paramount
@ssuring Value

Implementing the Zero Trust Model – The Microsoft Way

Zero Trust Network Access

(Part Two, of a 3-part series)

Ashok Chandrasekharan

Vice President - Microsoft/ Cloud Security

Paramount Computer Systems

Shiju Chandroth

SME - Microsoft/ Cloud Security

Paramount Computer Systems

In part 1 of our **Zero Trust** series, we covered what **Zero Trust** is, how it's different from other solutions available now, and how it can be set up. You can check it out on our website or by clicking here.

In this 2nd part, we aim to help organizations understand ZTNA, to arrive at their **Zero Trust** readiness and the advantages and disadvantages of the **Zero Trust** framework.

The **Zero Trust** framework is now a major component of securing data and infrastructure in an organizations' digital transformation initiative. This is achieved and made possible by ensuring all users are authenticated, authorized and continuously validated for security configuration and posture. This is done before they're given access to the organization's data and applications, regardless of whether they are within or outside the organization's network.

According to Gartner, interest towards ZTNA has grown more than 127% in the first 4 months of 2021 compared to the same time period in 2020

One of the ways organizations can set up a **Zero Trust** Framework, is with the help of ZTNA.

Zero Trust Network Access

Microsoft defines **Zero Trust** as a model that assumes breach and verifies each request, as though it originates from an open network. Regardless of where the request originates from or what resource it accesses, Zero Trust teaches us to "never trust, always verify." Here's Microsoft's Zero Trust Model:

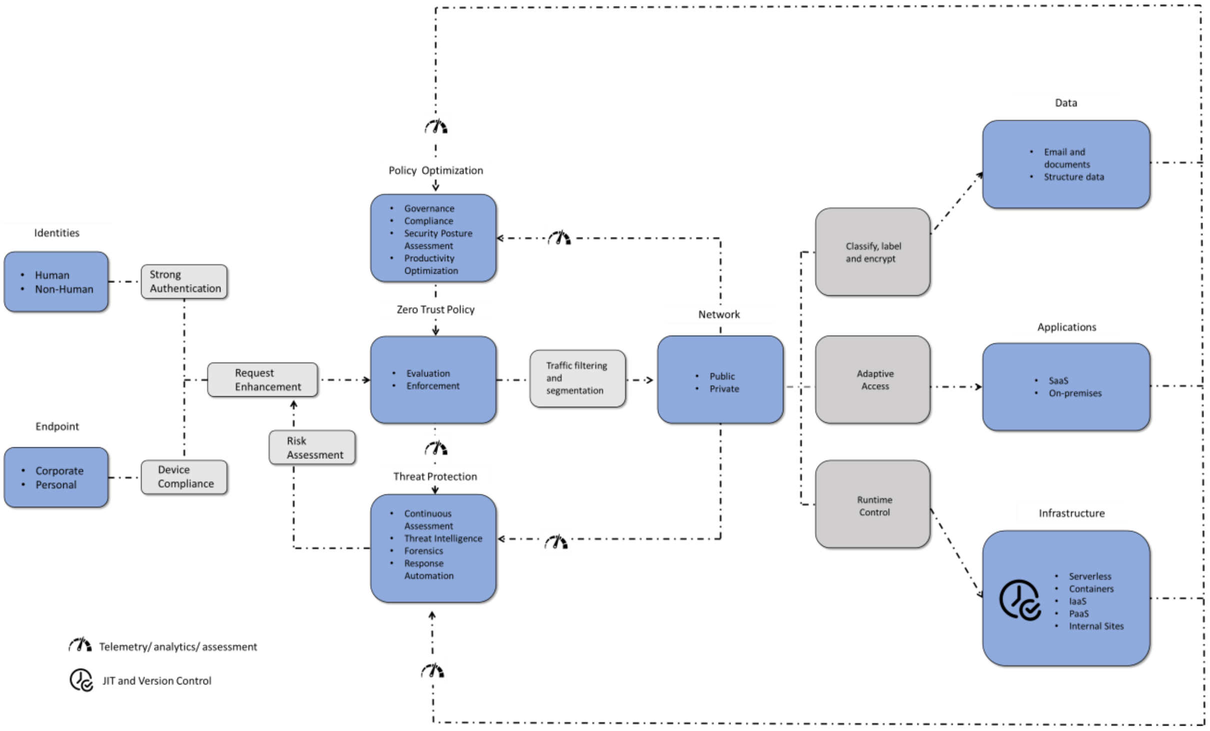


Figure 1: A holistic approach to Zero Trust should extend to your entire digital estate – inclusive of identities, endpoints, network, data, apps, and infrastructure. Zero Trust architecture serves as a comprehensive end-to-end strategy and requires integration across elements - Microsoft

Building on this concept of **Zero Trust**, ZTNA is a solution that can provide adaptive, granular, context aware and secure access to data and applications. Let's look at:

- What it is?
- How does it work?
- How is it implemented?
- How is it delivered?

– What Is It?

ZTNA as a product or service **provides secure remote access** to an organization's data, applications and services supported by clearly defined access control policies. Users are granted access to applications or resources only after they have been authenticated to the ZTNA service. ZTNA services provide a secure, encrypted tunnel that shields applications and services (that would usually be visible) from IP addresses. They also help bridge security gaps in other secure remote access technologies and methods (like VPNs) by ensuring access is granted only to specific services and applications.

> As of January 2021, Microsoft product and service offerings were featured in 33 different **Gartner magic quadrants**, and it was the leader in 20 of these. In the 10 most important magic quadrant's covering key Microsoft product offerings, Microsoft was a leader in all of them come on an often a dominant leader
>
> Gartner *Vendor Rating: Microsoft* - ID G00737912

– How Does it Work?

Based on reports from Gartner[1], despite starting off as an alternative to VPNs during the COVID-19 pandemic, organizations began taking a closer look at ZTNA as a solution to architect remote access in a safe manner. Here's how the two compare:

Table 1: VPNs and ZTNA compared

Virtual Private Networks	Zero Trust Network Access
Network centric model with a simple IP to port relationship. Works on the principle "*Trust, then verify*"	**Identity-centric model** that works based on identity, context and multi-dimensional profile. Works on the principle: "*Never Trust, always verify*"
Open Ports allow users complete access to the authenticated network, enabling uncontrolled lateral movement	**Infrastructure is cloaked** to ensure authorized users can access only approved resources, preventing lateral movement
Not sensitive to context. Authentication strength and access levels are not adjusted based on user context, access location or device capabilities	**Automatically detects** changes to user profile and network infrastructure, adjusting user access accordingly
It is **hardware bound**, difficult to deploy, static and unscalable as infrastructure changes	It is **software bound**, and provides elasticity and scalability across all hybrid environments with API integrations
Users who need access to multiple resources may need to **switch from one VPN to another**, dealing with complex and error-prone policies	Users can have access to multiple network segments and resources via a **single connection point**
Its **siloed and static** nature makes it applicable only to remote user access, rendering it unable to protect on-premises users and networks	It is **flexible, dynamic, versatile and extensible**. It goes beyond remote users, to provide unified and secure access to everyone
Can be used to access cloud accounts securely, but cannot adjust to cloud environment changes easily	Designed to protect cloud environments

[1] Gartner *Emerging Technologies: Adoption Growth Insights for ZTNA* – G00743921

How Is this Implemented?

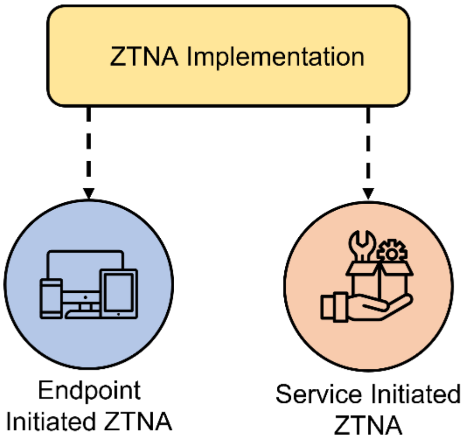


Figure 2: Types of ZTNA Implementation

Endpoint Initiated ZTNA: In this scenario, the end-user/ endpoint is initiating contact. An agent installed on the end-user contacts a ZTNA Controller, which authenticates the user and connects them to the service they are authorized to access. It is used in scenarios where the organization wants to provide nuanced, sophisticated access control.

Service Initiated ZTNA: In this case, a ZTNA broker establishes a connection between the user and the application. A ZTNA connector sits in front of business applications, which are either located on premises or on the cloud, establishing an outbound connection between the requested application and the ZTNA service broker. Once the user is authenticated for access to the application, traffic passes through the ZTNA service provider, isolating the application, and preventing direct access via a proxy. It is used when the organization is focusing on securing BYOD (unmanaged) devices and granting access to partners and customers

"More than 90% of organizations are implementing ZTNA-as-a-Service"

Gartner

How is it Delivered?

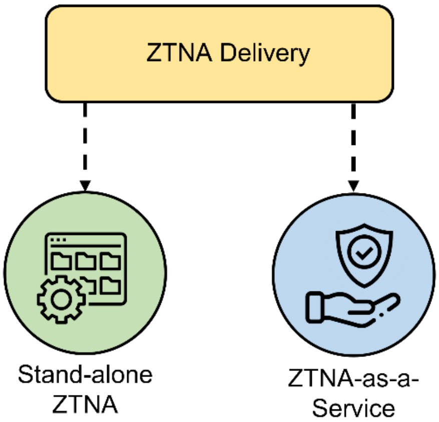


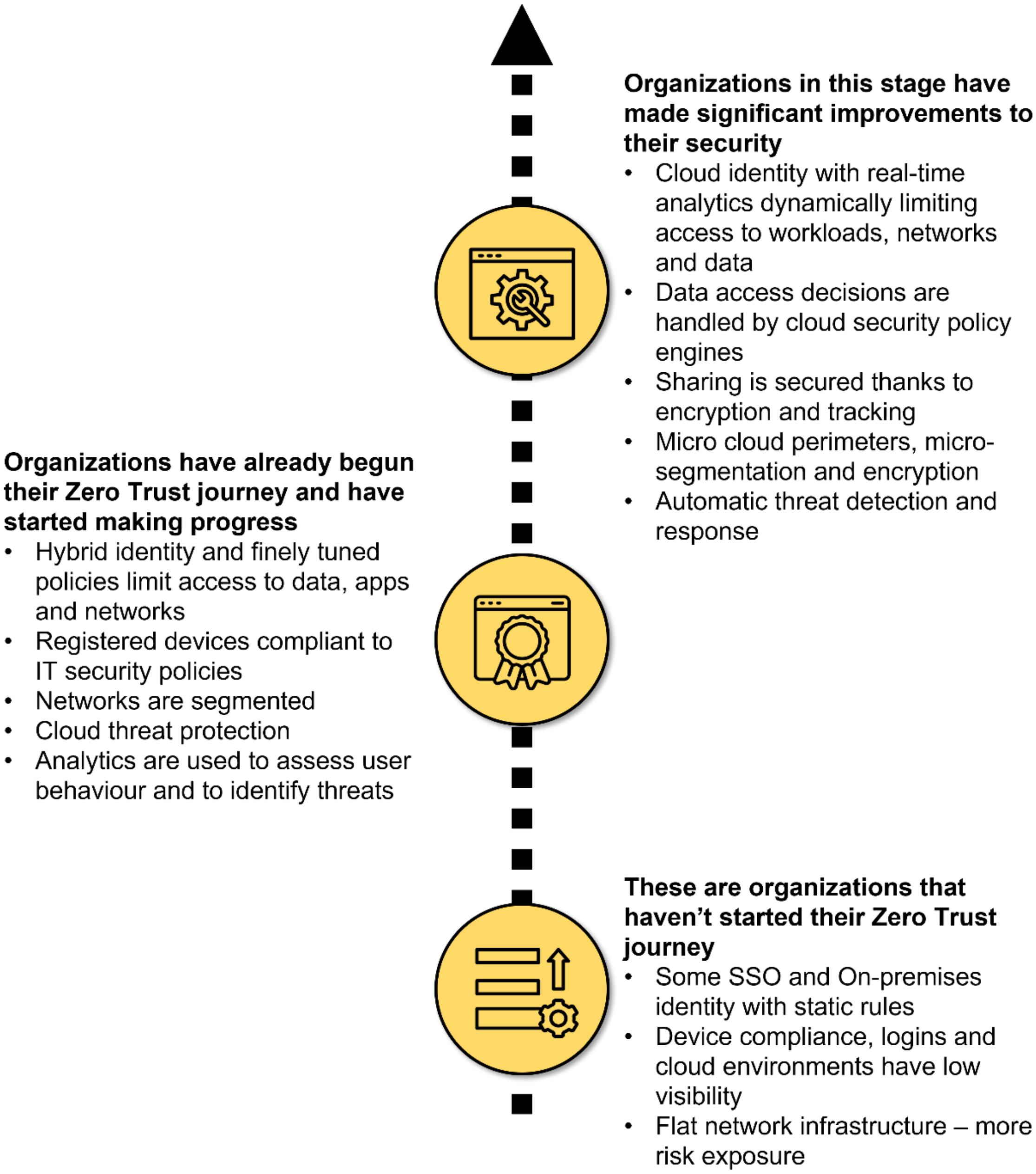
Figure 3: Types of ZTNA Delivery

Stand-alone ZTNA: The organization would have to deploy and manage all elements of the ZTNA solution which rests on the cloud or data center, orchestrating secure connections between the user and application

ZTNA-as-a-Service: Organizations in this scenario can leverage the cloud service’s infrastructure for everything. After acquiring user licenses and deploying connectors in front of secured applications, organizations can let the cloud provider handle concerns of connectivity, capacity and infrastructure

Determining Zero Trust Readiness

With each organization having its own requirements, technical implementations and security stages, the plan for **Zero Trust** implementation never remains the same. Keeping that in mind, this maturity model might help gauge where one’s organization stands in terms of **Zero Trust** implementation.



Organizations in this stage have made significant improvements to their security

- Cloud identity with real-time analytics dynamically limiting access to workloads, networks and data
- Data access decisions are handled by cloud security policy engines
- Sharing is secured thanks to encryption and tracking
- Micro cloud perimeters, micro-segmentation and encryption
- Automatic threat detection and response

Organizations have already begun their Zero Trust journey and have started making progress

- Hybrid identity and finely tuned policies limit access to data, apps and networks
- Registered devices compliant to IT security policies
- Networks are segmented
- Cloud threat protection
- Analytics are used to assess user behaviour and to identify threats

These are organizations that haven’t started their Zero Trust journey

- Some SSO and On-premises identity with static rules
- Device compliance, logins and cloud environments have low visibility
- Flat network infrastructure – more risk exposure

Figure 4: Microsoft’s Zero Trust Maturity Model

Setting Up a Zero Trust Model – Advantages and Disadvantages

Advantages

- **Decreased Vulnerability:** Provides better security to the organization, especially against lateral threats within the network (which could manifest under other security models)
- **Robust User Identification and Access Policies:** Enforces strong user management within the network, securing their accounts, and by extension- the network. Accounts are kept protected with MFA and biometrics. Users are categorized, granting them access only to data and applications required to do their tasks
- **Segmentation of Data:** Data is segmented based on type, sensitivity and use, ensuring critical/ sensitive data is protected. This way, potential attack surfaces are also reduced
- **Improved Data Protection:** Automated backups, and hashed/ encrypted message transmissions ensure data is protected both in storage and during transit
- **Great Security Orchestration:** The **Zero Trust** Model moves towards the goal of ensuring all security gaps are filled, thanks to all security elements working together in an effective and efficient manner. These elements together compliment one other

Challenges

- **Effort setting up:** Policy reorganization within an existing network can be difficult, since older policies are still required during the transition process. If legacy systems are incompatible with the **Zero Trust** Model, a new network may need to be created from scratch
- **Management of Varied Users:** Users may require monitoring with access only granted when necessary. And since there are many users who may use the company's services (customers, clients, third-party vendors), and multiple access points, each group would require a different **Zero Trust** policy
- **More Devices to Manage:** There are now multiple devices with their own properties and communication protocols within the organization. Each of them needs to be monitored and secured in a different manner
- **Complicated Application Management:** With varied applications across multiple platforms, app usage needs to be planned, monitored and tailored to the user's needs
- **Data Security**: Data stored in more than one location? Each of these sites need to be protected. Data configuration must be done adhering to the highest security standards

Conclusion

It is now abundantly clear that the advantages of setting up a **Zero Trust** Model greatly outweigh the negatives. With a closer look at ZTNA: What it is, how it's implemented and how it's delivered, we have highlighted why graduating to ZTNA from VPNs is great idea and is likely to bring massive improvements to an organization's security posture. Organizations must also have a strong understanding of their readiness to implement Zero Trust with the help of Microsoft's Maturity model.

Coming Up

In the final part of our ***Zero Trust*** Series, join us as we look at the Microsoft Cloud Applications that can help an organization achieve **Zero Trust**, as well as what Paramount can do to help in the next step of an organization's **Zero Trust** Implementation journey.

Contributors to the article:

Ashok Chandrasekharan, VP - Microsoft/ Cloud Security
Shiju Chandroth, SME - Microsoft/ Cloud Security
Amit Sharma, SME - Infrastructure & Network Security
Qusai Barwaniwala, SME - Identity and Access Management
Rahul Arun, Cloud Security Research Associate

The views, opinions, approach and designs expressed in this document are those of the authors and do not necessarily reflect that of Paramount Computer Systems. The contents of this document (in whole or in parts) may be shared with due credits and references only with consent from its authors.

Contact Paramount:
contact@paramountassure.com

Website:
www.paramountassure.com

DUBAI | OMAN | BAHRAIN | ABU DHABI | KUWAIT | KSA