When Should You Choose SSPM Over CSPM in Your Cloud Security Strategy?

Key Takeaways

- Cloud security posture management (CSPM) focuses on infrastructure-level misconfigurations in IaaS and PaaS environments.
- SaaS security posture management (SSPM) focuses on tenant configuration, user permissions, and governance within SaaS platforms.
- The difference between CSPM and SSPM lies in infrastructure risk versus application-layer risk.
- Most mature cloud security strategies require both CSPM and SSPM to eliminate posture blind spots.

Over the past decade, cloud adoption has transformed from simple infrastructure migration to something much more layered and complex. Organizations are no longer just running virtual machines in AWS or Azure. They are operating Kubernetes clusters, deploying serverless functions, automating infrastructure through code, and at the same time relying heavily on SaaS platforms such as Microsoft 365, Salesforce, ServiceNow, Slack, and dozens of other cloud-based services.

As this ecosystem expands, security leaders often face a critical architectural question: do we need cloud security posture management, SaaS security posture management, or both? On the surface, the terminology can be confusing. Both CSPM and SSPM promise posture visibility. Both claim to reduce cloud misconfigurations. Both integrate through APIs. But beneath the marketing language, they protect entirely different layers of risk.

Understanding the difference between CSPM and SSPM is not about semantics. It is about ensuring that your cloud security strategy does not leave gaps simply because you assumed one tool covered everything. Let’s unpack this carefully and technically, but in a way that reflects how these systems operate in real-world environments.

What is SSPM and how does it differ from CSPM?

At a conceptual level, both cloud security posture management and SaaS security posture management evaluate configuration risk. However, the layer at which they operate makes all the difference.

Cloud security posture management (CSPM) in practical cloud environments

Cloud security posture management works at the infrastructure level within public cloud platforms like AWS, Microsoft Azure and Google Cloud Platform. It looks at things like machines, storage buckets, Kubernetes clusters, IAM roles, network security groups, databases and serverless services. This means Cloud security posture management protects the environment that your engineering teams create and manage.

In a company the infrastructure is always changing. Development teams put out workloads change IAM permissions, update network rules and make applications bigger or smaller as

needed. These changes are necessary for the company to move quickly. They can also cause problems with the configuration. For example a storage bucket might become open to the public by mistake. A security group might allow anyone to send information in. An IAM role might get many administrative permissions just to get things done faster.

Cloud security posture management is always checking the cloud control-plane APIs to see if the configurations are okay based on standards like CIS, NIST, ISO 27001 or SOC 2 requirements. It finds problems before they are used against you. Cloud security posture management does not look at the information being sent or the processes that are running. Instead it checks the state of the cloud configurations. Points out any differences from what is considered safe.

If your organization builds applications or manages workloads, in public cloud environments Cloud security posture management is a part of making sure everything is done correctly. It makes sure that the infrastructure does not become insecure without anyone noticing as your CSPM use grows.

SaaS security posture management (SSPM) in SaaS-driven enterprises

SaaS security posture management works with the applications people use not with the underlying systems. When you use SaaS platforms like Microsoft 365 Salesforce, Google Workspace and ServiceNow you do not have control over the infrastructure. What you can control is how your account is set up what roles your users have how files are shared and what other apps are connected to your SaaS platform.

Over time the way you have set up your SaaS account can become a problem. For example, when employees get a job they might still have permissions they do not need. Contractors might finish a project. Still be able to access your system. Users might share files with people outside the company without realizing the risks. When other apps connect to your SaaS platform, they might ask for more access than they need. These problems do not show up when you look at your cloud infrastructure. They can cause real security breaches.

SaaS security posture management connects directly to the SaaS applications. Check how they are set up and managed. It looks at things like who has privileges, how permissions are changing over time, how files are being shared and what other apps are connected. This is different from security posture management, which looks at the underlying infrastructure. SaaS security posture management looks at how the SaaS applications set up and used.

If your employees use SaaS platforms a lot. And most companies do. SaaS security posture management is very important. It helps you control who can see your data and what they can do with it which is critical, for keeping your company safe.

Outsmarting Cloud threats in Cloud-First Organizations

- Outsmarting Cloud threats
- Early Detection
- Response Acceleration
- Industry Benchmarks

[Download the Whitepaper for the Full Insights]

Architectural comparison: difference between CSPM and SSPM

The most practical way to understand the difference between CSPM and SSPM is to view them side by side:

Dimension CSPM SSPM Security Layer Infrastructure (IaaS / PaaS) SaaS Application Layer Example Platforms AWS, Azure, GCP, Kubernetes Microsoft 365, Salesforce, Slack Primary Risk Focus Misconfigurations & exposure Permission drift & data governance Identity Scope Cloud IAM roles & service accounts SaaS admin roles & OAuth scopes DevOps Integration High (CI/CD, IaC validation) Moderate (tenant governance) Compliance Alignment Infrastructure benchmarks SaaS configuration baselines

This comparison highlights that cloud security posture management and SaaS security posture management address distinct but complementary domains.

When do you need CSPM?

If your organization operates workloads in public cloud environments, CSPM is not optional. It becomes essential as soon as infrastructure complexity increases.

1. Infrastructure misconfiguration at scale

In large cloud environments, configuration changes happen continuously. DevOps pipelines deploy resources automatically. Engineers update IAM roles. Network policies evolve. Each change introduces the possibility of exposure. Without continuous posture monitoring, security teams would need to manually audit thousands of resources, which is unrealistic.

Cloud security posture management continuously scans for misconfigurations such as publicly exposed storage, open network ports, unencrypted databases, and overly permissive IAM roles. For example, a Kubernetes cluster might inadvertently allow anonymous access to its API server. CSPM detects that configuration before an attacker exploits it.

The value of CSPM lies in proactive governance. It prevents infrastructure misconfiguration from

becoming a breach vector.

2. Cloud IAM and entitlement sprawl

In fast-growing cloud environments, identity quickly becomes the most underestimated risk layer. What begins as a small set of IAM roles often expands into hundreds or even thousands of role definitions across accounts and subscriptions. Developers grant temporary administrative access to troubleshoot issues. Automation scripts require broad permissions to function correctly. Service accounts accumulate privileges over time simply because no one revisits their scope after initial deployment.

The problem is not malicious intent. It is operational convenience. But over time, these conveniences turn into entitlement sprawl.

Cloud security posture management becomes critical at this stage because manually reviewing IAM policies is not realistic at enterprise scale. CSPM continuously evaluates role definitions, wildcard permissions, cross-account trust relationships, and unused access keys. It flags excessive permissions that violate least privilege principles.

For example, if a Lambda function role is granted full S3 administrative access when it only requires read permissions to a specific bucket, CSPM identifies the risk. If an IAM role is trusted by multiple external accounts unnecessarily, CSPM surfaces the trust exposure.

This identity-layer visibility is especially important because attackers frequently target privilege escalation rather than infrastructure misconfiguration alone. Without CSPM continuously analyzing entitlement posture, IAM drift becomes invisible until exploited.

3. Infrastructure-as-Code and shift-left validation

Modern cloud environments are rarely built manually. They are deployed through Infrastructure-as-Code tools such as Terraform, ARM templates, or CloudFormation. This automation accelerates development, but it also introduces systematic risk. If insecure configuration patterns are embedded in code templates, those vulnerabilities replicate at scale.

For example, a Terraform template may define security groups with open ingress rules for simplicity during development. If that template is reused across multiple environments without modification, the exposure becomes widespread.

Advanced cloud security posture management integrates directly into CI/CD pipelines, scanning Infrastructure-as-Code templates before deployment. This allows security validation to occur during development rather than after exposure.

This “shift-left” approach fundamentally changes risk management. Instead of detecting misconfiguration after production deployment, CSPM identifies posture weaknesses at the design stage. In organizations practicing DevOps or DevSecOps, this integration becomes essential. It reduces remediation cost, shortens feedback loops, and ensures that insecure infrastructure does not propagate into live environments.

When do you need SSPM?

1, SaaS identity and privilege drift

SaaS identity and privilege drift is a problem. SaaS environments are changing fast and most

security teams do not even realize it. When employees join a company they get roles and sometimes they get special privileges for a little while. They work with people from departments and sometimes they leave the company without losing all their access.

Over time all these permissions add up. This is different from cloud IAM, which is usually managed in one place and checked during audits. SaaS permissions are managed inside each application. Each SaaS platform has its own way of doing things. This makes it hard to keep track of everything.

SaaS security posture management is a way to constantly check who has what role in SaaS systems. It finds people with many privileges, old accounts that are not used users who are not active but still enabled and roles that conflict with each other. For example a person who used to be a project manager might still be able to export things from a CRM system even after they moved to a department. Without SaaS security posture management we might never notice this problem.

SaaS security posture management makes sure that people only have the privileges they need not for the infrastructure but also for the applications. It helps us see what is going on at the tenant level, which’s really important as more and more companies use SaaS. SaaS security posture management is essential, for SaaS identity and privilege drift.

2. OAuth integrations and third-party application risk

Many companies use lots of tools that work together through OAuth. This helps employees get work done faster by automating tasks syncing data or being more productive.

These tools often ask for a lot of access like being able to read and write emails or see all customer data.

The problem is that it’s hard to keep track of all these connections. Once employees agree to connect a tool the connection can stay active forever. Most security teams don’t have a system to monitor all these connections.

Managing SaaS security helps keep an eye on what OAuth permissions being used. It finds tools that have much access and points out tools that are no longer being used.

For example a marketing tool might be connected to Salesforce with access but not be used anymore. This is where managing SaaS security comes in to highlight the risk.

Many cyber attacks happen because hackers use OAuth tokens to get in. They do this because these tokens aren’t monitored like logins.

Managing SaaS security helps keep track of these connections and the risks they bring which isn’t covered by cloud security tools.

3, Data sharing configuration and collaboration risk

Collaboration is one of the greatest strengths of SaaS platforms, but it is also one of the most significant exposure points. Public sharing links, guest access permissions, and external domain collaboration can unintentionally expose sensitive data.

For example, an employee might generate an anonymous sharing link to distribute financial projections internally but accidentally configure it for unrestricted public access. That configuration may persist long after the document’s relevance expires.

SaaS security posture management continuously evaluates sharing settings against organizational baselines. It detects external exposure, mass sharing events, and policy deviations. Unlike endpoint monitoring tools, SSPM does not wait for data exfiltration to occur. It identifies risky sharing configurations proactively.

4. API token governance and automation security

Automation within SaaS environments relies heavily on API tokens. These tokens enable scripts and applications to access data programmatically. However, API tokens often lack lifecycle management. They may not expire automatically. They may be scoped too broadly. They may remain active long after the automation task ends.

SSPM provides visibility into token issuance, scope, and usage patterns. It identifies stale tokens, overly permissive access scopes, and anomalous API usage. In environments where automation drives productivity, API token governance becomes as important as user credential management.

Should organizations deploy CSPM and SSPM together?

This is where the conversation shifts from tool comparison to architectural strategy. In most mature environments, the answer is not either-or. It is layered defense.

Organizations today rarely operate exclusively in one domain. They build infrastructure in AWS or Azure while simultaneously storing sensitive intellectual property in SaaS collaboration platforms. Identity bridges these environments. A compromised SaaS account may grant access to cloud storage integrations. A compromised cloud IAM role may provide API-level access to SaaS automation scripts.

If an organization deploys only cloud security posture management, it secures infrastructure configurations but leaves SaaS governance risk largely unmonitored. Conversely, if it deploys only SaaS security posture management, it may enforce strict tenant controls while infrastructure misconfigurations remain exposed.

Attackers do not respect architectural boundaries. They pivot across identity, infrastructure, and application layers fluidly. That is why posture management must be layered and complementary. CSPM addresses infrastructure misconfiguration. SSPM addresses SaaS governance drift. Together, they provide comprehensive configuration visibility across cloud ecosystems.

Now the comparison becomes clearer when visualized:

Exposure Scenario CSPM Coverage SSPM Coverage Public cloud storage exposure Yes No Kubernetes RBAC misconfiguration Yes No SaaS admin over-permission No Yes Public document sharing in M365 No Yes IAM wildcard policy Yes No OAuth integration abuse No Yes

This layered deployment ensures that posture blind spots are minimized across both infrastructure and SaaS environments.

How does Fidelis support unified cloud posture and detection strategies?

Fidelis Security approaches cloud security with integrated visibility across infrastructure, SaaS, endpoints, and network environments.

- Unified monitoring across cloud workloads and SaaS tenants
- Correlation between posture drift and active threat behavior
- Hybrid and multi-cloud visibility support
- Context-driven detection beyond configuration assessment

This integrated model helps organizations move beyond siloed CSPM and SSPM approaches toward comprehensive visibility.

Agentless Cloud Security Posture Management at any Scale: Fidelis’ CSPM

- Fast and Automated
- Nothing to Install
- DevSecOps-Ready
- Continuous Compliance

Download Datasheet to Explore More!

Final Thoughts

Cloud security posture management secures the infrastructure you build. SaaS security posture management secures the applications your workforce depends on.

The difference between CSPM and SSPM is architectural. Most modern enterprises require both. The real decision is not which tool to choose — it is whether your cloud security strategy accounts for every layer of risk.

If your organization operates across cloud infrastructure and SaaS platforms, posture visibility alone may not be enough. Integrated detection and contextual correlation matter just as much.

Fidelis Security provides unified visibility across cloud, SaaS, endpoint, and network layers to reduce posture blind spots and improve security clarity.

If you are evaluating CSPM, SSPM, or both, consider exploring how a unified approach can strengthen your overall cloud security strategy.