DataDome | MCP PROTECTION SOLUTION BRIEF

Protect and Control Agentic Traffic in Real Time

Gain visibility into and secure MCP interactions to secure the next wave of AI-driven business.

Secure the next wave of AI-driven business

The problem: New Risks in Agentic AI Traffic

As enterprises adopt agentic AI, MCP (Model Context Protocol) servers are rapidly becoming the backbone of AI-powered operations—connecting agents, tools, and data in real time. But this new communication layer also creates fresh opportunities for abuse. Threats such as data scraping, business logic manipulation, prompt injection, and unauthorized access can compromise sensitive data and disrupt workflows. Insufficient visibility and control put operations, revenue, and trust at risk across modern agentic business workflows.

The solution: DataDome MCP Protection

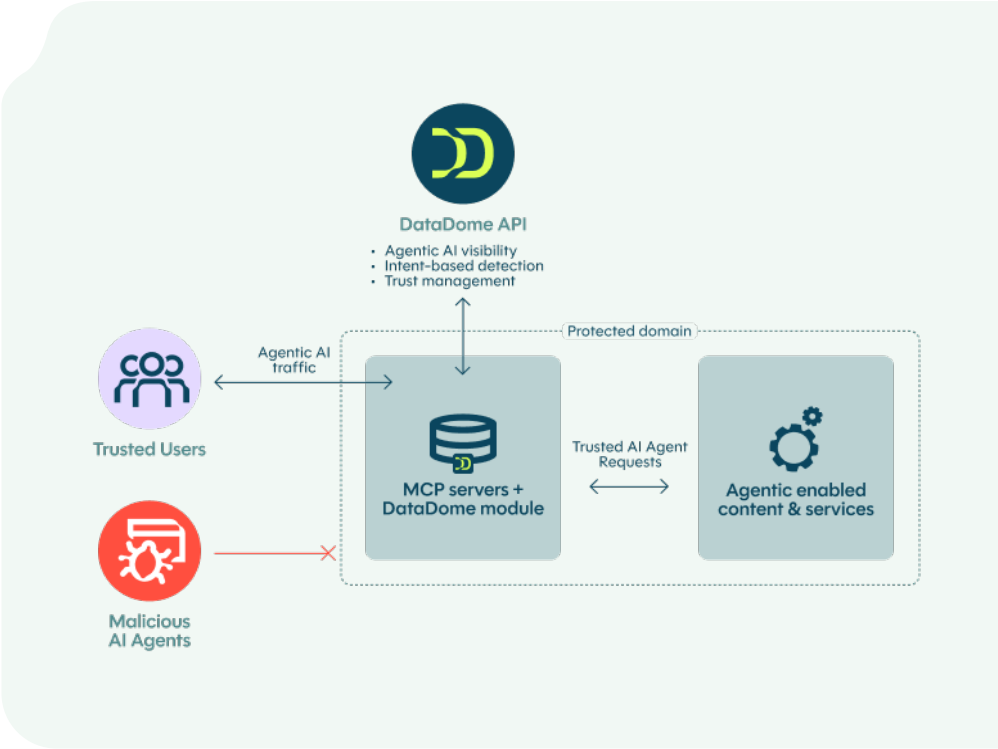
DataDome delivers the visibility, control, and trust enterprises need to manage the rise of agentic AI traffic. Every MCP request is identified and classified in real time, providing clear insight into how AI agents, users, and tools interact across systems.

With that visibility comes control.

DataDome enables organizations to define and enforce policies that govern MCP connections—deciding which agents, workflows, and transactions are allowed or blocked.

At the foundation is trust.

By verifying the type and intent of every interaction, DataDome ensures that only legitimate, transparent agentic traffic flows through your environment. The result is a secure, scalable framework for AI-driven business built on clarity, confidence, and control.



How MCP Server Protection Works

Secure innovation starts with trusted MCP traffic

Continuous Traffic Inspection and Classification

Every MCP request is analyzed in real time to identify and verify the type and intent of agentic traffic, ensuring only trusted interactions are allowed.

Comprehensive Visibility and Insights

A unified dashboard provides deep analytics into MCP activity, helping teams understand trends, optimize operations, and improve agentic AI performance.

AI-Driven Detection and Decisioning

DataDome's multi-layered AI models evaluate each request in under two milliseconds, delivering precise, low-latency protection at global scale.

Flexible Policy Enforcement

Define and adapt traffic rules that align with business priorities. Control how AI agents, tools, and human users connect, act, and exchange data.

Seamless Integration

Plug-and-play integration with standard MCP-enabled server-side modules, no re-architecture required.

Powering Safe, Seamless, and Scalable Agentic AI Operations

- **Build Trust in Every Interaction**
  Verified MCP traffic creates a secure foundation for trusted agentic AI adoption and long-term compliance confidence.
- **Enable Safe, Scalable Agentic AI**
  Protect AI innovation while keeping business operations seamless.
- **Gain Real Time Visibility & Control**
  Understand and manage agentic AI activity across every interaction.
- **Reduce Fraud, Abuse & Compliance Risk**
  Prevent unauthorized access, data leakage, and manipulation. Stop fraud and abuse in real time without affecting legitimate users or AI agents.

Want to learn more?
Request a live demo today