VIPERBYTE SECURITY

SOLUTION BRIEF

GovRAMP Authorization:

The Faster, Cheaper Path for Technology Vendors

How Viperbyte replaces the traditional authorization build-out for Snapshot & Core — deploy the monitoring infrastructure, skip the $600K+ stack.

TARGET READER	AUTHORIZATION LEVELS	FRAMEWORK	DOCUMENT DATE
Tech Vendor / SaaS CSP / ISV	GovRAMP Snapshot + Core	NIST SP 800-53 Rev 5	August 2026

1. GovRAMP Authorization — What It Is and Why It Matters

> **THE MARKET:** State, local, tribal, and territorial (SLTT) governments collectively spend over $142 billion annually on technology. Most state procurement offices now require or strongly prefer GovRAMP-authorized vendors. Without authorization, your product sits outside the procurement vehicle — regardless of how good it is.

GovRAMP (formerly StateRAMP) is the state and local government equivalent of FedRAMP. It is a standardized security authorization program that allows a cloud service provider (CSP) to be assessed once and recognized across multiple state/local procurement programs. Authorization demonstrates that your product meets NIST SP 800-53 security controls and is safe for government agencies to procure and use with sensitive data.

The Three Authorization Levels

Level	Controls (~)	Assessment	Best For
Snapshot	~45 NIST 800-53 controls	Annual 3PAO assessment + self-attestation	Entry point to government market. Covers lower-sensitivity data. Fastest path to authorization — 6–9 months with the right tooling.
Core	~125 NIST 800-53 controls (Low baseline)	Annual 3PAO assessment + continuous monitoring	Required for most substantive government contracts. Covers moderate-sensitivity data. Full ConMon obligation.
Authorized (Full)	~325 NIST 800-53 controls (Moderate)	Full 3PAO + annual pen testing	Equivalent to FedRAMP Moderate. Required for highest-sensitivity state data. This document focuses on Snapshot and Core.

The Authorization Lifecycle — What You're Committing To

GovRAMP is not a one-time event. Authorization requires an initial assessment AND an ongoing continuous monitoring (ConMon) obligation. This is the piece most vendors don't fully price when they decide to pursue authorization.

Phase	Timing	What's Required
Pre-Authorization Prep	3–12 months (varies by readiness)	Gap assessment → build/configure compliant monitoring infrastructure → write System Security Plan (SSP) → document policies → prepare evidence package.
Initial 3PAO Assessment	60–90 day engagement	Certified assessor reviews all controls, tests technical implementations, interviews staff, reviews documentation. Findings report issued.
Authorization Decision	30–60 days post-assessment	GovRAMP PMO reviews assessment package. Authorization granted (or remediation required). Listed on GovRAMP Authorized Product List.
Continuous Monitoring (ConMon)	**Monthly — every year until authorization lapses**	Monthly: vulnerability scan results, POA&M updates, incident reports, configuration change logs. Annual: full assessment refresh + penetration test. THIS IS THE ONGOING COST MOST VENDORS UNDERESTIMATE.

2. The Traditional Authorization Build-Out — What Vendors Are Forced to Spend

Before a 3PAO assessor can evaluate your product, you must first BUILD a compliant security monitoring environment — or pay someone to build it for you. This is the part of GovRAMP that blindsides most vendors. The assessment fee is the smallest line item. The infrastructure build and ongoing ConMon are where the real money goes.

Pre-Authorization Infrastructure Build (One-Time)

Component	Typical Tool(s)	One-Time Cost	What It Provides
SIEM / Log Management	Splunk, Azure Sentinel, Elastic	**$40K–$80K (implementation)**	Centralized log collection, alerting, correlation. AU and SI controls depend on it.
Vulnerability Management	Tenable.io, Qualys, Rapid7	**$15K–$25K (setup + first yr)**	Periodic and continuous vuln scanning. RA-5 requires documented scan results.
Endpoint Detection & Response	CrowdStrike, Defender P2, SentinelOne	**$20K–$40K (deployment)**	Malware detection, host-based monitoring. SI-3 and IR-4 controls.
Network Boundary Monitoring	Palo Alto, Cisco, pfSense	**$15K–$35K (firewall + config)**	SC-7 boundary protection. Traffic inspection and logging at perimeter.
Identity & Access Management	Okta, Azure AD P2, Ping	**$10K–$20K (implementation)**	AC-2, AC-3, IA-2, IA-5 controls. User provisioning, MFA enforcement.

Documentation & GRC Platform	Atlassian, ServiceNow, Drata	**$15K–$30K (first year)**	SSP writing, POA&M tracking, evidence management. Required for assessment package.
RPO Engagement (Registered Practitioner Org)	CMMC/GovRAMP RPO or MSSP	**$100K–$200K (full engagement)**	Guides gap assessment, writes SSP, preps evidence package, manages 3PAO relationship. The biggest check you'll write.

Ongoing Annual Costs After Authorization

Annual Obligation	Annual Cost	Why It Never Goes Away
ConMon MSSP (monthly reporting service)	**$84K–$120K/yr ($7K–$10K/month)**	GovRAMP requires monthly vulnerability scan reports, POA&M updates, and incident reports submitted to the PMO. Most vendors outsource this entirely. Not optional — missed ConMon = authorization revoked.
3PAO Annual Assessment Refresh	**$40K–$80K/yr**	Full re-assessment annually for Core. Snapshot requires annual self-assessment plus periodic 3PAO validation. Evidence package must be current.
Tool Licensing (SIEM, vuln scanner, etc.)	**$60K–$120K/yr**	Splunk ingestion costs, Tenable asset licenses, EDR per-endpoint fees — these run every year regardless of how many government contracts you have.
Annual Penetration Test (Core requirement)	**$20K–$40K/yr**	GovRAMP Core requires annual pen testing of the authorization boundary. Must be conducted by an approved assessor.

$609,000
Year 1 — Build + Authorize
Infrastructure + RPO + 3PAO + SSP docs + first-yr tools

$204,000
Years 2–3 — Stay Authorized
ConMon MSSP + tool licensing + annual assessment (per yr)

$1,017,000
3-Year Traditional TCO
$609K year 1 + $204K × 2 · Before internal headcount

> **THE TRAP:** Year 1 is the build cost. But authorization MAINTENANCE — ConMon, annual assessments, tool renewals — runs $200K/year forever. Many vendors let authorization lapse rather than pay it. That's not an option if your government revenue depends on being on the Authorized Product List.

3. The Viperbyte Path — Deploy the Infrastructure, Skip the Build

Viperbyte is an on-premises autonomous AI security platform that ships as a hardware appliance. When deployed in your authorization boundary, it replaces the SIEM, vulnerability scanner, network monitoring, and ConMon reporting engine in a single deployment. The compliance dashboard maps

directly to GovRAMP Snapshot and Core NIST 800-53 controls and generates continuous monitoring artifacts automatically — every day, not just audit month.

What Viperbyte Replaces in the Traditional Build

Traditional Component	Status With Viperbyte	What Viperbyte Provides Instead
SIEM / Log Management ($40K–$80K build)	**ELIMINATED**	Viperbyte's Network Intelligence Engine ingests all network telemetry on-prem — continuous log correlation, real-time alerting, 365-day retention. No Splunk license. No ingestion costs. AU and SI controls satisfied.
Vulnerability Management ($15K–$25K first year)	**ELIMINATED**	Viperbyte continuous passive scanning + on-demand Pentest Report generation. RA-5 satisfied with timestamped scan artifacts exportable for the assessor.
Network Boundary Monitoring ($15K–$35K)	**ELIMINATED**	nft/ipset enforcement layer + Network Intelligence Engine monitors all boundary traffic. SC-7 satisfied with live enforcement log as evidence.
ConMon MSSP ($84K–$120K/yr)	**ELIMINATED**	Viperbyte generates all ConMon artifacts automatically: monthly vuln scan results, incident reports, configuration change logs, POA&M supporting data. No MSSP contract. No monthly reporting fee. This is the biggest cost Viperbyte eliminates.
RPO Engagement ($100K–$200K)	**DRAMATICALLY REDUCED**	Viperbyte's compliance dashboard pre-maps all controls to evidence. RPO scope reduces to SSP writing and gap review — not full evidence collection.
Documentation / GRC Platform ($15K–$30K)	**SUBSTANTIALLY COVERED**	Viperbyte compliance dashboard tracks all 800-53 controls with evidence pointers. Export to structured JSON or human-readable report for assessor package.
Endpoint Detection & Response ($20K–$40K)	**PARTIAL — OPTIONAL**	Viperbyte covers ALL network-connected assets agentlessly via SPAN. EDR agents add depth on managed endpoints — beneficial but not required for coverage.
Identity & Access Management ($10K–$20K)	**INGESTS / ENHANCES**	Viperbyte Identity Engine attributes every network session to a named user. AC-2, IA-2, IA-5 controls satisfied through behavioral attribution + MFA signal ingestion.

3-Year TCO — Viperbyte Path to GovRAMP Core

Cost Item	Amount	Notes
Viperbyte platform license	**$47,000/yr**	Annual platform license. Includes compliance dashboard, ConMon reporting, threat intel feeds, and all

		sensor layers.
Viperbyte hardware appliance(s)	**$7,000 one-time**	1–2 appliances for authorization boundary. Deployed in vendor's data center or colo.
SSP + policy documentation (RPO, reduced scope)	**$50,000 one-time**	Viperbyte pre-maps controls — RPO writes the SSP document and gap narrative. One-time engagement only.
3PAO assessment (shorter due to Viperbyte evidence)	**$80,000 one-time**	Assessor reviews Viperbyte compliance dashboard + exports instead of assembling a binder. Assessment timeline compressed. Lower total fee.
Annual pen test (Core requirement)	**$25,000/yr**	Required annually for Core. Viperbyte's passive scan data provides pre-test intelligence to the pen test team — reduces scope and duration.

$209,000

Year 1 — Deploy + Authorize

Viperbyte license + hardware + RPO + 3PAO + pen test

$72,000

Years 2–3 — Stay Authorized

Viperbyte license ($47K) + annual pen test ($25K) per yr

$353,000

3-Year Viperbyte TCO

$209K yr 1 + $72K × 2 · vs $1,017,000 traditional

65%

Cost Reduction

$664,000 in 3-year savings vs traditional path

THE KEY DIFFERENCE: Traditional path: you pay $200K/year FOREVER to maintain authorization because you need an MSSP to run ConMon and a licensing stack to generate evidence. Viperbyte path: ConMon is automatic. Year 2 and 3 cost $72K — not $204K. The savings compound every year you stay authorized.

4. NIST SP 800-53 Control Coverage — Snapshot & Core

The table below maps key NIST 800-53 controls across GovRAMP Snapshot and Core to Viperbyte's coverage level. Controls marked 'S' appear in Snapshot. Controls marked 'C' are Core additions. Coverage levels: FULL (Viperbyte satisfies the control technically and generates evidence), SUBSTANTIAL (Viperbyte covers the technical requirement; policy document still needed), PARTIAL (Viperbyte contributes but additional tooling required), NOT COVERED (policy/people/physical — no tool satisfies this).

Level	Control	Name	Coverage	Viperbyte Satisfaction
S	AC-2	Account Management	SUBSTANTIAL	Identity Engine maintains live inventory of all accounts observed on network. Unauthorized accounts flagged automatically. Policy

				doc required for account lifecycle.
S	AC-3	Access Enforcement	SUBSTANTIAL	nft ruleset enforces network access decisions. Identity-based session control. Application-layer enforcement requires IAM integration.
S	AC-17	Remote Access	FULL	VPN session log attributed to named user. Impossible travel detection. Every remote session recorded with user, device, source geo, and duration.
S	AU-2	Event Logging	FULL	All network events, DNS queries, identity sessions, and enforcement actions logged continuously. 365-day retention. Tamper-evident timestamps.
S	AU-3	Content of Audit Records	FULL	Every log entry includes: timestamp, source, destination, user identity, action, outcome. Fully attributed — no anonymous events.
S	AU-6	Audit Record Review	FULL	Compliance dashboard provides automated audit review with alerting on anomalies. Assessor can query any time window.
S	AU-12	Audit Record Generation	FULL	All sensors generate audit records continuously. No gap windows. Evidence exportable as structured JSON or compliance report.
S	CM-7	Least Functionality	SUBSTANTIAL	Device behavioral baseline detects unexpected services and connections. Unauthorized service discovery triggers anomaly alert.
S	CM-8	System Component Inventory	SUBSTANTIAL	Viperbyte device registry: every network-connected component profiled with MAC, hostname, OS hint, vendor (OUI), first/last seen, and behavior state.
S	IA-2	Identification & Authentication	SUBSTANTIAL	Identity Engine attributes every session to a named user via Zeek NTLM/Kerberos and

				MS365/Azure AD. MFA bypass flagged. Policy required for auth enforcement.
S	IA-5	Authenticator Management	PARTIAL	Viperbyte monitors for weak authentication signals and MFA bypass events. Actual credential management requires IAM platform integration.
S	IR-4	Incident Handling	SUBSTANTIAL	Real-time incident detection with automated evidence chain generation. Every incident timestamped with full context. Written IR plan still required.
S	RA-5	Vulnerability Scanning	FULL	Continuous passive vulnerability assessment + on-demand Pentest Report. Timestamped scan artifacts exportable for monthly ConMon submission.
S	SC-7	Boundary Protection	FULL	nft/ipset enforcement at authorization boundary. 1.38M threat intel indicators. Every inbound/outbound decision logged. Deception Layer profiles boundary attacks.
S	SI-2	Flaw Remediation	SUBSTANTIAL	Viperbyte identifies unpatched services via threat intel cross-reference. Actual patch deployment requires endpoint management tooling.
S	SI-3	Malicious Code Protection	FULL	DNS Security Engine blocks malware C2 callbacks. Deception Layer catches active malware. Covers agentless devices agents miss.
S	SI-4	System Monitoring	FULL	Continuous behavioral monitoring across all network-connected assets. Big Brain AI correlates events into kill-chain sequences. F1=0.9924.
C	AC-4	Info Flow Enforcement	FULL	DNS Security Engine enforces information flow policy at DNS layer. nft zones

				enforce network segmentation. Unauthorized data paths detected.
C	AU-9	Protection of Audit Info	FULL	Audit records written to append-only log. Viperbyte enforcement log is tamper-evident by architecture. No user can modify historical records.
C	CA-7	**Continuous Monitoring**	FULL	THIS IS THE CONMON CONTROL. Viperbyte IS the continuous monitoring engine. Monthly ConMon artifacts generated automatically: scan results, incident log, config change log, POA&M supporting data. Zero MSSP required.
C	CM-2	Baseline Configuration	SUBSTANTIAL	Device baseline: every asset profiled over time. Behavioral deviation from established baseline triggers alert. Baseline exportable as evidence.
C	CM-6	Configuration Settings	SUBSTANTIAL	Unauthorized configuration changes surface as behavioral anomalies. Formal configuration management policy still required as documentation.
C	IR-5	Incident Monitoring	FULL	Real-time incident feed with severity scoring. Every event correlated across all sensors. AI brain tracks incident progression across kill chain.
C	IR-6	Incident Reporting	FULL	Evidence chain exports provide structured incident report artifacts in the format required for GovRAMP ConMon incident reporting submissions.
C	SC-8	Transmission Confidentiality	SUBSTANTIAL	Viperbyte monitors for unencrypted CUI transmission. Flags cleartext protocols on sensitive data paths. Encryption enforcement requires network policy.

5. ConMon — The Ongoing Requirement That Kills Vendor Authorization Budgets

> **THE REALITY OF CONMON:** GovRAMP authorization is not a certificate you hang on the wall. It is an active obligation. Miss a monthly ConMon submission and your authorization status moves to 'Inactive.' Miss two and it lapses entirely. Every state agency that procured your product based on your authorization now has a problem — and so do you.

The GovRAMP Continuous Monitoring program requires vendors to submit a package every month. Most authorized vendors outsource this entirely to an MSSP at $7,000–$10,000/month because assembling it manually requires dedicated staff who understand NIST 800-53 evidence requirements. Viperbyte eliminates this cost entirely.

Monthly ConMon Submission Requirements vs Viperbyte Output

GovRAMP Monthly ConMon Requirement	Traditional Method	Viperbyte Output
Vulnerability Scan Results (all assets in boundary)	Run Tenable/Qualys scan. Export report. Format for GovRAMP template. Review findings. Update POA&M. Staff: 8–12 hrs/month.	Viperbyte continuous passive scan. On-demand Pentest Report generation. Export as structured artifact. Zero manual effort. CA-7 satisfied.
POA&M Update (Plan of Action & Milestones)	MSSP reviews open findings. Updates remediation status in GRC platform. Submits formatted POA&M to GovRAMP PMO. Staff: 4–6 hrs/month.	Viperbyte compliance dashboard tracks open findings per control. Export current control status as POA&M supporting evidence. Automated.
Incident Report (any security events)	MSSP reviews SIEM alerts. Writes incident narrative. Submits within required timeframe (72 hrs for significant incidents).	Viperbyte evidence chain auto-generates incident report artifact for every detected event — timestamped, attributed, with full context.
Configuration Change Log (all boundary changes)	Change management tickets pulled from ServiceNow/Jira. Formatted for GovRAMP. Cross-referenced against baseline. Staff: 3–5 hrs/month.	Viperbyte device baseline tracks all configuration deviations automatically. Change log exportable with timestamps, entity, and delta from baseline.
Inventory Update (asset additions/removals)	Manual reconciliation of CMDB against scan results. Any new assets require evidence of security controls. Staff: 2–4 hrs/month.	Viperbyte device registry auto-updates as new assets appear on the network. NEW/LEARNING/KNOWN state lifecycle tracked per device. Exportable as inventory.
Encrypted Transmission Evidence (SC-8, Core)	Network scan for unencrypted protocols. Review SSL/TLS configurations. Document any exceptions. Staff: 2–3 hrs/month.	Viperbyte continuously monitors for cleartext transmissions on sensitive paths. Flags unencrypted protocols automatically. Evidence record auto-generated.
MONTHLY STAFF COST (MSSP or internal)	**$7,000–$10,000/month ($84K–$120K/year) for a dedicated ConMon MSSP**	**Included in Viperbyte platform license. $0 additional per month. All artifacts generated automatically.**

6. 3PAO Assessment Experience — Binder vs Dashboard

Traditional Path — What Assessment Prep Looks Like

- **Months 1–3:** Gap assessment. RPO identifies deficiencies. Remediation begins.
- **Months 3–8:** Infrastructure build. SIEM configured. Logs flowing. Vuln scans running.
- **Months 8–10:** Evidence collection. Screenshots from every tool. Log exports. Dashboard printouts.
- **Month 11:** Binder assembly. RPO organizes evidence by control family. Review cycle. If any control lacks evidence — remediation pause. Timeline slips.
- **Month 12–14:** 3PAO assessment week. Static binder reviewed. Interviews. Technical tests.
- **Typical time to authorization:** 12–18 months from decision to authorized status.
- **Total cost to authorization:** $465K–$610K before annual ConMon begins.

Viperbyte Path — What Assessment Prep Looks Like

- **Week 1:** Deploy Viperbyte appliance in authorization boundary. Passive monitoring begins immediately — zero configuration required.
- **Weeks 2–4:** Connect integrations: MS365/Azure AD, LDAP/AD connector, VPN. Identity attribution active. Compliance dashboard begins populating.
- **Month 2:** 30 days of behavioral baseline accumulated. Vuln scan baseline established. ConMon artifacts generating automatically.
- **Months 2–3:** Engage RPO for SSP writing only — not evidence collection, not tool management. Viperbyte compliance dashboard IS the evidence.
- **Months 3–5:** 90–150 days of continuous Viperbyte evidence. Hand 3PAO assessor this document + live dashboard access.
- **Typical time to authorization:** 6–9 months — 40–50% faster than traditional path.
- **Total cost to authorization:** $209K — 66% below traditional path.

Assessment Factor	Traditional Path	Viperbyte Path
Time to authorization	12–18 months	6–9 months (40–50% faster)
Evidence type	Point-in-time binder assembled before audit. Could have been staged.	365-day continuous record. Assessor picks any date to verify.
Evidence gaps mid-assessment	Common — timeline pauses while missing evidence is located or created.	All covered controls have live evidence. No gaps. No pauses.
RPO/MSSP engagement scope	Full engagement: gap analysis, build, evidence collection, binder, ongoing mgmt.	SSP writing only. Viperbyte handles the rest.
All-in authorization cost	$465K–$610K	**$209K (66% less)**

7. What Viperbyte Does Not Cover — Remaining Gaps and How to Close Them

> **HONEST ACCOUNTING:** Viperbyte covers the technical monitoring and evidence generation requirements for the majority of GovRAMP Snapshot and Core controls. It does not write your policies, train your staff, secure your physical facilities, or manage your cryptographic keys. The remaining gaps are real — but they are documented, finite, and addressable for far less than the cost of the full traditional build.

Control	Name	Gap Type	How to Close It (and What It Costs)

AT-2 / AT-3	Security Awareness & Role-Based Training	**People — training records required**	KnowBe4 or Proofpoint Security Awareness. Annual phishing simulation + course completion records. ~$5K–$8K/yr for 100 staff.
MP-6 / MP-7	Media Sanitization & Use	**Policy + procedure document**	Written policy covering media classification, sanitization before disposal, USB controls. One-time document — $2K–$4K with your RPO.
PE-2 / PE-3	Physical Access Controls	**Physical controls + documentation**	Badge reader, visitor log, locked server room with access log. If you colocate, provider's PE controls may cover this via inheritance.
SC-12	Cryptographic Key Management	**Policy + KMS tool required**	Documented key lifecycle policy + key management system (AWS KMS, Azure Key Vault, HashiCorp Vault). Viperbyte monitors for unencrypted transmissions but does not manage encryption keys.
SA-9	External System Services	**Policy — third-party service inventory**	Written inventory of all external services your product uses. Each must have FedRAMP/GovRAMP authorization or documented risk acceptance.
PL-2	System Security Plan	**Documentation — SSP required**	The SSP is the single most important authorization artifact. Viperbyte compliance dashboard populates most technical content automatically. RPO writes the narrative layer. Cost: $30K–$50K one-time.

Total cost to close all remaining gaps: $40K–$70K one-time (SSP + policy docs + KMS) + $5K–$8K/year (security awareness training). Even with these gaps fully closed, the Viperbyte path remains 65% below the traditional authorization cost.

8. Getting to GovRAMP Authorization With Viperbyte — The Path Forward

> **THE DECISION:** GovRAMP Snapshot or Core authorization with Viperbyte: $209K to authorize + $72K/year to stay authorized. Traditional path: $465K–$610K to authorize + $204K/year to stay authorized. The 3-year savings: $664,000. Speed advantage: 6–9 months vs 12–18 months. The government market you unlock: $142 billion in annual SLTT technology spend.

Recommended Authorization Sequence

- **Week 1–2:** Deploy Viperbyte appliance in authorization boundary. Connect to network. Passive monitoring begins immediately.
- **Week 2–4:** Configure integrations: MS365/Azure AD identity attribution, LDAP connector for on-prem AD, VPN session logging.
- **Month 1–2:** Viperbyte accumulates 30–60 days of baseline. Compliance dashboard begins mapping Snapshot/Core controls to live evidence.
- **Month 2–3:** Engage RPO for SSP writing. Viperbyte compliance dashboard exports provide the technical control evidence.
- **Month 3–4:** Close remaining gaps: KMS implementation, security awareness training launch, physical access documentation.
- **Month 4–6:** 90–180 days of continuous Viperbyte evidence. Schedule 3PAO assessment. Hand assessor live dashboard access.
- **Authorization granted:** ConMon begins on Day 1. Viperbyte auto-generates monthly submissions. No MSSP contract required.

Snapshot vs Core — Which Level to Target First

Level	Time to Authorization (with Viperbyte)	3-Year TCO (with Viperbyte)	Strategic Rationale
GovRAMP Snapshot	**4–6 months**	**~$280,000**	Fastest path to the authorized product list. Gets you into the procurement vehicle immediately. Upgrade to Core once government revenue justifies the expanded scope.
GovRAMP Core	**6–9 months**	**~$353,000**	Required for most substantive government contracts. Viperbyte's continuous monitoring satisfies the ConMon obligation automatically.

Viperbyte Security · GovRAMP TCO figures based on published industry estimates — individual vendor costs vary by boundary scope and existing infrastructure · NIST SP 800-53 Rev 5 · GovRAMP Program Management Office requirements as of 2026 · viperbytesecurity.com · sales@viperbytesecurity.com