Implementing the Zero Trust Model – The Microsoft Way

(Part **Three**, of a 3-part series)

Amit Kumar Sharma

SME – Infrastructure and Network Security

Paramount Computer Systems

Shiju Chandroth

SME - Microsoft/ Cloud Security

Paramount Computer Systems

Rahul Arun

Research Associate – Cloud Security

Paramount Computer Systems

March 2022

Zero Trust has now become an integral part of any organization's security infrastructure and framework. Our **Zero Trust** series aims to provide a greater understanding over this revolutionary concept.

In Part 1 of our Zero Trust series, we covered what Zero Trust is, how it's different from other solutions and how it can be set up. The article can be found here: https://bit.ly/ZT_part1

In Part 2, we took a closer look at ZTNA: What it is, how it's implemented and how it's delivered, and how organization can determine their readiness to implement a Zero Trust. The article can be found here: https://bit.ly/ZTPart2

In this final part, we will showcase how a Zero Trust framework can be implemented, taking advantage of technologies from Microsoft and AppGate, with the help of a use case

Use Case – Achieving Zero Trust

Problem Statement – Before Zero Trust

With standard security controls, identities and devices can be compromised due to the absence of:

- Proper identity management
- Proper access management
- Sufficient device management
- Sufficient context-based access systems

In the below diagram we attempt to represent the potential challenges that can be faced by an organization across: Identity management, Access Control, Application Management and Data Security

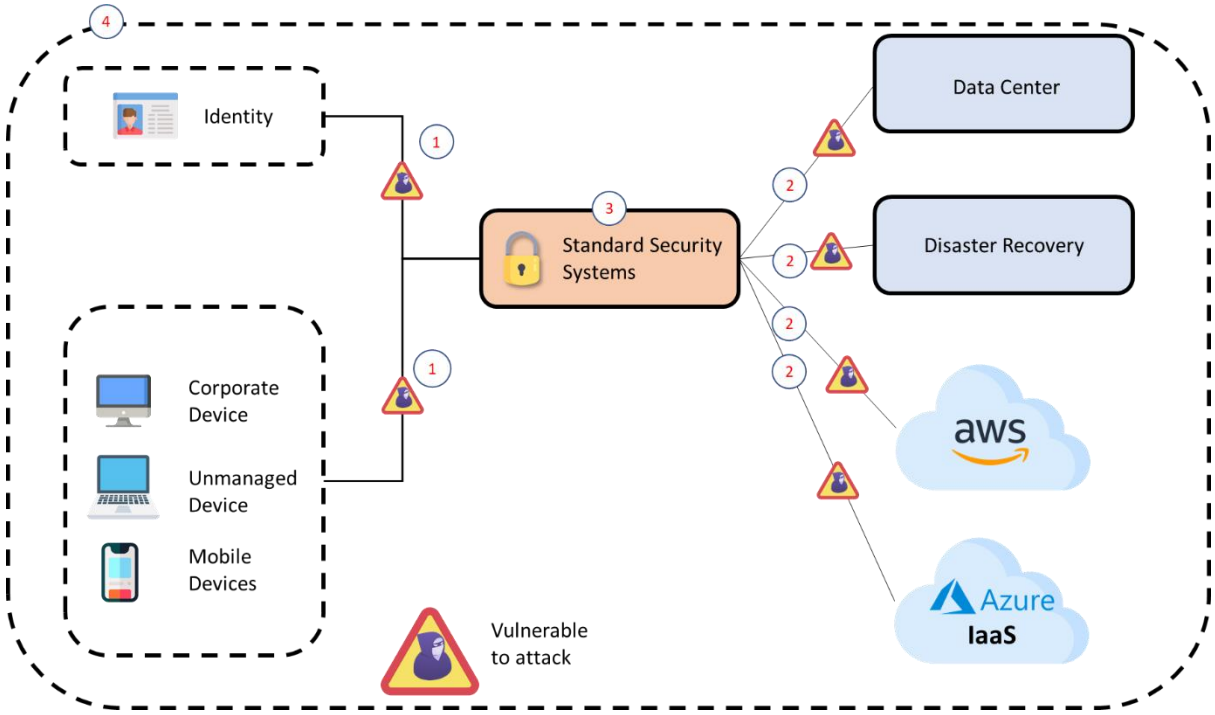

Figure 1: The infrastructure before Zero Trust

1 Employee Identity and Device Management	2 Application Security	3 Context-based Solution	4 Data protection
Having to deal with employee identity devices (managed/ unmanaged)	Managing security of applications on the cloud, on-premises across multiple platforms & data centers	The requirement for a single solution that provides access to all the required platforms, based on context	Protecting the data flowing in and out of the network
Potential Risks: • Over-privileged access • Not having end to end encryption • Open for DOS attacks and lateral movement	**Potential Risks:** • Cloud services may be subject to malicious activity • Unauthorized access to SaaS applications • Unauthorized data transfer between applications leading to data theft	**Potential Risks:** • Access from unauthorized device • Spoofed/ leaked credential • Open access	**Potential Risks:** • Data leakage • Data misuse • Loss of organizational reputation

Figure 2: Challenges and risks faced by an organization

The Zero Trust Solution – With Microsoft and AppGate SDP

The below blueprint represents a simple, yet effective strategy to mitigate the challenges using two robust solutions:

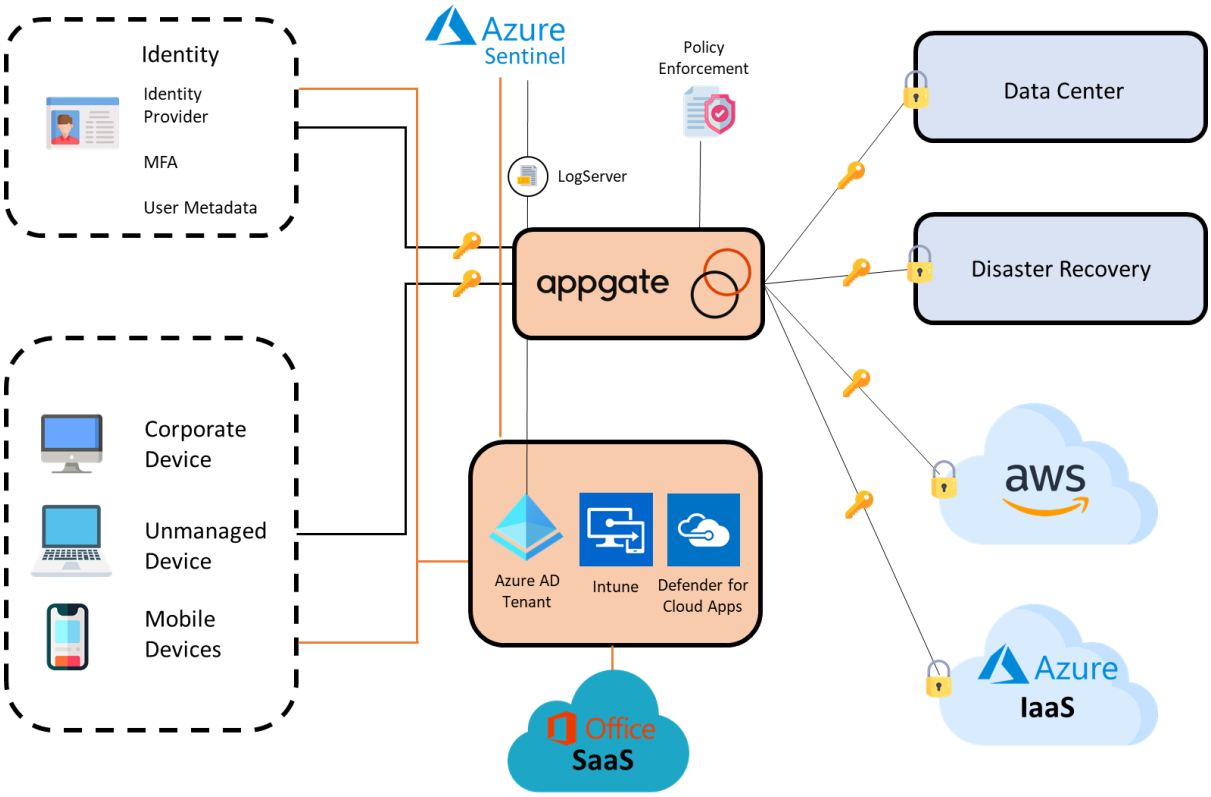

Figure 3: The Zero Trust Solution - With Microsoft and AppGate SDP

The next table details the solution that can be adopted, the risks mitigated, and the processes enabled.

1 Employee Identity and Device Management

Having to deal with employee identity devices (managed/ unmanaged)

Potential Risks:
- Over-privileged access
- Not having end to end encryption
- Open for DOS attacks and lateral movement

The Solution:
- **Azure Active Directory:** A cloud-based identity and access management service
- **Microsoft Intune:** A cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM)

The Process:
- The user is authenticated with Azure Active Directory, which is a store of identities and roles that are allowed to gain access to different organizational resources
- While AppGate ensures only the right people get access to the resources, Microsoft Intune protects the organizational data present within the user's device with MDM or MAM capabilities, based on the specification provided by the organization

2 Application Security

Managing security of applications on the cloud, on-premises across multiple platforms & data centers

Potential Risks:
- Cloud services may be subject to malicious activity
- Unauthorized access to SaaS applications
- Unauthorized data transfer between applications leading to data theft

The Solution:
- **Microsoft Defender for Cloud Apps**: A Cloud Access Security Broker (CASB) that operates on multiple clouds, and provides rich visibility, control over data travel and sophisticated analytics to identify and combat cyber threats across all your cloud services

The Process:
- For users to gain access to SaaS applications, organizations can take advantage of Microsoft Defender for Cloud Apps (formerly Microsoft Cloud Apps Security)

3 Context-based Solution

The requirement for a single solution that provides access to all the required platforms, based on context

Potential Risks:
- Access from unauthorized device
- Spoofed/ leaked credential
- Open access

The Solution:
- **AppGate SDP:** A ZTNA solution that provides users with secure access to enterprise and cloud-based resources

The Process:
- A user who wants to access the organization's systems will connect to a AppGate policy server/ controller (which can be on-premises or on the cloud).
- A key exchange will take place between the server and a corporate device. This is done with a TLS key.
- The device is authenticated if it's carrying a valid key. After this, the user is authenticated.
- Here the details provided by the user are matched with the information within Azure Active Directory. The device's configurations like firewall status, update status and other properties are matched with the policies specified by the organization
- AppGate then provides the user with a token that approves his/ her access to a cloud service, data center or resource of their choice

4 Data protection

Protecting the data flowing in and out of the network

Potential Risks:
- Data leakage
- Data misuse
- Loss of organizational reputation

The Solution:
- **AppGate SDP**
- **Microsoft Sentinel**: A cloud-native, scalable, security information and event management (SIEM) and Security Orchestration Automation and Response (SOAR) solution

The Process:
- Despite having its own SIEM solution, AppGate SDP does not collate the logs from the other components involved in the process. For this, Microsoft Sentinel is used
- Microsoft Sentinel provides a holistic view of logs from managed devices, Intune, AppGate SDP, Microsoft Defender for Cloud. The SIEM and SOAR solution enables investigators to have access to multiple logs within a single platform

Success Criteria

- Ensuring users have access to resources when required, enabling projects to be completed in a timely manner
- The organization's network is protected from attackers with malicious intent
- The organization was able to control user access to their network regardless of their location
- AppGate was able to provide context based, dynamic access to users by setting up a secure connection
- Enabling security engineers to protect the organization with the help of logs brought into a single platform (Azure Sentinel) to provide a holistic view over the activities of the remote workforce

Conclusion

With the solutions offered by Microsoft and AppGate SDP, organizations can ensure that sensitive information within devices remains protected, and that only the right people are given access to the network. This way, ensuring the different tenants of **Zero Trust** are satisfied.

For more on how Paramount can help your organization achieve its **Zero Trust** goals, you can get in touch with us at *www.paramountassure.com*.

Or send us an email at: ashok.c@paramountassure.com

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, Research Associate - Cloud Security