Cloud Security Alliance unveils framework to improve SaaS security – Info

Data: 2025-09-28 13:39:02

Autor: Inteligência Against Invaders

Independent security experts have welcomed what's billed as the first standardized set of SaaS (software as a service) security controls. The SaaS Security Capability Framework (SSCF), launched this week and backed by the Cloud Security Alliance, is designed to close long-standing gaps in third-party risk management.

The framework is designed to addresses the need for an industry standard that defines the minimum technical security capabilities SaaS applications should provide, particularly those that fall within the customer's scope under what's commonly known as the Shared Security Responsibility Model.

Organizations have built sophisticated zero trust architectures around their on-premises and IaaS (Infrastructure as a service) environments. However, by contrast, the security controls of SaaS applications have long been opaque.

This disconnect creates a massive, unnecessary risk that the SSCF aims to bridge. Publication of the guidance follows recent attacks targeting Salesforce SaaS applications that have focused industry concerns around the more general issue of the security of cloud-based applications.

Lefteris Skoutaris, associate vice president for GRC Solutions at Cloud Security Alliance, said: "The SSCF addresses a critical gap in SaaS security by establishing the first industry standard for customer-facing security controls. This framework exemplifies CSA's mission to unite diverse industry partners (from SaaS providers to enterprise customers) in creating practical solutions that translate compliance requirements into actionable security capabilities that organizations can actually configure and enforce."

SSCF specifies controls across six security domains:

Change control and configuration management
Data security and privacy lifecycle management
Identity and access management
Interoperability and portability
Logging and monitoring
Security incident management, e-discovery, and cloud forensics

These domains are designed to map high-level business requirements into tangible SaaS security features that customers can actually configure and rely on, such as log delivery, SSO enforcement, secure configuration guidelines, and incident notification.

The approach is designed to complement rather than replace business-focused security frameworks

such as ISO 27001.

“The SaaS Security Capability Framework represents a significant step forward for the industry,” said Brian Soby, co-founder & CTO of SaaS security posture vendor AppOmni, and SSCF lead author. “It provides a clear, consistent, and much-needed standard that will help organizations move past outdated risk assessments and truly build zero trust principles into their SaaS environments.”

Toward more consistent SaaS security controls:

The industry has long struggled with a lack of consistent SaaS ***security*** controls. Without an industry standard, enterprises, SaaS vendors, and security teams have ended up duplicating efforts or carrying unnecessary risks.

The SSCF tackles this long-standing challenge by offering a practical framework of security capabilities that can be adopted by SaaS vendors, providing more consistency across the industry while reducing potential security risks.

“CSA’s SSCF is a meaningful step forward for SaaS governance, setting clearer expectations for both vendors and buyers,” said David Brown, SVP of international business at firewall policy management firm FireMon. “But a framework only reduces risk when translated into operational controls, specifically continuous network-policy visibility, tight egress controls, and automated compliance checks.”

Brown continued: “Organizations that pair SSCF requirements with real-time network posture verification can prove controls work and materially reduce SaaS-related risk.”

Continuous validation:

A growing share of internet traffic is generated by non-human actors; bots, agents, automated systems that interact with SaaS apps in ways traditional monitoring often misses.

“The SSCF provides a much-needed benchmark for what ‘secure by default’ should look like in SaaS environments,” said Mayur Upadhyaya, CEO at APIContext. “Its focus on technical controls within the customer’s scope is timely, especially as the boundaries between internal users, third-party integrations, and machine-driven traffic continue to blur.”

Upadhyaya added: “A framework like SSCF can only be effective if it reflects this expanded surface area and encourages continuous validation, not just static configurations.”

Next steps:

If widely adopted, SSCF will offer enterprises more consistent security features across their SaaS portfolio. Vendors will gain the knowledge of what security controls will be expected by customers.

The next phase of the project will focus turning the framework into something more practical by developing implementation and auditing guidelines and an assessment and certification scheme. Rather than offering checklists that vendors are encouraged to follow, SSCF aims to offer measurable security improvements.

@John Leyden by CSO online