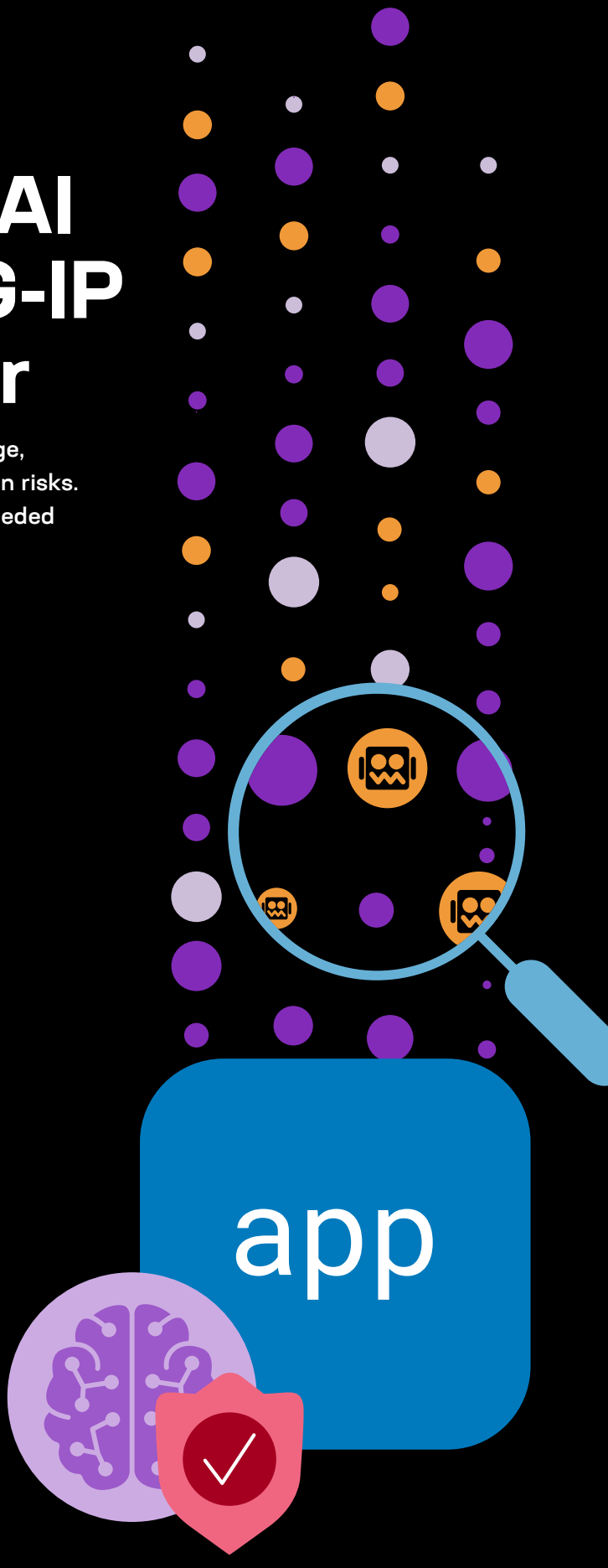
Solution Overview

Control Shadow AI Risks with F5 BIG-IP SSL Orchestrator

Shadow AI is quickly emerging as a critical security challenge, as unsanctioned generative AI tools create dangerous hidden risks. BIG-IP SSL Orchestrator delivers the visibility and control needed to mitigate these risks without compromising innovation.



Key Benefits

Eliminate AI blind spots
Decrypt SSL/TLS encrypted traffic to uncover Shadow AI activity and address hidden risks.

Enforce tailored security
Apply dynamic, risk-based controls to scrutinize high-risk actions—like unauthorized or secretive GenAI access—while maintaining performance for safe workflows.

Boost security awareness
Educate users in real time with contextual, programmable guidance to prevent mistakes—like uploading sensitive data to GenAI—and reinforce policies.

Simplify operations
Integrate seamlessly with existing security tools for centralized Shadow AI management.

In today's AI-driven, hybrid multi-cloud environments, blocking generative AI tools isn't practical–the smarter solution is to secure their use intelligently.

The Growing Risks and Challenges of Shadow AI

Generative AI (GenAI) tools like ChatGPT, Claude, and many others are rapidly transforming how organizations work—fueling automation, accelerating innovation, and enhancing productivity. These tools are no longer optional. They're becoming mission-critical across industries.

But with their rise in popularity comes a new class of security risk: Shadow AI—the unsanctioned use of AI tools by employees, contractors, or partners without IT or security oversight. A subset of Shadow IT, Shadow AI introduces critical blind spots and vulnerabilities, such as:

- **Data exposure:** Sensitive or proprietary information may be uploaded to external platforms, outside your organization's control.
- **Compliance risks:** Unauthorized AI usage can violate industry and government regulations like GDPR, HIPAA, or PCI DSS.
- **Hidden malware:** AI platforms typically operate over HTTPS or TLS, limiting visibility and increasing the chance of encrypted threats slipping through undetected.

These risks are compounded by the growing complexity of hybrid, multicloud environments, where workloads are distributed and security tools often operate in silos. For SecOps teams already stretched thin, monitoring and controlling AI activity across such environments is both difficult and time-consuming.

Simply blocking GenAI tools might seem like the easiest solution, but it's not practical for modern enterprises that depend on them to remain competitive in the AI-driven era. The challenge lies in securing AI usage intelligently while protecting your organization, sensitive data, and intellectual property without introducing operational bottlenecks or compromising innovation.

Key Features

Real-time traffic decryption
Expose GenAI activity hidden in encrypted traffic through proactive detection and control.

Dynamic traffic routing
Use service chaining to direct high-risk actions through DLP, WAF, or other inspection tools based on risk levels.

Granular policies
Leverage F5 Secure Web Gateway Services to allow, block, or confirm safe AI use on a user-by-user basis.

Programmable user coaching
Deliver customized, in-the-moment alerts to guide users and prevent violations of AI use policies—without extra external tools.

F5 BIG-IP SSL ORCHESTRATOR:

The Backbone for Detecting and Managing Shadow AI

F5® BIG-IP® SSL Orchestrator® is a cornerstone solution to secure GenAI usage without undermining productivity—or innovation. By combining deep visibility into encrypted traffic, intelligent orchestration, and seamless integration with your existing security stack, BIG-IP SSL Orchestrator enables a multi-layered approach to detect, control, and manage Shadow AI activity efficiently.

Decrypt and detect: Achieving critical visibility into encrypted traffic
Encrypted traffic is essential for protecting data in transit, but it also introduces significant blind spots for SecOps teams. These blind spots make it difficult to identify Shadow AI and to stop any sensitive data being shared inappropriately through unauthorized GenAI use. BIG-IP SSL Orchestrator eliminates this lack of visibility by decrypting encrypted traffic in real time. By gaining critical insights into AI-related behaviors, your organization can:

- **Detect Shadow AI activity:** Identify unsanctioned GenAI usage hidden within encrypted flows and address emerging risks before they escalate.
- **Intervene proactively:** Block malicious payloads and prevent sensitive data shares with external AI platforms, safeguarding your organization from compliance violations and data loss.
- **Enhance security tool efficacy:** Orchestrate decrypted traffic across your security stack to improve threat detection and enable efficient enforcement and inspection.

By removing encryption blind spots, BIG-IP SSL Orchestrator provides the foundation for detecting and managing Shadow AI.

Enforce intelligently: Dynamic service chaining for tailored control
While visibility is critical for uncovering risks, it's only the first step to managing the risks that Shadow AI brings. Effective security requires intelligent orchestration and enforcement. BIG-IP SSL Orchestrator's dynamic service chaining empowers SecOps teams to apply customized security measures by routing traffic through appropriate security tools based on risk level. For instance:

- **High-risk actions:** Route sensitive activities, such as file uploads or data transfers, through tools like Data Loss Prevention (DLP) scanners, Web Application Firewalls (WAF), or Intrusion Detection Systems (IDS) to prevent data exfiltration to GenAI software and detect malicious payloads.
- **Low-risk interactions:** Allow routine actions, such as AI-based text prompts, to bypass deep inspection, maintaining performance while minimizing latency.

This approach ensures that traffic receives the right level of security scrutiny without slowing down safe, productive AI usage. By dynamically tailoring traffic orchestration, BIG-IP SSL Orchestrator enables precise enforcement and optimized performance—all while simplifying management for SecOps teams.

Extend control: Advanced policy enforcement with F5 Secure Web Gateway Services
As part of its services catalog, BIG-IP SSL Orchestrator natively integrates with F5® Secure Web Gateway Services, enabling your organization to apply advanced, granular policies for managing GenAI usage. This integration not only expands the enforcement capabilities of BIG-IP SSL Orchestrator but also simplifies deployment and management by consolidating tools into a centralized platform.

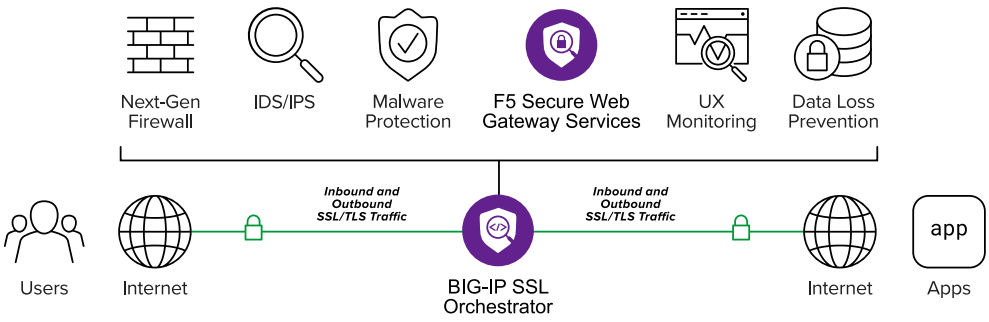


Figure 1: Uplevel your Shadow AI security posture by deploying F5 Secure Web Gateway Services with BIG-IP SSL Orchestrator—all in a click of a button.

With F5 Secure Web Gateway Services, your organization can further balance security with operational needs. For instance, you can:

- **Enable role-based access:** Grant GenAI access to lower-risk teams like Marketing or HR while restricting more sensitive departments like Finance or Legal from high-risk actions.
- **Protect regulated data:** Block personally identifiable information (PII), financial data, or other sensitive assets from being uploaded by users to unsanctioned tools, ensuring compliance with regulations like GDPR and HIPAA.

With F5 Secure Web Gateway Services as part of BIG-IP SSL Orchestrator's service catalog, deployment is simple, management is intuitive, and enforcement is precise.

Build awareness: Fostering a security-aware culture with user coaching

BIG-IP SSL Orchestrator adds an important additional guardrail to your Shadow AI security strategy with user coaching via Service Extensions. Fully programmable and simple to deploy, user coaching delivers real-time, contextual guidance to users—such as intercepting risky actions like uploading sensitive data to external AI platforms—without requiring any external tooling.

BIG-IP SSL Orchestrator provides a multi-layered approach to detect, control, and manage Shadow AI activity efficiently.

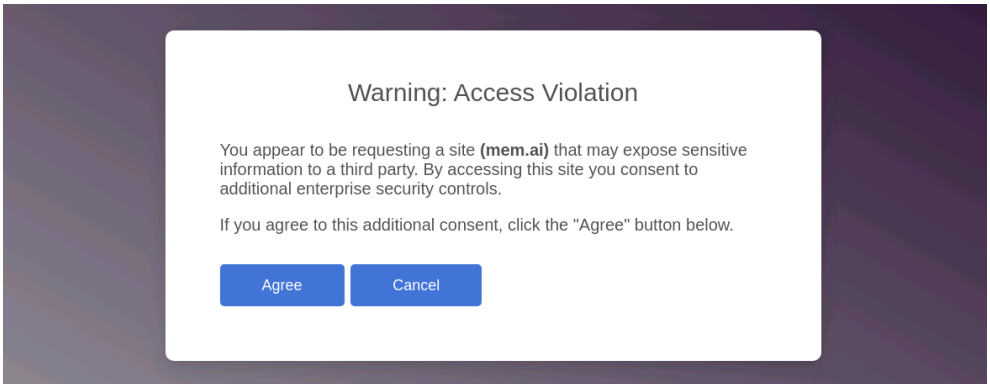


Figure 2: Easily incorporate user coaching, customizing its look, feel, and messaging with Service Extensions through BIG-IP SSL Orchestrator.

With it, you can:

- **Prevent mistakes at critical moments:** Minimize compliance violations and sensitive data exposure with tailored, in-the-moment guidance.
- **Reinforce policies seamlessly:** Deliver custom coaching messages directly through BIG-IP SSL Orchestrator to align with existing organizational policies, including your AI use policy.
- **Drive security awareness:** Promote accountability and long-term adherence to security protocols without interrupting productivity.

As an added layer of defense, user coaching will help your SecOps team ensure compliance and proactive risk management while empowering employees to make informed actions—all without relying on heavy-handed enforcement.

Conclusion

As GenAI transforms industries, the risks posed by Shadow AI require a smarter approach to security. BIG-IP SSL Orchestrator empowers organizations to efficiently manage Shadow AI activity by providing visibility into encrypted traffic, dynamic orchestration, tailored policy enforcement with F5 Secure Web Gateway Services, and proactive user coaching via Service Extensions.

With BIG-IP SSL Orchestrator, securing innovation is no longer a trade-off—it becomes a strategic advantage. This seamless, multi-layered solution simplifies Shadow AI management while protecting productivity, compliance, and your organization's critical assets.

Want to learn more about how F5 products and solutions can help you to achieve your goals? Contact F5.