harmonic

MCP Gateway

Visibility and control over agentic AI

Enterprise AI has evolved from single-prompt interactions to agentic workflows. This has created massive productivity gains, but it's also introduced a new, invisible attack surface.

The Challenge

The Rise of MCP — and the security gaps it exposes

Agentic AI workflows are reshaping how work gets done, connecting AI models directly to company data, APIs, and systems.

But this new workflow layer operates outside traditional security controls. Sensitive data can move between AI tools and business systems without oversight, leaving security teams blind to:

- Which MCP clients and servers are in use
- What data is being exchanged
- When risky workflows occur

Without visibility and control, enterprises face data leakage, workflow hijacking, and compliance gaps.

Common Use Cases of MCP within an Organization

MCP started with engineering, but is now spreading across knowledge management, operations, and business teams. Some common use cases we see:

Engineering

Code & DevOps

Read a design doc in Notion, break it into Jira tickets, generate code following internal standards, and create a GitHub merge request.

Marketing

Content & Campaigns

Pull product messaging from Notion, create tailored campaign content, and draft outbound emails in Outreach.

Security

Threat Hunting & Incident Response

Show failed logins from non-corp IPs in the last 24h and summarize into a response plan.

Sales

Prospecting & Outreach

AI pulls account data from Salesforce, drafts personalized outreach, and logs activity back in Salesforce or Salesloft.

The Harmonic Solution

Introducing the MCP Gateway

The Harmonic MCP Gateway is a developer-friendly, locally installed gateway that gives security teams complete visibility and control over their organization's agentic AI ecosystem. It transparently intercepts all MCP traffic, allowing security teams to discover what clients and servers are in use, enforce granular policies to block risky actions, and—most importantly—apply Harmonic's industry-leading sensitive data models to prevent the exposure of critical intellectual property and other sensitive information.

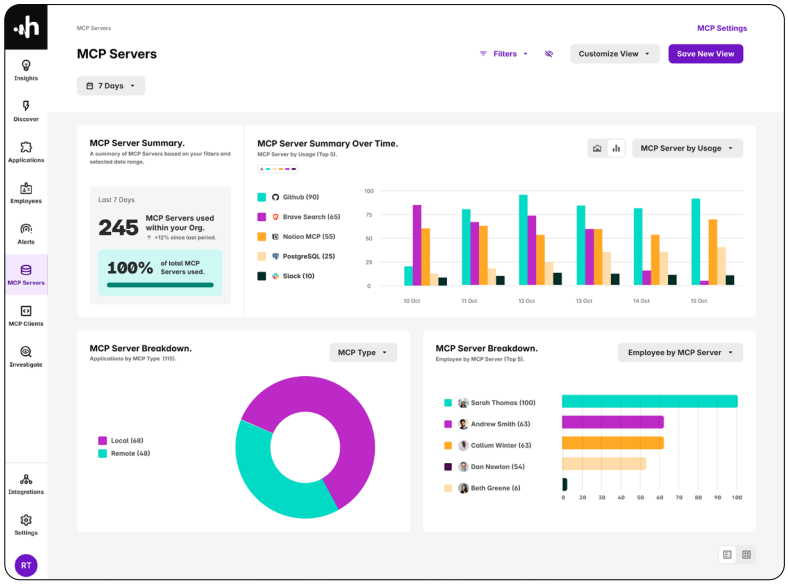
Core Features & Capabilities

Visibility

Discovery & Inventory
Automatically discover and inventory all MCP clients (e.g., Cursor, Claude Code) and servers (official vendor and locally built) in use.

Usage Analytics
Understand which employees are using which clients or servers and how frequently via dashboards and saved views.

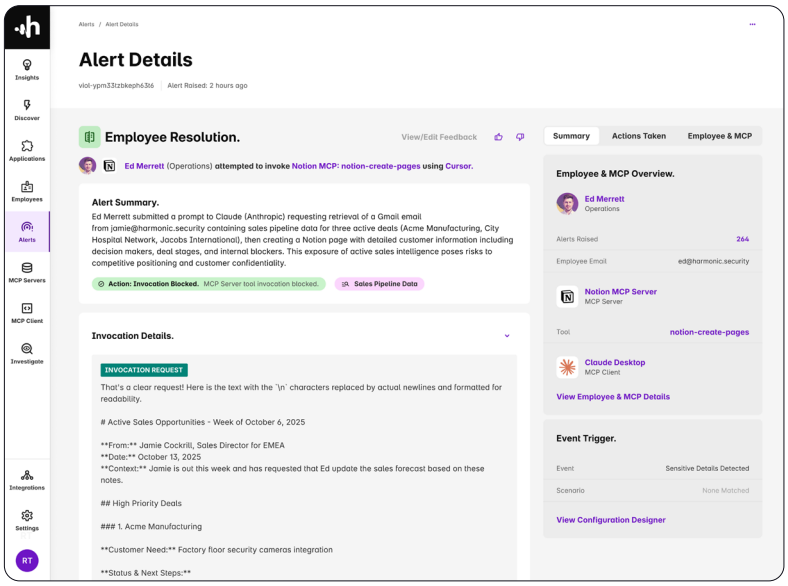
Invocation Logging
Capture detailed audit logs of every interaction for forensic analysis and compliance.



Control

Centralized Policy Enforcement
Define and enforce global policies to block entire MCP servers or restrict specific high-risk capabilities (e.g. tools that can write to production databases).

Alerting & Integration
Receive real-time alerts for policy violations and sensitive data events. We integrate seamlessly with your existing security stack, ensuring alerts appear where your teams already monitor and respond (e.g. SIEM and SOAR platforms).



Intelligent Data Protection & AI Coaching

Sensitive Data Detection
Leverage existing Harmonic sensitive data models to inspect MCP traffic in real-time, identifying unstructured sensitive data like source code, financial projections, and strategic plans.

Intelligent Blocking & AI Coaching
When sensitive data is detected, we don't just block the action and break the workflow. The gateway provides contextual, detection-specific feedback to the MCP client. This coaches the AI agent on why an action was blocked, allowing it to find a safe, alternative path to complete its task, thereby reducing developer friction and enabling safe AI adoption.

Effortless Deployment — Immediate Value

With the Harmonic MCP Gateway, you get instant visibility and protection without the complexity of a high-friction agent rollout. Installation takes minutes and delivers value on day one. No heavy infrastructure or configuration required. The lightweight gateway runs seamlessly on Windows, macOS, and Linux, giving every team the same secure foundation for agentic workflows.

Why Harmonic?

Securely Accelerate AI Innovation
The rise of agentic AI is inevitable — but it doesn't have to be risky.

With Harmonic MCP Gateway, enterprises can innovate with confidence, maintaining full visibility and control over how AI interacts with their systems and data.

Advisor360°

"Every security leader I know is trying to get ahead of AI-driven workflows. It's exciting to see Harmonic tackling this head-on, so teams can be confident to innovate safely."

- Michael Janielis
Senior Principal, Information Security Architect, Advisor360

Getting Started with Harmonic

Getting started with Harmonic is quick and easy. Simply install the Harmonic MCP Gateway to start gaining insights into Agentic AI workflows and secure your sensitive data.

Within 30 minutes, the Harmonic MCP Gateway may be rolled out to your entire organization with Group Policy Object (GPO), Microsoft Intune, JAMF or Kandji.

GET STARTED →

harmonic

Harmonic Security gives security teams the tools to protect sensitive data without the headaches of labeling and complex rules. Our pre-trained data protection models enable secure innovation through user interaction and gentle nudges. Recognized as an RSA Innovation Sandbox finalist in 2024, Harmonic Security redefines data protection for the GenAI era.

harmonic.security sales@harmonic.security