paramount
@ssuring Value

Implementing the Zero Trust Model – The Microsoft Way

(Part One, of a 3-part series)

Ashok Chandrasekharan
Vice President - Microsoft/ Cloud Security
Paramount Computer Systems

Shiju Chandroth
SME - Microsoft/ Cloud Security
Paramount Computer Systems

The last two years have been a time of great change. Organizations have been forced to rethink their security strategies, and get accustomed to the new normal. Focus has now phenomenally shifted towards digital transformation, hybrid work, employee well-being, and much more. Among these aspects of focus, none ranked higher than one: **Cybersecurity.** Suddenly, the (then) current security systems just weren't enough!

The pandemic created compelling situations for organizations to look **beyond their existing security model at the perimeter and network level.** In an attempt to classify users as "trusted" or "untrusted", providing trusted users access to permissible organization's data and applications, and governing this permission. This thought process however, was **no longer viable** thanks to an alarmingly high number of insider threats and attack sophistication. Data breaches we costing companies an average of $3.33 million dollars each.[1]

That's where **Zero Trust** stepped in.

In this 3-part series, we'll be detailing how organizations can understand **Zero Trust** better and how it can be adopted.

Part 1: This article discusses what exactly Zero Trust is, what it shouldn't be confused with, and how it can be set up

Part 2: ZTNA, how to determine ones Zero Trust readiness, advantages and challenges to the Zero Trust Model

Part 3: How Microsoft has geared its security stack to provide the Zero Trust framework to its clients

What Is Zero Trust?

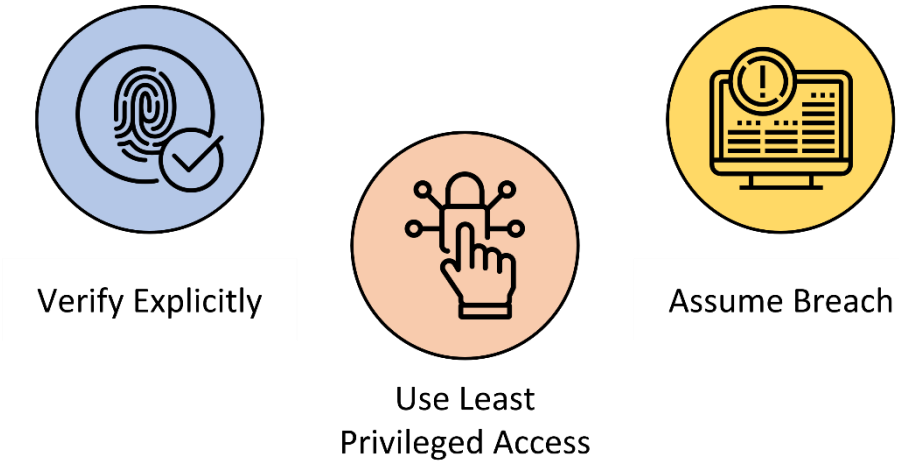

Figure 1: The three principles of Zero Trust

Coined back in 2010 by John Kindervagn, an analyst at Forrester Research, the term "**Zero Trust**" focuses on three main principles:

[1] Cost of a Data Breach Report – IBM Security

- **Verify explicitly**: Continuous authentication and authorization based on all data points (user identity, location, data classification, anomalies, service or workload, device health)
- **Use least privileged access**: User access is limited with just-in-time and just-enough-access, risk adaptive policies and data protection to ensure data protection and productivity
- **Assume breach**: Reduce blast radius and segment access. Verify end-to-end encryption and use analytics for greater visibility, easier threat detection and better defence

A Zero Trust Solution Should Not Be Confused With…

Legacy VPNs

- Legacy VPNs have a hard time scaling up to the harsh demands of the post-pandemic world. To increase capacity, they require proprietary, expensive and ancillary hardware
- Due to their simplistic nature, they require everything to be tunnelled. They add cost and complexity to the network, introducing additional strain to the already taxed bandwidth
- Despite MFA, security becomes a major concern for VPNs, as a bad actor with someone's VPN's credentials can access all of the organization's sensitive data

Cloud Access Security Brokers (CASB)

- CASB tools enable IT administrators to manage any data or application that the organization has stored/ hosted on the cloud. However, a major caveat when it comes the solutions is that their protection does not extend to on-premise applications and data

Zero Trust works on the motto:
Never Trust, Always Verify

That's why the **Zero Trust** Model is better. The model always assumes breach and verifies each request like it's from an open network. Each request is authenticated, authorized and encrypted before it can come through into the network. The principles of microsegmentation[2] and least privileged access are used to minimize lateral movement, and intelligence and analytics are used to respond to handle anomalies in real time.

[2] It is a technique that divides the network into logical and secure units to ensure threats are contained and not spread across the enterprise

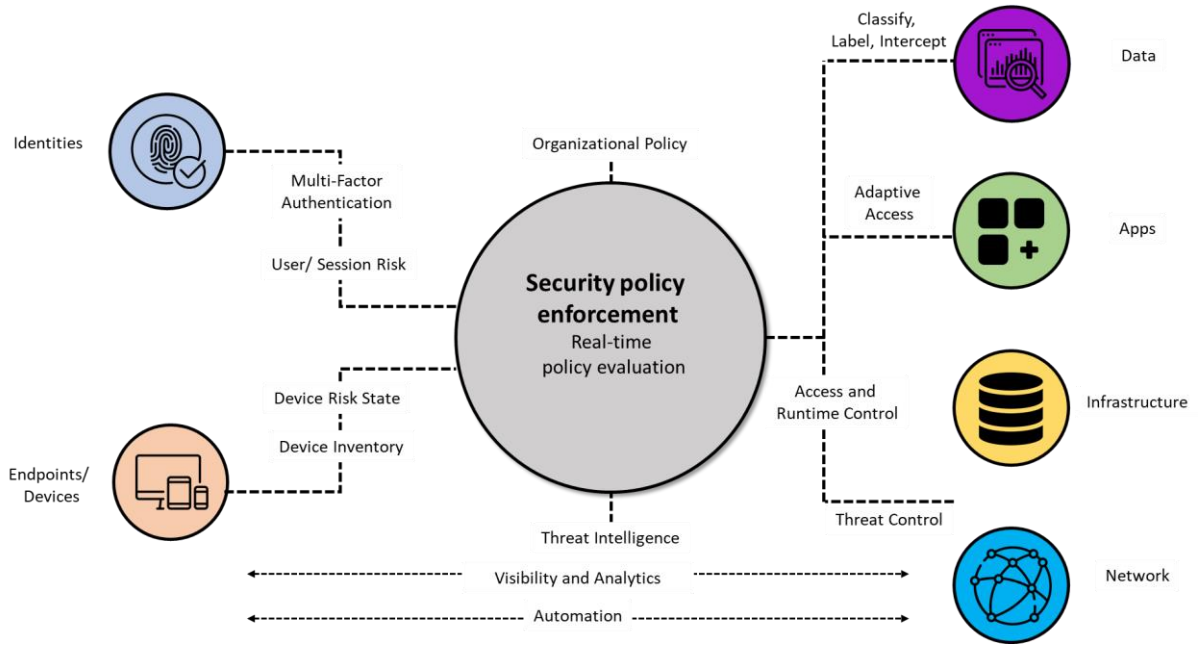

Figure 2: The Zero Trust Model takes into consideration identities, endpoints, network, data, applications and infrastructure alongside threat intelligence and organization policy to ensure security

How to Set Up a Zero Trust Model?

The steps to set up a **Zero Trust** Model are as follows:

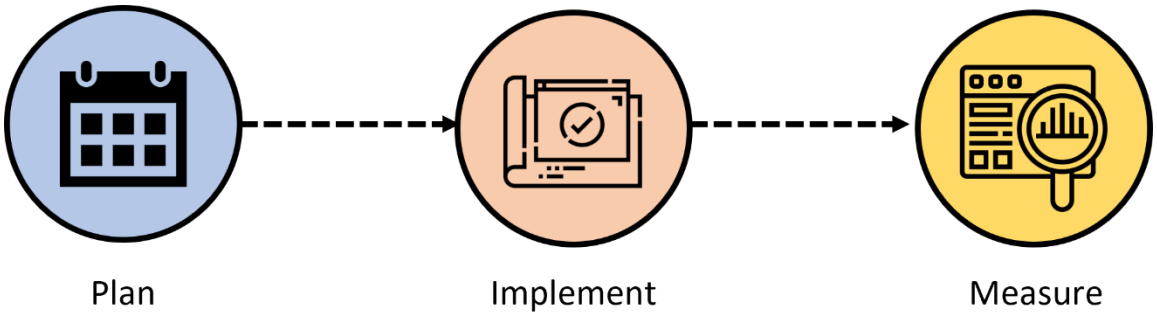

Figure 3: The three steps to setting up a Zero Trust Model

Step 1: Plan

Create a business case that closely adheres to the risks and strategic goals of the organization. The steps are:

- **Define a vision**: Setting up this model is a journey that can span many years. Clearly defining the organization's goals, outcomes and architectures make it more likely for it to succeed
- **Get buy-in from leadership:** Obtain leadership support for a clearer understanding and easier alignment of the plan with the organization's goals, budget allocations and internal alignment
- **Empower end-users:** The model enables tech teams to directly interact with end-users and making security a major component in improving their experiences and productivity

"By 2023, 60% of enterprises will phase out most of their remote VPNs in favor of Zero Trust Network Access "
- Gartner

Step 2: Implement

Create a strategy for **Zero Trust** deployment that spans multiple years, while prioritizing early actions suited to different business needs. Divide the implementation into different initiatives, and align them to business goals. Evaluate potential business impact, friction and challenges. Most technical strategies and architectures usually group into the following security initiatives:

- Productivity Security
- Modern security operations
- Operational security and IoT
- Datacentre, services, and API

Step 3: Measure

Track the successes of one's **Zero Trust** deployment to strengthen faith in the implementation to bring measurable improvements. These include:

- **Business improvement:** Measurements that aim to provide frictionless user and developer experiences.
    - Number of security interruptions
    - Deployment milestones
    - Visibility milestones
    - Average boot for managed devices (in seconds)
    - Average time for security evaluation of devices (in days)
- **Security effectiveness:** Measurements that highlight the organization's security posture and consequences of security incidents
    - Number of incidents (ordered by severity)
    - Deployment milestones
    - Visibility milestones
    - Improvements in security posture – tracked in Microsoft Secure Score
- **Security simplicity:** Measurements that indicate the simplification of security requirements
    - Number of duplicate tools that perform the same function
    - Number of security tools that require custom integration
    - Percentage of time spent by the IT team to deal with low value requests (Password resets)
    - Number of manual steps in repeating workflows
    - Percentage of false positives investigated
    - Ratio of time spent maintaining tools vs. actual response to incidents

Conclusion

The **Zero Trust** Model is the ideal solution, given our current security environment. We've covered what it is, how it's different from other solutions and how it can be set up. However, that's just scratched the surface of the concept that is **Zero Trust**.

Coming Up

In part 2 of our ***Zero Trust*** series, we'll be covering ZTNA, how one can determine the readiness of their organization to embrace the **Zero Trust** model and the advantages and challenges of setting it up. For more information, please get in touch with Paramount via our website or social media platforms.

Contributors for 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

Contact Paramount:
contact@paramountassure.com

Website:
www.paramountassure.com

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