Why True FedRAMP® Authorization Matters: Why Copado

In the federal market, security is not just a checkbox, it's the foundation for trust, system integrity, and mission-critical success. As government agencies continue their journey to cloud adoption, selecting solutions that are truly FedRAMP Authorized is essential to maintaining compliance, mitigating risk, and accelerating project approvals.

This datasheet explains why Copado is the most secure DevSecOps solution for Salesforce in the federal space and why competitors' claims of being FedRAMP "compliant" or "ISV FedRAMP certified" are misleading and present real vulnerabilities and risk.

FedRAMP is not limited to infrastructure. It covers the entire organizational boundary, including **software development processes, support teams, HR policies, and operational practices.**

Understanding FedRAMP Authorization

FedRAMP (Federal Risk and Authorization Management Program) is a U.S. government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services. Achieving FedRAMP Authorization requires:

- **Implementation of 325 NIST 800-53 controls, covering physical, operational, and technical safeguards**
- **Verification through an accredited Third-Party Assessment Organization (3PAO)**
- **Ongoing continuous monitoring and updates**
- **Personnel vetting, incident response plans, encryption protocols, and more**

The Risk of Misleading Compliance or Certification Claims

Competitors claim to be “FedRAMP compliant” or “ISV Certified” by relying on Salesforce’s FedRAMP Authorization to Operate (ATO), but this is misleading, violates FedRAMP branding guidelines, and exposes agencies to significant security and compliance risks. Other than Copado, no other Salesforce-based DevOps solution has been FedRAMP Authorized and has undergone the required 3PAO audit to validate its application, personnel, or development lifecycle. Misleading Compliance Claims introduces several risks:

Lack of Accountability for Secure Development

Without verified SDLC controls, there is no assurance that secure coding practices are being followed or that insider threats are being mitigated. This opens the door for poorly written or even malicious code to enter production environments.

Unverified Personnel Access

With no visibility into who is developing or supporting the solution, agencies risk exposure to unvetted or foreign nationals. This lack of transparency is especially dangerous for systems tied to critical infrastructure or national security, where insider threats could lead to sabotage, espionage, or unauthorized access to Personally Identifiable Information (PII).

Absence of Continuous Monitoring

Without mandated continuous monitoring, security vulnerabilities may go unnoticed for extended periods. Malicious activity or data breaches could remain undetected until they have already caused significant damage, resulting in loss of operational continuity, costly incident response efforts, and erosion of public trust.

Top 10 Security Controls Frequently Missing in Non-FedRAMP Authorized Software

Below are the top 10 gaps commonly found in unauthorized tools, exposing agencies to risk, inefficiencies, and compliance failures.

1. **System and Information Integrity (SI) - Continuous Vulnerability Scanning and Timely Remediation**
Unauthorized tools often lack continuous vulnerability scanning and fail to remediate issues within required timelines, leaving systems exposed.

2. **Identification and Authentication (IA) - Multi-Factor Authentication (MFA) for All User Types**
MFA is optional or inconsistently applied, especially for admin users, unlike FedRAMP, which mandates MFA for all access levels.

3. **Incident Response (IR) - Formalized Incident Response Plan and Timely Reporting**
Ad-hoc or informal processes replace the formal IR plans, testing, and government reporting required under FedRAMP.

4. **Configuration Management (CM) - Strict Baseline Configuration and Change Control**
Non-FedRAMP systems typically lack secure baseline configurations and structured change control, increasing the risk of misconfigurations.

5 **Access Control (AC) - Principle of Least Privilege and Well-Defined Authorization Boundaries**
Without enforced access boundaries, users may have more permissions than needed, violating least privilege principles.

6 **System and Communications Protection (SC) - FIPS-Validated Cryptography for Data in Transit and at Rest**
Many tools use basic encryption but lack the FedRAMP-required FIPS 140-2 validated modules for data protection at rest and in transit.

7 **Audit and Accountability (AU) - Comprehensive and Tamper-Proof Audit Logging**
Audit trails are often incomplete or tamperable, limiting accountability and forensic readiness.

8 **Personnel Security (PS) - Rigorous Personnel Screening and Separation of Duties**
FedRAMP requires background checks and separation of duties, often not formally implemented in non-authorized environments.

9 **Contingency Planning (CP) - Comprehensive System Backup and Disaster Recovery Plan**
While backups may exist, they're rarely tested or maintained with the rigor and documentation FedRAMP demands.

10 **Security Assessment and Authorization (CA) - Continuous Monitoring and Annual Assessments**
Unlike FedRAMP-authorized systems, non-compliant tools skip ongoing assessments and 3PAO audits, reducing visibility into security posture over time.

Copado: The Only Salesforce DevSecOps Platform with FedRAMP Authorization

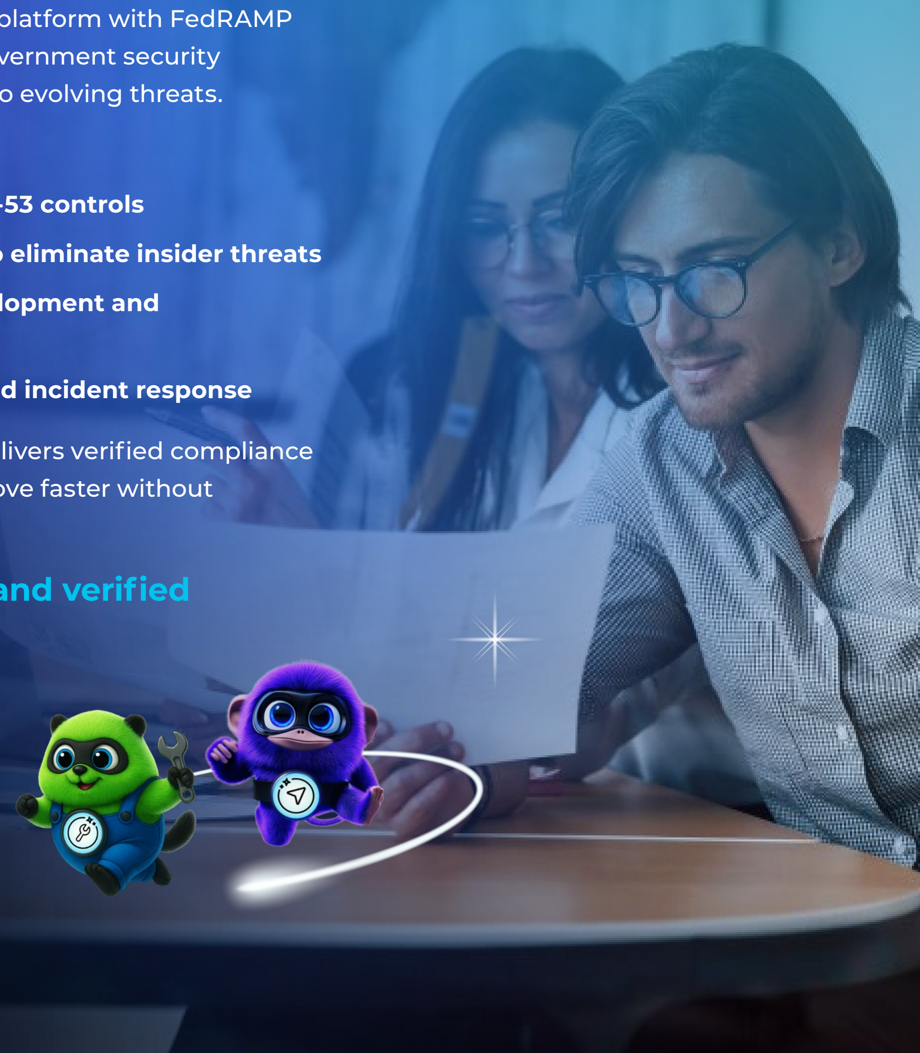
Copado is the only Salesforce-native DevSecOps platform with FedRAMP Moderate Authorization, meeting the strictest government security standards and continuously monitored to adapt to evolving threats.

With Copado, federal teams get:

- ✓ **Verified implementation of all 325 NIST 800-53 controls**
- ✓ **U.S.-based support and personnel vetting to eliminate insider threats**
- ✓ **End-to-end SDLC visibility with secure development and automated testing**
- ✓ **Operational oversight for audit readiness and incident response**

While others make misleading claims, Copado delivers verified compliance and trusted security, empowering agencies to move faster without compromising on trust.

Choose the only secure, compliant, and verified path forward. Choose Copado.



Learn More

COPADO