Barracuda AI Security

Discover, assess and govern AI risk—without adding complexity

Artificial intelligence is transforming how work gets done. Employees are rapidly adopting generative AI tools embedded in SaaS applications or accessed directly through the web, often without IT approval or clear understanding of how data is processed, retained or shared. This phenomenon, commonly referred to as Shadow AI, introduces new and largely invisible data, privacy and compliance risks.

Barracuda AI Security helps organizations regain control. Delivered through the BarracudaONE platform, AI Security provides visibility into AI usage, applies meaningful risk context and delivers practical guidance to help organizations establish guidelines around AI adoption. Whether customers rely on existing third-party controls or choose a fully integrated Barracuda approach, Barracuda AI Security enables security teams to move from uncertainty to informed action.

Why it matters

You can't govern what you can't see. AI adoption is already happening across organizations, often outside established security and approval processes. Employees routinely experiment with AI tools to improve productivity, but in doing so may unintentionally expose sensitive corporate or personal data, creating immediate compliance and privacy risks.

For many organizations, particularly those with limited security resources, AI security presents additional challenges:

- **Lack of visibility into AI usage:** IT teams often have no clear view of which AI tools are in use, by whom or for what purpose.
- **No shared understanding of AI risk:** Not all AI tools present the same level of data, privacy or compliance exposure, yet most organizations lack benchmarks to assess risk consistently.
- **Policies lag behind reality:** Without visibility and context, AI policies remain theoretical and unenforceable.
- **Operational constraints:** Security teams and MSPs need simple, low-touch solutions that fit existing workflows rather than adding new point tools.

Barracuda AI Security addresses these realities by focusing first on visibility and risk understanding, laying the foundation for practical AI governance.

Solution overview

Barracuda AI Security is a solution capability delivered through the BarracudaONE platform that combines AI discovery, risk classification and policy enforcement. Rather than positioning AI security as a standalone product, Barracuda integrates these capabilities into the same platform customers already use to manage their broader security posture.

At its core, Barracuda AI Security enables organizations to:

- Discover AI tools in use across the environment
- Assess the relative risk of each AI service using clear classification
- Understand where AI usage may introduce data protection or compliance concerns
- Get actionable recommendations to guide governance decisions

This approach helps organizations move from reactive concern to informed, confident AI adoption, without requiring deep AI expertise or complex deployments.

How it works: Flexible paths to AI risk insight and control

Barracuda AI Security supports different operational models, depending on how customers prefer to enforce policy and manage controls.

AI risk insight using Cisco Umbrella DNS

Many organizations already use third-party network- or DNS-based security tools to manage web access. In this scenario, customers can ingest AI usage data from an external control, such as Cisco Umbrella DNS, into BarracudaONE.

BarracudaONE then provides:

- **Centralized visibility** into discovered AI services
- **AI risk classification** to highlight tools that may pose higher data or compliance risk
- **Dashboards and recommendations** to support governance decisions

In this model, BarracudaONE serves as the system of insight and guidance, while **policy enforcement and remediation actions are performed directly within Cisco Umbrella DNS**. This allows customers to enhance AI risk understanding without disrupting existing enforcement architectures.

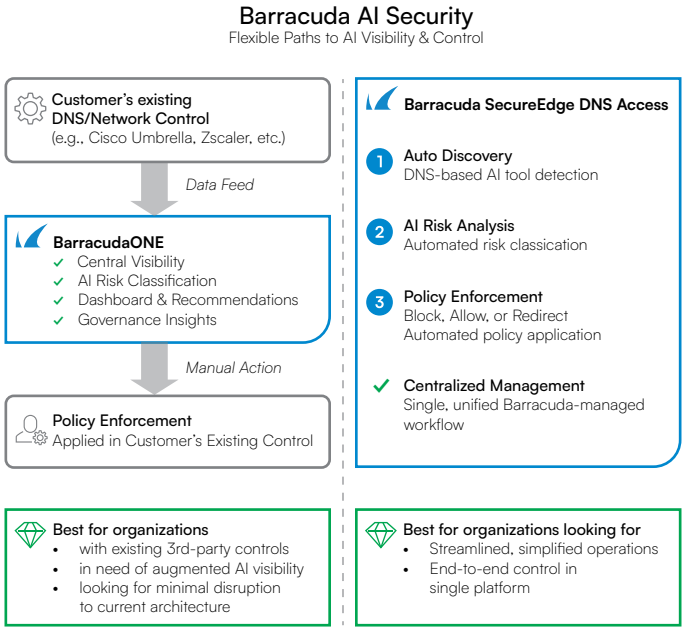
End-to-end AI governance with Barracuda SecureEdge

For customers seeking a more streamlined and operationally efficient approach, **Barracuda SecureEdge** delivers an integrated, end-to-end AI security experience.

Using any SecureEdge Access plan starting from SecureEdge DNS Access, organizations can:

- **Automatically discover AI tools** through DNS-based visibility, including unsanctioned or unknown services
- **Analyze AI risk** using Barracuda's AI risk classification
- **Enforce policy** by blocking, allowing or redirecting users to approved AI tools
- **Manage everything centrally** through a Barracuda-managed workflow

SecureEdge DNS Access enables organizations to move from AI risk insight to enforcement in just a few clicks—without deploying complex infrastructure or managing multiple tools. This makes SecureEdge the simplest path from discovery to control.



Customer benefits

Barracuda AI Security delivers practical value for IT and security decision-makers:

- **Visibility**: Discover AI tools employees are using, including Shadow AI that would otherwise remain hidden.
- **Risk context**: Understand which AI services present higher data, privacy or compliance risk through clear classification.
- **Operational simplicity**: Gain AI risk insight without deploying complex, standalone AI security products.
- **Flexible enforcement**: Support both third-party enforcement models and fully integrated Barracuda SecureEdge workflows.
- **Confidence in governance**: Establish realistic guidelines that align with how AI is being used in the organization.

Why Barracuda

BarracudaONE AI Security reflects Barracuda's long-standing focus on integrated platforms, cyber resiliency and ease of use. By embedding AI security capabilities directly into BarracudaONE, Barracuda eliminates the friction, cost and operational burden typically associated with emerging security categories.

Rather than forcing customers to define AI security from scratch, Barracuda helps organizations understand what acceptable AI risk looks like and provides the tools to manage it. With the option to extend insight through existing controls or adopt SecureEdge for end-to-end governance, Barracuda empowers organizations to embrace AI innovation, securely and confidently.