eScan Enterprise DLP Expands AI Tenant Control to Claude and Manus After Meta Acquisition

As artificial intelligence tools become deeply embedded in enterprise workflows, MicroWorld Technologies Inc.'s eScan has broadened its Enterprise DLP capabilities to include tenant-level control for Anthropic's Claude.ai and Manus.im, the autonomous AI platform recently acquired by Meta.

The move comes at a time when Indian enterprises are facing mounting compliance pressure under the Digital Personal Data Protection (DPDP) Act. Organizations are increasingly concerned about employees accessing powerful AI systems through personal accounts, leading to data exposure risks that operate outside corporate monitoring frameworks.

The AI Productivity Paradox Deepens

The AI productivity surge has introduced new governance challenges. Since Meta completed its acquisition of Manus in December 2025, enterprises have been closely watching the platform's evolution. Unlike conventional AI chat interfaces, Manus operates as a self-directed execution engine capable of browsing the internet, generating and deploying code, analyzing datasets, and delivering structured reports with minimal human input. The system has already processed more than 147 trillion tokens and created over 80 million virtual computing environments, underscoring its scale and autonomy.

"The Samsung semiconductor leak demonstrated what happens when employees share sensitive data with ChatGPT," said **Govind Rammurthy, CEO & Managing Director, eScan**. "But Manus represents a different category of risk entirely. It's not just receiving data – it's autonomously executing tasks that could involve accessing corporate systems, writing code for production environments, or conducting competitive research using proprietary information. Without tenant control, organizations have zero visibility into what employees are asking these agents to do."

Rising Enterprise Adoption of Claude

Claude, developed by Anthropic, has also seen strong enterprise adoption, particularly among development and strategy teams leveraging it for documentation, code validation, and analytical workflows. Like other AI assistants, Claude permits login through personal email IDs and third-party single sign-on providers, including Google and Microsoft, creating governance blind spots similar to those that initially drove demand for tenant controls on ChatGPT.

How eScan's Workspace Tenant Control Works

To address these concerns, eScan Enterprise DLP's Workspace Tenant Control now extends endpoint-level authentication monitoring to both Claude.ai and Manus.im. When users attempt

to log in through personal credentials or external SSO services such as Google, Apple, or Microsoft, the system intercepts and blocks the attempt. Access is granted only when corporate domain credentials are used, ensuring all activity remains within an auditable enterprise environment aligned with DPDP compliance requirements.

For Manus, this oversight becomes especially critical as Meta prepares deeper integrations across its ecosystem. The company has outlined plans to embed Manus capabilities across Facebook, Instagram, WhatsApp, and its broader Meta AI stack. Under eScan's framework, attempts to access Manus via personal Meta accounts—whether directly or through social platforms—are similarly restricted unless corporate authentication standards are met.

"Organizations told us they blocked ChatGPT entirely after the Samsung leak," **Rammurthy** explained. "Then they blocked Claude when developers started using it for code review. Now they're asking about Manus because employees are using it for market research and competitive analysis. Blocking every AI tool isn't sustainable – employees will find workarounds. Tenant control lets you enable productivity while maintaining governance."

The Broader Cybersecurity and Compliance Context

The broader cybersecurity landscape reinforces the urgency of such controls. GitHub reported 39 million exposed secrets on its platform in 2024. A compromise involving tj-actions in March 2025 impacted CI/CD credentials across 23,000 repositories. In February 2025, a Pune-based individual reportedly lost ₹43 lakh in a scam involving AI-generated deepfakes. With regulatory scrutiny intensifying, data governance is no longer solely an IT concern but a board-level compliance priority.

eScan's Workspace Tenant Control already supports authentication governance across widely used enterprise platforms, including Google Workspace, Microsoft 365, Dropbox, Atlassian, Slack, Webex, Autodesk, Zoom, WeTransfer, ChatGPT, and GitHub. By adding Claude and Manus to this ecosystem, the company aims to deliver a unified compliance layer covering both traditional SaaS platforms and next-generation AI agents.

Future Outlook: Responsible AI Adoption

The updated functionality is now integrated into eScan's Enterprise DLP suite, with further AI platform integrations expected based on evolving enterprise demand. As generative and autonomous AI systems continue to redefine workplace productivity, maintaining visibility and control over corporate data flows is emerging as a foundational requirement for responsible and secure AI adoption.