Why Zero Trust User Access is vital for secure remote working?

This is how we see it.

Wipro and Microsoft recently hosted a joint CISO panel event on the topic of Zero Trust user access for a secure remote working environment. The purpose of this white paper is to discuss the role played by Zero Trust user access in securing the remote working, elaborate some of the key points from the CISO panel discussions and learn how Microsoft security solutions enable organizations to secure their users, devices, network, applications, and data through Zero Trust security approaches.

The trusted perimeter is no longer effective

A rare global crisis like COVID-19 has transformed human life as well as the enterprise operating model. Working remotely on a massive scale is bringing new security challenges to organizations as untrusted networks and unhealthy devices are being leveraged to connect to the enterprise network, systems and services. While leveraging existing remote connectivity solutions and trust-model dependent security solutions to meet the remote working requirements, organizations are witnessing their attack surface grow in today's increasingly hostile threat landscape. All the CISOs in the panel echoed the same opinion - the need to rethink the fundamentals of perimeter centric and trust-based security and the way it protects enterprise critical applications, data, devices, and users.

Zero Trust – The new security fundamental

Today, organizations require a security model that effectively adapts to the complexity of the current modern workplace environment and safeguard from the evolving threat landscape. It should efficiently support the mobile workforce and protect users, devices, applications, and data wherever they are located.

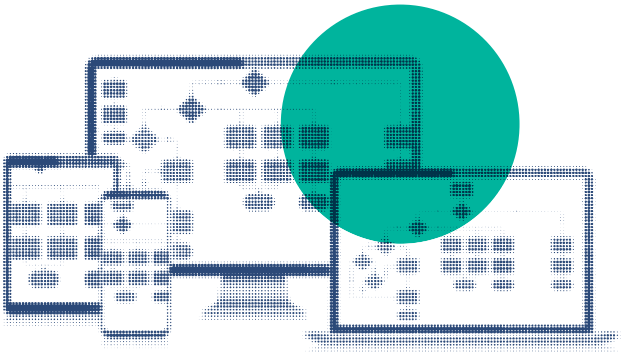
The Zero Trust security model is not new and it has been in discussions and practice for quite some time. However, it was majorly leveraged in a narrowed scope among risk signal sources sources such as network, data, applications, users, and devices. They work independently and do not share the threat signals and intelligence with each other, preventing it from being a comprehensive and effective security model. However, they all share the common Zero Trust principles such as:

- Verify explicitly
- Apply least privilege access
- Always assume breach

But with the new normal working atmosphere, we are all in a perimeter-less world and identity is the new perimeter. Hence the Zero Trust should start from the user access, and it is very critical that the enterprise access management solution supports the above three core Zero Trust security principles. Based on a majority view of the CISOs at the panel discussion on the Zero Trust user access, it appears that several organizations are in the process of adopting the Zero Trust security model and would start with identities.

Start your Zero Trust journey with Microsoft Security Stack

Microsoft provides a strong foundational security solution to kick start your zero trust journey. Azure Active Directory Conditional Access helps organization to provide granular access to users and devices to access applications and data securely by leveraging billions of threat signals and providing real-time threat protections.



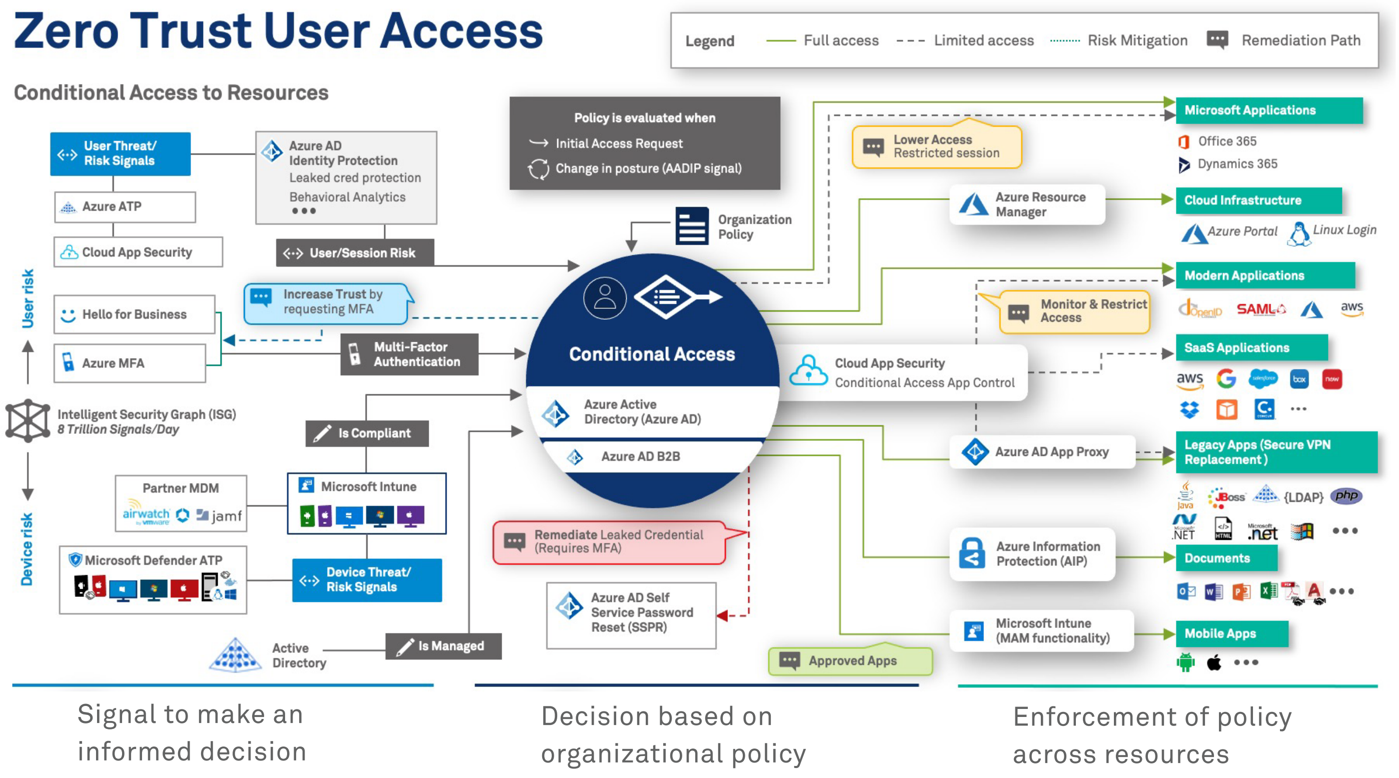


Figure 1: Microsoft working model of Zero Trust User Access reference

Azure AD native integrations with mobile device management systems (Intune), Advanced Threat Protections (ATPs) and Cloud App Security provide a strong Zero Trust orchestration platform to enforce your organizational Zero Trust user access policies. Microsoft Graph APIs allow integrating with third party risk signals and automating real-time risks remediation before the user trust is established to gain access to corporate data.

Microsoft security solutions provide adequate building blocks to drive your Zero Trust user access implementation. Some of the key pillars of the Zero Trust user access include:

Multi-factor authentication and password-less support to increase the identity trust

Device lifecycle management capabilities and native integration with mobile device management solutions like Intune for device compliance and hygiene status

Identity protection to detect and mitigate real-time user and session risks

Conditional access policies to orchestrate your Zero Trust policies and provide granular access to corporate applications and data

Native support of integrations with various threat and risk signals from Microsoft intelligent security network, Advanced Threat Protection solutions (Azure ATP, O365 ATPs, ASC, and Microsoft Defender ATP), Azure information protection for data classification, protection, cloud app security, and the ability to integrate with third party risk signals via graph APIs

Enforcement policy engine to mitigate real-time threats during user access

Conclusion and Takeaways

From the collective view points from the panel discussion, it is obvious that most of the organizations are re-prioritizing their security programs to focus on strengthening their remote workplace environment by adopting Zero Trust security principles.

Some of the key learnings from this event include:

- Expanding and securing the organization's existing VPN infrastructure to support the massive remote workforce is top priority
- Leveraging cloud-based (like Azure AD) identity and authentications for corporate resources such as workstations and apps can help solve scalability issues, improve security and enrich user experiences
- Enforcing two-factor authentications for all remote users accessing corporate resources are vital to secure user identities
- Leveraging virtual desktop solutions (like WVD) for users that use personal devices to access corporate resources help provide controlled data sharing
- Ensuring that necessary information protection and data loss prevention controls are in place to safeguard sensitive data
- Strengthening third-party risk management practices to actively oversee the supply chain so that only trustworthy third parties are used
- Zero Trust is a journey and starts with adopting the Zero Trust user access approach to strengthen the remote working environment

About Author

Prakash Narayanamoorthy

Microsoft Security Practice Partner & Principal Security Architect

Wipro Ltd

Prakash spent 17+ years in the Identity and Security domain, and helped multiple large global organizations to solve complex IAM challenges.

Wipro Limited
Doddakannelli,
Sarjapur Road,
Bangalore-560 035,
India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 180,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at **info@wipro.com**