Aquia

The SaaS Visibility Gap: Why Federal Enterprise Architecture Is Increasingly Incomplete

White paper

JANUARY 2026

Author: Daniel Wallace, principal security architect, Aquia

www.aquia.us | federal@aquia.us

Table of Contents

Executive Summary

Federal agencies invest millions annually maintaining enterprise architecture (EA) frameworks, technical reference models, and governance processes designed to align IT investments with mission objectives. Yet despite this rigorous documentation, a parallel technology landscape is proliferating largely invisible to traditional architecture: decentralized software-as-a-service (SaaS) adoption.

The problem is clear:

When Aquia investigated the SaaS landscape for a large federal customer, we discovered more than **1,500 distinct applications** operating on its networks. Nearly **600 were business-critical** applications that had never been formally assessed, less than 15% were integrated with identity management, and approximately **276 lacked any FedRAMP** or provisional authorization.

Why this matters now: Federal agencies are executing multi-billion-dollar modernization initiatives under Office of Management and Budget (OMB) M-23-22, implementing zero trust architecture under M-22-09, and meeting federal data strategy requirements. These strategic initiatives assume you know what you have. Zero trust requires comprehensive asset inventories — you cannot verify what you cannot see. When EA documentation excludes hundreds of operational applications, these initiatives fail before they begin.

Why traditional controls fail: Even agencies deploying cloud access security brokers (CASB) or secure access service edge (SASE) frameworks face a fundamental reality — network-based controls cannot govern SaaS adoption through personal devices, API access, shadow integrations, or mobile applications using certificate pinning.

The solution: Aquia's three-step SaaS governance framework bridges the gap between documented architecture and operational reality:

1. **Discover** through Aquia's proprietary, automated RADAR platform — developed specifically for the needs of the public sector — providing continuous visibility into actual application landscapes
2. **Manage** through a rapid cloud review (RCR) methodology — codified into federal policy in June 2024 as the government's first centralized SaaS risk review process
3. **Secure** through continuous SaaS security posture management (SSPM), validating ongoing compliance

Proven results: For one of our customers, this approach discovered 1,500+ applications, achieved a 95.33% remediation rate for critical findings, and demonstrated a 91.92% reduction in compliance violations.

SaaS governance doesn't replace EA — it provides the operational visibility needed to make enterprise architecture accurate in a cloud-native world.

The Challenge

Every year, federal agencies invest millions in maintaining their enterprise architecture (EA) — comprehensive technical reference models (TRMs), detailed application portfolios, governance frameworks, and technology standards that guide IT decision-making across the enterprise. EA teams process thousands of technical assessments annually, evaluate emerging technologies against established standards, and maintain sophisticated governance structures to ensure IT investments align with mission objectives.

But there's a growing challenge: while EA teams meticulously document and govern technology decisions through formal channels, a parallel technology landscape is proliferating through decentralized software-as-a-service (SaaS) adoption — largely invisible to traditional architecture processes.

Your enterprise architecture isn't inaccurate. It's just increasingly incomplete.

Did you know?

The average cost of a data breach in the U.S. in 2025 was **$10.22 million,** according to IBM's "Cost of a Data Breach Report."

Federal agencies aren't just managing technology — they're executing multi-million dollar modernization initiatives under the Office of Management and Budget (OMB) M-23-22, implementing zero trust architecture under M-22-09 and the Cybersecurity and Infrastructure Security Agency's (CISA's) Zero Trust Maturity Model, and meeting federal data strategy requirements for data-driven decision making. Technology Modernization Fund investments, Cloud Smart strategy implementation, and agency-wide digital transformation all share a fundamental dependency: accurate visibility into the enterprise technology landscape.

These initiatives assume you know what you have. Zero trust requires comprehensive asset inventories — you cannot verify what you cannot see. The federal data strategy demands centralized data governance — impossible when mission-critical data resides in undocumented repositories. Cloud Smart requires informed migration planning — infeasible when your application is 40-60% invisible.

When enterprise architecture documentation excludes hundreds of operational applications, these strategic initiatives fail before they begin. You cannot modernize or govern what you cannot see.

The Disconnect Between Architecture and Reality

Modern enterprise architecture represents the pinnacle of IT governance practice — sophisticated systems for evaluating technologies, maintaining standards, publishing approved solutions, and ensuring compliance. Technical assessments flow through structured review processes. Standards are documented. Decisions are tracked. Architecture diagrams are maintained.

Meanwhile, across the enterprise, teams are adopting dozens — sometimes hundreds — of SaaS applications entirely outside this governance framework. Survey tools, collaboration platforms, development utilities, analytics dashboards … Each one is a gap in your architecture and a blind spot in your technology inventory.

This isn't a hypothetical problem. We worked with a large federal agency to investigate their SaaS landscape and discovered over 1,500 distinct SaaS applications operating on their networks. Nearly 600 of those applications were business-critical applications that had never been formally assessed or approved, less than 15% were integrated with identity management, and approximately 276 lacked any FedRAMP or provisional authorization.

Think about what this means for enterprise architecture: the agency was maintaining detailed architecture documentation, technology standards, and governance processes while hundreds of applications operated completely outside their architectural visibility. Their EA wasn't failing at its job — it simply had no mechanism to see what it couldn't govern.

This isn’t a unique scenario. Similar patterns exist across federal agencies of all sizes — civilian, defense, and health alike.

The FedRAMP Compliance Crisis Hidden in Plain Sight

The 276 applications discovered without FedRAMP or provisional authorization represent more than technical debt — they represent material non-compliance with federal mandate.

OMB M-24-15 requires agencies to obtain and maintain authorization for all cloud services that process federal data and introduces a “presumption of adequacy” for existing authorizations to speed adoption. Agencies attest compliance in FISMA reports. Yet discovery reveals hundreds of unauthorized applications in production.

The compliance gap exists because of a process disconnect: A $5,000 SaaS subscription via purchase card takes 48 hours. The same solution requiring FedRAMP takes 6-9 months. The incentive structure actively encourages non-compliance.

Implications Beyond Policy Violations

Data sovereignty risk

Federal data in foreign data centers

Audit exposure

Office of Inspector General (OIG) findings trigger expensive remediation

Breach liability

Security incidents create legal and reputational damage

Congressional oversight

High-profile breaches draw appropriations consequences

Why Traditional EA Can't Solve the SaaS Problem

Enterprise architecture operates on formal intake processes. Teams submit requests. Architects review proposals. Technologies are assessed against standards. Decisions flow through governance bodies. This works exceptionally well for infrastructure, major systems, and enterprise platforms that require capital investment and procurement processes.

SaaS breaks this model entirely.

A product manager signs up for a collaboration tool with a credit card. A developer adopts a CI/CD platform. A business unit procures analytics software. These decisions happen in days or hours, not the weeks or months traditional EA processes require. By the time EA teams would conduct a technical assessment, the application is already in production with live data.

Many federal EA teams recognize this challenge. They're managing TRMs with hundreds or thousands of annual entries — new technology assessments, updates to existing standards, evaluations of emerging capabilities. That's substantial work, but it still assumes that technologies flow through formal assessment channels.

What about the technologies that don't? What about the applications procured through purchase cards, adopted without IT involvement, or deployed by teams who don't know the TRM exists? What about the contractor-introduced tools, the pilot programs that became permanent, the "temporary" solutions now processing mission-critical data?

This is where SaaS governance becomes foundational infrastructure for enterprise architecture.

Why Traditional Controls Fail: The CASB and SASE Paradox

Many agencies deploy cloud access security brokers (CASB) to prevent unauthorized SaaS adoption. More mature agencies are implementing secure access service edge (SASE) frameworks that converge CASB, zero trust network access (ZTNA), secure web gateway (SWG), and firewall-as-a-service into unified cloud-delivered security. Yet shadow SaaS proliferates even in SASE-enabled environments. Why?

- **Personal devices and bring your own device (BYOD):** Users access SaaS from personal laptops and mobile devices that never traverse agency security controls — SASE or otherwise.
- **Application programming interface (API) and command-line interface (CLI) access:** Developers use command-line tools, software development kits (SDKs), and direct API calls that bypass web-based inspection layers entirely, regardless of how sophisticated the SASE implementation.
- **Pre-established accounts:** SASE can block signup pages, but cannot prevent users from creating accounts outside the network perimeter and then accessing those authenticated sessions through allowed domains.

- **Shadow integrations:** Users connect approved SaaS applications to unapproved services via API webhooks and integrations. SASE sees traffic to the approved application but remains blind to downstream data flows.

- **Encrypted tunnels and split tunneling:** Personal virtual private networks (VPNs), encrypted connections, and split-tunnel configurations bypass SASE inspection points.

- **Mobile application access:** Native mobile apps often use certificate pinning and proprietary protocols that resist SASE inspection, particularly for consumer-grade SaaS with mobile-first architectures.

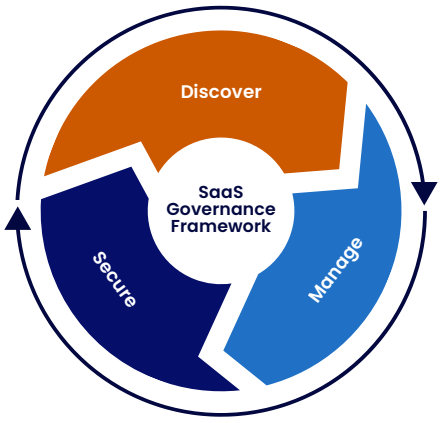
Even agencies implementing CISA's zero trust architecture with mature SASE deployments face a fundamental reality: network-based controls can only govern traffic that flows through controlled infrastructure. As the federal workspace operates across distributed locations, contractor networks, personal devices, and cloud-native applications, the percentage of SaaS adoption visible to network controls continues to decline.

SASE represents a significant advancement in cloud security architecture, but it doesn't eliminate the need for discovery-based SaaS governance- it makes it more essential. Effective SaaS visibility requires mechanisms that work independently of network topology, discovering applications based on actual usage patterns rather than network traffic inspection.

SaaS Governance: Closing the Loop on Architecture Maintenance

Effective SaaS governance doesn't replace EA — it completes it. It bridges the gap between documented architecture and operational reality through a three-step framework that directly supports EA objectives: discover, manage, and secure SaaS consumption.

DISCOVER	Leverage AI-empowered automated tooling to continually inventory SaaS applications across the enterprise.
MANAGE	Implement automated artifact collection and analysis, integrating with the agency's ongoing authorization program, and creating centralized intake workflows that scale SaaS onboarding.
SECURE	Deploy posture management tools for continuous monitoring of configuration settings and security controls, automatically detecting policy violations and misconfigurations.



Discover: Making the Invisible Visible

Current state: the configuration management database (CMDB) shows infrastructure. Security tools report vulnerabilities. None show the complete picture. Result: CIOs make $50M+ IT investment decisions based on portfolio data excluding significant portions of operational applications.

Effective SaaS governance creates the single pane of glass federal leadership requires, transforming fragmented tools into a comprehensive enterprise command center:

- **Unified portfolio** spanning on-prem, infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and SaaS.
- **Real-time compliance** showing FedRAMP status and security posture
- **Financial intelligence** including shadow IT expenditures
- **Risk aggregation** across the entire technology estate
- **Executive reporting** suitable for OMB and Congressional briefings

> **You cannot architect what you cannot see. Modern SaaS governance begins with comprehensive, automated discovery that reveals the actual application landscape regardless of how those applications were procured or deployed.**

Aquia developed a proprietary discovery platform — RADAR (Rapid Application Discovery, Analysis, and Reporting) — that integrates with existing infrastructure to automatically identify SaaS consumption across enterprises.

Unlike commercial discovery tools that may struggle with complex, decentralized environments, RADAR was purpose-built to handle disparate systems and provide enriched metadata, including:

- **Compliance posture** (FedRAMP status, SOC2, ISO 27001, HIPAA)
- **Geographic data** (headquarters location, data center locations)
- **Integration status** (SSO connectivity, identity management integration)
- **Categorical classifications** (security tools, collaboration platforms, development tools)
- **Usage patterns** (active vs. dormant applications, user populations)

The result: a living inventory of SaaS applications with high-accuracy detection of both managed and unmanaged, sanctioned and unsanctioned solutions. This inventory becomes the foundation for accurate EA documentation — not a snapshot frozen at quarterly reviews, but continuous visibility into the technology landscape as it actually exists.

For federal EA teams managing TRMs, imagine the value of automated discovery that continuously validates whether technologies in production actually align with approved TRM entries. Applications using deprecated standards would be immediately visible. Unapproved technologies would trigger assessment workflows. Technical debt would be quantified rather than estimated. Portfolio rationalization decisions would be data-driven rather than based on incomplete inventories.

Manage: Integrating SaaS into Architecture Governance

Every unapproved SaaS application is an undocumented repository outside your data governance framework.

When mission-critical data resides in unknown locations, chief data officers cannot implement the federal data strategy that was introduced via OMB M-19-18 to move federal agencies away from "ad-hoc" data management and toward a unified, mature data culture that supports evidence-based policymaking, service delivery, and transparency. Data classifications fail. Data loss prevention (DLP) cannot monitor unknown destinations. Analytics produce incomplete insights.

SaaS governance closes this loop by discovering data repositories, mapping data flows, enforcing classification, and enabling the comprehensive data architecture that chief data officers need.

Discovery reveals the problem. Management provides the mechanism to govern it.

Our team established a streamlined risk assessment methodology specifically designed for SaaS applications that can't wait months for traditional ATO processes. This process, which we called Rapid Cloud Review (RCR), evaluates vendor-provided industry reports (SOC2, ISO 27001) against federal security standards, requests specific artifacts (architecture diagrams, penetration test results, SBOM, contingency plans), and enables risk-based decisions about SaaS adoption.

The process maps all required artifacts back to authoritative sources to ensure compliance with agency security controls, providing a documented path from vendor attestations to federal requirements. Critically, in June 2024, this process was codified into policy through the risk-based decision framework and integrated into the agency's IS2P2 policy requirements — making SaaS governance not just a program, but an institutionalized policy that other federal agencies are now studying as a model.

Here's what this means for EA: instead of SaaS adoption happening outside EA governance, it flows through a structured evaluation process aligned with architectural standards. Applications are assessed against security requirements. Data flows are documented. Integration patterns are reviewed. Technical risks are identified before applications reach production scale. Most importantly, these evaluations feed directly into the EA's technology inventory and portfolio management processes.

For agencies managing sophisticated TRM workflows, the RCR methodology provides a parallel evaluation track — formal, rigorous TRM assessments for major technologies requiring deep analysis, and streamlined RCR evaluations for SaaS solutions requiring faster turnaround, with both feeding into the same comprehensive technology inventory and architectural documentation.

Secure: Continuous Validation of Architecture Compliance

Traditional EA produces point-in-time documentation. A system gets an ATO. An application passes technical review. A solution is added to the approved technology list. But technology doesn't freeze — it drifts, especially SaaS. Generally available product capabilities can change overnight without notice. Configurations change. Patches are applied. Security controls degrade. Integration points multiply. SaaS-to-SaaS interconnections increase. What was compliant at assessment may no longer be compliant weeks or months later.

SaaS security posture management (SSPM) tooling provides continuous monitoring that validates ongoing compliance with organizational standards. On one federal contract, our SaaS governance team embedded real-time posture monitoring across 78 environments onboarded into the agency's SSPM platform, monitoring against both security frameworks and architectural standards.

The Power of Continuous Validation

- **Over 62,000 security findings identified** across the monitored portfolio
- **95.33% remediation rate** for critical issues
- **Six business units achieved 100% remediation** of critical severity misconfigurations across all environments
- **91.92% reduction in compliance violations** overall (from over 5,000 violations to 404)
- **Over 1,800 threat signals delivered** to support incident response

This represents a fundamental shift in how EA maintains accuracy: instead of static documentation reviewed periodically, EA becomes a living system continuously validated against operational reality. The TRM doesn't just list approved technologies — it monitors whether deployed instances remain compliant with the standards that justified their approval.

For federal agencies managing continuous diagnostics and mitigation (CDM) requirements, SSPM tooling integration provides automated visibility into SaaS security posture that feeds directly into agency-wide cybersecurity dashboards — closing a significant gap in most agencies' CDM implementations.

Why Traditional Tools Don't Solve This Problem

Belief	Reality
Our CMDB has this.	CMDBs track formally procured assets, not shadow IT adopted without IT involvement.
ServiceNow provides visibility.	IT service management tools track formalized changes, not business unit self-service adoption.
Network monitoring shows this.	It shows traffic flows, not application identity, compliance status, or risk posture.
We have discovery tools.	Most focus on infrastructure, lacking SaaS-specific metadata like FedRAMP status and data residency.
Our CASB covers this.	Blind to API-driven interconnections and "shadow integrations" between cloud platforms.
Our SASE platform secures this.	SASE is designed for secure access, not architectural inventory. Because of certificate pinning, SASE often must "bypass" inspection for mission-critical apps (like Slack or Zoom) to keep them from breaking, creating a massive visibility gap in the very places where sensitive data lives.

Existing tools answer, "What did we procure?" SaaS governance answers, "What are we using and is it authorized?"

Integration with Enterprise Architecture Tools and Processes

The power of SaaS governance isn't just in discovering applications or assessing risks — it's in how this capability integrates with existing EA infrastructure:

- **Application Portfolio Management:** Discovery data feeds directly into CMDBs and application portfolio tools, ensuring EA teams have accurate, real-time data for rationalization decisions, technology lifecycle management, and investment planning.
- **Technology Standards Enforcement:** Continuous monitoring validates that deployed SaaS applications comply with enterprise technology standards — encryption requirements, data residency policies, integration patterns, authentication mechanisms — enabling automated compliance checking rather than periodic manual audits.
- **Architecture Modeling:** Automated discovery of actual data flows, integration points, and dependencies provides ground truth for architecture diagrams and models, ensuring that logical and physical architectures reflect operational reality.
- **Cost Optimization:** Comprehensive SaaS visibility enables duplicate capability identification, license optimization, and vendor consolidation.
- **Risk Management:** Real-time security posture monitoring, compliance tracking, and threat signal generation integrate with enterprise risk management frameworks, providing continuous risk assessment rather than point-in-time evaluations.

SaaS governance provides the missing infrastructure that makes EA operationally accurate.

Automated discovery ensures EA documentation reflects reality, not aspirations

Continuous monitoring validates that approved architectures remain compliant in production

Integration with EA tools creates a single source of truth spanning formally procured and organically adopted technologies

Risk-based assessment brings shadow IT into governance without creating procurement bottlenecks

Policy codification ensures governance is sustainable beyond individual programs or personnel

The Bottom Line: Architecture Integrity Depends on Operational Visibility

Federal enterprise architecture exists to ensure efficient and holistic design, development, execution, and maintenance of information resources aligned with mission objectives. That mandate depends entirely on an accurate understanding of the current state.

When hundreds of applications operate outside architectural visibility, transformation becomes impossible. You can't rationally plan technology consolidation if you don't know what technologies exist. You can't enforce standards if you can't identify violations. You can't manage technical debt if you can't measure it. You can't execute digital transformation if your architecture documentation describes a system that doesn't exist.

For one large federal agency, this comprehensive approach has delivered measurable results across all three dimensions of EA value — operational efficiency, risk reduction, and mission enablement.

Visibility

1,500+ Applications discovered that existed outside formal EA oversight, with 625 business-critical applications requiring governance

Governance

79 Comprehensive risk assessments completed, establishing structured evaluation for previously ungoverned SaaS adoption

Security

95.33% Remediation rate for critical findings, 91.92% reduction in compliance violations, and over 62,000 security issues identified

Compliance

#1 First-ever centralized SaaS risk review process codified into federal policy, providing a repeatable model for other agencies

Cost

$10.22M In estimated savings for every data breach avoided, per IBM research

The Path Forward for Federal Agencies

Federal agencies face a choice: continue maintaining architecture documentation that grows increasingly disconnected from operational reality, or integrate SaaS governance as foundational EA infrastructure.

The technology landscape isn't going back to centralized procurement and waterfall assessments. According to industry analysis, the global government cloud computing market is projected to grow at 16.7% annually through 2030, with U.S. federal cloud budgets nearly doubling from 2020 to 2025. The question isn't whether to govern this growth, but how to do so in ways that strengthen rather than circumvent EA.

For agencies managing sophisticated EA frameworks and TRMs with hundreds or thousands of annual assessments, SaaS governance offers a path to maintain architectural integrity at scale — ensuring that the architectures you design are the architectures you actually operate.

The alternative (meticulous documentation of an increasingly fictional technology landscape) serves no one. Not the enterprise architects working to maintain standards. Not the mission teams trying to deliver capabilities. And certainly not the citizens depending on these systems to deliver critical services.

Enterprise architecture's value proposition has always been creating order from chaos, enabling informed decision-making, and aligning technology investments with mission outcomes. SaaS governance doesn't change that mission — it provides the operational visibility needed to make it achievable in a cloud-native world.

Aquia implemented the federal government's first-ever SaaS governance program. For more information on how we can help you secure and maintain your agency's enterprise architecture and SaaS footprint, contact us at federal@aquia.us.

Practical next steps for federal EA teams:

1. **Assess your visibility gap:** Conduct discovery to understand the delta between your documented architecture and operational reality
2. **Establish risk-based evaluation:** Implement streamlined assessment processes for SaaS that balance speed with rigor
3. **Integrate with existing EA tools:** Connect SaaS governance data to your CMDB, portfolio management, and risk management systems
4. **Implement continuous monitoring:** Move from point-in-time assessments to ongoing validation of architectural compliance
5. **Codify into policy:** Formalize SaaS governance processes into agency policy to ensure sustainability

About Aquia

Aquia is a service-disabled Veteran-owned small business (SDVOSB) specializing in cloud infrastructure, cybersecurity, and compliance automation. Founded by Veterans who understand the unique challenges of government technology modernization, our team brings deep expertise in federal systems integration. We are passionate about helping our government partners maximize outcomes and challenge the status quo.

Contact information
Brandon Utt, VP of Business Development
brandon.utt@aquia.us | 908-268-9911

Trusted By

U.S. Department of Veterans Affairs
CMS Centers for Medicare & Medicaid Services
uspto
U.S. Department of Health & Human Services Office of Inspector General
Cloud One Fast Secure Streamlined
Platform One Department of Defense
CDC
U.S. Securities and Exchange Commission
USDA
Maryland
U.S. Air Force
U.S. Digital Service
Nava
leidos
Omni Federal
Skyward IT Solutions
noblis
coforma
KesselRun
Datalock Consulting Group
nuix
RegScale
Excella
BigBear.AI
cantaloupe
Valley IT Solutions

Awardable Platform One
2025 Elev8 GovCon Honoree
Great Place To Work. Certified Mar 2024-Mar 2025 USA
builtin 2025 Best Places to Work
Inc. Best Workplaces Honoree 2024
Fortune Best Small Workplaces 2024
Google Cloud Partner
aws Partner Advanced Tier Services

- Public Sector
- Authority to Operate
- Security Services Competency