DEEPWATCH™
Always Watching. Always Protecting.

www.deepwatch.com

# Strategy Guide:

## The Triad of Cloud Application Security Monitoring in 2026

**Published: Mar 10, 2026**

Analysis by:
**Deepwatch Threat Intelligence**

DEEPWATCH™
Always Watching. Always Protecting.™

# Executive Summary

As we enter 2026, we continue to observe the trend that the perimeter continues to dissolve. Organizations no longer manage a "network"; they manage a web of interconnected SaaS platforms, proprietary APIs, and AI-driven data flows. To secure this landscape, security leaders must monitor three non-negotiable pillars: **SSPM**, **WAAP**, and **DSPM**. While consolidation in the industry is beginning, a "single pane of glass" remains elusive, requiring a best-of-breed strategic approach.

# PILLAR 1:
# SaaS Security Posture Management

## (SSPM) **Focus:** The Identity & Integration Layer

The primary risk in 2026 is not just "settings," but the **SaaS-to-SaaS Supply Chain**. When you integrate a tool like Salesloft or Zapier into your Salesforce, you create a "hidden" trust path. Here are a few recommendations for vendors that understand these risks and help mitigate them.

- **AppOmni:** Still the enterprise standard for preventing **"Configuration Drift."** Their 2026 platform now includes automated "reversion" scripts that undo unauthorized setting changes in real-time.
- **CrowdStrike (Falcon Adaptive Shield):** Since its integration, this has become the top choice for companies already using CrowdStrike. It excels at mapping **non-human identities** (service accounts and AI agents) which now outnumber human users 5-to-1.
- **Obsidian Security:** The leader in **SaaS Identity Threat Detection and Response (ITDR)**. Their "Knowledge Graph" tracks how users move *between* apps, flagging "Impossible Travel" or unusual data exports across different platforms.
- **Wing Security:** The most agile solution for managing **Shadow SaaS**. Its automated remediation engine can instantly revoke permissions for high-risk Oauth integrations without IT intervention.

# PILLAR 2:
# Web Application & API Protection

## (WAAP) **Focus:** Traffic Integrity and Edge Defense

The primary risk in 2026 is not just "settings," but the **SaaS-to-SaaS Supply Chain**. When you integrate a tool like Salesloft or Zapier into your Salesforce, you create a "hidden" trust path. Here are a few recommendations for vendors that understand these risks and help mitigate them.

- **Cloudflare:** The dominant force in **Automated Bot Management**. Cloudflare uses global threat intelligence to filter out sophisticated "low-and-slow" scraping attacks that mimic human behavior to bypass traditional rate limiting.
- **Akamai:** The benchmark for **API Behavioral Analytics**. Akamai monitors the "logic" of API calls, identifying when an attacker is attempting to manipulate parameters (BOLA/BFLA attacks) to access data that doesn't belong to them.
- **F5 (Distributed Cloud):** Provides a unified monitoring fabric for **Multi-Cloud Environments**. It ensures that security policies remain consistent whether an application is hosted in a private data center, AWS, or Azure, preventing "security silos."

# PILLAR 3:
# Data Security Posture Management

## (DSPM) **Focus:** The Asset & Content Layer

DSPM has evolved from "discovery" to **"Active Data Protection."** It is not enough to know where your data is; you must know how it is *behaving*. The following vendors are leading the shift toward data-centric security.

- **Cyera:** The pioneer of **AI-led Data Classification**. It can now process petabytes of data to find "Secrets in the Wild"—API keys or passwords accidentally saved in unstructured docs or chat logs.
- **Varonis:** The "Gold Standard" for **Unstructured Data**. Its 2026 focus is on "Least Privilege Automation," which automatically removes access to files that haven't been touched in 30 days, drastically reducing the blast radius of a breach.
- **Sentra:** Specifically designed for **Cloud-to-Cloud Data Flows**. As data moves from an AWS bucket to a Snowflake warehouse to a Slack channel, Sentra ensures the security policy "follows" the data.

# The Consolidation Alternative: The "All-in-One" Platform

While the three pillars (SSPM, WAAP, DSPM) have traditionally required specialized vendors, **Wiz** has largely emerged as the primary alternative for organizations looking to consolidate their security stack into a single **Cloud-Native Application Protection Platform (CNAPP)**.

### How Wiz "Does Most"

Wiz uses a "Security Graph" methodology to show how a vulnerability in a web app, a misconfiguration in a SaaS setting, and a sensitive data store are all connected.

- **In Place of SSPM:** Wiz for SaaS provides visibility into major platforms like Microsoft 365, Salesforce, and GitHub. While it may not have the niche configuration depth of a specialist like AppOmni, it effectively flags the most critical risks, such as "Shadow Admins" or public sharing of internal documents.
- **In Place of DSPM:** Wiz is widely considered a leader in integrated DSPM. It performs agentless scanning of cloud buckets and databases to identify PII (Personally Identifiable Information) without needing to install software on every server.
- **In Place of WAAP:** This is the only area where Wiz is an *alternative* rather than a direct replacement.
    - **The Difference:** A WAAP (like Cloudflare) is **"Outside-In"**—it sits in front of your app to block bad traffic.
    - **The Wiz Approach:** Wiz is **"Inside-Out"**—Wiz's "Runtime Sensor" is their biggest selling point. It uses eBPF technology, which is the "gold standard" for monitoring Linux/Container workloads without slowing them down to monitor the application's internal behavior. It discovers all your APIs and tells you if they are "exposed" to the internet, but it typically relies on an external WAF for the actual real-time blocking of DDoS attacks.

# Strategic Comparison: Best-of-Breed vs. Unified Platform

Ultimately it is up to each organization to decide what path best suits their needs. Here is an example of how you can go about tackling this problem in two different paths:

| Strategy | Example Recommended Stack | Best For |
|---|---|---|
| **Best-of-Breed** | AppOmni + Cloudflare + Cyera | Enterprises with strict regulatory requirements (Finance/Healthcare) that need "inch-wide, mile-deep" security for every layer. |
| **Unified Platform** | Wiz + Cloudflare | Cloud-native companies that prioritize speed and want to reduce "tool fatigue" by having 80% of their monitoring in one dashboard. |