Moving applications to the cloud has allowed organizations to rapidly respond to changing customer needs, be more agile to changing business requirements, and save money.

Along with the significant benefits, the shift to the cloud has also amplified the threat landscape. Once an application goes live in the cloud, it is globally available to adversaries that will look for vulnerabilities in the software and misconfigurations in how it was set up and deployed.

Traditional perimeter security based on traditional networking concepts, even when they are virtualized, does not solve the challenges unique to the cloud and hybrid deployments, adds unnecessary cost, and is too complex to deploy, negating the very agility and scalability benefits of the cloud for in the first place.

Zscaler Cloud Security Posture Management (CSPM) automatically identifies and remediates application misconfigurations in SaaS, IaaS, and PaaS to reduce risk and ensure compliance. Zscaler CSPM is part of the comprehensive, 100-percent cloud-delivered data and workload protection capabilities in the Zscaler Zero Trust Exchange platform.
Zscaler CSPM Key Capabilities

**Cloud misconfiguration visibility and remediation**
- Compare SaaS and public cloud application configurations to industry and organizational benchmarks, reporting violations, and automating remediation.

**Compliance reporting and remediation**
- Compare SaaS and public cloud application deployments against 14 different laws, regulations, and security standards to provide visibility into compliance violations while automating remediation.

**Prevents application vulnerabilities**
- Identify OS and application vulnerabilities and configuration issues to ensure applications are hardened against attacks and data breaches.

**Secures container environments**
- Identify Kubernetes container environment misconfigurations, processes running as root, privileged containers, and compliance violations.

**Part of a larger data protection platform**
- The Zscaler Zero Trust Exchange platform provides unified data protection with DLP and CASB capabilities for internet, data center, and SaaS applications, and ensures that public cloud applications are configured to prevent data exposure and maintain compliance.

“Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes.”

— Gartner