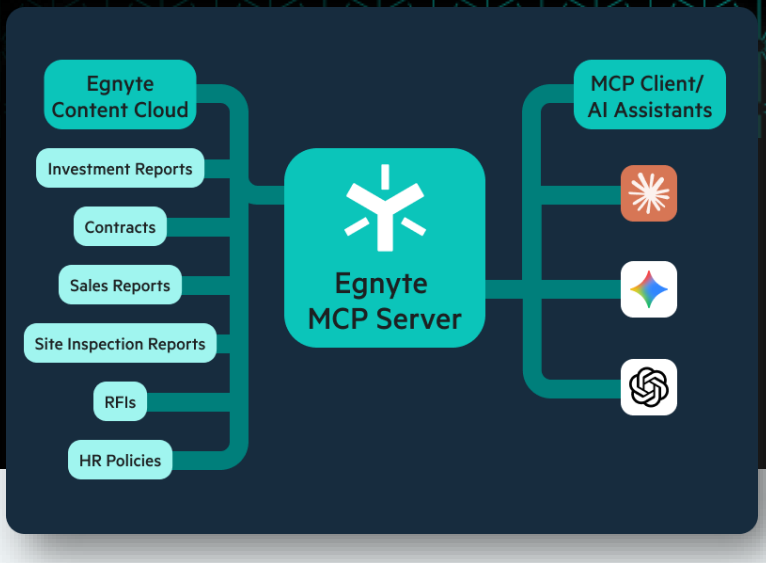
EGNYTE

MCP Server Security Brief

Secure AI Access Without Compromising Business Data

Egnyte's MCP Server securely connects approved AI tools like ChatGPT, Claude, and Microsoft Copilot to business content, enabling faster search, summarization, and analysis while preserving existing security, governance, and compliance controls.



Existing permissions stay fully enforced

MCP Server enforces existing user permissions, ensuring AI tools access only authorized content without introducing new security risks.

Stateless architecture reduces data exposure

Egnyte MCP Server is fully stateless. It never stores prompts, file content, or AI queries after a request is completed, reducing long-term data exposure.

Prompt injection protection

MCP Server doesn't parse or execute file content. It securely delivers files as stored, while prompt injection defenses remain the responsibility of the AI platform.

Egnyte MCP Server is designed to help organizations safely unlock AI productivity while preserving enterprise security. Its strongest protection elements include:

- ✓ Permission-based access
- ✓ Stateless architecture (no data retention)
- ☐ Secure verified authentication
- ✓ Client allowlisting (approved client access)
- ✓ Auditable admin oversight

Egnyte enables secure AI access to business content while preserving governance, compliance, and data privacy, helping teams work faster with confidence.

www.egnyte.com | © 2026 by Egnyte Inc. All rights reserved.

MCP Server's Advanced Security Features

OAuth authentication protects access

Egnyte uses OAuth 2.1 with PKCE (Proof Key for Code Exchange), an industry-standard authentication protocol that confirms only approved users and applications can securely access company content through expiring tokens, controlled access, and strong protection against unauthorized use.

Audit logs support compliance

All MCP-related file actions are logged through Egnyte's Audit Reports, giving security and compliance teams visibility into how AI tools access business data. Enhanced MCP-specific audit events will further strengthen compliance, governance, and security investigations.

Admin controls provide business oversight

MCP Server runs on top of Egnyte's public APIs, delivering the same audit logs and reporting as standard API activity. Admins maintain full control through client allowlisting, approved app access, AI Safeguards and the ability to block tools, revoke access, or disable MCP entirely from the admin console.

Managed cloud service lowers supply chain risk

Egnyte MCP Server is a fully managed cloud service—customers don't install or manage software dependencies, reducing supply chain risk from compromised packages or updates. Security is maintained under Egnyte's SOC 2 Type 2 and ISO 27001-certified programs.

API rate limits prevent misuse

Egnyte MCP Server follows plan-based API rate limits, quotas, and throttling controls to prevent misuse—slowing suspicious activity while allowing admins to revoke access instantly.

Data privacy and residency remain protected

Egnyte MCP helps organizations maintain privacy and compliance by processing data within the customer's regional infrastructure, preserving data residency, and encrypting data in transit. It doesn't store content and never uses customer data for AI training.

EGNYTE

Egnyte is a leader in secure content collaboration, intelligence, and governance, trusted by more than 23,000 customers to increase employee productivity, drive operational efficiencies, and secure mission-critical content. Egnyte's AI-powered platform empowers organizations to create, share, and protect their information at scale, with specialized solutions designed to meet the unique needs of organizations in architecture, engineering, and construction (AEC), financial services, life sciences, and other industries.
For more information, visit www.egnyte.com.

Contact Us

+1-650-968-4018

1350 W. Middlefield Rd.

Mountain View, CA 94043 USA

www.egnyte.com