Application security is critical to protecting sensitive data and maintaining user trust, but it also faces numerous risks and challenges that organizations must address.These organizations may not have the human resources or infrastructure to establish security teams, strategies, and tools, or provide training on secure coding practices across all development areas.Regardless of the security standards in place, organizations remain vulnerable to internal threats, whether from their employees, contractors, or other legitimate parties who gain access to applications that have inherent security risks or unintentionally pose similar risks.Here are some of the key challenges: Cybercriminals are cunning and constantly devise smarter methods to exploit vulnerabilities.Organizations need to keep pace with threats and attacks while continually monitoring and adapting security practices.Organizations often operate under resource constraints, which hinders the proper implementation of security practices in application development.Too much security can inhibit users' progress, so organizations must understand that this balance is key to achieving a high level of security without losing user engagement.Organizations should examine and monitor any vulnerabilities associated with third-party components.It is important to ensure that security practices are effective before implementing them.The use of third-party libraries and services carries inherent risks in the supply chain.If any third-party component is compromised, the less secure application could be compromised, putting these organizations at risk.This, if not addressed, can lead to security vulnerabilities.A balance must be struck between security and usability.