# Application Security Posture Management (ASPM): mettere ordine nel rumore degli strumenti di sicurezza applicativa



L’ASPM, sigla di Application Security Posture Management, nasce da un paradosso della sicurezza applicativa moderna: più strumenti si aggiungono per trovare le vulnerabilità nel codice, meno chiaro diventa quali contino davvero. Un’organizzazione che sviluppa software esegue oggi analisi statica, analisi dinamica, controllo delle dipendenze open source, ricerca di segreti, scansione dei container e dell’infrastruttura come codice: ognuno di questi strumenti produce la propria lista di risultati, con le proprie priorità e il proprio cruscotto. Quello che dovrebbe essere più controllo diventa un rumore di fondo di migliaia di segnalazioni scollegate, in cui i difetti gravi si perdono tra falsi positivi e duplicati.

L’ASPM è la risposta a questo disordine: un livello che raccoglie i risultati di tutti quegli strumenti, li mette in relazione, elimina i doppioni e li ordina per rischio reale, così che chi sviluppa e chi difende guardino finalmente la stessa mappa invece di dodici elenchi diversi. È una promessa attraente, ed è anche il motivo per cui la categoria è cresciuta in fretta e si è affollata di fornitori. Come per ogni etichetta di moda, la domanda utile non è che cosa promette, ma che cosa consolida davvero, e come distinguerlo dal marketing.

# Il problema: troppi strumenti, nessuna priorità

Negli ultimi anni la sicurezza del software si è arricchita di strumenti specializzati, ciascuno bravo a vedere una cosa sola. Il SAST legge il codice sorgente in cerca di errori, il DAST attacca l'applicazione in esecuzione, l'analisi delle dipendenze cerca le librerie open source vulnerabili, altri strumenti ancora scovano segreti dimenticati nei repository o configurazioni sbagliate nell'infrastruttura come codice. Presi uno per uno funzionano; presi insieme, si ostacolano. Nessuno di loro sa quello che sanno gli altri, e nessuno colloca ciò che trova nel contesto dell'applicazione reale.

Il conto lo pagano due categorie di persone. I team di sicurezza, che si ritrovano davanti a decine di cruscotti separati e a un totale di segnalazioni impossibile da governare, senza un criterio comune per dire quale difetto affrontare per primo. E gli sviluppatori, sommersi da avvisi che spesso sono duplicati dello stesso problema visto da strumenti diversi, o falsi positivi, o vulnerabilità in codice che non viene mai eseguito. Quando tutto è segnalato come urgente, niente lo è: è la definizione stessa dell'affaticamento da alert, e il terreno su cui i difetti che contano passano inosservati. La pressione, per giunta, è in aumento, perché la generazione di codice assistita dall'AI produce software più in fretta di quanto gli strumenti riescano a esaminarlo, gonfiando ancora il volume delle segnalazioni. Il problema, si noti, non è la mancanza di strumenti, ma la mancanza di un punto di vista unico che li tenga insieme, e non lo risolve un altro scanner: lo risolve un livello di governo che sta sopra a quelli esistenti.

# Che cosa fa un ASPM

Un ASPM, nella sua accezione originaria, non cerca

vulnerabilità: le riceve. Si collega agli strumenti di analisi già in uso, ne importa i risultati e su quei dati fa un lavoro che nessuno dei singoli strumenti può fare. Prima li mette in correlazione ed elimina i duplicati, riconoscendo che la stessa falla segnalata da tre scanner diversi è un problema solo, non tre. Tiene un inventario delle applicazioni e delle loro componenti, così da sapere che cosa esiste prima ancora di valutarlo. Poi arricchisce ogni segnalazione di contesto, cioè risponde alle domande che decidono la gravità reale: quel pezzo di codice viene effettivamente eseguito, è raggiungibile da un aggressore, l'applicazione è esposta su internet, tratta dati sensibili, è in produzione o in un ambiente di prova. Una vulnerabilità teoricamente critica in un componente mai richiamato conta meno di una media in un servizio esposto e centrale, e solo il contesto permette di distinguerle.

Su questa base l'ASPM ordina i problemi per rischio effettivo, non per la severità astratta assegnata dal singolo strumento, traccia il legame tra il codice sorgente e ciò che gira in produzione, e in molte piattaforme impone regole lungo la catena di sviluppo, bloccando per esempio una build che introduce una dipendenza vietata, oltre a seguire nel tempo l'andamento della postura. Non a caso, nella definizione di mercato di Gartner, gli strumenti ASPM gestiscono in continuo il rischio applicativo lungo il ciclo di vita del software: ne raccolgono, analizzano e prioritizzano i problemi, ingeriscono i dati di più strumenti, mantengono un inventario del software, correlano i risultati e permettono di applicare le policy di sicurezza. È una direzione che il mercato prende sul serio: secondo le riprese pubbliche dell'aggiornamento del gennaio 2025 dell'Innovation Insight di Gartner, entro il 2027 l'80% delle organizzazioni dei settori regolamentati che fanno analisi di sicurezza applicativa adotterà una qualche forma di ASPM, contro il 29% stimato allora. Va però detto subito, perché conta per tutto il resto, che una parte del mercato non si limita a ricevere i dati altrui ma integra scanner propri: è la linea di faglia attorno a cui ruota il vero dibattito

sulla categoria.

## Da ASOC alle altre “posture”: un vicinato affollato

L’idea non è nata dal nulla. L’ASPM è l’evoluzione di una categoria precedente, l’ASOC, cioè l’orchestrazione e correlazione della sicurezza applicativa. La differenza è che l’ASOC si fermava a orchestrazione e correlazione, mentre l’ASPM aggiunge i due ingredienti che rendono utile quel lavoro: il rischio e il contesto. Non basta mettere in fila gli elenchi, bisogna sapere quali voci contano e perché, ed è questo salto, dalla raccolta alla priorità, a definire la categoria.

Attorno all’ASPM si affolla una famiglia di sigle che finiscono tutte in “posture management”, e conviene tenerle distinte per non confondere strumenti che guardano oggetti diversi. L’SSPM sorveglia la postura delle applicazioni SaaS che un’azienda usa ma non sviluppa; il CNAPP e le posture di cloud e dati presidiano ciò che accade negli ambienti cloud in esecuzione. L’ASPM, invece, ha per oggetto le applicazioni che l’organizzazione costruisce, lungo tutto il ciclo di sviluppo. Da tenere fuori dal confronto è il DevSecOps, che non è un prodotto ma il metodo con cui la sicurezza entra nel processo di sviluppo: l’ASPM semmai lo strumenta, dandogli i dati e i controlli, non lo sostituisce.

Nel 2026, però, il vicinato si è fatto più stretto e più insidioso. Nel suo Hype Cycle for Secure Software Engineering del 2 giugno 2026, Gartner colloca l’ASPM accanto a due categorie in ascesa, la sicurezza del codice generato da agenti AI e la sicurezza della supply chain del software, e descrive ormai le piattaforme ASPM come strumenti che centralizzano la visibilità e la governance del rischio di sicurezza applicativa, una formula più orientata al governo che alla semplice correlazione. È il segno che la categoria

non sta più da sola. E il 17 giugno 2026 è arrivato il primo Magic Quadrant dedicato proprio alla software supply chain security, con diciotto fornitori valutati: una categoria promossa a disciplina autonoma, spinta anche dal Cyber Resilience Act europeo, che dall'11 dicembre 2027 imporrà requisiti di trasparenza sulla filiera del software, trasformando in obbligo ciò che oggi è buona pratica. Il risultato è che i confini dell'ASPM oggi non premono solo dal lato del cloud, ma anche da quello della supply chain e da quello, più largo, della gestione continua dell'esposizione, il CTEM: nato come programma metodologico in cinque fasi e diventato nel mercato un'etichetta di piattaforma, che ambisce a governare il rischio dal codice fino alla produzione in un quadro unico.

## Il nodo vero: aggregatore, piattaforma o categoria che si dissolve

Sotto l'etichetta comune convivono due filosofie molto diverse, e capirne la differenza è la chiave per non comprare fumo. Da un lato c'è l'ASPM come aggregatore neutro, indipendente dai fornitori, che non esegue scansioni proprie ma ingerisce i risultati degli strumenti che l'azienda ha già, correlandoli e prioritizzandoli. Dall'altro c'è l'ASPM come piattaforma tutto-in-uno, che integra le proprie capacità di analisi e la gestione della postura in un unico prodotto, riducendo il numero di fornitori invece di orchestrarli. La scelta non è di poco conto: la prima strada rispetta gli investimenti già fatti ma dipende dalla qualità di ciò che riceve, la seconda semplifica ma lega a un solo fornitore.

Su questa faglia si è consumata la critica più netta alla categoria. L'analista indipendente James Berthoty di Latio sostiene già dal 2023 che l'unico ASPM dotato di senso sia una piattaforma che esegue davvero le scansioni, e che chi si

limita a ingerire i risultati altrui non è un ASPM ma un fornitore di gestione delle vulnerabilità, e non c'è motivo di chiamarlo in altro modo. È la vecchia legge del "garbage in, garbage out": un cruscotto alimentato con dati scadenti restituisce spazzatura ordinata meglio. Nel suo rapporto del febbraio 2026 sul mercato della sicurezza applicativa, costruito su oltre cento colloqui con fornitori, professionisti e acquirenti, la tesi si fa ancora più tagliente: Berthoty parla della "morte silenziosa dell'ASPM come categoria autonoma di gestione", assorbita da piattaforme più ampie di gestione dell'esposizione capaci di seguire il rischio dal codice al cloud, in una disciplina che l'AI sta scuotendo alla radice cambiando insieme le capacità degli scanner e il modo di lavorare degli sviluppatori. E non è un'opinione isolata: la stessa premessa, cioè che l'ASPM non regga più da solo, affiora nei segnali di mercato già visti, per quanto le direzioni di assorbimento divergano, dal primo Magic Quadrant sulla supply chain alla convergenza che gli stessi fornitori rivendicano tra ASPM, analisi del codice e sicurezza della filiera, fino alla spartizione di scena con altre due categorie nell'Hype Cycle del 2026.

## Come valutarlo oltre il marketing

La conseguenza pratica è che un ASPM va giudicato su ciò che fa alla fine, non su ciò che dichiara di consolidare. Il primo criterio è la qualità della correlazione e della deduplica: quanto bene riconosce che segnalazioni diverse sono lo stesso problema, e quanto affidabile è l'analisi di contesto con cui stabilisce se una vulnerabilità è davvero raggiungibile e sfruttabile. Un buon strumento riduce il numero di voci da guardare in modo drastico e difendibile; uno cattivo si limita a impilarle. Vale la pena chiedere ai fornitori non la lunghezza dell'elenco di integrazioni, ma la profondità di quelle poche che contano per il proprio stack.

Il secondo criterio è l'effetto sul lavoro reale di chi

corregge. Un ASPM utile accorcia il tempo che passa tra la scoperta di un difetto e la sua correzione, porta la segnalazione alla riga di codice e alla persona giusta, e impone regole senza sommergere di blocchi chi sviluppa. Contano più questi risultati misurabili della bellezza del cruscotto unico, che è facile da mostrare in una demo e inutile se dietro non c'è una vera prioritizzazione basata sul rischio. Conviene infine chiedersi se lo strumento si incastri nella più ampia strategia di gestione dell'esposizione dell'organizzazione o se aggiunga solo un altro silo: alla luce di dove sta andando il mercato, un ASPM che non dialoga con il resto rischia di nascere già vecchio.

## Cosa aspettarsi, senza illusioni

L'ASPM risponde a un problema autentico e ormai diffuso, quello della proliferazione di strumenti scollegati e dell'affaticamento da alert che ne consegue, e in questo senso non è l'ennesima sigla ma una tappa logica: dopo aver moltiplicato gli strumenti che trovano i difetti, serviva qualcosa che decidesse quali contano. Ma è bene ricordare che cosa non è. Non è, o non è soltanto, uno scanner in più; non elimina la necessità degli strumenti da cui riceve i dati; e non rende sicura un'applicazione da solo, perché eredita la qualità di ciò che gli arriva, e un inventario di segnalazioni mal prioritizzate resta inutile per quanto sia ben impaginato. Sopra di sé, per giunta, sente la spinta della gestione dell'esposizione e del codice generato dall'AI, al punto che la sua stessa autonomia come categoria è in discussione, e il suo destino più probabile è di sopravvivere come funzione dentro piattaforme più larghe più che come prodotto a sé. Il valore, quando c'è, resta però quello di sempre e non dipende dall'etichetta: trasformare il rumore di dodici strumenti in una lista di cose da fare in ordine di importanza. Trattato come una scatola magica che risolve la sicurezza applicativa, l'ASPM è una delusione annunciata; trattato per ciò che è, cioè un livello di governo che vale quanto la qualità delle

sue priorità, è uno dei modi più concreti per far tornare governabile la sicurezza del software.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/aspm-application-security-posture-management/