BANYAN SECURITY

CISO's Guide to Zero Trust Access

The Ins and Outs of Zero Trust Security

An Guide for CISOs and Executives

Intro

Zero Trust represents a necessary evolution of security. It has become a term that can not be taken at face value, requiring buyers to seek additional context so they can fully understand and find their best path forward. To succeed with Zero Trust Network Access (ZTNA) requires a new focus with a new technology, and it's all too easy to revert back to thinking of this as a new type of VPN. Learning from the downfall of security solutions in the past, successful Zero Trust Network Access needs to delight end-users making their job easier. It accommodates all modes of work, across all types of workers from contractors, developers, executives, and everyone in between. It is easier to manage, integrating within the enterprise framework of tools, and supports security across hybrid and multi-cloud environments. This paper will look at these elements helping security leaders understand the ins and outs of Zero Trust to clarify what it can do for them when done right.

Zero Trust really means Zero 'Unverified' Trust. Learn how security operations change when there is continuous verification of trust that links people and devices to organizational resources. While this may sound simple, in reality it is not, when you look at the various types of workers, devices, environments, and their roles and responsibilities. We'll look at the need for agnostic infrastructure and device coverage, granular resource segmentation and least privilege benefits, and where you can gain operational efficiency and lower security risk across your organization.

Origins and Principles of Zero Trust

Zero Trust is based on the realization that traditional security models operate on the outdated assumption that a perimeter exists and things inside the perimeter can be explicitly trusted. In our current cloud-first, work-from-anywhere model, implicit trust should be considered a vulnerability. Without continuous validation any trusted element can be abused. This can be seen with compromised credentials, user privilege escalation, device or workload exploitation, as well as lateral movement and data exfiltration.

Relevant industry Zero Trust sources

1 Forrester's Zero Trust eXtended (ZTX)

2 Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA)

3 NIST SP 800-207

2010
Forrester: Build Security Into Your Network's DNA: The Zero Trust Network Architecture, early reference to this term.

2014
Google: Published BeyondCorp as a practical application of the Zero Trust framework. Access granted based on user and device.

2015
Banyan Security formed to deliver Zero Trust Access solutions

2017
"Jump Start Zero Trust with Forrester's Reference Architecture"
ZT - Forrester[1]

2018
Gartner: Zero Trust Is an Initial Step on the Roadmap to CARTA (Continuous Adaptive Risk and Trust Assessment)

2018
Forrester: Zero Trust eXtended Ecosystem (ZTX), with data being a key component of the model

2018
"Zero Trust is an initial step of the roadmap to CARTA"
CARTA - Gartner[2]

2021
Banyan Security Delivers Team Edition

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses.

National Security Agency
https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

Digital transformation is moving business faster. Workflow changes and new applications are being created at an accelerated pace. Zero Trust Network Access is the way to keep up with these changes and set the foundation for decreasing the risk of a security breach. When everything is constantly being re-verified, security is more rigorous.

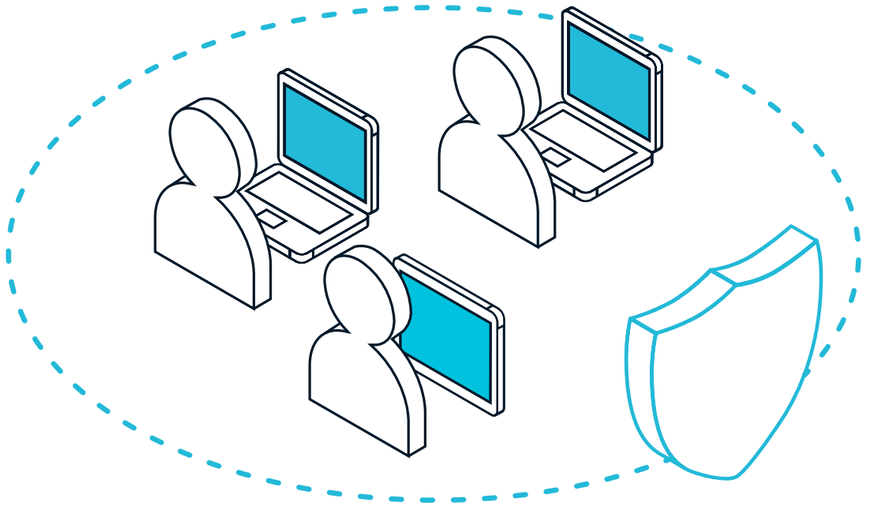
Trust has a freshness date, expiring after minutes, and is continually renewed after verification is confirmed.

Zero Trust Network Access Principles

1. A trust broker (product or service) provides logical access based on identity and context (where context ideally includes device, and application/resource sensitivity) with specific boundaries that apply to an application, environment, or resource, and is dynamically informed by policies for each request.
2. Access policies establish the security posture requirements for the device and identity pairing establishing the contextual parameters that must be met before granting access.
3. Every device, user, and network flow is authenticated and authorized, and are continuously re-verified.

The Evolution of Zero Trust Network Access Solutions

We'll look at the evolution of remote access solutions, and how the principles of Zero Trust Network Access have been incorporated in this fast-evolving market. This broadens our focus from what is Zero Trust Network Access to looking at management overhead, attack surface risk, and use case coverage.



The Beginning – VPNs

Virtual private networks (VPN) take the approach of enabling access based on successfully authenticating to a network, and once access is granted all resources on that network are accessible. It's a trust model based on an assumed perimeter and user authentication to the network. Authorization to the resources on the network is usually managed by other controls like Active Directory or privilege access management.

When the focus is on granting access based solely on identity, the downfall is that there tends to be a proliferation of VPNs because of the various roles and responsibilities. VPNs need to support the various types of workers in your organization. For example, contractors and developers need access to a cloud-environment, and the subsequent bastion hosts that segment access to various development resources often do not have centralized security oversight. This increases risk across an organization's attack surface. Management overhead is high, and control is low using outdated privileged networks and tunnels.

Moving to the Cloud – VPN as a Service

This stage reduced the management overhead of VPNs by providing them as a cloud service. However, the focus is still on access by identity, using the diverse privilege solutions in play combined with encrypted access tunnels. The management of various VPNs with their hardware and software configuration decreases with a single point for oversight. However, a new concern is that the organization's data is now forced to flow through these vendor clouds, becoming a 'Man in the Middle' (MitM) to an organization, between the users and resources to which they connect. Many vendors in this space expanded their original services from content distribution networks to now provide these remote secure access services. If consistently deployed, these services employ traffic "hairpins", creating bottlenecks without solving any of the privilege management issues, limiting their adoption into complex environments and infrastructure.

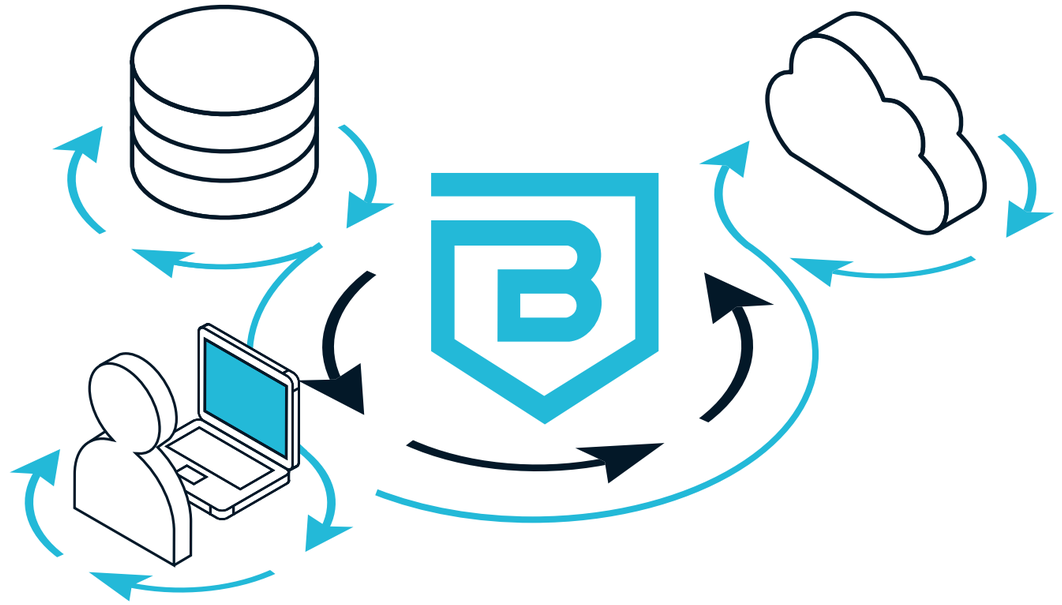
Cloud-Native Zero Trust – Early Entrants

These solutions begin to address the least privilege requirement for Zero Trust Network Access. Not necessarily removing the need for VPNs, they help organizations narrow access based on identity and resource and consolidate oversight into a cloud-native security solution. Like VPNs as a Service, these solutions pose a problem because organizations do not own their own data plane, instead having their data traverse through a MitM cloud. For any organization facing industry regulations based on data classification and sensitivity, this can be a big issue. As an overlay solution, the various vendors have specific infrastructure that they support, leaving gaps in how large enterprises can meet their ZTNA needs. There is support for identity and network continuous verification but there are weaknesses with SaaS solution support. Instead of connecting identity to service by default, they work around by using IP restrictions, very much like a whitelist. There is some support for DevOps, but these solutions still come up short when complex environments or tools like Kubernetes are utilized.

The full intent of Zero Trust Network Access cannot be achieved without incorporating the ability to manage access based on granular policy, informed by the verification of user, device, and resource.

No-Boundaries Zero Trust Solutions

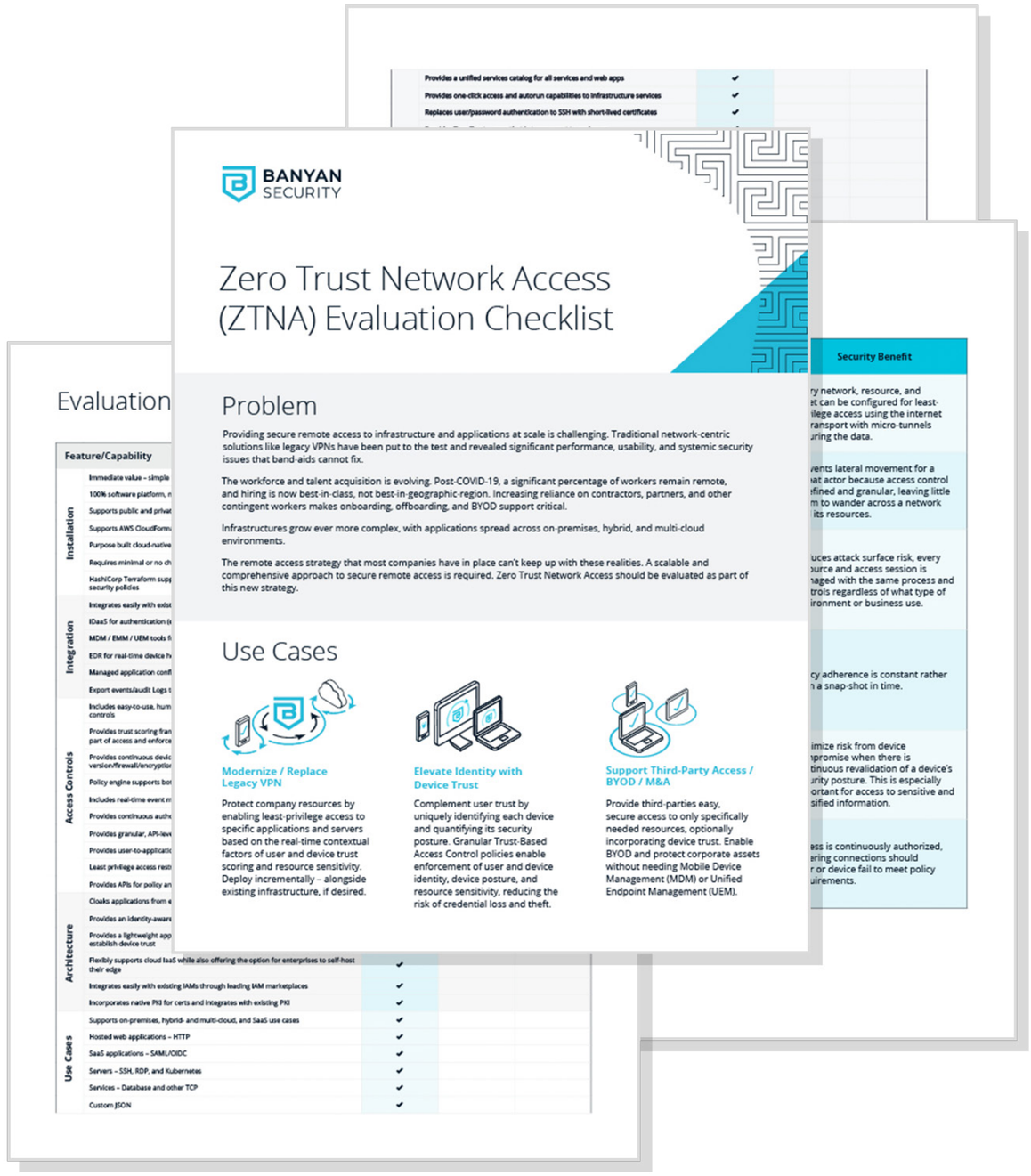
Zero Trust Network Access, individually or part of a broader Secure Access Service Edge (SASE) architecture, actually moves security off the network, focusing on protection with continuous security context around users, devices, applications, and workloads. Access privileges are driven by rules and policies that are consistently applied regardless of user location to ensure identity is vetted and device trust is established and continuously authorized or authenticated (use of multi-factor authentication). Without the limitation of having to be within a specific cloud, or connect with a VPN, these solutions allow users from anywhere, using the internet, to access the specified resources they need to work. Being environment-agnostic is a benefit because access to on-premises, public cloud, hybrid- and multi-cloud environments, container resources, or SaaS solutions can be protected with Zero Trust without requiring architectural changes to the business' infrastructure. Also important is that these cloud-native solutions do not risk data privacy or security by forcing traffic through a vendor cloud, and provide high-performance, resilient, and secure connections.



A key aspect of Zero Trust is least-privilege access, eliminating overly-broad access grants, permitting access to only what is needed for a user's role and responsibility. Organizations can create granular policies and establish that users can only connect once device verification and security posture status are validated. These cloud-first solutions are built for "work from anywhere" mobility.

Preparing for No-Boundaries Zero Trust Network Access

Changes to existing remote access solutions may be met with hesitation and even confrontation. There are concerns that work productivity will be jeopardized and that there will be a high overhead cost and educational ramp for end-users and administrators alike. Equally problematic is when an organization looks at Zero Trust Network Access and implements it like a VPN granting users broad access to all applications, thus missing out on its key security benefits. These concerns can be alleviated when a fresh mindset is put in place and there is an understanding of the necessary operational changes and their benefits. Download the Zero Trust Network Access Evaluation Checklist.



Moving Forward

Building Relationships, Setting Privileges – *based on Context*

No-Boundaries Zero Trust Network Access will be a relationship builder for your organization. Business leaders and their teams will play a role in identifying the types of users and the specific applications and resources they need whether on-premises, cloud, or SaaS. Working together to understand the data classification that each user role interacts with so the appropriate device security policy can be set will be key.

However, since ZTNA is based on logical access, all of the resources based on a role can be grouped together. No longer do multiple administrators, across siloed technologies, have to grant access. With continuous authentication and authorization a new user experience of 'one-click' secure access can be established. Any concerns about a lag in productivity are dispelled. ZTNA Administrators configure these granular access policies to look at the context and elements of the user, device, and application/ resource sensitivity. Unlike the configuration of a VPN, or even firewall, these policies are logic-based and represent the relationships of the elements and do not rely on any IP or subnet configuration that requires extended IT knowledge.

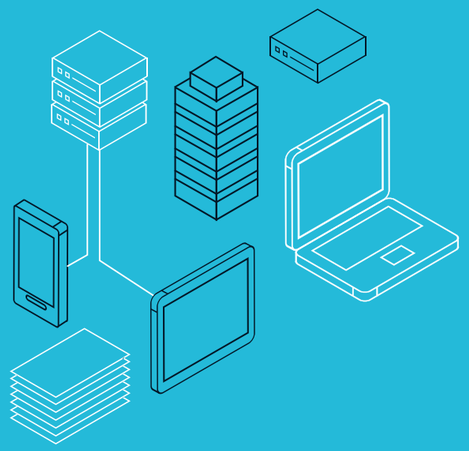
Business Guide for Successful Outcomes

Supporting DevOps Teams

DevOps teams work on multiple projects, across various development environments and infrastructure that is fluid by definition, leading to a complex mesh of infrastructure and services that is hard to manage.

ZTNA Benefits for DevOps Environments:

- No inadvertent misconfiguration or manual effort in setting up bastion hosts or multiple VPNs for different users or environments, saving time and minimizing risk.
- In minutes any DevOps team member can quickly access all needed tools, resources, cloud services, and distributed code repositories.
- Remote infrastructure access that traditionally needed special exceptions from IT and security teams because of key management and vulnerabilities (SSH/RDP) or difficult to support (like Kubernetes) are no longer a concern.
- Diverse authentication conventions can now be dropped utilizing ZTNA for centralized set-up and management. DevSecOps or team leaders can easily configure the logic-based access policies in minutes.
- User-to-application segmentation can be used to limit contractors or workers based on specific geolocations that would cause compliance or security issues if they had broad access across a project.
- Because access is not tied to networks, when projects migrate to new cloud infrastructure or to another location there is no need to change access policies because it is based on resource/URL, the front-end components.



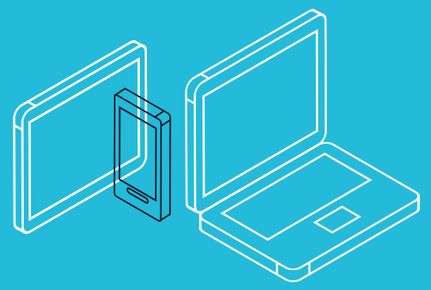
Addressing Enterprise Security Complexity

Once organizations have enterprise-wide authentication moving to Zero Trust can seem overwhelming. Unlike other security roll-outs, don't try to convert every individual all at once; rather, choose manageable projects that allow you to rapidly show progress and realize value. This could be tackling a specific application, a project team, or a department. The goal is to eliminate overly-broad access and implement granular access policies that were not feasible with other solutions. Learn about the data and application sensitivity and the various roles and responsibilities of the user groups. Look at the access controls in place across internal resources and where they are missing when SaaS solutions or other cloud services are used. This level of complexity can now easily be addressed and managed with ZTNA, including one of the key contributors to breaches and risk, the security posture of the user's device(s). Work is anywhere and now ZTNA can provide secure access for diverse workforces that include employees, contractors, consultants, and partners using on-premises, hybrid, and multi-cloud applications and resources.

Addressing this type of roll-out ZTNA provides the following outcomes:

Benefits:

- Centralized oversight and identification of all of the 'shadow' IT or additional SaaS solutions the business utilizes.
- Enrich authorization with data from mobile device management solutions already in place.
- Gain broad coverage for mobile and BYOD, knowing that device security posture is appropriate for the sensitivity of data and applications being accessed.
- Gradually replace legacy VPNs, support the future of work, digital transformation, and security in the age of ransomware, removing the vulnerabilities that these systems pose to an organization if not well-managed and frequently patched.
- Flow granular logs to SIEM and SOC automation systems that tie identity, resource, and device natively in the log.
- Reign in security policy exceptions, gain consistency in delivering least-privilege access for any type of worker within your organization, making compliance and auditing easier.



Enabling BYOD and Third-Party Access

As the workforce and talent acquisition evolves, post-COVID, a significant percentage of workers want to remain remote. Hiring is now best-in-class, not best-in-geographic-region. Employers need the ability to flexibly accomodate the types of devices and work that will now be a hybrid of in-house and remote. Security that allows for a device to register and meet a required security posture that fits the type of work aligned with the user identity is the goal. For users the focus is on convenience and not losing control of their devices.

ZTNA is an excellent solution that reduces complexity, increases usability, and improves security.

Benefits:

- Leverages existing enterprise-wide identity solutions.
- Removes the cost of providing managed devices, and per-device license cost for MDM solutions for trusted non-employees such as contractors, partners, and contingent workers.
- Reduce the risk of lost/stolen credentials with identity and device key pairing that secures and provides a way to achieve passwordless access.
- All access to resources can be logged and flow into SIEM and SOC monitoring.

Summary

Zero Trust is more than just a technology change, it is a new model that gives organizations a way to achieve user to application segmentation. What seemed impossible to achieve with complex and sophisticated network rules and VPN configurations is now centralized with a trust broker. Logical Zero Trust Network Access policies can be easily created and even shared among those who manage access privileges. Continuous authorization of users and the security posture of the device they are utilizing, informs in real-time whether the security access policies are being met before access is granted. While it may sound daunting, organizations will gain operational efficiency and lower their overall security risk. When done right, ZTNA gives on-campus and remote employees, contractors, consultants, and other third-parties an easy, frictionless way to engage with your organization. Better security and more productivity could be just around the corner.

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 legacy VPNs. Deep visibility provides actionable insight while continuous authorization with device trust scoring and least privilege access deliver the highest level of protection with a great end user experience. 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

CISOGuide_20220428