Securing the modern workplace

Wipro Security Services and Microsoft 365 E5 Security & Compliance Solutions

wipro CyberSecurity by CyberSecurists

Microsoft 365

Foreword

Wipro and Microsoft have come together to fortify customers' workplace transformation journeys with Microsoft 365 Security and Compliance Solutions & Services.

This partnership provides customers with the seamless and quick adoption of Microsoft 365 security and compliance solutions, and continuous improvements through managed services to strengthen their modern workplace environment.

wipro | CyberSecurity by CyberSecurists.

"As a Microsoft Gold and Global strategic security partner, we have a successful history of transforming workplaces with powerful, mission-critical, Microsoft-based security solutions that meet the needs of enterprises worldwide. With the recent acquisition of Edgile, we have further strengthened our Microsoft security consulting and advisory capabilities to accelerate our customers' modern workplace initiatives with Microsoft 365 E5 Security & Compliance."

- Tony Buffomante
Senior Vice President
and Global Head,
Cybersecurity and Risk Services,
Wipro Limited

Microsoft | Microsoft Security

"'Our mission, together' - We often say that security is a team sport, and Microsoft has never been more committed to working with our partners to protect customers and create a more secure world for all. I am grateful to be on this journey with you, our partner community, and I am inspired by the work you do every day. Through this mission, we have the power to shape the world in positive and profound ways, with customer trust at the heart of everything we do."

- Vasu Jakkal
Corporate Vice President
Security, Compliance, Identity and Privacy
Microsoft

Securely enabling the new way of working at the modern workplace

In the current digital era, enterprises are dealing with a multitude of identities through various personas (employees, partners, consumers, system identities, etc.) and connected things. The enterprise data, applications and server residency have been moving from on-premises governed zones to multi-cloud environments.

The explosion of cloud and mobile applications, along with rapid adoption of cloud workloads, has opened huge security risks and widened the gap with on-premises centric security solutions that work in silos.

To combat and stop advanced threats that are evolving around the new way of remote working, enterprises need easily deployable, multi-layered, and integrated security solutions with cognitive intelligence for their modern workplace environments. Adopting Zero Trust security principles will significantly improve the overall security of the enterprise workplace.

Typical expectations at the modern workplace

Organizations to allow majority of the workforce to securely work remotely

Employees allowed to use personal devices (BYOD) to access corporate resources and be compliant

Users to be allowed to securely access corporate resources through untrusted and insecure network (e.g., home network)

Shadow IT problems realized due to greater adoption of SaaS apps by internal departments that bypass central IT, requiring security controls to be in place to control unsanctioned, risky apps and prevent data exfiltration

Securely enabling the new way of working at the modern workplace

Common challenges

- How do we ensure that all remote user sign-ins to corporate resources are protected from malicious attacks?
- How do we ensure visibility of corporate data is protected while allowing managed and unmanaged devices access through trusted and untrusted networks?
- Are my current security controls sufficient to monitor, detect, and respond to advanced and real-time attacks on identities, devices, and apps?
- Are my privileged admins connecting remotely protected from privilege escalation attacks?

Securely enabling the new way of working at the modern workplace

Secure remote working is the foundation of modern workplace

The significant increase in remote working and mobility, multi-cloud adoption, and digitization has pushed enterprises to go boundary-less. This has created newer security challenges to combat continuously evolving threats. The modern workplace demands enhanced user experiences, improved compliance, and intelligent, integrated security solutions to safeguard organizational sensitive assets at cloud scale.

Common security risks in the modern workplace

- Identity takeovers and password attacks
- Complete access to networks instead of individual applications
- Risk of malware transmission from home to corporate networks
- Access to malicious websites
- Possibility of confidential data leakage and uncontrolled data sharing
- Lack of controls to detect and stop user or endpoint behavioural anomalies

Attackers are now very active in targeting remote working users and devices to penetrate the corporate network, making it paramount to protect identities, devices, and apps holistically to ensure a secure and compliant workplace.

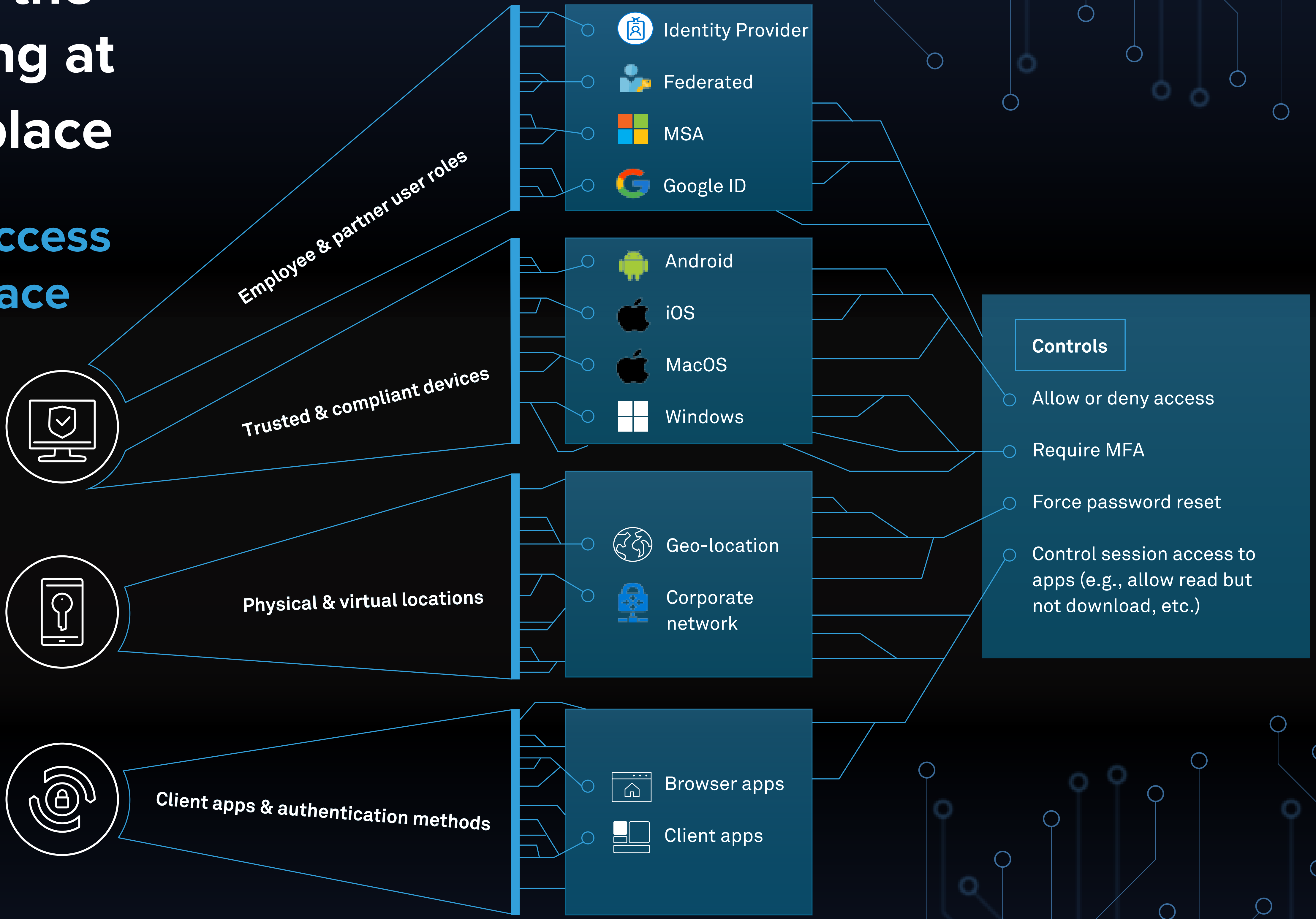
Securely enabling the new way of working at the modern workplace

Approach to secure access at the modern workplace

- Who are your users? What apps are they trying to access? How are they doing it? Why are they doing it that way?

- What conditions are required to access a corporate resource?

- What controls are required based on those conditions?


Employee & partner user roles
Identity Provider
Federated
MSA
Google ID
Trusted & compliant devices
Android
iOS
MacOS
Windows
Physical & virtual locations
Geo-location
Corporate network
Client apps & authentication methods
Browser apps
Client apps
Controls
Allow or deny access
Require MFA
Force password reset
Control session access to apps (e.g., allow read but not download, etc.)

Zero Trust – The new security fundamental for modern workplace

Today, organizations require a security model that effectively adapts to the complexity of the current modern workplace environment and safeguards 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 has been in discussions and practice for quite some time. However, it was primarily leveraged in a narrowed scope among risk signal sources such as network, data, applications, users, and devices. These typically 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 including:

- Verify explicitly
- Least privilege
- Assume breach

Begin the ZT journey with key controls

Identities

- ○ Strong authentication (e.g., multi-factor authentication or passwordless authentication)
- ○ Automated risk detection and remediation
- ○ Adaptive access policies to gate access to resources

Endpoints

- ○ Data loss prevention policies and controls for all unmanaged and managed devices
- ○ Real-time device risk evaluation and endpoint threat detection
- ○ Devices registered with identity provider

Apps

- ○ Ongoing shadow IT discovery and risk assessment
- ○ Granular access control to apps (e.g., limited visibility or read only)
- ○ Policy-based access control for apps

Network

- ○ Secure access controls to protect networks
- ○ Threat protection and filtering with context-based signals
- ○ All traffic encrypted

Infrastructure

- ○ Access to threat detection tools for security operations team
- ○ Cloud workload protection across hybrid and multi-cloud
- ○ Granular visibility and access control across all workloads (virtual machines, servers, etc.)

Data

- ○ Access decisions governed by security policy engine
- ○ Data classified and labeled
- ○ The most sensitive files persistently protected with encryption

Automation & Orchestration

- ○ End-to-end visibility established with a centralized platform for investigation and response
- ○ Threat data is collected and analyzed across domains (identities, endpoints, apps, network, infrastructure)
- ○ Automated investigation and response enabled

Wipro’s Modern Workplace Security Solution

A comprehensive solution from Wipro and Microsoft to simplify and strengthen protections for work wherever it happens

Modern workplace demands

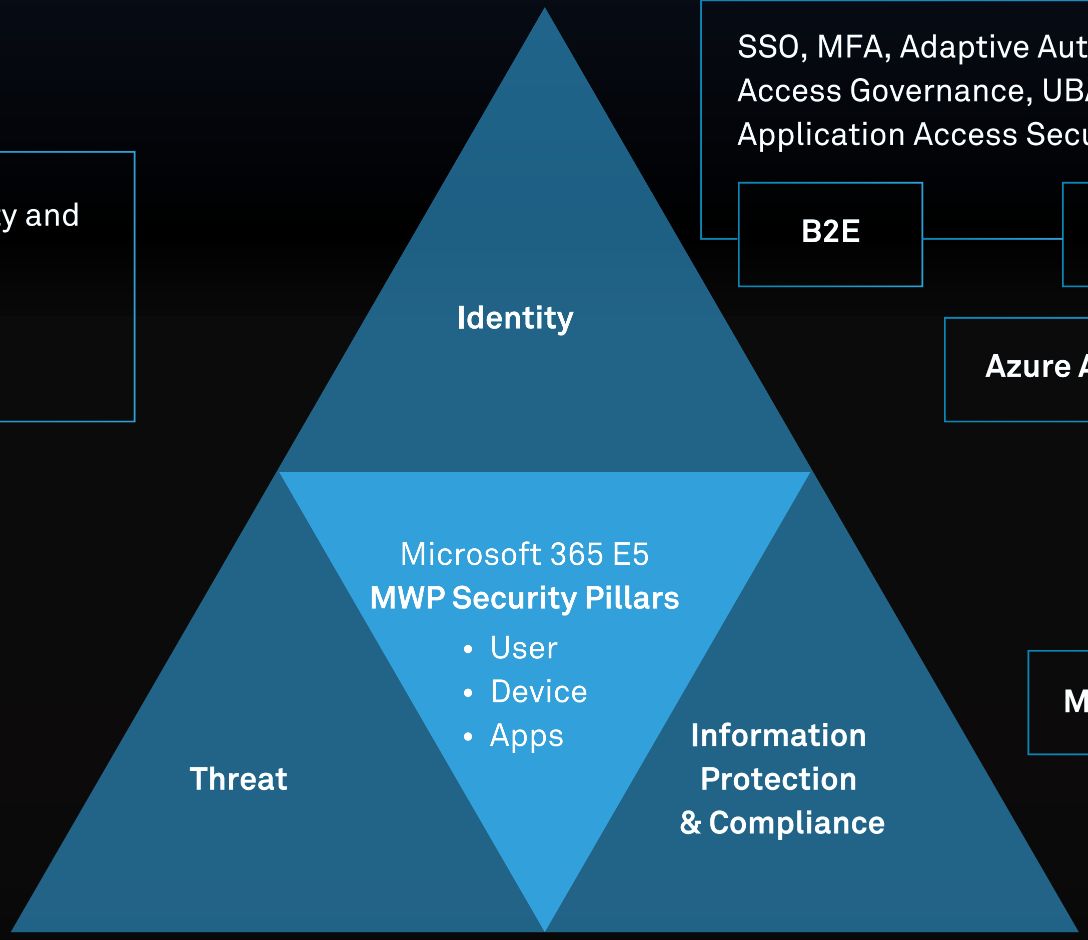
- Remote working
- Mobility
- Hybrid / Multi-cloud
- Digitization

Security expectations

- User experience
- Improved compliance
- Intelligent protection
- Lower costs
- Zero Trust

- Comprehensive & integrated security and compliance solutions for workplace
- Cloud delivered and AI/ML powered

Microsoft 365 Defenders



Identity

Microsoft 365 E5

MWP Security Pillars

- User
- Device
- Apps

Threat

Information Protection & Compliance

SSO, MFA, Adaptive Authentication, Privileged Identity, Access Governance, UBA, Secure Hybrid Access, Application Access Security, RBAC, Consumer IAM

B2E **B2B** **B2C**

Azure Active Directory

Microsoft Information Protection

Endpoint Protection	Identity Protection	Office 365 Protection	Cloud Apps Protection & Compliance	Information Protection	Compliance

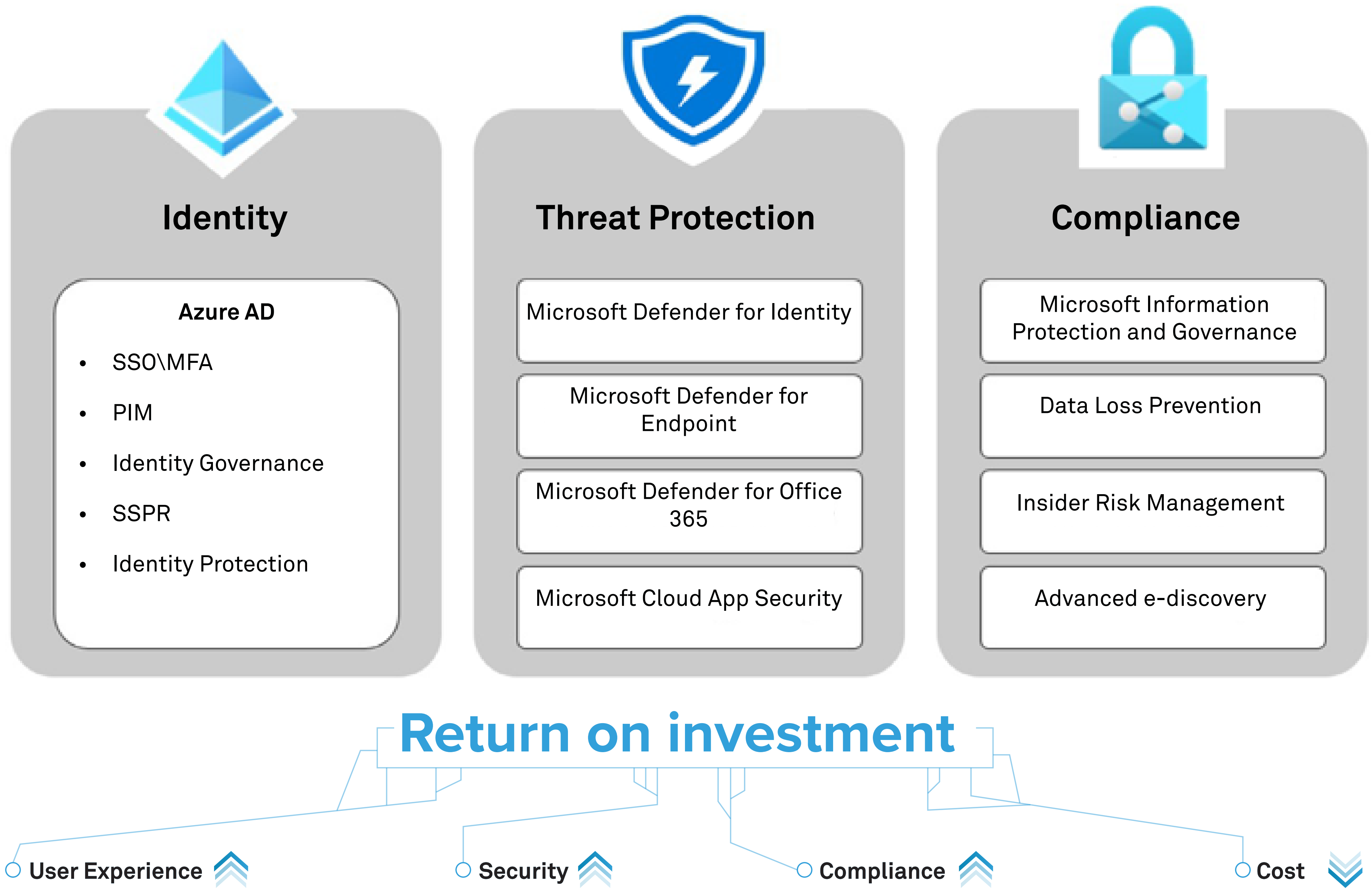
Across physical and virtual machines and devices, email and CASB leveraging Microsoft 365 Defenders MCAS, Endpoint Manager, and Windows 10 security

Data discovery, classification & labelling, controlled sharing, DLP, auditing & monitoring, eDiscovery across Office 365 and SaaS apps and endpoints

Why Microsoft 365 E5 Security & Compliance Solutions for the modern workplace?

- Seamless Single Sign-on with Adaptive Multi-factor authentication via Azure Active Directory service
- Automated digital identity lifecycle management and governance to improve efficiency for all personas
- Password attack surface reduction (password protection and password-less)
- Improved privilege identity governance
- Identity threat visibility and protection
- Improved security posture through identity, endpoints (EDR), and cloud app advanced threat visibility with automated response via Microsoft 365 Defenders
- Advanced threat protection for Office 365 apps
- SaaS threat visibility via shadow IT discovery and controls
- Improved compliance posture through data classification, labelling, and protection policies
- Data loss preventive capabilities to strengthen compliance
- Insider risk management to proactively identify and prevent insider risks
- Efficient and quick digital evidence collection to preserve for litigation cases via advanced eDiscovery and record management solutions.

Microsoft 365 Enterprise E5



Identity

Azure AD

- SSO\MFA
- PIM
- Identity Governance
- SSPR
- Identity Protection

Threat Protection

- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Cloud App Security

Compliance

- Microsoft Information Protection and Governance
- Data Loss Prevention
- Insider Risk Management
- Advanced e-discovery

Return on investment

- User Experience ↑
- Security ↑
- Compliance ↑
- Cost ↓

Achieving Zero Trust user access at the workplace

Azure AD native integrations with mobile device management solutions (MEM/Intune), advanced threat Protections, and cloud app security provide a strong Zero Trust orchestration platform to enforce your organizational Zero Trust user access policies. Microsoft Graph APIs allow integration with third-party risk signals and automate real-time risk remediation before 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.

Azure Active Directory

- Adaptive MFA
- Privilege access
- Password-less
- Identity protection
- Continuous risk evaluation
- Real-time identity threat mitigation

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

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

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

Native support for integrations with various threat and risk signals from Microsoft intelligent security network, advanced threat protection solutions (Microsoft 365 Defenders and Azure Defenders), Microsoft information protection for data classification, protection, and cloud app security

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

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

Combating advanced threats at the workplace with Microsoft 365 Defenders

What do Microsoft 365 Defenders do?

- Protect against attacks and coordinate defensive responses across the suite through signal sharing and automated actions
- Provide full visibility on the attack across product alerts, behaviors, and context for security teams by joining data on alerts, suspicious events, and impacted assets to 'incidents'
- Automate response to compromised assets by triggering self-healing remediation
- Enable security teams to perform detailed and effective threat hunting across endpoint and Office data

Microsoft 365 Defenders Services

Microsoft Defender for Endpoint

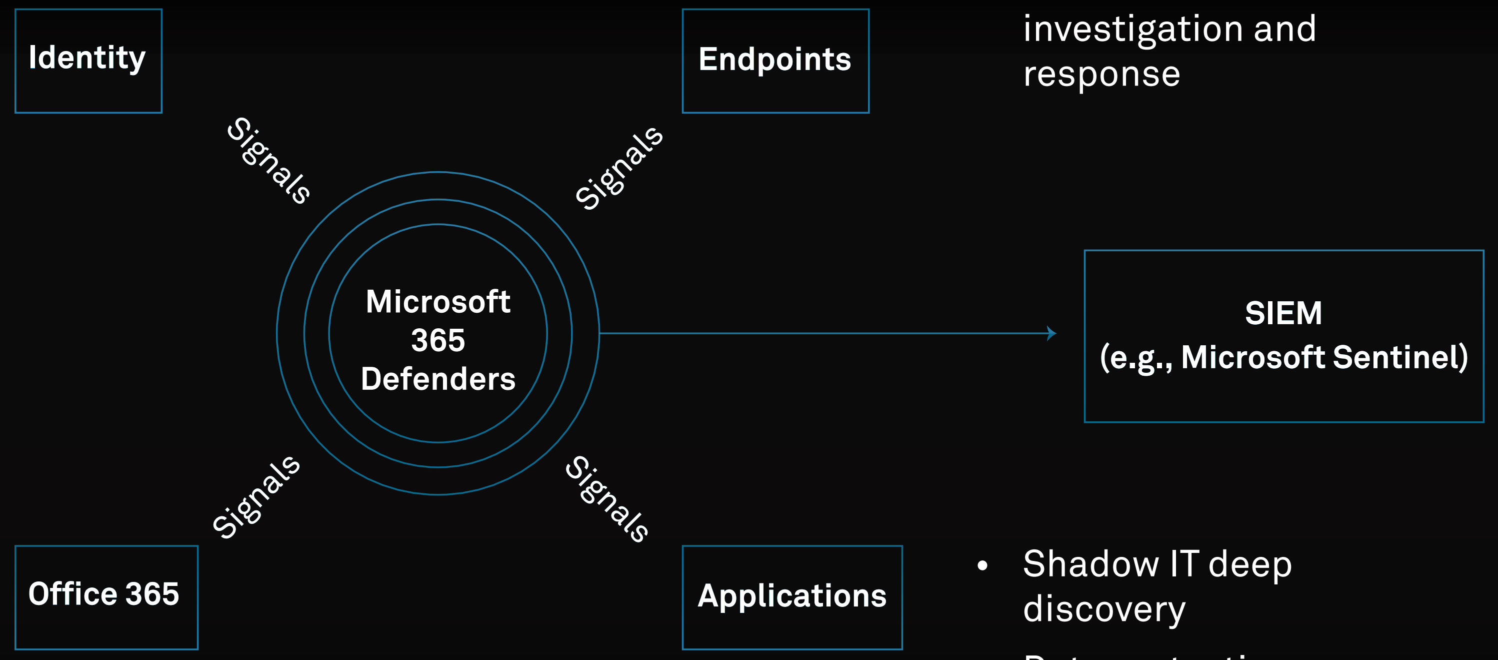
Microsoft Defender for Office 365

Microsoft Defender for Identity

Microsoft Cloud App Security

- Identify and detect threats on AD domain
- Compromised identities visibilities
- Malicious insider actions

- Preventive protection
- Post-breach detection
- Automated investigation and response



Identity

Endpoints

Signals

Signals

Microsoft 365 Defenders

SIEM (e.g., Microsoft Sentinel)

Signals

Signals

Office 365

Applications

- Safeguards against malicious threats
- Safe links
- Safe attachments
- Anti-malware / Anti-spam

- Shadow IT deep discovery
- Data protection controls
- Threat protection

Benefits of integrated threat management

- Cross-product single pane of glass
- Combined incidents queue
- Automatic response to threats

- Self-healing for compromised devices, user identities, and mailboxes
- Cross-product threat hunting

Meeting compliance at the workplace through Microsoft 365 E5 Compliance

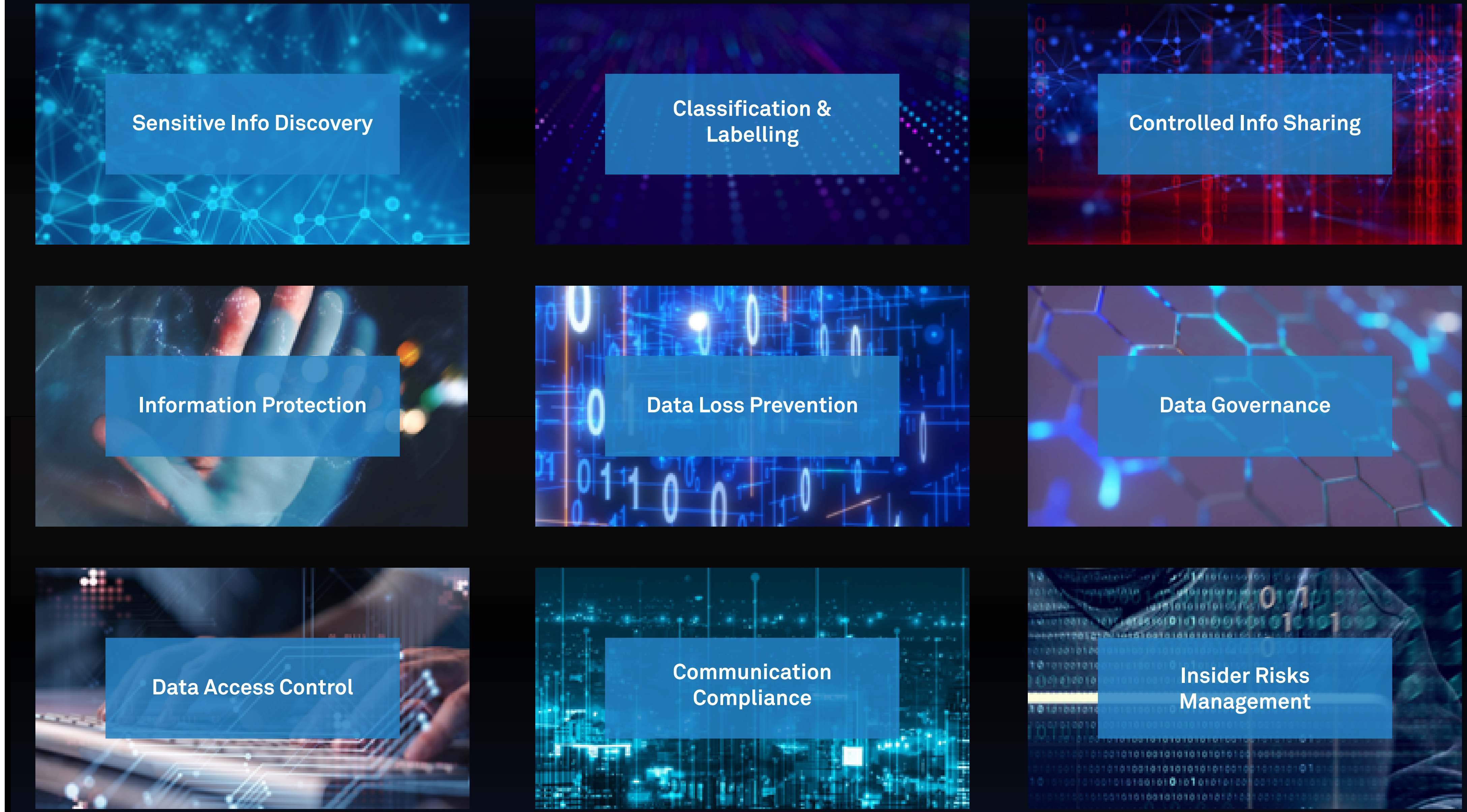
Business data will always be an attractive target for cybercriminals. As business reliance on data and remote work continues to grow, the risks of data loss become greater. Meeting various regulatory compliances is a challenging task to any organization and a robust compliance solution is vital to identifying and preventing data exfiltration.

Microsoft information protection can control and help secure email, documents, and sensitive data shared by users. Policy-based classification, persistent protection, and tracking features help protect shared data on-premises or in the cloud.

Today, businesses must protect more data that is:

- Generated by more users, applications, and devices
- Stored in more places and by more partners and providers
- Governed by many regulatory requirements and internal policies
- Subject to exposure, theft, or tampering by cyberattacks that are increasing in frequency and sophistication

A comprehensive approach to discover and protect organizational sensitive data leveraging Microsoft 365 E5 Compliance



Sensitive Info Discovery

Classification & Labelling

Controlled Info Sharing

Information Protection

Data Loss Prevention

Data Governance

Data Access Control

Communication Compliance

Insider Risks Management

Microsoft Information Protection

Data Loss Prevention

Record Management

Advanced eDiscovery

How can Wipro help customers to strategize and adopt Microsoft 365 E5 Security & Compliance?

5 E5 Security &
Compliance:

Timelines	Considerations/Outcome
Beyond	• Greater visibility to threats landscape • Enhanced attack surface reduction • Integrated threat detection and response • Optimal compliance
Short Term (180 days)	• Enhanced threat detection and protection • Improved attack surface reduction • Enhanced compliance
Immediate (30-60-90 days)	• No / low user impact • No / low infra impact • High visibility to threats landscape • Improved threat protection • Improved compliance

Microsoft 365 E5 Security & Compliance: Immediate and short-term rollout approach

Immediate (30-60-90 days)	Short Term (180 days)	Beyond
Defender for Identity Deployment	Defender for Identity Deployment	Passwordless Sign-in
Shadow IT discovery through MCAS	Defender for Identity Deployment	Insider Risks Mgmt., Adv. eDiscovery
Office 365 ATP Deployment for Safe Links, Safe Attachments	Defender for Endpoints AV/EDR	MCAS for all SaaS Apps
Sensitive Data Discovery through MIP for Office 365	MIP Label Taxonomy planning and deploy default lavels for Info Protection	Microsoft 365 Defenders ASR & AIR (auto response)
Default DLP policies in Audit mode	Office 365 DLP policies in override mode	Endpoint DLP/Migration
Enable Identity Protection for AAD SSO apps	Enable PIM for all Azure Admin Roles	EDR Migration
MCAS integration with AAD Conditional Access	MCAS for Public Cloud (Azure, AWS)	SSO/MFA Migration
Immediate Threat Visibility, Reduction & Compliance	Transformation Journey for an Extended threat visibilty, detection and response & Improved compliance	

Delivered through

- **3-week cloud accelerator workshop for value conversations, demos, and next steps**
- **1-week rollout strategy & planning workshop**
- **3-4 month implementation services**
- **Managed security services (24x7)**

Quick starts to a secure & seamless modern workplace journey

Theme	Business Value & Imperative	Scope & Duration (2 - 16 weeks)
Unstructured Data Protection	• Toxic data in unstructured stores presents significant risk • Solution identifies risky data and remediates with controls • Foundation for ongoing data protection and remediation program • Transition to Managed Service for Information Security	• Data Security Workshops • Information Discovery and Security Rapid Deployment • Insider Risk/Compromised Account Identification
Threat Protection	• Understand the full Microsoft security platform • Increase signals visibility end-to-end supporting Zero Trust models • Identify hidden threats in the AD environment • Improve endpoint security posture and compliance • Increase security and compliance on cloud apps & office apps	• Threat Protection Workshop • Microsoft Defender – Rapid Security Improvement
Digital Identity Experience	• Improves employee satisfaction through modern experience • Modern approaches for experience-based training and self service • External user journeys fully transparent and customizable • Increase visibility and control on Privilege user access	• Identity Lifecycle management Foundation • User access experience Improvement • Privilege Identity Governance Deployment • Zero trust user access

Wipro’s Microsoft security advantages

End-to-end enterprise security solutions and services delivered through industry-leading Microsoft security stack from one strategic IT services partner

Access to over 8,000 global cybersecurity experts, with over 1,000 Microsoft Security trained and over 500 Microsoft Security certified

Enabling greater innovation and rapid value-added services through strategic Microsoft partnerships

Center of Excellence (CoE) and IP-based solutions help customers to streamline and improve cloud security adoption, control visibility, and governance for application workloads while accelerating SSO application on-boarding to Azure platform

Two decades of enterprise cybersecurity experience to bring a holistic and integrated security approach for public, private, and hybrid cloud adoption

Value-added solutions and integrated service delivery to simplify, expedite, and seamlessly implement security solutions, with 24x7 managed services support through Wipro’s Global Cyber Fusion Center

Credentials

GOLD Security Competency

Advanced Specializations in Identity, Threat Protection, Information Protection & Governance and Cloud Security

Top 5 MSSP

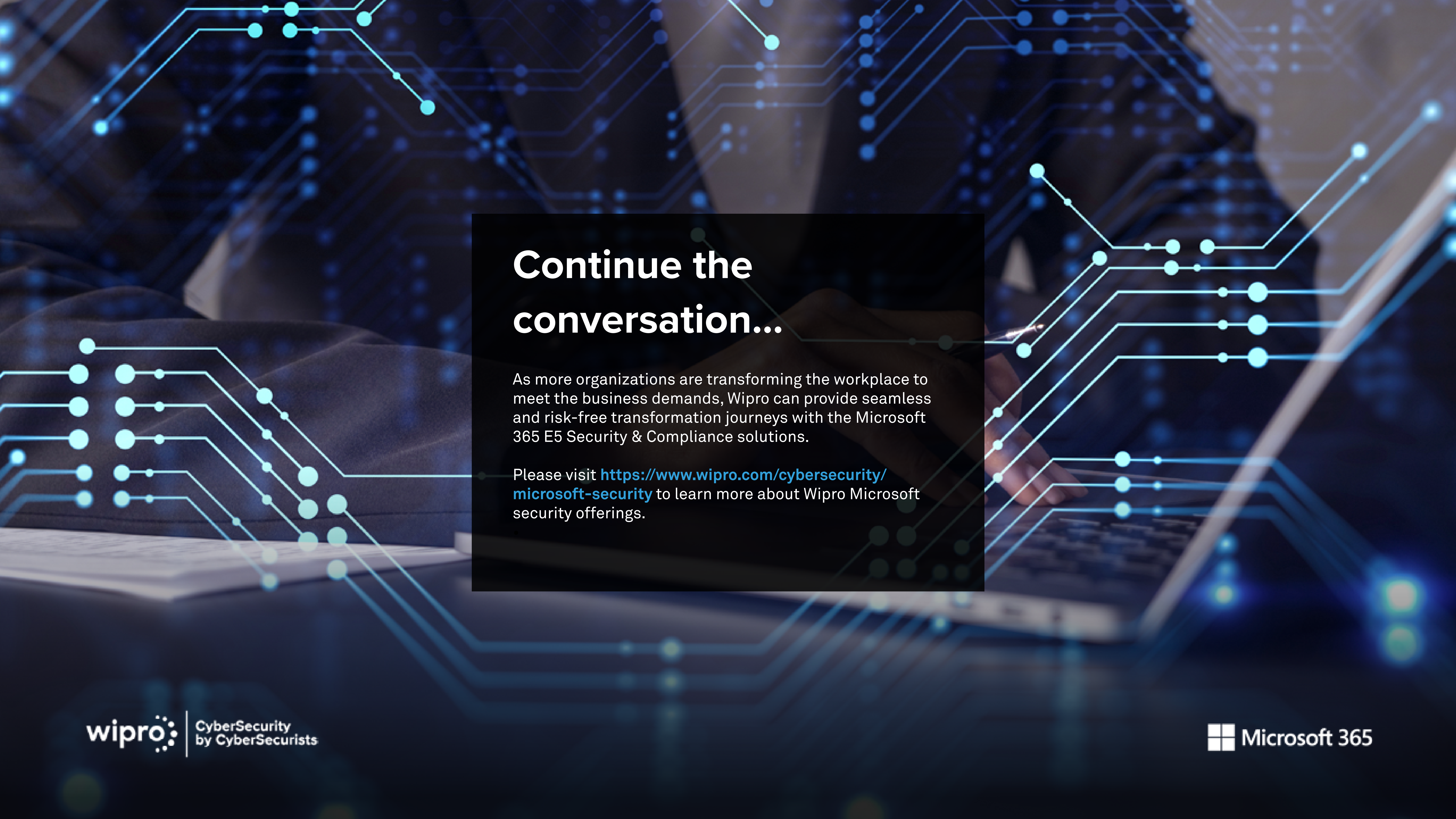
Top 5 Advisory for Security, Compliance & Identity

Top 5 Security SI

Member of

Microsoft Intelligent Security Association

Microsoft



Continue the conversation...

As more organizations are transforming the workplace to meet the business demands, Wipro can provide seamless and risk-free transformation journeys with the Microsoft 365 E5 Security & Compliance solutions.

Please visit https://www.wipro.com/cybersecurity/microsoft-security to learn more about Wipro Microsoft security offerings.

wipro CyberSecurity by CyberSecurists

Microsoft 365