

# WitnessAI and F5 BIG-IP SSL Orchestrator

**SEE EVERYTHING,  
PROTECT EVERYWHERE**

AI applications are growing at a stunning rate, with thousands of LLM-driven applications available on the internet today. As enterprise employees use these apps to perform their work more effectively, they may put confidential customer data or company IP such as source code, at risk. Those same AI applications may also convince employees to take action that is harmful to the organization. Security organizations are overwhelmed by the sheer number of AI apps, and can't simply block them all at the firewall. Even worse, firewalls, zero-trust proxies, and endpoint agents are blind to the conversations that employees hold with GenAI apps.

Today, F5 customers using BIG-IP SSL Orchestrator already enjoy powerful capabilities for gaining visibility into encrypted application traffic at scale. With WitnessAI, BIG-IP users can now get deep insights into enterprise **AI traffic** as well.

WitnessAI is designed to intercept traffic from third-party AI applications at the network level, with no endpoint agent required. It creates a catalog of all AI apps being used in your network, shows the risk of those apps, and captures the full employee conversations with those apps — so that you can understand how your people are using AI, and to help them use it safely and effectively.

It includes policy-based controls over data redaction, safe responses, and access based on identity and intention. With WitnessAI you can easily implement your corporate acceptable use policies for AI, and enforce them everywhere, even in native apps such as Microsoft Word with Copilot — all without an install on the user's machine.

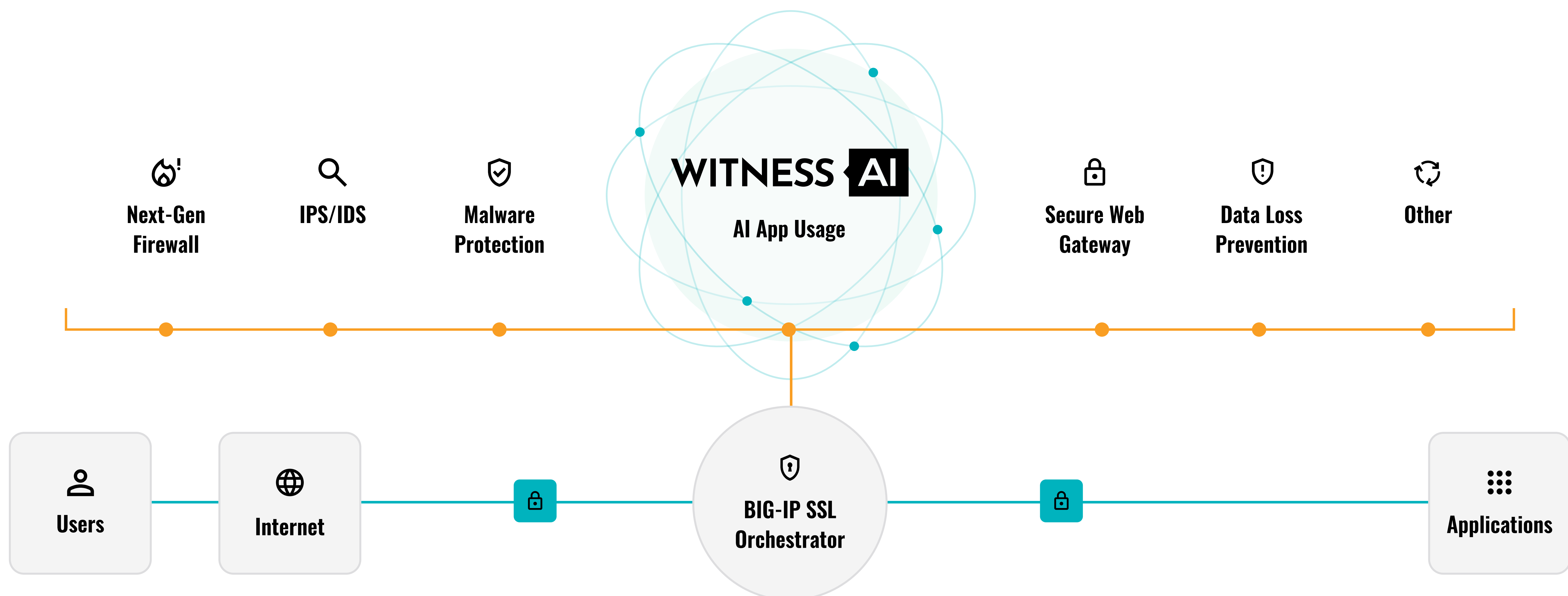
## WITNESS/OBSERVE

Witness/OBSERVE eliminates “shadow AI” by creating a catalog of AI apps being accessed by employees, and supports compliance by logging every AI conversation and classifying it for risk and intention.

## WITNESS/CONTROL




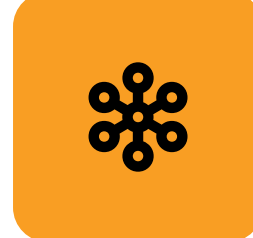

Witness/CONTROL activity guardrails enforce corporate AI acceptable use policy based on identity and intended use — even in native apps such as Microsoft Word with Copilot, all without an agent installed on end users' machines. Together, these products enable safe use of AI via governance and risk management.

With the easy-to-deploy integration between F5 BIG-IP SSL Orchestrator and WitnessAI, organizations gain visibility and control over all encrypted traffic, including traffic to the thousands of AI applications already available to your employees on the internet. Through a single platform for inspecting and controlling all network and AI traffic, joint customers can enhance, secure, and optimize existing technology investments. The integrated solution not only secures data submitted to a third-party AI app, but also prevents harmful responses from those apps, protecting users from misinformation or unlawful influence. Together, F5 and WitnessAI help organizations of any size give their people AI superpowers to work more productively and effectively.



*WitnessAI is available as an integrated connection with BIG-IP SSL Orchestrator.*

## BENEFITS FOR F5 BIG-IP CUSTOMERS

-  Gain visibility into all network traffic, including encrypted access to any AI application on the internet
-  Apply policy-based control to gain flexible, dynamic protection of employee activity
-  Ensure privacy of sensitive information, including customer records, corporate IP, and source code
-  Enable use across LLMs, applications, cloud platforms, and security products — no endpoint agent required
-  Protect native AI app use, such as Microsoft Office with Copilot and Visual Studio Code with Github Copilot

## About WitnessAI

WitnessAI enables safe and effective adoption of enterprise AI, through security and governance guardrails for public and private LLMs. The WitnessAI Secure AI Enablement Platform provides visibility of employee AI use, control of that use via AI-oriented policy, and protection of that use via data and topic security.

Learn more at [witness.ai](https://witness.ai).