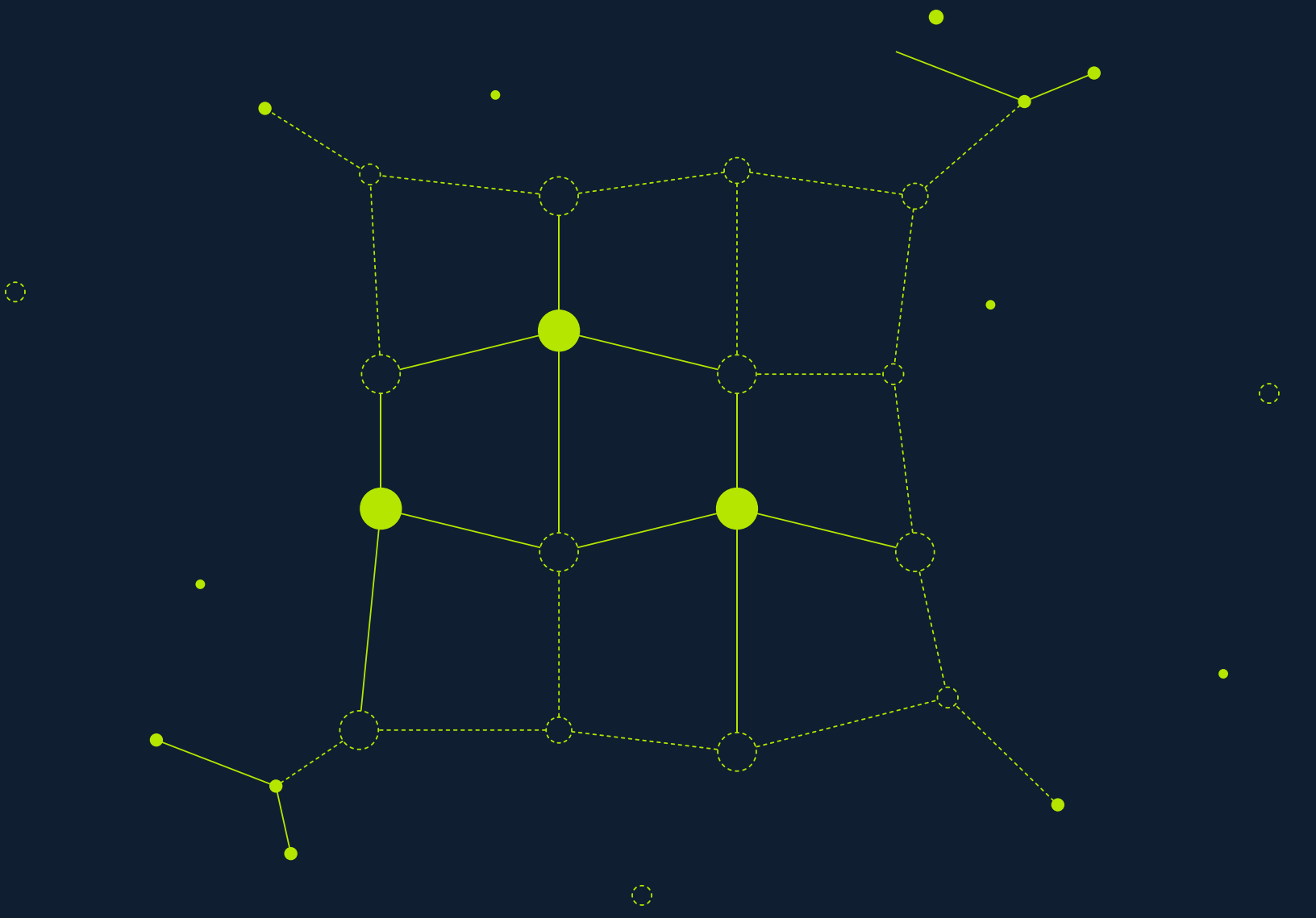
reco

Choosing Your SSPM Vendor

Legacy SSPM Can't Keep Up with Today's Dynamic SaaS Environments



Least privilege access is the golden rule: Users get only the permissions they need to do their jobs. However, if security is too tight, then people can't work. Reco strikes the perfect balance, automatically flagging risky permission combos while keeping workflows smooth.

Say goodbye to spreadsheet nightmares. Reco automates access reviews, identifies weak passwords, shared credentials, and outdated admin access before attackers do. Security teams can easily certify entitlements, revoke unnecessary access, and generate audit-ready reports—without the last-minute compliance panic.

Threat Response: Context Helps Speed Remediation

Discovery, posture management, and access control help secure your SaaS environment, but some threats will still slip through. When that happens, speed matters—the faster the response, the smaller the damage.

The Dynamic SaaS Security Platform detects active threats by spotting signs of intrusion like suspicious access and exfiltration attempts. When a critical event is found, context-based alerts guide security teams to the threat with verified remediation steps.

Reco's Knowledge Graph maps users, apps, and data interactions, helping teams prioritize and fix vulnerabilities effectively. Seamless SIEM and SOAR integration automates response, eliminating manual delays. Reco also supports forensic investigations, mapping security risks to the MITRE ATT&CK framework for deeper analysis. No guesswork, just immediate action.

Reco Overcomes Limitations of Legacy SSPMs

There is no shortage of SSPM offerings in the marketplace today — by a recent count, at least ten. Obviously, their features and capabilities will vary from product to product, but many if not most exhibit the same limitations, from inadequate coverage of SaaS applications and inability to detect shadow SaaS applications to poor threat response and compliance challenges. Each limitation is explained in a separate section below, along with how Reco solves the problem.

Inadequate Coverage of SaaS Applications

For SSPM to be completely effective, you need integrations for all your important SaaS applications. Unfortunately, most SSPM solutions focus on a limited set of popular applications, leaving numerous other SaaS apps unprotected. As a result, your SSPM system may not provide the desired function from day one.

Reco understands the need to offer as many standard integrations as possible. Unlike other vendors, we offer a catalog of more than 160 in-the-box, feature-full integrations – three times what many SSPM vendors offer – and the number keeps growing. When it comes to custom integrations, our SaaS App Factory™ can add new integrations in days, significantly faster than legacy SSPMs (see figure 3).

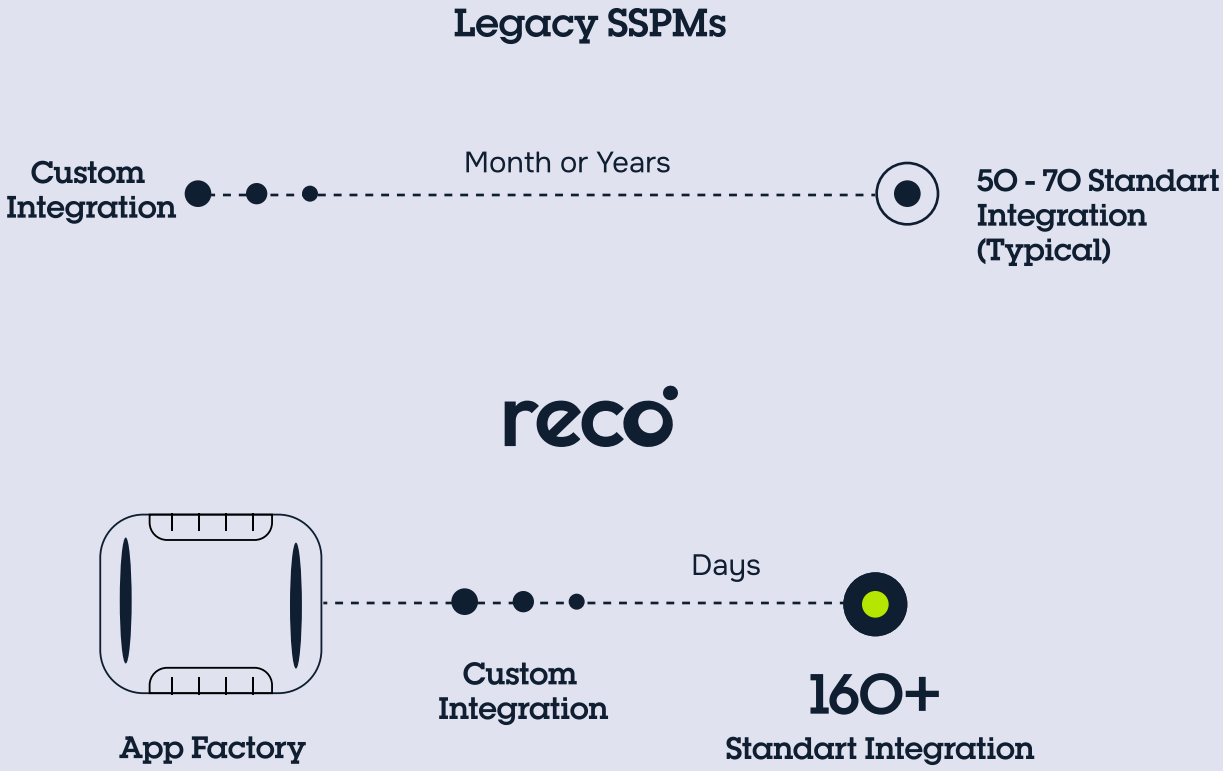


Figure 3. Integration support, legacy SSPMs versus Reco

Inability to Detect Shadow SaaS

Legacy SSPM tools often have no way to discover Shadow SaaS apps, that is, unauthorized SaaS applications adopted without IT approval. If you don't know what's in your SaaS environment, how can you ever protect it?

Reco discovers everything, including Shadow SaaS and connections between legit SaaS and shadow SaaS – something that most SSPMs cannot do (see figure 4). Furthermore, we continuously monitor your SaaS environments, looking for new shadow SaaS and connections. We give you the clearest possible view of your complete SaaS landscape – and we keep it current.

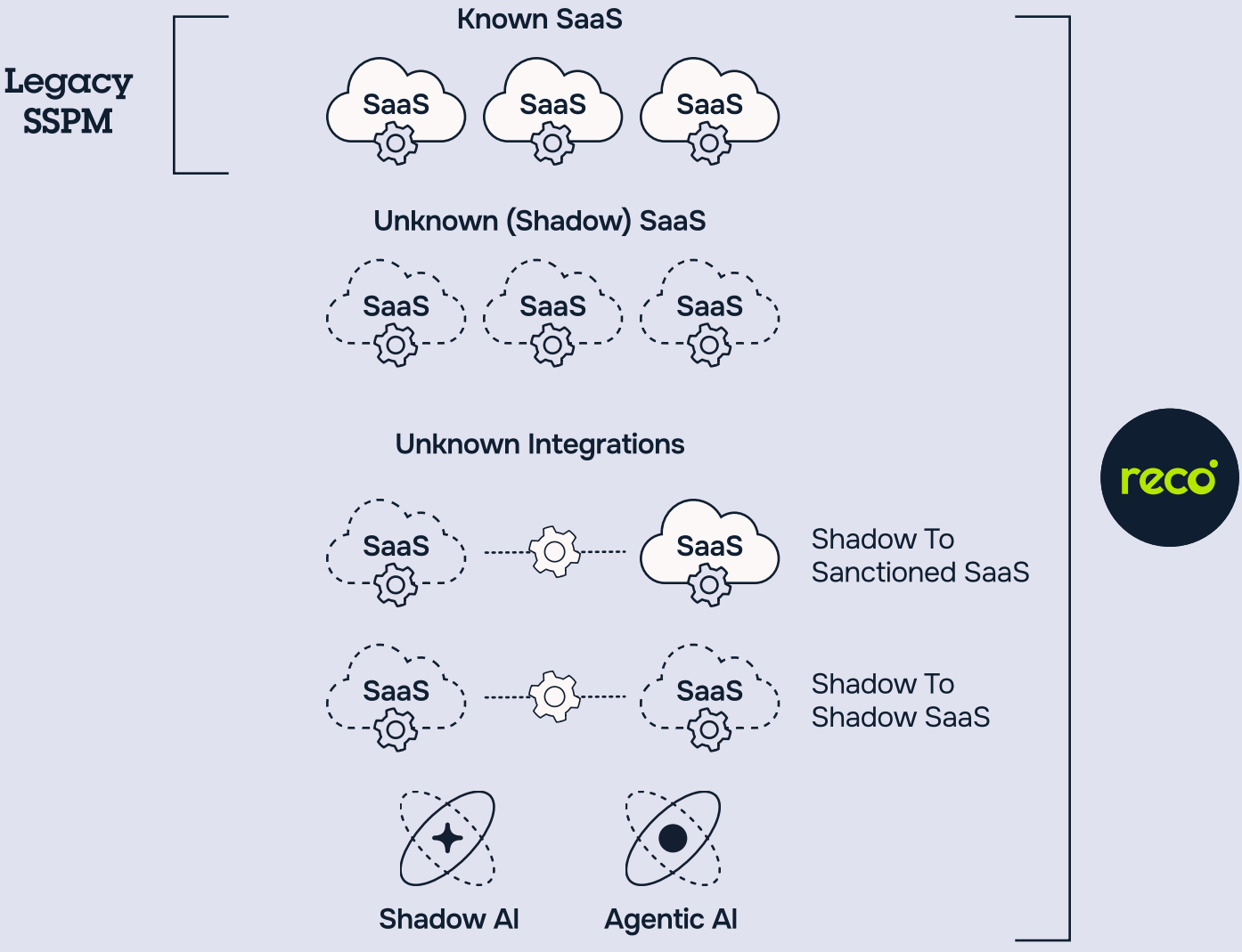


Figure 4. Reco discovers all SaaS applications —sanctioned and shadow— and all Saas-to-SaaS integrations, sanctioned and shadow.

Figure 5. How Reco reduces misconfiguration vulnerability

Incomplete Context

SSPM vendors have been slow to understand the importance of context in SaaS security. Most SSPM offerings allow administrators to discover problems that arise according to specific configurations but may not be able to help them fully understand the context in which the problem occurs.

Reco understands that context is everything in SaaS security – think of our approach as SSPM+. Reco uses advanced analytics around persona, actions, interactions and relationships to other users, and then alerts on exposure from misconfigurations, over-permission users, compromised accounts, and risky user behavior. Captured in our Knowledge Graph module, this comprehensive picture is generated continuously and empowers security teams to take swift action to effectively prioritize their most critical points of risk. By providing a complete and ongoing view of these threats, Reco empowers security teams to quickly identify and focus on the most critical risks, allowing them to take action before problems escalate.

Using SSPM With Other Security Technologies

Today's enterprise environments are usually hybrid cloud deployments that involve multiple clouds, public and private, and subscriptions to hundreds of SaaS applications. In that context, SSPM is one of a handful of powerful tools that together can provide security coverage for the entire hybrid environment (see figure 7)

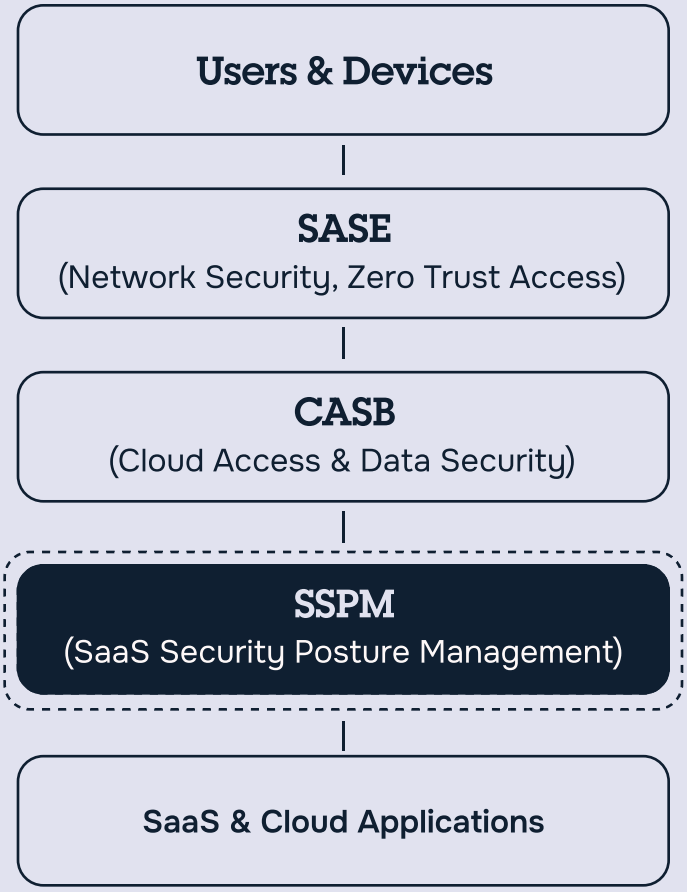


Figure 7. SSPM in the Hybrid Stack

SSPM plays well with other security tools like DSPM, SASE, CASB, and CSPM to create a stronger defense for cloud deployments (see figure 8). When these technologies are used together, they help protect cloud applications from security risks like misconfigurations, unauthorized access, and data leaks. Each tool has its own role, but combining them makes cloud security more effective and reliable.

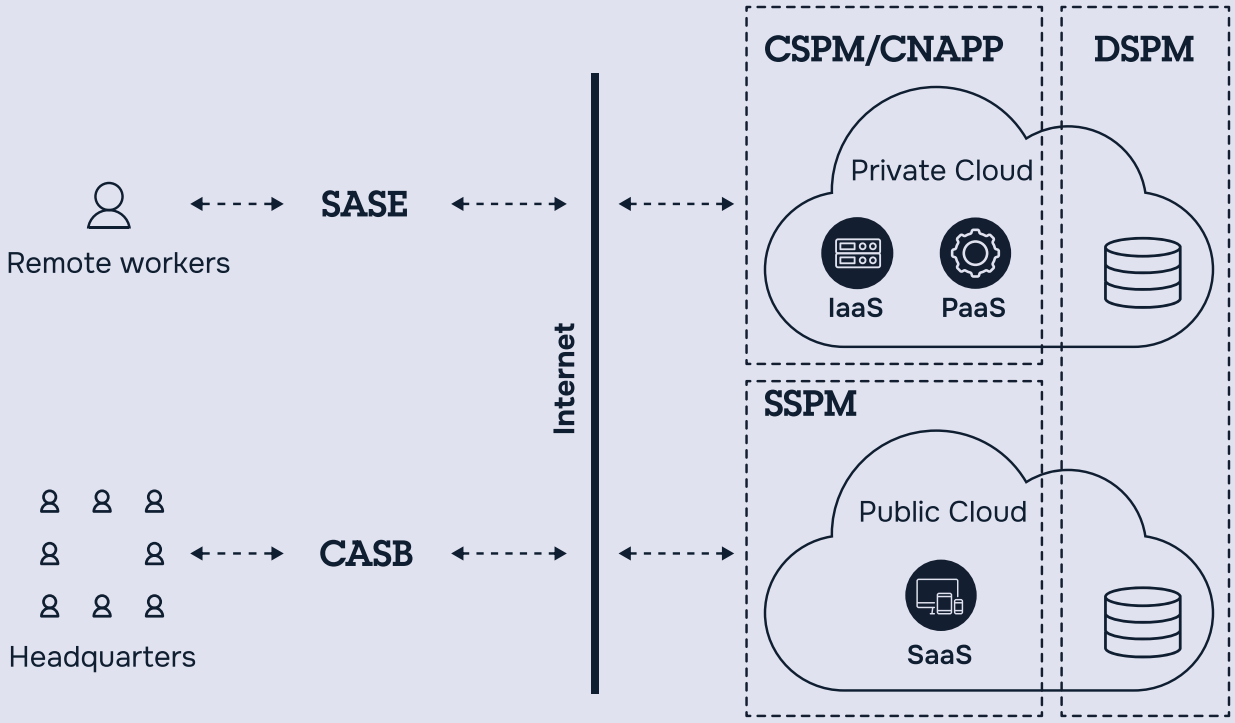


Figure 8. Security Areas for Complementary Technologies

Cloud Access Security Broker (CASB)

CASB is a security solution that monitors and protects data, applications, and user activity across cloud services, including SaaS, PaaS, and IaaS. CASBs were first introduced in the 2010s, about a decade before the rollout of the first SSPMs.

In the early days, some organizations used CASBs to provide basic SaaS security. However, as the number of SaaS applications grew, many found that traditional CASB solutions do not fully address all security concerns, especially regarding the internal configurations of SaaS applications.

Organizations with existing CASB installations can benefit from adding SSPM because it focuses on the role of configuration in SaaS security — something for which CASB was not designed. CASB monitors traffic and alerts after threats appear, but SSPM takes a proactive approach, preventing breaches by fixing misconfigurations before they cause vulnerabilities.

SSPM integrates with DevSecOps workflows, automating security fixes and enforcing policies, while CASB focuses more on access control and data sharing. Unlike CASB's proxy-based deployment, which can slow down performance, SSPM's API-based approach ensures smooth security management without affecting network speed.