-the-middle
CDN cloud architecture



USE CASES

VPN Alternative for Zero Trust Access

Zero Trust Access for DevOps

Zero Trust Access for BYOD & 3rd Parties

Download our latest datasheet



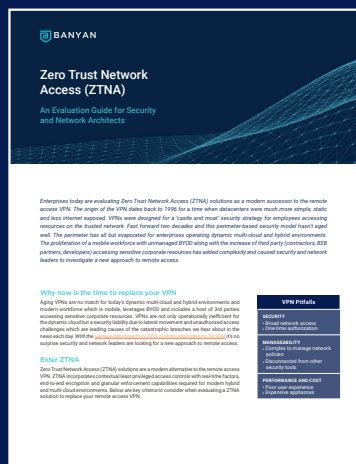
USER EXPERIENCE

Frictionless access does not
interfere with end users'
existing workflow



NETWORK

Requires no changes to existing
network infrastructure



Banyan has developed a comprehensive ZTNA Evaluation Guide and Checklist for your use and reference when making decisions about your Zero Trust Network Access implementation.



BANYAN

Banyan Security provides secure, zero trust "work from anywhere" access for employees, developers, and third parties without relying on network-centric solutions like VPNs. User and device trust scoring along with continuous authorization ensures the highest level of protection while providing seamless and productive access to hybrid and multi-cloud apps, hosts, and servers. 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 or follow us on Twitter at [@BanyanSecurity](https://twitter.com/BanyanSecurity).

www.banyansecurity.io | 415-289-9414 | info@banyansecurity.io | 142 Minna Street, San Francisco, CA 94105
©2021 Banyan Security, Inc. All rights reserved.