



AI & SOFTWARE GOVERNANCE

• ENDPOINT CONTROL PLANE

• SHADOW-AI DISCOVERY

• EXTENSION & PACKAGE GOVERNANCE

• SUPPLY-CHAIN FIREWALL

An endpoint security control plane for the AI era - visibility, contextual risk and one-click remediation across the apps, extensions and AI tools nobody reviewed.

ABOUT BLOOM SECURITY

Bloom Security is an endpoint security control plane that gives security teams visibility and control over everything running on corporate endpoints - applications, browser extensions, code libraries and AI tools. A live, fleet-wide inventory feeds contextual risk analysis combining marketplace intelligence, static analysis and behavioral sandboxing, and risky findings are fixed with one-click remediation that previews the change and notifies the affected employee.

Founded in 2025 in Tel Aviv by Palo Alto Networks and Dig Security veterans, the company came out of stealth in July 2026 with a \$20 million seed round led by Glilot Capital Partners and Ten Eleven Ventures, and reports deployments at dozens of large enterprises across the United States and Europe.

The gap it closes is new: every endpoint now runs software no one reviewed - AI agents and coding assistants, unvetted browser extensions, third-party packages pulled from public registries. Security teams cannot review it all, and blocking it all slows the business down. Bloom runs that review continuously, blocks malicious packages at install time across npm, the Chrome Web Store and Open VSX, and reins in overpermissioned AI agents and MCP servers.

THE PROBLEM

Every endpoint now runs software nobody reviewed - AI agents, browser extensions, packages from public registries. Reviewing it all is impossible; blocking it all stops the business.

HOW BLOOM SECURITY SOLVES IT

Bloom Security inventories every tool on the fleet, scores risk in context, and remediates with one click - blocking malicious packages at install time.

CAPABILITIES

Live Inventory

A real-time, fleet-wide inventory of the software, browser extensions and AI tools on every endpoint - including where each one came from and what it can access.

Granular Remediation

Removes risky tools, revokes permissions and fixes misconfigurations with a change preview and built-in employee communication - surgical fixes, not blanket blocks.

Contextual Risk Analysis

Combines marketplace intelligence, static analysis and behavioral sandboxing, then weighs risk in context: the user's role, their data access, configurations and the other tools on the same endpoint.

Supply Chain Prevention

Blocks malicious or policy-violating packages at install time across npm, the Chrome Web Store and Open VSX - a supply-chain firewall that stops software at the door.

QUICK FACTS

FOUNDED: 2025, Tel Aviv (out of stealth July 2026)

LEADERSHIP: Itay Keren (CEO), Ofir Balassiano (CPO), Itay Frishman (CTO)

FUNDING: \$20M seed - Glilot Capital Partners & Ten Eleven Ventures

MODULES: Live Inventory · Risk Analysis · Remediation · Supply Chain Prevention · AI Guardrails

WHO BUYS IT CISOs, security engineering, IT & endpoint teams

See Bloom Security [on your own terms.](#)