ACCELERATING PRODUCT GROWTH WITH SECURE ZERO TRUST REMOTE ACCESS

Banyan Security has evolved into a leading Zero Trust Network Access (ZTNA) platform, trusted by enterprises across the globe. With its acquisition by SonicWall, the company has expanded its footprint to over 100,000 customers, strengthening its cybersecurity capabilities. The organization's core mission is to enable seamless, secure, and scalable remote access through continuous authentication, identity-aware proxies, and real-time risk assessment.

CYBERSECURITY IN THE MODERN ERA

As organizations increasingly operate in a digital-first world, cybersecurity has become a paramount concern. Traditional security models that rely on perimeter-based defense mechanisms, such as Virtual Private Networks (VPNs) and firewalls, have been found lacking in today's threat landscape.

Enterprises need a modern, scalable, and adaptive security approach that can handle evolving risks while enabling seamless remote work. This is where Zero Trust Network Access (ZTNA) emerges as a critical solution.

KEY CHALLENGES

THE LIMITATIONS OF PERIMETER-BASED SECURITY

Traditional security models assumed that once a user was inside the network perimeter, they could be trusted.

VPNs, while encrypted, created a single point of failure—if compromised, attackers could move laterally across the network.

Organizations lacked visibility into what users did once they gained access, leading to potential data breaches.

Illustrative Example

Imagine an enterprise with multiple office locations. Employees in different regions connect to internal systems using VPNs. However, once a hacker gains access to one location's VPN credentials, they can move freely within the company's network, accessing sensitive information such as payroll records and customer data.

Because perimeter-based security assumes all internal users are trusted, the system fails to recognize unauthorized access until it's too late.

SCALABILITY AND PERFORMANCE BOTTLENECKS

As remote work surged, VPNs struggled with high latency and poor performance, leading to employee dissatisfaction.

Centralized security gateways created congestion, especially as organizations expanded globally.

Banyan Security needed to migrate its identity systems and expand its infrastructure to handle the fast-growing number of users.

Illustrative Example

A software engineer in India working for a U.S.-based firm needed to access development environments in California. Each request had to be routed through the company's VPN gateway in the U.S., significantly slowing down performance.

During peak hours, the increased load on the gateway resulted in frustrating delays and reduced productivity.

LACK OF GRANULAR ACCESS CONTROL

Existing security models lacked fine-grained policy enforcement.

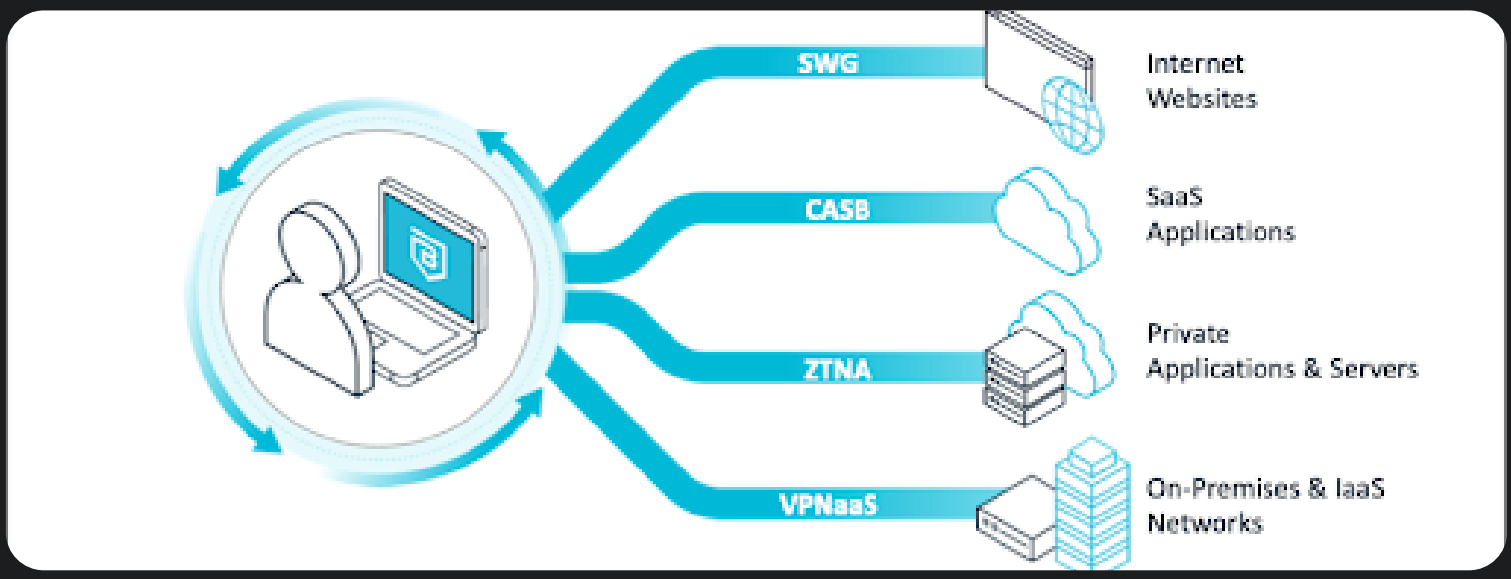
Organizations needed contextual access control based on device security posture, user identity, and geolocation.

Ensuring secure access for remote employees required continuous authentication and risk assessments.

Illustrative Example

An employee logging in from a company-issued laptop should ideally have more access rights than someone using a personal device from an unknown location.

Without granular control, both users receive the same level of trust, exposing critical resources to potential security threats.



THE SOLUTION

Implementing Zero Trust Network Access (ZTNA)

Identity-Aware Proxy for Secure Access

Banyan Security implemented a proxy-based architecture to validate every user request before granting access. Instead of trusting internal or external users by default, it enforced continuous verification through Identity Providers (IDPs) like Google, Azure AD, and Okta.

Mutual TLS (mTLS) for Device Authentication

Unlike traditional VPNs that authenticate only the user, Banyan Security used mutual TLS (mTLS) to verify both the user and their device. Only devices meeting security policies, such as updated antivirus and the latest OS patches, were granted access.

Granular Policy Enforcement with Trust Scores

Every user and device received a dynamic trust score, enabling real-time access decisions. Organizations could also enforce region-based restrictions, blocking access from high-risk geographies.

DNS Filtering for Phishing and Malware Protection

Banyan Security introduced DNS filtering to prevent employees from accessing malicious websites. Enterprises could create policies to block social media sites or restrict unverified domains.

Scalable Infrastructure with Global Points of Presence (PoPs)

Banyan Security deployed PoPs in seven global locations for seamless connectivity. Users were routed to the nearest PoP for low latency and high availability. New features like SCIM integration, global edge, and granular trust control further strengthened security.

THE RESULTS

90% Reduction in Security Breaches

Eliminating VPN-based lateral movement reduced the attack surface.

50% Faster Remote Access

Identity-aware proxies and regional PoPs boosted response times and productivity.

Accelerated Product Growth

Simplified VPN transition, accelerating adoption and market growth.

Seamless Customer Onboarding

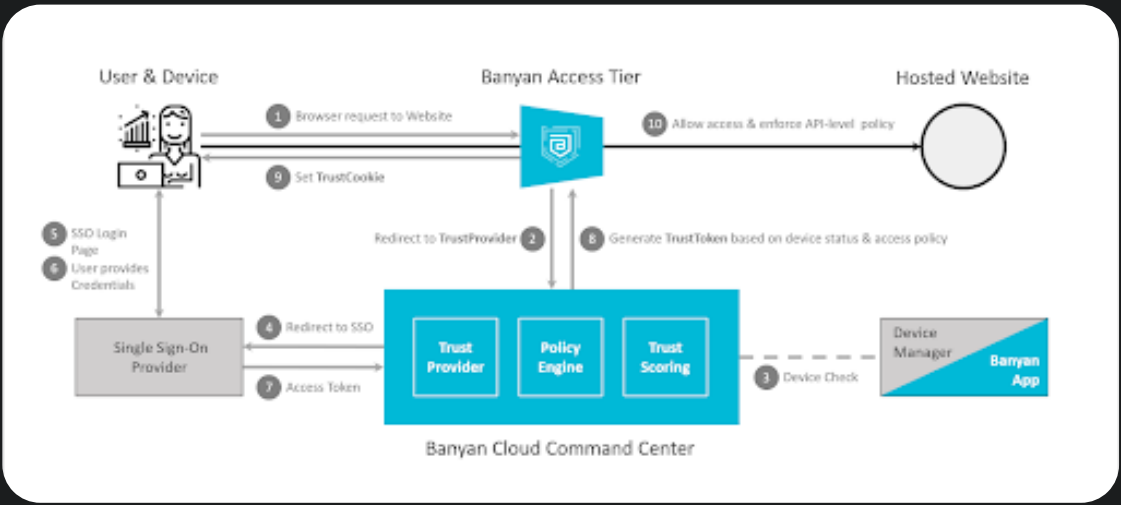
Automated provisioning cut onboarding time, improving efficiency.

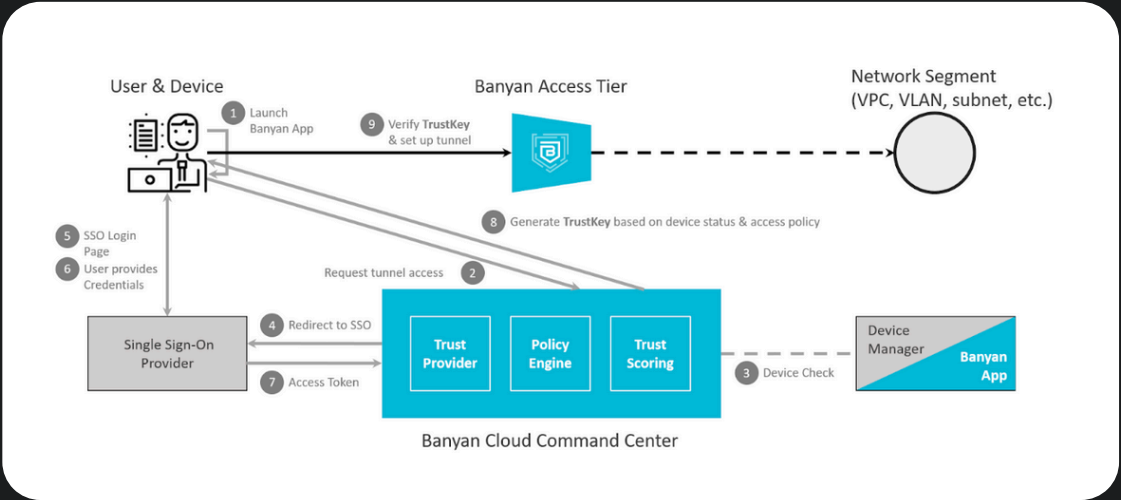
Enhanced Security and Threat Protection

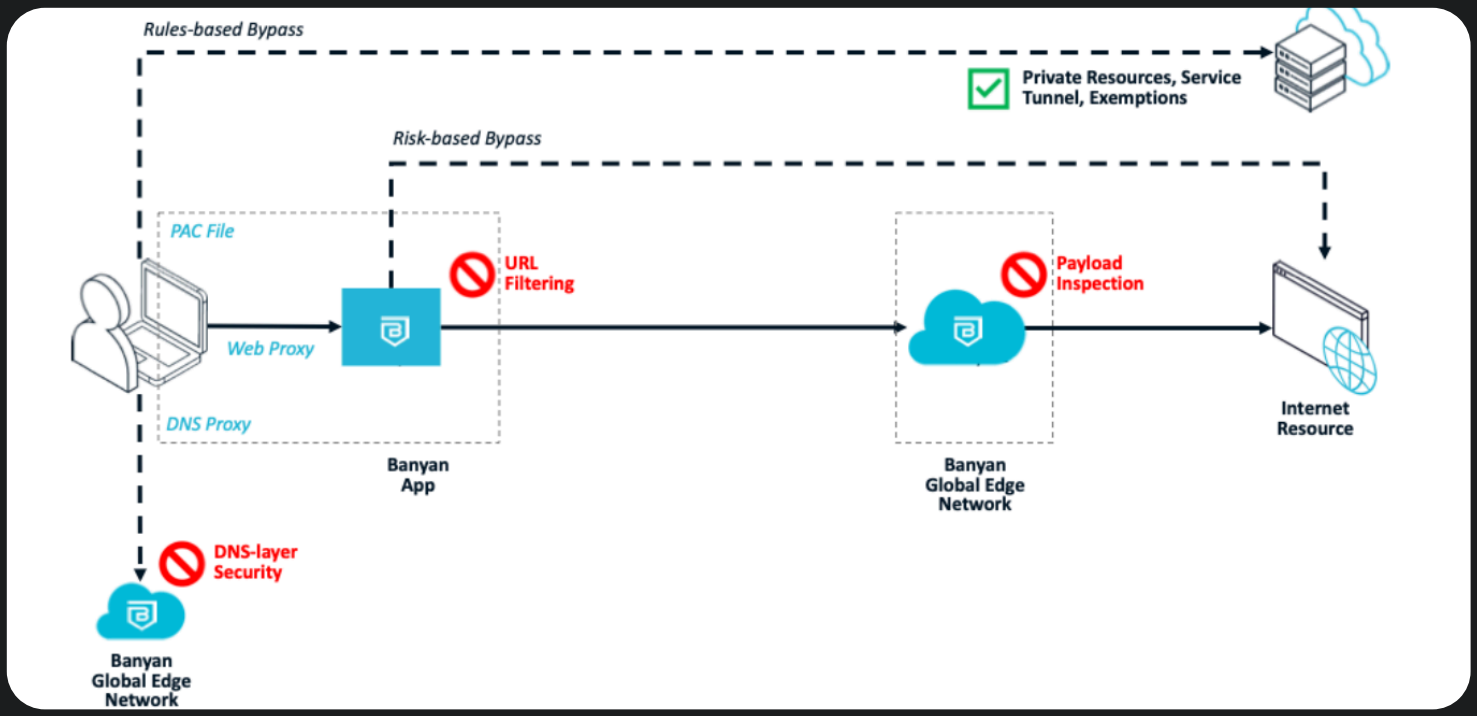
Internet Threat Protection blocked phishing and malware, securing data.

Scalability for Growth

Integrated with SonicWall's 100k+ customers, ensuring reliability & scalability.


User & Device
Banyan Access Tier
Hosted Website
1 Browser request to Website
9 Set TrustCookie
10 Allow access & enforce API-level policy
5 SSO Login Page
6 User provides Credentials
Redirect to TrustProvider 2
8 Generate TrustToken based on device status & access policy
Single Sign-On Provider
4 Redirect to SSO
7 Access Token
Trust Provider
Policy Engine
Trust Scoring
3 Device Check
Device Manager
Banyan App
Banyan Cloud Command Center


User & Device
Banyan Access Tier
Network Segment (VPC, VLAN, subnet, etc.)
1 Launch Banyan App
9 Verify TrustKey & set up tunnel
8 Generate TrustKey based on device status & access policy
5 SSO Login Page
6 User provides Credentials
Request tunnel access 2
Single Sign-On Provider
4 Redirect to SSO
7 Access Token
Trust Provider
Policy Engine
Trust Scoring
3 Device Check
Device Manager
Banyan App
Banyan Cloud Command Center


Rules-based Bypass
Private Resources, Service Tunnel, Exemptions
Risk-based Bypass
PAC File
URL Filtering
Payload Inspection
Web Proxy
DNS Proxy
Banyan App
Banyan Global Edge Network
Internet Resource
DNS-layer Security
Banyan Global Edge Network

ADDITIONAL INSIGHTS

Automated Onboarding: *Banyan Security developed a seamless onboarding experience, automating infrastructure provisioning for enterprises migrating from legacy VPNs.*

Zero Trust as an Industry Standard: *With growing regulatory mandates around cybersecurity, Zero Trust adoption is expected to rise, positioning Banyan Security as a leader in the space.*

Continuous Innovation: *Post-acquisition by SonicWall, Banyan Security continues to enhance its platform with advanced security analytics and AI-driven risk assessment.*

THE SUMMARY

Banyan Security's transformation showcases how Zero Trust Network Access (ZTNA) can replace traditional, perimeter-based security models. By eliminating VPN vulnerabilities, enforcing continuous authentication, and deploying global PoPs, Banyan Security successfully scaled its security infrastructure to serve over 500,000 customers.

Through a combination of identity-aware proxies, mutual TLS authentication, and policy-driven access controls, Banyan Security ensures organizations achieve maximum security without compromising user experience. As cybersecurity threats evolve, its Zero Trust framework provides the agility, scalability, and resilience enterprises need to stay ahead.

THE TECHNOLOGY

Golang | AWS | GCP | REACT | Cloud SQL | Postgres | Big Query | Google DLP | SCIM | MTLS | OIDC | SAML 2.0