BACKSLASH

SOLUTION BRIEF

Vibe Coding Security

Accelerate the adoption of vibe coding and AI-native software development in your organization – safely and securely.

The Backslash platform leverages the capabilities of modern IDEs and coding agents such as Cursor, Claude Code, Gemini Code Assist, Windsurf, and GitHub Copilot to provide visibility, governance, and protection across AI developer environments. It also monitors use of MCP servers while ensuring that AI-generated application development adheres to security best practices and compliance requirements, reducing risks and exposures.

Understanding The Security Challenges of Vibe Coding

The extensive use of AI in coding presents new security risks and may also amplify familiar ones. These include:

Lack of visibility:
Security teams don't know where developers are using vibe coding tools and MCP servers, permissions they are granted, and their risk posture.

MCP (Model Context Protocol) server risks:
MCPs are new APIs for the AI world, enabling interconnectedness between LLMs and other systems. Without proper vetting, reduced permissions, and monitoring, they can introduce data leakage and prompt injection risks.

Unsecured IDEs and coding agents:
Lack of proper hardening and overly permissive access to file systems, networks, and identity can create a new attack surface and expose developer workstations, systems, and the network.

Old threats, new AI-based vectors:
Even with trusted, well-configured components, it is possible for malicious or compromised AI agents to exfiltrate sensitive data, perform prompt injections, escalate privileges, and install backdoors.

Trusted by Forward-Thinking Organizations

Industry leaders trust Backslash to secure their vibe coding journey:

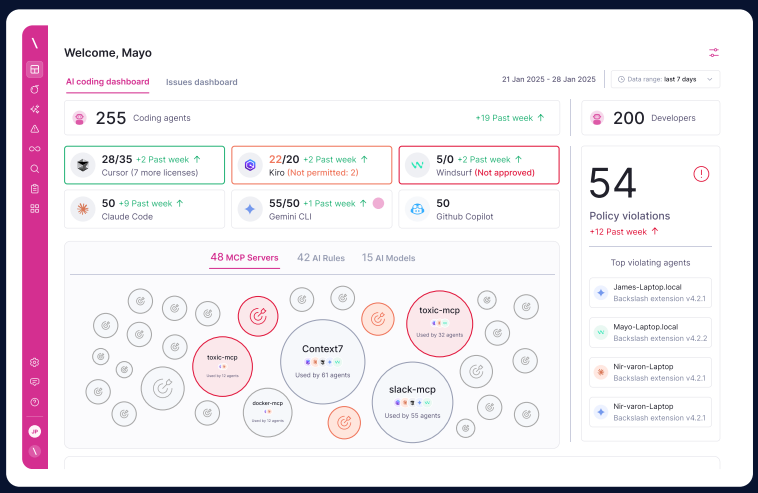
Fortune 100	Fortune 100	Top 10	Top 5	Top 10
Insurance Company	Media Giant	Gaming Company	Cybersecurity Provider	Global Telco.

monday.com | ARMIS | Anaplan | CHIPOTLE | Watershed | PandaDoc

Why Backslash? Our Approach

BACKSLASH

Backslash takes a completely fresh, comprehensive approach to vibe coding security—not merely enhancing old shift-left approaches with AI assistants, our platform combines dedicated security controls for all aspects of the vibe coding stack, providing security teams with the visibility, governance, and active protection needed to overcome shadow use of AI and ongoing threats from the rapidly evolving ecosystem.



Unique Advantages

Visibility & Posture

Unified Visibility & Risk Posture

Single-pane-of-glass dashboard shows the LLMs, IDEs, and MCPs used by developer and their associated risks.

Broad Cross-Platform Support

Covers the entire vibe coding stack including GitHub Copilot, Windsurf, Cursor, Claude Code, Google Code Assist, and more.

Easy to Deploy

Scales for broad coverage via MDM, to be centrally controlled and updated.

Centralized Governance

IDE & Coding Agent Hardening

Ensures consistent secure configuration of tools such as Cursor, Claude Code, and GitHub CoPilot.

MCP Vetting & Hardening

Scans MCPs for excessive permissions, vulnerabilities, and malware; enforces secure configuration of MCPs in use.

Centralized Policy-Driven Governance

Enforces security best practices for the use of LLMs, agents, and MCPs across all developer teams.

Active Protection

Real-Time Monitoring

Monitors for anomalous behavior, including data leakage, prompt injection, configuration drift and privilege escalation attempts.

Threat Detection & Response

Detects and intercepts multiple threats, including data leakage and prompt injection attempts.

Tracing for Forensics

Arms forensics and response teams with detailed event data for incident investigation.

For more information, visit www.backslash.security or GET A DEMO