BANYAN SECURITY

The CIO's Guide to Replacing Legacy VPNs

VPNs are part of the IT fabric in just about every organization. Undoubtedly, this fabric has changed dramatically over time as companies began to wear their technological "garments" in different ways.

One such IT garment is the Virtual Private Network (VPN). With origins dating as far back as 1996, companies started using VPNs to connect users to corporate networks.

So why are we still struggling with legacy VPN technologies and how can we move toward a world of modern 'work from anywhere' access?

That's what we explore in this guide.

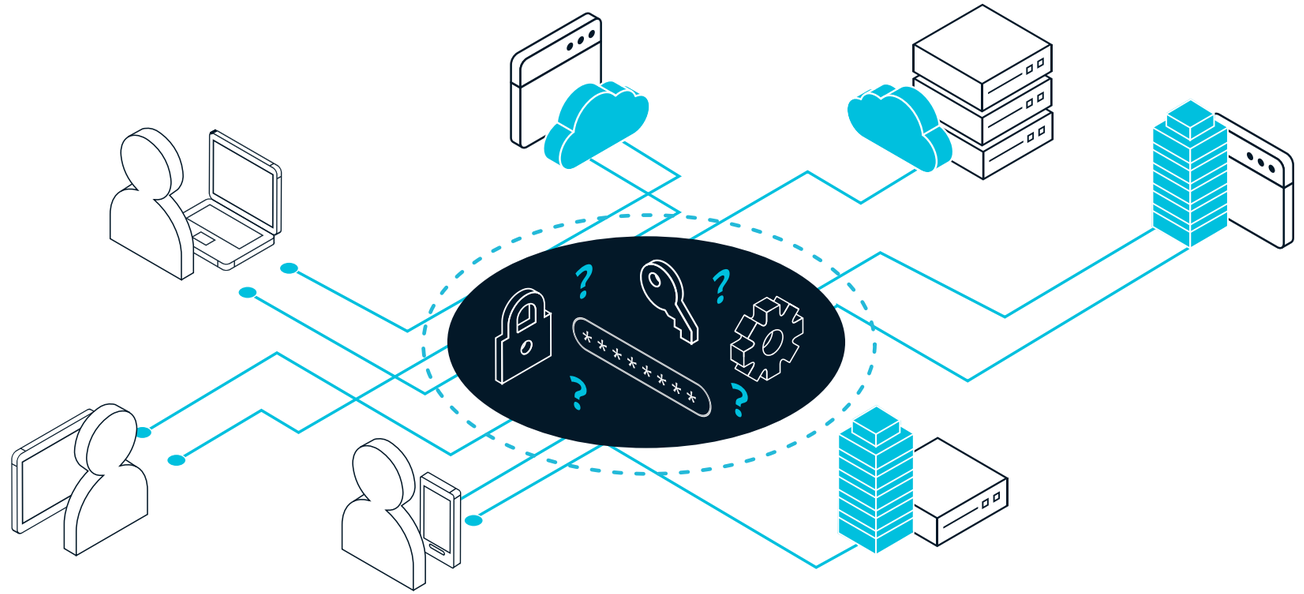
Why We're Stuck with Traditional VPNs

Providing secure remote access is a core requirement for every business. Many organizations have historically addressed this need by building perimeters around their on-premises data centers. This approach worked when the systems, applications, and users stayed within that perimeter.

After decades of incremental change in remote access technologies and deployment models, *everything* is now offered in the cloud. The VPN software stack is available as a container image to load into your cloud environment. Or perhaps, you access the VPN as a service – directly through a cloud service provider's marketplace.

Regardless of the deployment model, a common denominator runs throughout this brief walk down memory lane: legacy VPN technologies just don't cut it for today's operating environments.

It's time to get "unstuck."



Why We Need to Get Unstuck and Move Beyond Traditional VPN Technologies

As enterprises progress along their digital transformation journey, they must enable secure remote access across their on-premises, hybrid, and multi-cloud environments. Traditional network-centric VPNs were not designed to meet the scale, performance, and usability requirements of modern and increasingly complex organizations.

VPNs rely on networking controls such as IP whitelisting and segmentation that generate a significant ongoing workload for IT. They also create a massive security liability in the process as they offer overly-broad access to sensitive corporate assets and infrastructure which permits lateral movement that adversaries can use for ransomware and other malicious activity.

And with an increasing set of diverse users – from employees to contractors and third-party partners – secure access to these resources is required from a variety of on-premises and remote locations using a myriad of devices.

Legacy VPNs are struggling to meet the demands of the modern hybrid enterprise.

How to Tell If You're Stuck in Legacy VPN Land

If you manage the firewalls and VPNs in your organization, you know first-hand and all too well the pain of configuration, management, and resulting end-user frustrations. If you aren't responsible, but your team is, ask them what it's like to manage multipl siloed VPNs and IP whitelisting. The expression on their faces will likely tell you all you need to know.

Even if you aren't involved in the day-to-day management of devices and systems, you likely have first-hand knowledge of how well (or poorly) these technologies scale and keep things running smoothly for the business. To find out, consider asking these questions:

- Are you constantly wondering if there is a better way to manage remote access?
- Can you handle the near-constant onboarding and offboarding of users?
- Does the process of providing access to consultants, partners, and other third-parties flow smoothly while ensuring secure, least privileged access for them?
- How fast can you complete the 10-fold number of transactions compared to last year's results – to help the business achieve its aggressive financial objectives?

A VPN almost always has an indirect role in each scenario and may even have a direct role in specific situations. As noted earlier, the legacy VPN is part of the IT fabric – but that doesn't mean it needs to be.

If the problem is so apparent, then why isn't the solution equally obvious? For starters, most enterprises have significant business processes set up around their legacy VPNs, so a wholesale replacement can seem daunting if not entirely infeasible.

Putting full-blown swap-outs aside, it's hard to change the infrastructure to do something different, even at the smallest scale. Things tend to break with change, and breaking business processes is not a good thing. Plus, a change in one area often requires changes in another, making the source of the problem difficult to track down when something goes awry.

The Role of Zero Trust in Getting Businesses Moving Securely

68% As noted by IDC, **VPNs were used in 68% of major security incidents** involving remote access tools. Trends like this are prompting enterprises to look towards zero trust network access.

80% For example, Gartner predicts that by 2022, **80% of new digital business applications open to ecosystem partners will be accessed through a zero-trust network**.

60% By 2023, **60% of enterprises will phase out most remote access VPNs** in favor of zero trust network accesss. (Gartner)

IDC also predicts that by 2022, budgets for modern software-defined secure access solutions will quadruple as flaws in legacy VPN remote access solutions are illuminated by the massive work-from-home migration. Supporting this prediction, most enterprises indicate that zero trust ranks high, often #1 or #2, in their planned initiatives.

However, while a zero-trust goal is desired, what's missing is an achievable plan for getting there. Not knowing how much effort zero trust will require or how to measure progress against the goal is frightening.

What does the journey from a legacy VPN to real zero-trust access look like? Let's take a look.

Critical Requirements for Your VPN Replacement Project

Focus on reducing organizational complexity, improving the user experience, and bringing security in line with today's requirements

- Fast, direct connectivity to resources without hairpinning traffic.
- Improve user experience with modern passwordless and 1-click access.
- Remove reliance on complex IP whitelisting.
- Reduce operational burden by using cloud-managed solution.
- Reduce costs by leveraging existing investments in IaaS and device management.
- Enhance security posture by granting access based on user, device, and resource contexts.
- Provide application access instead of network access.

Banyan has compiled a list of essential criteria to consider for additional help selecting a zero trust network access solution to replace your legacy VPN.

Getting Started with Zero Trust Network Access

Start by asking your team the tough questions:

> **Are they frustrated by the complexities in managing and maintaining the VPN?**

> **Are they tired of dealing with user complaints about connecting through the VPN?**

> **Are they worried the VPN isn't delivering protection and value like it used to?**

Once you get those answers, you'll likely conclude that a change is necessary and you can begin to research how a zero trust network access (ZTNA) solution would fit into your organization:

Simplify IT Operations

- Incrementally deploy zero trust access on a per-application/service/user/team basis with no disruption to existing infrastructure.
- No more IP whitelisting. Simple, human-readable policies apply consistently across environments.
- Dramatically reduce helpdesk tickets regarding credential loss, theft, and updates.
- Simplify network segmentation.

Deliver a Great User Experience

- Gain one-click access to services and applications deployed in private clouds and IaaS environments.
- No more hairpinning of network traffic for better performance.
- Consistent user experience independent of user or resource location.
- Support passwordless access if desired.

Improve Security Posture

- Offer resource access based on context of user, device, and resource sensitivity.
- Continuously enforce policy and suspend access if user or device no longer meet security requirements.
- Easily establish least privilege access to applications and services.
- Prevent lateral movement and the spread of malware/ransomware across networks.

How Zero Trust Remote Access Works as a VPN Replacement

Zero trust network access eliminates many of the issues inherent with traditional and inflexible VPNs, which are complex to deploy, scale, and manage, while providing inadequate security against today's requirements.

In contrast, the Banyan Zero Trust Remote Access solution scales effortlessly to meet your hybrid and multi-cloud demands – while giving you the highest operational security posture possible across any IaaS and on-premises environment.

We enable enterprises to own their data plane while simplifying management through three fundamental building blocks:

1. **Incremental ZTNA and tunnel-based access deployment** using Cloud Command Center for consistent, unified policy.
2. **Visibility into users, devices, and resources** informs progress on the organization's zero trust journey.
3. **Integration with existing tools and infrastructure** eases management and improves security.
4. **Continuously authorize who has access to what, when** to ensure users and devices always meet policy requirements.

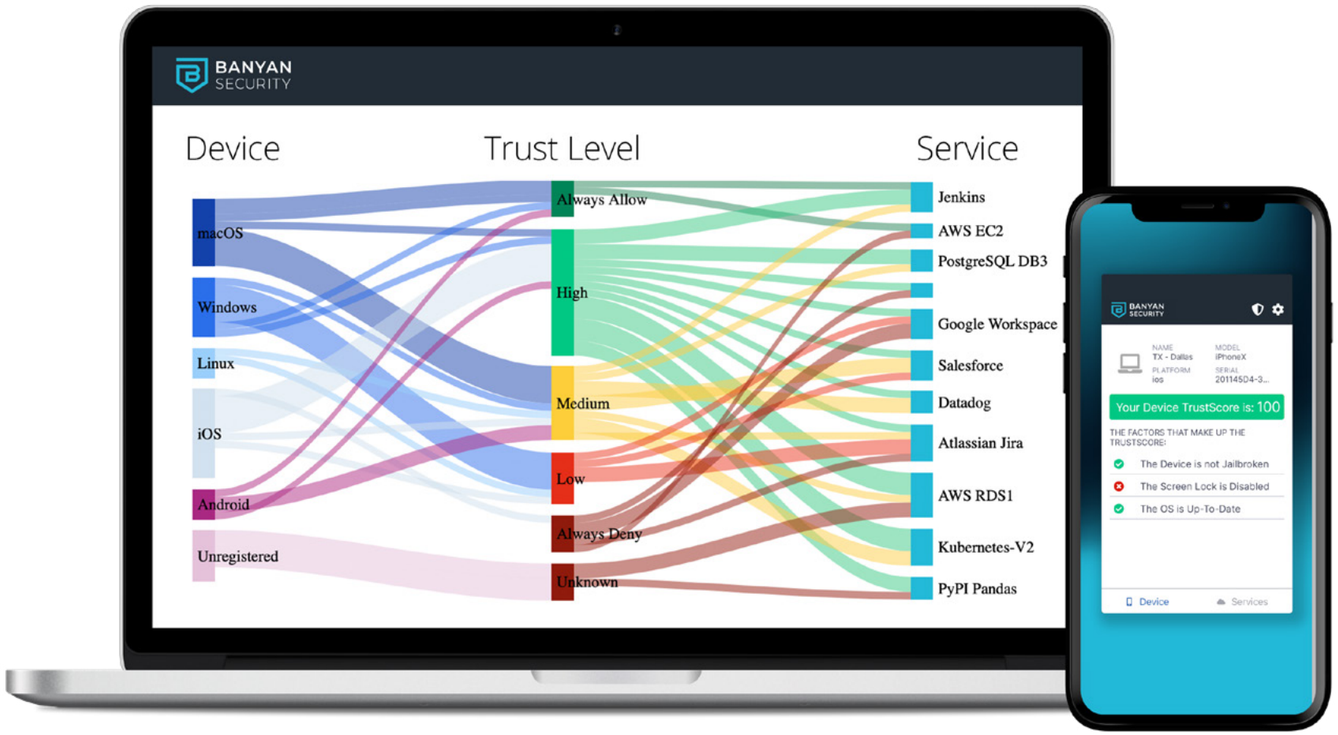
Critical capabilities provided by the Banyan Zero Trust Remote Access solution include incremental deployment, actionable visibility, automated service discovery and publishing, and continuous authorization with device trust.

Being able to roll out Banyan for selected services and applications alongside any existing access technology means you de-risk the deployment while demonstrating rapid progress.

You can achieve granular trust-based policy control and visibility across all devices connecting to your organization with actionable visibility. The deep visibility provides insight into who is using which resources from what devices and locations.

Continuous authorization with device trust scoring and least privilege access delivers the highest level of protection without sacrificing end-user productivity. Access is immediately suspended when user and device trust or device security posture no longer meet required thresholds. Users can directly see their Banyan TrustScore and steps to resolution, enabling self-remediation, thus reducing costly service desk tickets.

Seamless Secure Access for Your Hybrid Environment



By leveraging device trust, your environment can require certified unique identification of user devices and real-time assessments of device risk postures before granting access to critical business systems. Using continuous authorization with device trust delivers the following benefits:

1. **Access policy** against the context of user identities, device trust, and resource sensitivity.
2. **Lightweight app installation** initiated directly by users or via silent installs to support all device types.
3. **Device authorization** to uniquely register all devices, regardless of platform type, requires no device management software on the system.
4. **Banyan TrustScore**, immediately visible upon application installation, enables users to self-remediate if devices do not meet the security posture requirements for a requested resource.
5. **Continuous re-authorization** of user and device trust enforces access policy requirements, immediately disconnecting when users or their devices are no longer compliant.

With Banyan Zero Trust Remote Access, you no longer must be stuck using legacy VPN technologies. We offer the most seamless secure remote access solution for your hybrid environments – built on a zero trust network access model.

Zero Trust Remote Access: Your Path to Legacy VPN Freedom

As enterprises move to hybrid and multi-cloud environments, organizations need a solution like Banyan's Zero Trust Remote Access offering. The solution addresses the challenges of secure remote access for entire ecosystems while ensuring easy adoption by end-users and easy management by the IT staff. Just as significantly, the platform extends across on-premises and IaaS to public cloud ecosystems.

There's a different siloed user and admin experience in the legacy VPN world, depending on whether the user is on-premises or remote. With Banyan, the experience is the same – delivering actual manageable work-from-anywhere productivity – without operational and management complexity.

Remember, zero trust isn't an overnight project where a single switch is flipped, and you suddenly have a no-VPN environment. Plan to make the transition over time.

The Banyan Zero Trust Network Access platform allows you to make this journey incrementally, alongside your existing VPN environment as your business and risk requirements dictate. The platform also enables you to minimize risk exposure and improve your security posture as the transition takes place – rather than taking the "boil the ocean" rip-and-replace approach.

For applications where a modern tunnel is needed, Banyan has you covered with its Service Tunnel functionality. This modern tunnel, based on open-source WireGuard, includes Banyan's unique continuous authorization along with device trust – thus providing key zero trust capabilities.

Ultimately, zero-trust remote access can eliminate many of the issues inherent with traditional and inflexible VPNs. If you are looking for a way to remove the complexities and insecurities associated with traditional VPNs, take a moment to consider the Banyan Zero Trust Remote Access solution, which will help you scale effortlessly to meet your hybrid and multi-cloud demands – giving you the highest operational security posture possible.

To learn more about replacing your VPN with a zero-trust access platform, visit Banyan Security at **www.banyansecurity.io**.

Schedule Demo | **Experience Test Drive** | **Get Free Team Edition!**

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. Deep visibility provides actionable insight while continuous authorization with device trust scoring and least privilege access deliver the highest level of protection without sacrificing end user productivity. Banyan Security 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.

BANYAN SECURITY

Banyan Security, Inc. | +1 415-289-9414 | www.banyansecurity.io

CIOGuide_20211215