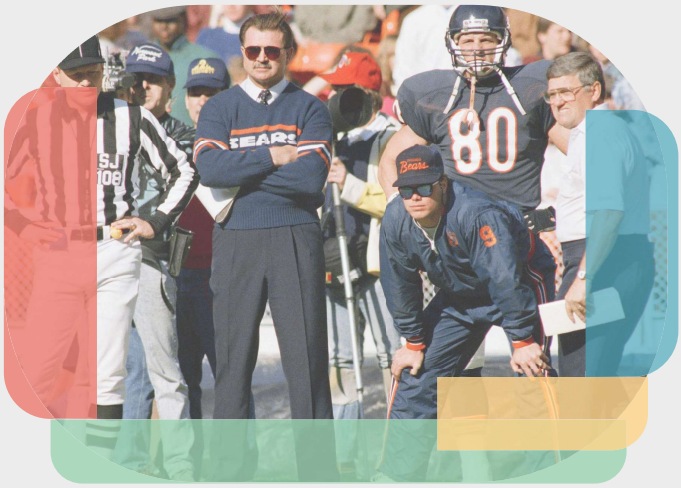
WHITE PAPER

Dynamic Defense

The Playbook for Zero Trust Network Access



Imagine a game of football where players had to stand still on the gridiron. The goal is the same: get the ball to the opposing team's endzone. There are still coaches and playbooks. The field is still a hundred yards from end to end. There are still 53-man rosters with 11 players from each team in play. But it wouldn't be very fun to watch, would it? Defense wouldn't be able to do much defending without chasing down the QB or receiver. The offense would always have the upperhand, easily making it the other endzone with a series of easy lateral passes. Defensive players would be relying on pure luck to pick off a pass or block a Hail Mary.

That's how a lot of companies approach cybersecurity. Defenses are static, network-based perimeters. Security protocols are more concerned with the network and its segments instead of users, assets, and resources. Of course, a solid wall will prevent the most basic intrusions. If a peewee football team went up against an NFL-level defense, the NFL linebackers would most likely be able to stop any squad of middle schoolers from running the ball down the field. But these days, the playing field is level. Threat actors know what they're up against, and their tactics are constantly becoming more sophisticated. And, as we know, blocking the outside doesn't account for the threats on the inside.

This is why cybersecurity teams are increasingly turning to Zero Trust Network Access (ZTNA), a set of guiding principles for workflow, system design, and operations that can be used to improve the security posture of businesses of all sizes and protect resources of any sensitivity level. Static playbooks don't work these days. To win, defenses must be dynamic. Defenders must be able to *move.*

Zero Trust Defined

Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems. The main idea is evaluating trust on a per-transaction basis rather than implied trust based on network location. In other words, the system does not implicitly trust a user and grant them full access to a network just because they're using the right password on their personally-assigned computer. With ZTNA, a user has to prove who they are each time they want to access a different segment of an information environment. Accessing individual resources is granted on a per-session basis.

This doesn't mean a user's account isn't considered in identifying a user is who they claim to be - but accurate user identification requires extra diligence in a zero trust environment. Other identification attributes include artifacts like network location, times and dates of requests, previously observed user behavior, and installed credentials.

Zero trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero trust assumes there is no implict trust granted to assets or user accounts based solely on their physical or network location.

NIST Definition

Start Small and Scale

A companywide ZTNA rollout is a daunting task for many IT teams. ZTNA policies can cause unneeded friction across the corporate workforce if teams don't plan accordingly. It can also be risky to implement these policies all at once – risky for network security, productivity, and business in general.

We recommend building on ZTNA step-by-step. The project can be initiated with a limited scope and budget and expanded quickly once certain rules are proven successes. Start with a single use case, like remote worker access. Establish wins and share the results with stakeholders so they become believers in the dynamic approach of ZTNA.

Before you begin a ZTNA rollout, it's important to get everyone involved on the same page. Network engineers will probably be guiding most of the decision-making during the project. Operations personnel should be involved too. It will also be necessary to collaborate with third parties who will need ongoing access to specific applications. Of course, security teams will provide policy guidance on security and compliance and advise stakeholders about risks. However, they shouldn't own the risk itself.

Remote Work Use Case

The popularity and normalization of remote work is one of the strongest use cases for launching a ZTNA conversion project. While we've seen many companies call their employees back to the office after the height of the COVID pandemic, as many as 27% of fulltime employees work remotely at least a few days per week. The traditional security approach for remote workers centers on using virtual private networks (VPN). With most VPN protocols, the network connection is implicitly trusted. But the traditional approach doesn't cut it anymore. VPN usage rarely mitigates the pitfalls of unsecured home Wi-Fi networks or stolen credentials, nor do they prevent ransomware from proliferating.

NTG recommends starting a ZTNA rollout in one department for a particular group of users. For example, content marketers need access to publication tools and creative assets (maybe from a server located at HQ or a cloud-hosted file sharing service), but other employees probably don't need that access. Role-based application access, one of the core tenets of zero trust, ensures that each employee receives only necessary permissions.

Zero Trust Components

An effective zero trust architecture involves several components seamlessly working together. There is no "out of the box," singular device or application that constitutes zero trust. That would defeat the purpose of a dynamic defense anyway. Again, we recommend starting slow, but if you're going to start with something impactful, start with the policy engine, sometimes referred to as the "brain" of a zero trust security fabric.

- **Policy Engine**: Responsible for the ultimate decision to grant access to a resource for a given subject. The policy engine combines enterprise policy and input from external sources like threat intelligence services.
- **Policy Administrator**: Responsible for establishing and/or shutting down communication paths between a subject and a resource. This generates any session-specific authentication and authentication token, or credential used by a client to access an enterprise resource.
- **Policy Enforcement Point**: Responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The policy administrator forwards or receives policy updates to the policy enforcement point.
- **Continuous Diagnostics and Mitigation System**: Gathers information about an asset's current state and applies updates to configuration and software components. The system also provides the policy engine with the information about the asset making an access request.
- **Industry Compliance System**: Ensures the enterprise remains compliant with any regulations it may fall under.
- **Threat Intelligence Feed**: Provides information from internal or external sources that help the policy engine make access decisions. The feed is usually comprised of multiple data sources and should provide information about newly discovered attacks or vulnerabilities.
- **Network and System Activity Logs**: Aggregates asset logs, network traffic logs, resource access actions, and other events that provide real-time feedback on the security posture of enterprise information systems.
- **Data Access Policies**: Consists of attributes, rules, and policies about access to enterprise resources. These policies are the starting point for access authorization since they provide basic access privileges for accounts and applications.
- **Enterprise Public Key Infrastructure (PKI)**: Responsible for generating and logging certificates issue by the enterprise to resources, subjects, services, and applications.
- **ID Management System**: Responsible for creating, storing, and managing enterprise use accounts and identity records.
- **Security Information and Event Management (SIEM):** Responsible for collecting logs for analysis.

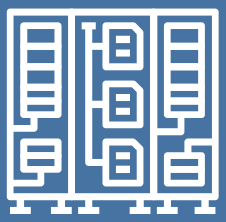
Network Requirements for ZTNA

1. Assets must have basic network connectivity. LAN provides basic routing and infrastructure.
2. Must be able to distinguish between owned & managed assets and a device's security posture.
3. Must observe all network traffic (we have several solutions for network visibility!)
4. Resources should not be reachable without accessing a policy enforcement point (PEP).
5. Data plan and control plan must be logically separate (ensures policy enforcement points can't be turned off unintentionally).
6. Enterprise assets must be able to reach policy enforcement points.
7. The policy enforcement point should be the only component that accesses the policy administrator.
8. Remote enterprise assets should be able to access enterprise resources without traversing enterprise network infrastructure first.
9. Enterprise assets may not be able to reach certain PEPs due to policy or observable factors. For example, Ttere may be a policy constraining mobile assets from reaching certain resources if the requesting asset is located outside the enterprise's country.

Migrating to Zero Trust

Migration to a ZTA requires a different strategy depending on the enterprise's current cybersecurity posture and operations. Enterprises should reach a baseline of competence before it becomes possible to deploy a significant ST-focused environment.

It's possible to build a ZTA from the ground up, but such a task is incredibly difficult for organizations with existing networks. The degree of success depends on how dependent new infrastructure is on existing resources. In other words, it's rare that any significant enterprise can migrate to a ZTA in a single technology refresh cycle. There is usually an indefinite period when ZTA workflows coexist with non-ZTA workflows. Enterprises should ensure that common elements are flexible enough to operate in a ZTA and perimeter-based hybrid security architecture. Migration usually requires a partial redesign.



Less than 1% of large enterprises have a mature zero trust program in place today, and even by 2026, Gartner predicts that number will only reach 10%

Gartner 2023

Migration Continued

Migrating to ZTA also requires detailed knowledge of your assets (physical and virtual), subjects (including privileges), and business processes. Incomplete knowledge leads to business process failure like denied requests due to insufficient information. This is especially an issue if there are unknown “shadow IT” deployments operating within an organization. Therefore, it is important to conduct a survey of assets, subjects, data flows and workflows. Awareness forms the foundational state that must be reached before a ZTA deployment is possible. An enterprise cannot determine what new processes or systems need to be in place if there is no knowledge of the current state of operations. Surveys can be conducted in parallel, but both are tied to examination of business processes of the organization.

Common Pitfalls

An attacker could also disrupt the PEP or PE/PA which spells trouble considering enterprise resources cannot connect to each other without the PA’s permission. Enterprises can mitigate this threat by having policy enforcement reside in a properly secured cloud environment or be replicated in several locations following guidance on cyber resiliency. This doesn’t eliminate the risk. Botnets can produce massive DoS attacks against internet service providers and disrupt service to millions of internet users. Attackers can also block or intercept traffic to a PEP or PA from a portion or all the user accounts within an enterprise. Moreover, a hosting provider might accidentally take a cloud-based PE or PA offline. Cloud services have experienced disruptions in the past, both infrastructure as a service and software as a service.

Insider threats are a concern with any security architecture. Even though zero trust architecture is based on no implicit trust, attackers can still compromise an existing account or device to gain a foothold. Accounts with access policies around desired resources would be primary targets for attackers. They use phishing, social engineering, or a combination to obtain credentials of valuable accounts.

Machine learning techniques can be used to analyze traffic that cannot be decrypted and examined. These techniques allow enterprises to categorize traffic as valid or possibly malicious and subject to remediation. Sometimes, enterprises cannot perform deep packet inspections.

Put the most restrictive access policies possible on resources that are vital to security. They should only be accessible from designated or dedicated administrator accounts.

ZT is a cybersecurity strategy and framework that embeds security principles throughout the [DoD] Information Enterprise (IE) to prevent, detect, respond, and recover from malicious cyber activities. This security model eliminates the idea of trusted or untrusted networks, devices, personas, or processes, and shifts to multi-attribute-based confidence levels that enable authentication and authorization policies based on the concept of least privileged access.

ZT focuses on protecting critical data and resources, not just the traditional network or perimeter security. ZT implements continuous multi-factor authentication, micro-segmentation, encryption, endpoint security, automation, analytics, and robust auditing to Data, Applications, Assets, Services

DAAS 2022

Final Word

Of course, zero trust architecture isn't guaranteed to prevent threat actors from accessing a network or exfiltrating data because nothing can guarantee that. A properly implemented and maintained zero trust architecture is great, especially if it's complemented with existing strong policies, continuous monitoring, and general cyber hygiene, but it can be a complicated undertaking.

NTG's founders and technical staff have been implementing zero trust solutions for the DOD and commercial enterprises since before the concept was referred to as "ZTNA." We've experienced all the pitfalls and successes that inevitably happen in a ZTNA project. Of course, NTG uses a zero trust architecture for our remote staff and HQ. We have also implemented zero trust solutions for the Pentagon as a subcontractor to Leidos on the JSP program.

If your organization is looking to adopt zero trust architecture (whether to comply with regulatory standards or to modernize your security fabric), NTG is here to help.

Contact Us: (813) 885-7500 | sales@ntgit.com