LOGICALIS
Architects of Change

Microsoft
Solutions Partner

Executive Brief

Agentic AI at Enterprise Scale

What Business and Security Leaders Must Know

Forward-thinking companies are not just layering AI on top of existing business capabilities, they are using AI to fuel business transformation. To drive this transformation, frontier firms are starting by redesigning software architecture around agentic AI solutions.

Executive Summary

- Frontier firms achieve measurable impact by redesigning software architecture, business processes, and workflows to be AI-first rather than "AI on top."
- Agentic AI transforms enterprise software architecture into interconnected networks of autonomous agents with identity, memory, and decision-making capabilities. With proper governance, organizations can protect agents, while mitigating risks related to shadow AI.
- Microsoft Agent 365 provides enterprise-grade oversight through identity management, policy enforcement, and lifecycle controls. Combined with Work IQ, Fabric IQ, and Foundry IQ intelligence layers, organizations deploy agents safely at scale. Security is woven into workflows through Entra Agent ID and ambient protection.
- As a Microsoft partner with five solution designations, Logicalis delivers strategic architecture, implementation expertise, and managed services to help organizations drive transformation with enterprise agentic AI.

The Enterprise Impact of Agentic AI

Agentic AI means software that works autonomously, either in the background or with people. Unlike traditional automation that follows predetermined scripts, agents understand context and can make decisions based on that information. In this new software architecture, enterprise applications evolve from static tools into living networks of agents that can reason, coordinate, and act on their own accord.

This new software paradigm promises new levels of productivity, efficiency, and creativity, but with it comes changes that impact today's digital environment:

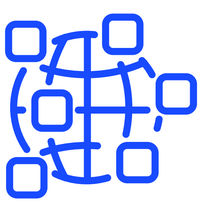
The Cloud is Evolving

The cloud is shifting from resource allocation for compute and storage into a substrate for orchestrating autonomous agents that reason, decide, and act. Development teams can now build agents that connect to multiple data sources, understand business semantics, and coordinate with other agents across the enterprise.

This architectural shift fundamentally changes how organizations approach cloud strategy and governance. Infrastructure and unified governance frameworks must now span traditional cloud resources, as well as the autonomous agents operating within them.

As agents proliferate across the organization and the cloud, security, compliance, and observability become even more critical. IT leaders must maintain visibility into what agents are doing, how they're accessing data, and what actions they're taking across the organization. Without this visibility, organizations risk creating new attack surfaces, compliance violations, and operational blind spots that undermine the value agents deliver.

Productivity Takes on a New Meaning



When agents become part of daily workflows, the nature of work will change dramatically. Rather than navigating multiple applications, memorizing menu hierarchies, or mastering intricate software workflows, employees can interact with agents that proactively surface relevant information and handle routine tasks.

Workflows also become simpler: employees describe what they need in natural language, lightening the cognitive load and freeing them to spend time on more valuable work. They no longer need to remember where information lives or which tool to use for each task.

Instead, agents interface with software and understand context across conversations, documents, and decisions, enabling them to anticipate needs, deliver the right information at the right time, and accelerate productivity.

Security is Undergoing a Paradigm Shift

To keep pace with agentic AI, security architecture must shift from securing human access to governing autonomous actors.

Traditional identity and access management are designed only for human actors. Now, however, agentic software operates autonomously, makes decisions independently, and executes actions across multiple systems rapidly.

For security teams, this means treating agents with the same identity rigor applied to employees: authentication, authorization, continuous monitoring, and audit trails for every action.

Fundamentally, agentic AI also implies that security can no longer be treated as an afterthought. It must be woven into workflows as ambient protection that understands organizational context and adapts in real time to emerging threats. With proper governance, security teams can deploy agentic AI confidently and reduce the risk of shadow AI.

The Pillars of Agentic AI

Deploying agentic AI at enterprise scale requires addressing four foundational challenges. Organizations that get these pillars right can scale agents confidently. Those that don't risk creating security exposures, compliance gaps, and operational chaos as agents proliferate.

Pillars of Enterprise Agentic AI

Governance	Identity	Intelligence	DevOps
Agent 365	Entra Agent ID	Work IQ, Fabric IQ, Foundry IQ	Azure AI Foundry, Agent Factory, GitHub
Registry Access Control Visualization Interoperability Security	Zero Trust Conditional Access Auditing	Data Memory Context	Development Testing Deployment

Governance to Protect Agents and Prevent Shadow AI

By 2028, businesses are expected to have 1.3 billion AI agents[1] automating workflows. Yet most organizations don't have a way to observe, secure, or govern agentic systems.

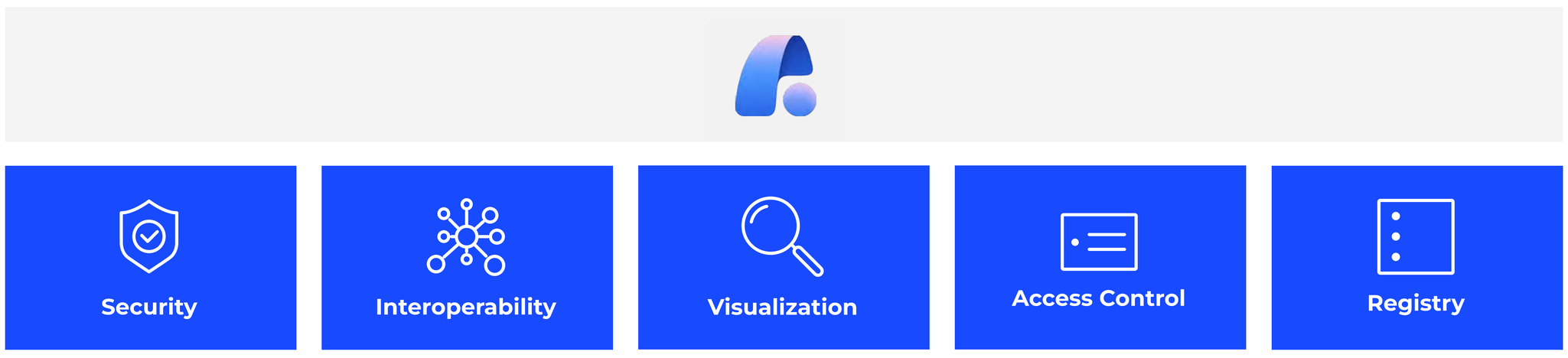
Without proper governance, AI agents can easily become the new shadow IT: autonomous software that spreads across the organization without visibility or accountability.

Microsoft Agent 365[2] enables organizations to observe, manage, and secure AI agents whether they're created with Microsoft platforms, open-source frameworks, or third-party tools. It includes Microsoft security solutions like Defender, Entra, Purview, and Foundry Control Plane to help protect and govern agents, plus productivity tools including Microsoft 365 apps and the Microsoft 365 admin center for agent management.

1. www.blogs.microsoft.com/blog/2025/11/05/beware-of-double-agents-how-ai-can-fortify-or-fracture-your-cybersecurity/#_ftn1
2. www.microsoft.com/en-us/microsoft-365/blog/2025/11/18/microsoft-agent-365-the-control-plane-for-ai-agents/

Agent 365 delivers five key capabilities that make enterprise-scale governance feasible:

1. **Security** through Microsoft Defender detects threats targeting agents and blocks attacks in real time by coordinating with Microsoft Entra identity protections
2. **Interoperability** across Microsoft platforms, open-source frameworks, and partner clouds ensures agents can access data and applications stored in Microsoft 365, Dynamics 365, and external systems
3. **Visualization** through a unified dashboard provides a complete map of connections among agents, users, and resources across the organization
4. **Access Control** assigns every agent a unique identity enabling granular permission management
5. **Registry** provides a continuously updated inventory of all agents operating across the organization



Microsoft Agent 365 marks a new chapter in how organizations build, secure, and scale their agents. This is a shift from isolated experiments to enterprise readiness, where agents operate as part of a unified, governed, and productive system.

Identity as the Foundation for Securing Autonomous Software

Autonomous agents make decisions and take actions across systems without intervention at every step. Because they operate independently and access the same systems people do, Microsoft's security solution involves extending identity management to include AI agents.

Entra Agent ID[3] provides the foundation for securing agents with the same rigor organizations apply to employees, through conditional access policies, activity auditing, and permission models. This extends zero trust principles to include agents in the enterprise identity system, ensuring every autonomous action is authenticated, authorized, and auditable.

At Microsoft Ignite 2025, Entra Agent ID advanced to public preview with capabilities specifically designed for AI agents. Organizations can now:

- **Register and manage AI agents** by assigning distinct identities as soon as agents are created
- **Govern agent identities** by managing permissions, ownership, and complete lifecycle just as they do for users or applications
- **Protect AI agents** by implementing zero-trust frameworks through conditional access, identity protection mechanisms, and network safeguards

Included in Microsoft Agent 365, Entra Agent ID takes the same security solutions used to manage and secure people and extends it to agents. Microsoft Entra secures agent access to resources, Microsoft Purview protects and governs data, Microsoft Intune secures endpoints, and Microsoft Defender shields agents from threats and vulnerabilities. Integration with other tools, from Power BI to Microsoft 365, streamlines new agent-based workflows into the existing Microsoft technology stack.

Data Platform: Building the Intelligence Layers

Agents need context to operate effectively. That is, they need to understand how people work, what data means to the business, and where to find relevant information across multiple sources. To provide this context, Microsoft offers three solutions:

Work IQ brings intelligence to Microsoft 365, understanding organizational context across Teams, SharePoint, Outlook, and other collaboration tools. This layer enables agents to comprehend communication patterns, project relationships, and workflow dependencies.

Fabric IQ turns Microsoft Fabric into an intelligence platform and provides agents with a deep understanding of data relationships, business logic, and analytical patterns. It enables data agents to autonomously discover insights, identify anomalies, and recommend actions grounded in comprehensive business context.

Foundry IQ provides a fully managed knowledge system that grounds agents across Microsoft 365, Fabric, custom applications, and the web through a single endpoint. This intelligence layer enables development agents to build, test, and deploy solutions that integrate seamlessly with existing enterprise systems.

Together, these intelligence layers provide agents with the broader context that ensure their actions are productive and aligned with business objectives.

3. www.techcommunity.microsoft.com/blog/microsoft-entra-blog/microsoft-entra-what's-new-in-secure-access-on-the-ai-frontier/4468732

Development and Deployment, From Concept to Production

Building, testing, and deploying agents at scale requires new development workflows. Organizations need environments for agent creation, integration with existing DevOps practices, and ways to manage agents through the entire lifecycle, from development to retirement.

Azure AI Foundry[4] and Agent Factory[5] provide the comprehensive development environment for building, testing, and deploying agents at enterprise scale. The Foundry Agent Service simplifies agent development through pre-built templates, integration with Microsoft Graph and external APIs, and seamless orchestration capabilities.

The Agent Factory program accelerates development by providing access to pre-built agent blueprints, reference architectures, and best practices from Microsoft and partner implementations. Organizations can leverage proven patterns for common use cases to reduce development time and implementation-related risks.

Integration with GitHub allows agent developers to apply standard DevOps practices to agent development, including version control, automated testing, continuous integration, and phased deployment. With this integration, agents benefit from the same engineering rigor applied to traditional software development, ensuring they maintain quality and reliability, even at enterprise scale.

Building Your Agentic Future

with Logicalis and Microsoft

The shift to agentic AI requires enterprises to fundamentally reimagine their business architecture, workflows, and operating models. Organizations that approach this transformation with the proper strategy and expert partnership position themselves to capture substantial competitive advantage.

Microsoft's platform provides the foundation for this transformation with solutions that span governance, security, intelligence, and development.

Logicalis provides expertise in strategic architecture, a proven methodology for implementation, managed services, and ongoing optimization.

Microsoft Partner Excellence
Leading partner in the Microsoft Cloud Partner Program, twelve advanced specializations, and five solution designations

Deep Technical Expertise
Advanced certifications and direct relationships with Microsoft product teams

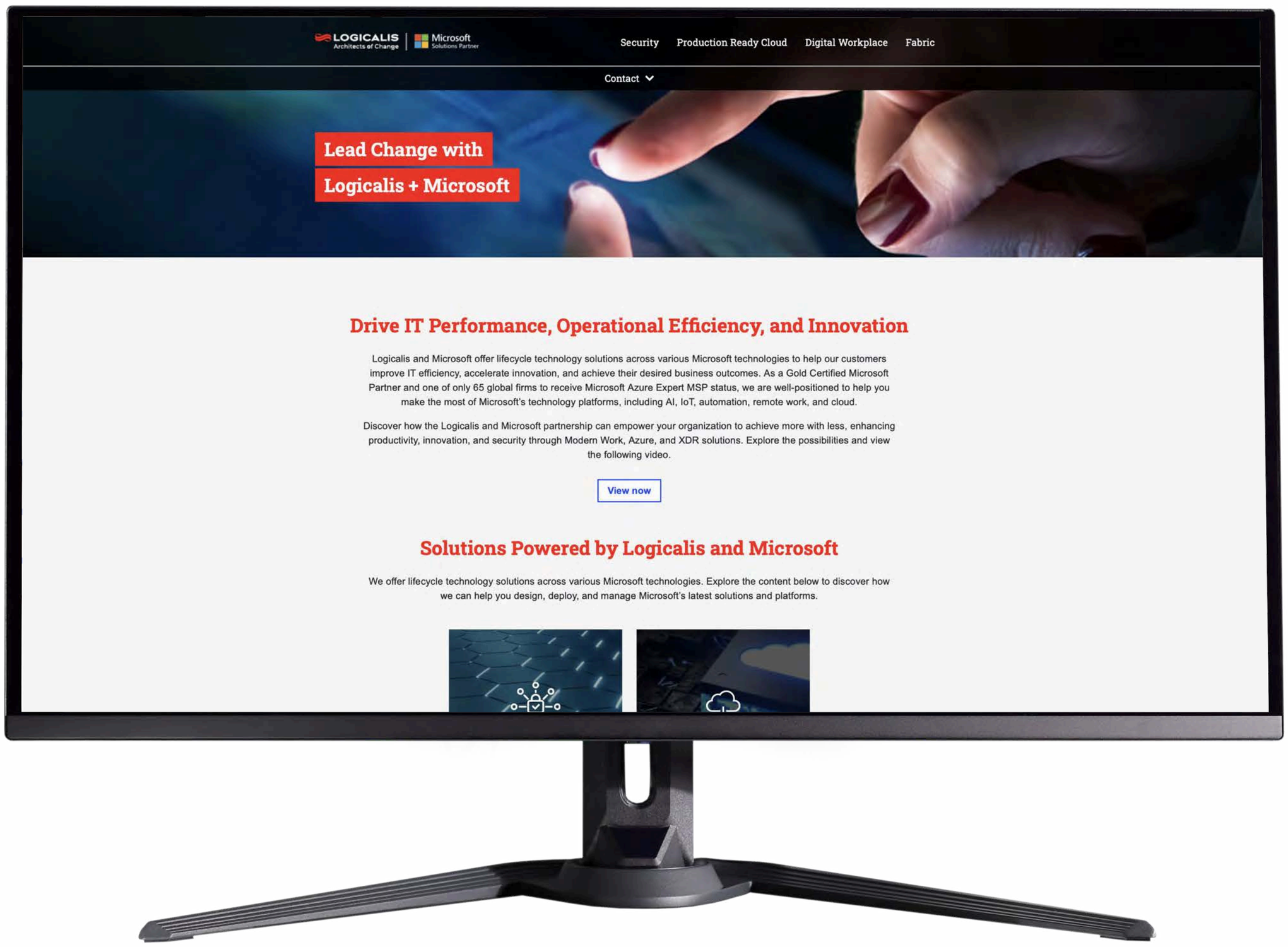
End-to-End Services
Complete support from assessment through managed operations, including architecture, deployment, adoption, and optimization

4. www.techcommunity.microsoft.com/blog/azure-ai-foundry-blog/foundry-agent-service-at-ignite-2025-simple-to-build-powerful-to-deploy-trusted-/4469788
5. www.techcommunity.microsoft.com/blog/azure-ai-foundry-blog/introducing-microsoft-agent-factory/4470732

Together, this partnership enables organizations to deploy agentic AI with confidence, minimize risk, and maximize business value.

If your team is ready to drive transformation with Microsoft's agentic AI portfolio, schedule a complimentary executive briefing today.

Schedule a free executive briefing



LOGICALIS Architects of Change | Microsoft Solutions Partner