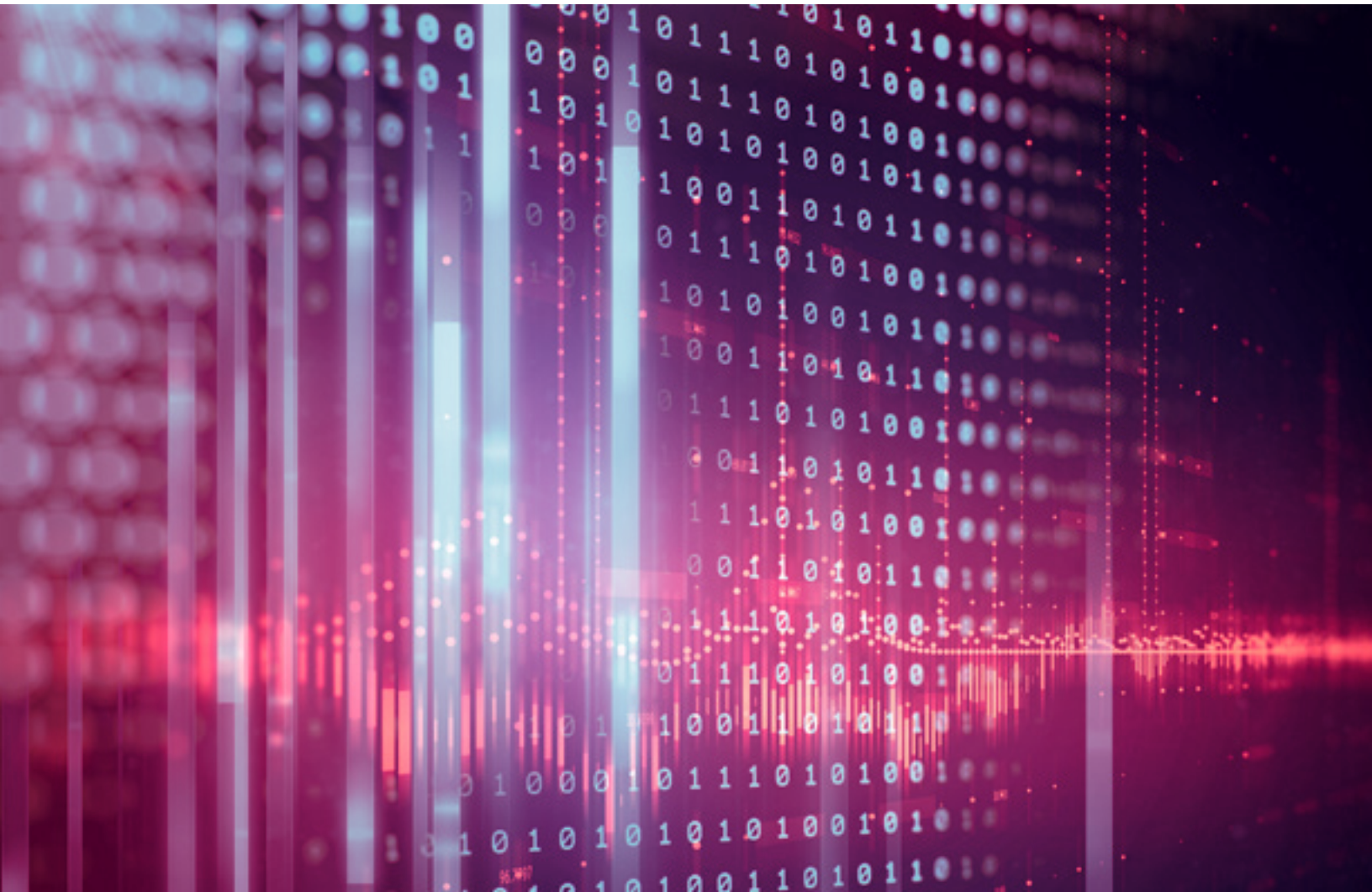
CAPCO | DIGITAL

ZERO TRUST ARCHITECTURE (ZTA)

MODERN WORK ANYWHERE ARCHITECTURE WITHOUT VPN



CONTEXT

In the 12th Century, Mongols successfully raided walled cities, one after the other, leading to demise of walled-city architecture for protection. In our modern 21st century, the classic “moat and castle” network design is going through a similar phase as the high-trust flat network with high-cost and less-scalable tunnel “VPN”, no longer provides a trusted expansion of the network in today’s remote world.

Today’s attackers see this vulnerability with the traditional VPN model, as VPN alone does not have limiting controls if compromised. This risk is increased with attackers shifting towards identity attacks using credential stuffing versus brute force attacks. This is all due to how easily and cheaply it is to purchase compromised credentials on the dark web. This attack vector exploitation has been further accelerated due to:

- An increase in cloud adoption and usage of SaaS across organizations.
- Enterprise applications (e.g., O365, ERP and other systems) getting transitioned to the cloud, does not allow the usual approach of having a Demilitarized Zone (DMZ) protecting internal networks from untrusted traffic.

So, how do we protect against this changing enterprise application landscape? Organizations across the world need to lead the adoption of Zero Trust Architecture (ZTA) for cybersecurity, as their first principal of implementation. ZTA is scalable and has a cloud-native foundation as its approach assumes an attacker is already in the network.

ZERO-TRUST OVERVIEW

A broad security model that has been considered for implementation is modern cloud-native architecture for enterprise applications. The National Institute of Standards and Technology (NIST) fundamentally defines “Zero Trust” as having no trusted zones in the network and assuming attackers are present in your network. The Zero Trust (ZT) approach leverages continuous resource monitoring and dynamic risk evaluations in order to protect every individual asset/resource against a potential attacker within the network, hence “Zero Trust.”

FOUNDATIONAL PRINCIPLE

NIST defines the following core tenets to start establishing Zero Trust Architecture:

- Enterprise Resources: All data and computing services are considered resources.
- Secured Communication: All communication is secured, regardless of network location.
- Session-Based Access: Access to individual enterprise resources is granted on a per-session basis. Authentication and authorization to one resource will not automatically grant access to a different resource.
- Dynamic Risk Evaluation: Access to resources is determined by dynamic policy. All resource authentication requests and authorizations are dynamic and strictly enforced before access is allowed.
- Resource Monitoring: Enterprise monitors and measures the integrity and security posture of all owned and associated assets.
- Asset State Tracking: The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

IMPLEMENTATION APPROACHES

NIST classifies various implementation deployment models of ZTA in the following three approaches. However, in real life, it will include some aspects of the strategies that are being outlined below and, most likely, an amalgamation approach comprising all of them:

1. **Device Agent/Gateway-Based Deployment**
2. **Resource Enclave-Based Deployment**
3. **Resource Portal-Based Deployment**

All three approaches compose of a control plane and a data plane. However, the variations lie within structure of the data transmission layer (data plane). Overall, **Device Agent/ Gateway-Based Deployment** provides the highest control/ accuracy given that every individual resource is connected through a gateway that the agent is accessing through the enterprise management agent (a.k.a "asset"). However, due to legacy approaches, the enterprise may choose to have a varied implementation due to resource limitation costs, or unviability due to resource type. This may result in the inability to host a gateway and hence require a smaller trust zone for data to travel from the gateway to the resource, which alludes to a second model looking like a "**Resource Enclave-Based Deployment**"; this is where a gateway grants access to a cluster or "enclave" of resources rather than at an individual level. The third model "**Resource Portal-Based Deployed**," is a variation where the enterprise does not have control over the agent/device that initiate requests. This model is no different than how an enterprise today enables its online services to its customers through browser isolation and protecting endpoints with Content Delivery Network (CDN) and Distributed Denial-of-Service (DDOS) firewalls, etc.

- **Device Agent/Gateway-Based Deployment:** This model entails device agent and gateway-based Policy Enforcement Point (PEP) . To implement this model, integration is required with two major components: user endpoint and the application the user is trying to access. This model is not much different from the API Gateway-based model, however the key point of decision-making lies with the Policy Engine. The Policy Engine is a separate component which collects heuristics and access rules from diverse systems.

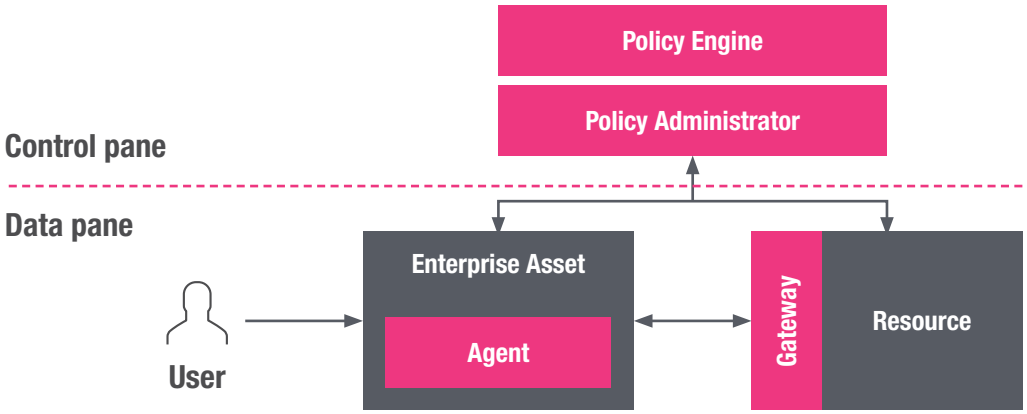


Figure 1: Device Agent/Gateway-Based Deployment

- **Resource Enclave-Based Deployment:** This model is similar to the Device Agent/Gateway-Based Deployment, however, the Policy Enforcement Point (PEP) is in-front of a cluster or “enclave” of resources rather than a single resource.

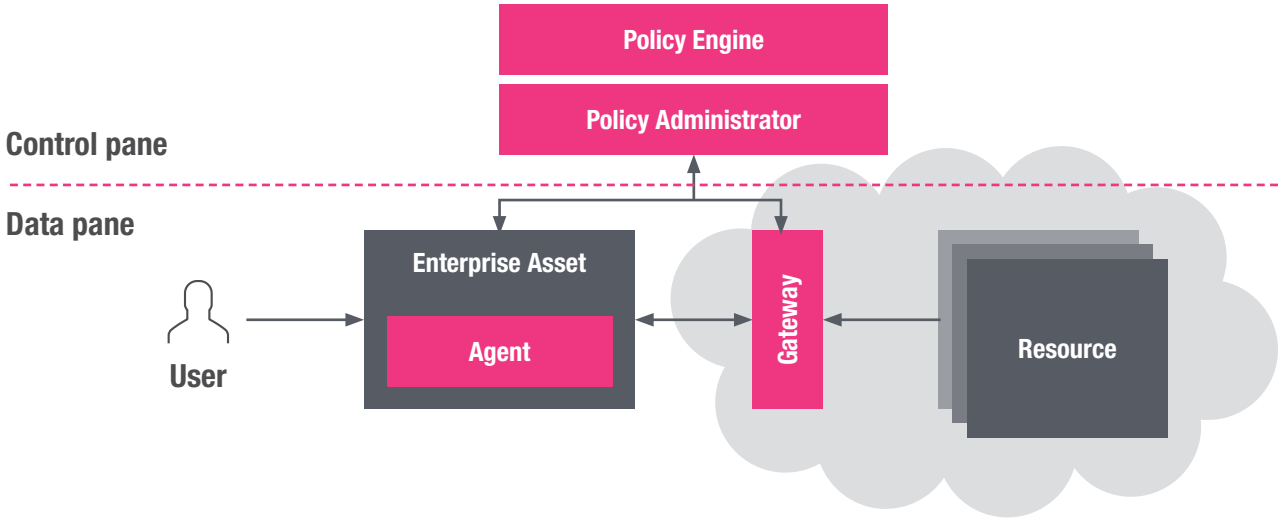


Figure 2: Resource Enclave-Based Deployment

- **Resource Portal-Based Deployment:** Like the other two models a gateway is placed in front of the resources, in order to control user access. The key difference is that the Policy Enforcement Point (PEP) is not integrated with the user endpoint nor the application the user is trying to access, which reduces control based on contextual information.

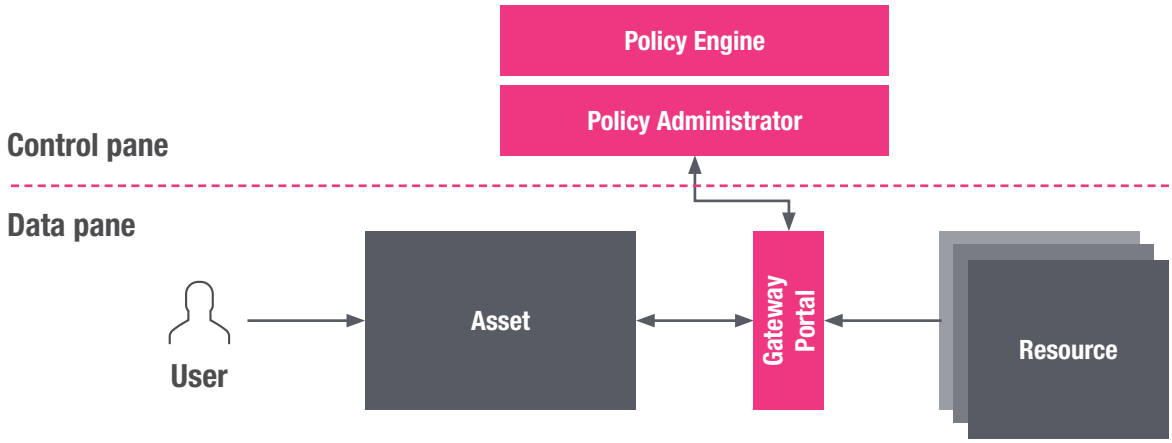


Figure 3: Resource Portal-Based Deployment

POLICY ENGINE

The heart of Zero Trust Architecture (ZTA) is the Policy Engine (PE). PE is ultimately the decision maker on granting or refusing access using various datasets per session basis. This allows to move away from the user-id/password-based authentication and authorization model. For example, some key datasets (data source components) considered in implementations are:

- Agent Device Diagnostics Results
- Industry Cyber Security Inputs
- Device Activity Logs
- Resource Status
- User Access Management
- Resource Access Policies
- Network/System Activity Logs
- Geo-Location and Use Activity Logs

This "Adaptive Digital Identity" takes all the data source components into consideration before a user can have access to an enterprise resource.

Most enterprises will not implement a Policy Engine but buy one from a leading solution provider. The Policy Engine providers are actively innovating and providing interesting approaches to mitigate threats. However, the biggest hindrance has not been solution capability but the implementation and configuration of the architecture that best suits their needs. This leads to our clients asking how they go about enabling this "ZTA" in their organization.

APPROACH/JOURNEY FOR TRANSITION TO ZERO TRUST ARCHITECTURE

The good news is that this does not mean you have to start building your organization network and access policy from scratch; there are hybrid opportunities that can be leveraged. Every organization can follow different approaches to implementing Zero Trust Architecture that is ideal for their user flows and resource usages. The key success for migrating to any ZTA-based implementation from a legacy flat network depends on multiple factors. Based on our research and industry experience, we have classified overall success factors into the following buckets:

1. **Right Initiation**
2. **Operational Success Factor**
3. **Executional Success Factor**

Right Initiation:

- **Identify Resources**: Business critical resources, where they reside and what data they contain.
- **Transaction Flow**: Map the transaction flow by identifying user-groups and resource access across all critical data source components.
- **Use-Case Based Implementation**: Identify the high impact use-cases that would primarily benefit from leveraging ZTA to drive targeted solutions.
- **Device Management and Configuration**: Review against forecasted growth and current capability management.
- **Automate processes as much as possible**: Establish strong pipeline requirements to drive network efficiencies and reliability for the user base.

Operational Success Factor:

- **Buy-In from the Top**: This is an enterprise-wide initiative and will require organization-wide support and interactions. Given the holistic nature of it across the enterprise, executive governance is an absolute must for success.
- **Build an Inter-Disciplinary Team**: The transition to ZTA will require network, enterprise asset management, domain services, risk, fraud, etc. – a cross-domain leadership team is needed.
- **Establish Consistent Funding**: Such a large transformational journey requires consistent funding for a duration of a two-/three-year timeframe to do a gradual transition of the platform and applications.

Executional Success Factor:

- **Self-Service Enablement**: As the capabilities mature, the size and scale of such network transformation requires that individual application owners can self-service a large portion of ACLs and other access requirements. ZTA enablement must follow the same customer-first mindset. In this case, the customers are application developers and owners.
- **Establish Common Implementation Patterns**: Define well-documented common patterns for enabling ZTA for common use-cases within the organization; for example Web/HTTPS-based applications, device management, etc.
- **Project categorization into Sub-Projects**: Given the size and scale of such complex initiatives, it will require detailed planning that involves breaking overall ZTA migration projects into smaller milestones.
- **Exception Scenario Planning**: Issues will arise due to production failures and cyber-security implications. Having a well-established plan to deal with this will be critical and necessary to keep momentum in the program.
- **Phased Roll-out**: Large-scale transformation applies even more at such an intrinsic level. Do not onboard large/mission-critical applications. Don't expect everything to go according to plan and be open to change or adapt your plan as your implementation proceeds.
- **Long Tail Planning**: Certain use-cases, such as legacy thick clients, NFS usage, etc., will require an extended timeline and changes to actual use-cases and business applications. It will require that the enterprise be committed to tackling these scenarios.

WHY SHALL I ADOPT ZTA?

- **Reduced Risk of Cyber Security Breach**: Increasing the cyber-security paradigm for the overall organization by fine-grained network access control.
- **Remote Working**: ZTA inherently allows applications to be accessible from anywhere in the post COVID-19 world. This remote working trend will further accelerate and, in fact, ZTA can be a huge productivity enabler in such a model.
- **New Onboarding/VPN Reduction**: COVID-19 has shown that VPN based architecture is hard to scale and can cause significant cost pressures. Users, especially in branches, contact centers, etc., can be easily onboarded in a ZTA model.
- **Scalable and Analytics driven:** A ZTA-based cybersecurity approach has security principles embedded throughout the data flow, hence it is highly scalable and allows data-driven decision-making with its strong reliance on active monitoring.

CONCLUSION

Today's landscape requires change/reliability for the future. Given the nature of cloud-based applications and adoption of SaaS solutions combined with an increased need to enable safe remote working, ZTA allows for a scalable and dynamic approach to securing resources. With "**Adaptive Digital Identity**" being the cornerstone of ZTA, Zero Trust goes beyond configuration of profiles and enables optimal control for a secure user experience.

REFERENCE

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
- https://www.adobe.com/content/dam/cc/en/security/pdfs/Adobe-ZEN-WP.pdf
- https://medium.com/google-cloud/what-is-beyondcorp-what-is-identity-aware-proxy-de525d9b3f90
- https://www.okta.com/resources/whitepaper/zero-trust-with-okta-modern-approach-to-secure-access/
- https://cloud.google.com/beyondcorp

AUTHORS

Frank Alfieri, Principal Consultant
Frank.Alfieri@capco.com

Vikas Sharma, Advisor
Vikas.Sharma@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO

JN_3269