# Accelerate AI adoption safely while maintaining visibility and control

Barracuda® AI Data Security helps businesses see AI usage, protect sensitive data, enforce responsible AI use, and demonstrate compliance.

## Barracuda AI Data Security plans

Employees are already using Copilot, ChatGPT, Claude, Gemini, and other AI tools to move faster. Barracuda AI Data Security is an AI security and governance solution that helps businesses see AI use, protect sensitive data, enforce responsible AI use, and demonstrate compliance. The solution helps businesses strengthen AI governance while accelerating AI adoption safely.

Two plans meet you where you are: Premium delivers security operations center (SOC)-backed detection and response for Microsoft 365 Copilot with low-touch, agentless deployment, while Premium Plus adds real-time, inline prevention that helps stop sensitive data from reaching the AI service.

*This datasheet covers the Premium and Premium Plus plans.*

## Barracuda AI Data Security Premium

Respond to AI risks and threats with low-touch deployment.

### Benefit

Turn AI visibility into action with agentless, out-of-band protection and no inline traffic routing. Premium delivers agentless discovery and AI-domain control across supported AI tools, with SOC-backed detection and response for Microsoft 365 Copilot.

### Description

Barracuda AI Data Security Premium delivers continuous, SOC-backed detection and response for Microsoft 365 Copilot with Barracuda Managed XDR. It connects through authorized provider application programming interfaces (APIs), with no agent, endpoint client, or inline component, so it is fast and straightforward to deploy. Copilot prompt security appears directly in the Barracuda Managed XDR dashboard, where Copilot prompt logs and compliance data are ingested and evaluated against industry standards. Because Premium operates through provider APIs rather than inline inspection, Barracuda Managed XDR detects and responds after a violation occurs instead of blocking it in real time. For visibility and domain-level control across other AI tools, Premium uses SecureEdge DNS access to identify and manage AI applications. The result is always-on AI security response with minimal implementation effort.

### Deployment

Delivered as a Barracuda Managed XDR service, backed by the 24/7/365 Barracuda SOC. Agentless and out-of-band, Barracuda Managed XDR connects to Microsoft 365 Copilot through authorized provider and compliance APIs, with nothing installed on endpoints and nothing in the traffic path. Copilot prompt security, detection rules, and Automated Threat Response are managed in the Barracuda Managed XDR dashboard. Optional SecureEdge DNS access adds AI application visibility and control across other tools. It provides post-activity detection and response rather than real-time prevention.

## Barracuda AI Data Security Premium Plus

Protect sensitive data before it reaches AI services.

### Benefit

Protect sensitive data before it reaches AI services. Premium Plus adds real-time, inline inspection and enforcement for leading AI tools, so users can be warned or activity can be blocked before sensitive data reaches the AI service.

### Description

Barracuda AI Data Security Premium Plus adds real-time prevention to the capabilities included in Premium. Delivered inline through SecureEdge Premium Access, user traffic flows through the SecureEdge Access agent and cloud PoPs, where prompts and file uploads to leading AI tools, including Copilot, ChatGPT, Claude, Gemini, and Perplexity, are inspected synchronously. Configurable AI policies can trigger a warning to the user or block the activity before sensitive data reaches the AI service. Every inspected prompt is captured in a prompt audit log, with detected sensitive values redacted to help prevent raw secrets or personally identifiable information from being stored in the log.

Premium Plus layers real-time AI-related threat prevention on top of Premium's capabilities: discovery, posture, and Barracuda Managed XDR threat detection and response.

### Deployment

Delivered inline through SecureEdge Premium Access, full Security Service Edge (SSE). Requires the SecureEdge Access agent on user devices, with traffic routed through SecureEdge cloud PoPs for synchronous inspection and enforcement. Real-time policies can block activity or warn users before they submit prompts and uploads to five supported AI tools: Copilot, ChatGPT, Claude, Gemini, and Perplexity.

Premium Plus also includes the discovery, posture, and Barracuda Managed XDR detection-and-response capabilities of Premium. It is managed through SecureEdge Manager and requires endpoint agent deployment and traffic routing to enable real-time prevention.

## Barracuda AI Data Security — Detailed feature comparison

Premium provides agentless detection and response with low deployment effort. Premium Plus includes Premium and adds real-time, inline inspection and enforcement for supported AI tools.

| CAPABILITIES | PREMIUM | PREMIUM PLUS |
|---|---|---|
| **DISCOVERY AND POSTURE** | | |
| Shadow AI discovery (which AI tools are in use) | ✓ | ✓ |
| AI Data Security risk assessment and AI risk report | ✓ | ✓ |
| AI security posture and risk baseline | ✓ | ✓ |
| Continuous monitoring | ✓ | ✓ |
| **DETECTION AND RESPONSE (BARRACUDA XDR)** | | |
| Copilot prompt security in the Barracuda Managed XDR dashboard | ✓ | ✓ |
| Copilot prompt log and compliance API data ingestion | ✓ | ✓ |
| MITRE ATT&CK-mapped threat detection rules | ✓ | ✓ |
| Automated Threat Response (ATR) | ✓ | ✓ |
| 24/7/365 SOC-backed service | ✓ | ✓ |
| AI agent activity monitoring | ✓ | ✓ |
| Expanded integrations (ChatGPT, Claude, and additional AI tools) | — | ✓ |

| CAPABILITIES | PREMIUM | PREMIUM PLUS |
|---|---|---|
| **INLINE PREVENTION (SECUREEDGE)** | | |
| SecureEdge DNS access — AI-domain visibility and control | ✓ | ✓ |
| Real-time inline inspection of prompts and file uploads | — | ✓ |
| Pre-submission warning or blocking | — | ✓ |
| Real-time inspection coverage by AI tool (Copilot, ChatGPT, Claude, Gemini, Perplexity) | — | ✓ |
| Prompt Audit Log (sensitive values redacted) | — | ✓ |
| **DEPLOYMENT AND OPERATIONS** | | |
| Delivered through | Barracuda XDR | SecureEdge Premium Access |
| Deployment model | Out-of-band | Inline / in-path |
| Endpoint agent requirement | Client Certificates and JWT | Client Certificates and JWT |
| Shared IP | — | ✓ |
| Traffic routed through SecureEdge PoPs | — | ✓ |
| Enforcement timing | Detection and response (after the fact) | Real-time prevention |
| Implementation effort | Low (agentless) | Moderate (agent + routing) |
| XDR dashboard | ✓ | ✓ |
| SecureEdge Manager | ✓ | ✓ |

## Key features by plan

### Barracuda AI Data Security Premium

- **AI app discovery and posture baseline.** See which AI tools employees are already using and establish your AI security posture and risk baseline, creating the foundation Premium uses for detection and response.
- **Copilot prompt security in the XDR dashboard.** Copilot prompt logs and compliance data are ingested and surfaced directly in the XDR dashboard for investigation and control.
- **MITRE ATT&CK-mapped detection.** High-fidelity detection rules mapped to MITRE ATT&CK identify risky and malicious Copilot activity.
- **Automated Threat Response.** Automated Threat Response can initiate containment actions for confirmed threats, reducing the need for manual intervention.
- **24/7/365 SOC-backed.** Barracuda's global, follow-the-sun SOC investigates alerts and drives response around the clock.
- **Agentless, out-of-band deployment.** Connects through authorized provider APIs for a fast, low-touch way to switch on AI security response, with nothing inline.
- **SecureEdge DNS control for other AI tools.** Extend visibility and domain-level control to the other AI tools employees reach beyond Copilot.

### Barracuda AI Data Security Premium Plus

- **Everything in Premium.** Premium Plus builds on Premium capabilities for AI app discovery and posture, Copilot prompt security in the XDR dashboard, MITRE ATT&CK detection, Automated Threat Response, and 24/7/365 SOC coverage, with real-time prevention layered on top.
- **Real-time inline prevention.** Prompts and file uploads are inspected synchronously, and users can be warned or activity can be blocked before sensitive data reaches the AI service.
- **Coverage for the leading AI tools.** Inline protection for five supported AI tools: Copilot, ChatGPT, Claude, Gemini, and Perplexity.
- **Prompt Audit Log.** Every inspected prompt is captured as audit-ready evidence, with sensitive values redacted so the log never stores raw secrets or PII.
- **Full SSE via SecureEdge Premium Access.** Delivered inline through SecureEdge Premium Access to inspect generative AI prompts and uploads across managed devices.