stackArmor

A TYTO ATHENE COMPANY

2025

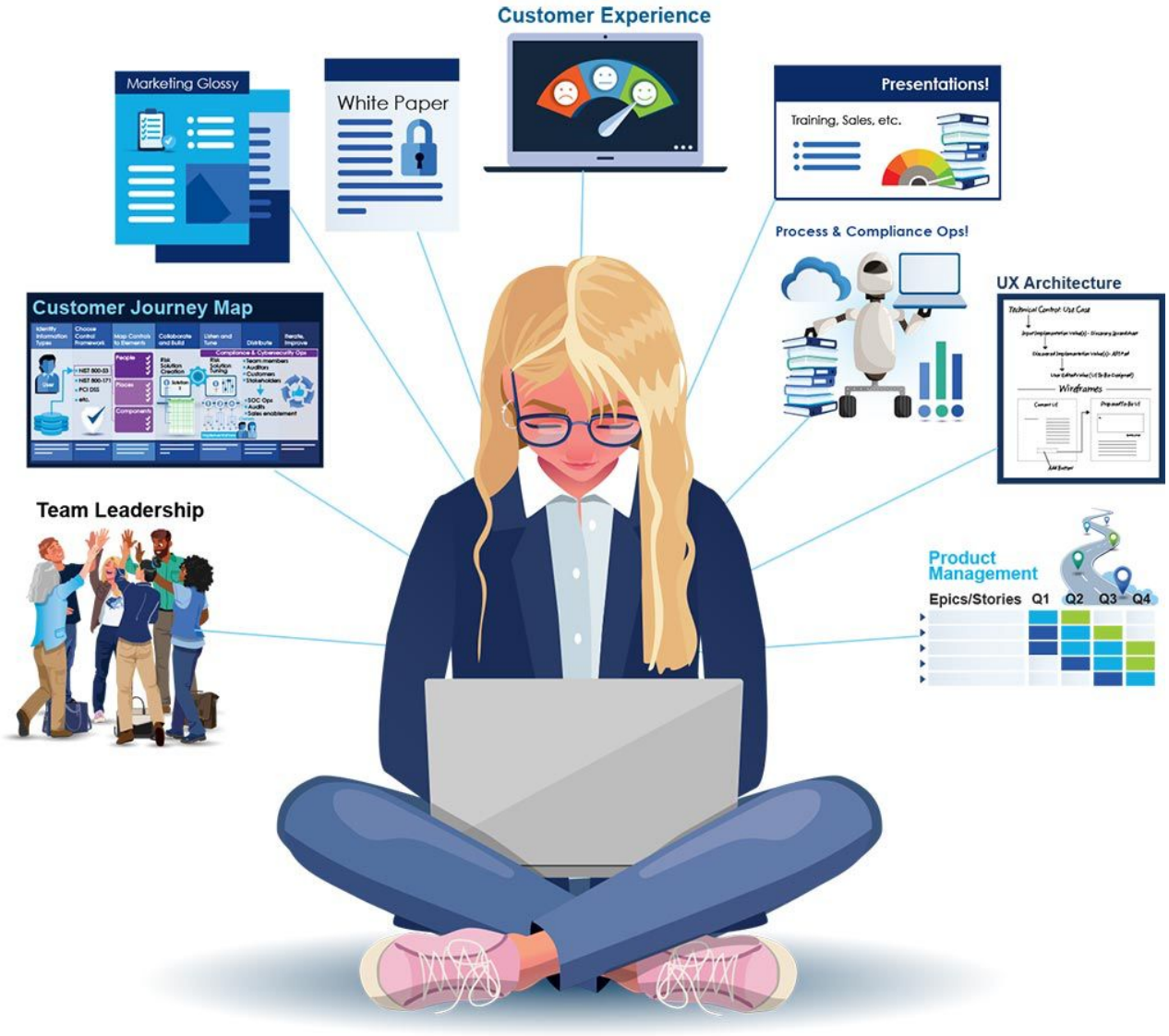
AUG - DEC

Sarah Hensley

Annual Performance Report

Hire Date: Aug 21, 2024

"A jack of all trades is a master of none, but oftentimes better than a master of one."



The contents in this review cover some of the highlights of my work for the last 3 ½ months of 2025. It hopefully represents both the breadth and depth of my continued contributions and value to stackArmor.

Contents | What I Accomplished in the last 3½ Months of 2025

2025 Performance Highlights = stackArmor's ROI

Customer Satisfaction (Avg NPS)

9.1 (Exceptional)

NPS of 9.1 for reporting customers is considered an "exceptional" score for those customers, with 9.2+ being "world class."

EM Team Employee Retention

100%

Doubled the team size my first year, and fought hard to repair morale, build a culture of accountability, establish adequate onboarding and training support, and prevent turnover.

Multi-Role Fulfillment

6+ Roles

Provided leadership & delivered consistently in all of these roles:

- *CX Thought Leader*
- *Product Manager*
- *Engagement Manager*
- *Marketing "Director"*
- *Technical Writer*
- *Graphic Artist*

IP/Artifacts Created

100+

100s of Illustrations
4 Journey Maps
Company Intranet
2 White Papers
10+ Glossies
10+ Arch Diagrams
4 Quick Ref Guides
7 Newsletters
8 Blogs
EM Playbook
Product Roadmap
Product Strategic Plan
CX/EX Program
CX/Ops Analysis Tool
Multiple Trainings
Company Brand Guide
& Many More...

Out of Pocket $ Investment

Well Over $1k

Out of My Pocket: (What I paid for that solely or primarily benefits stackArmor)

- *Stock Art Subscription*
- *2 AI Tool Subscriptions*
- *sA Branded Shirts for Tradeshow*
- *Flipbook Subscription*
- *PDF Reducer Subscription*

Time Investment (Hrs/week)

45-50

*Gave the company **15+ months of man hours** in my first 12 months, and continued the trend working through much of my holiday PTO time.*

2025 Goals | Updates for Aug - Dec

These are my original 5 goals that I fully delivered on by my anniversary date of Aug 21, 2025 (removing the couple that members the c-suite cancelled and the ones for my first 3 months of employment). This shows that I actually continued to deliver against them, plus a whole lot more.

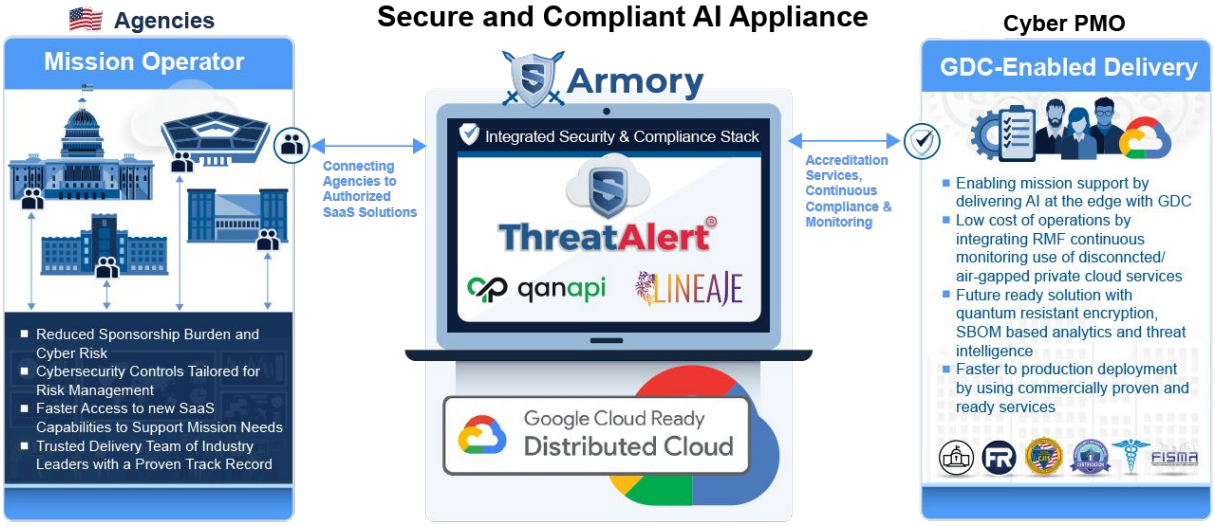
Goal		Status	Ref Links
1	Establish a Clear Description of the Customer Journey for stackArmor Service Offerings	Completed all 3 – by Jan 2025, updated multiple times throughout the year.	pg. 26
2	Establish the customer journey map for Armory as a part of product management	Completed pre August 21, and updated in Dec 2025.	pg. 7
3	Create Armory Program Management Guide and PMO Establishment	Completed pre August 21, and did a follow-up Product Management Presentation with Tyto to try to energize and get buy-in from the team on the need for product management.	pg. 10-12
4	Author at least 3 blogs or articles for publishing (ask from GP)	Completed (3 newsletters before Aug 21), then authored 4 newsletters and edited/designed 5 blogs (with Johann) from Aug-Dec, in addition to 2 massive white papers.	pg. 22-25, 29-34, 41-43
5	Establish Clear Branding and Definitions around stackArmor IP and Offerings (ThreatAlert Security Workbench, Security Toolbox, Serverless Relay, Container Scanner, etc.)	Completed, and did additional work on this goal for GP by creating a set of combined stack/Tyto logos, and building out a series of ad mocks that are now being re-created by marketing using my mocks.	pg. 36

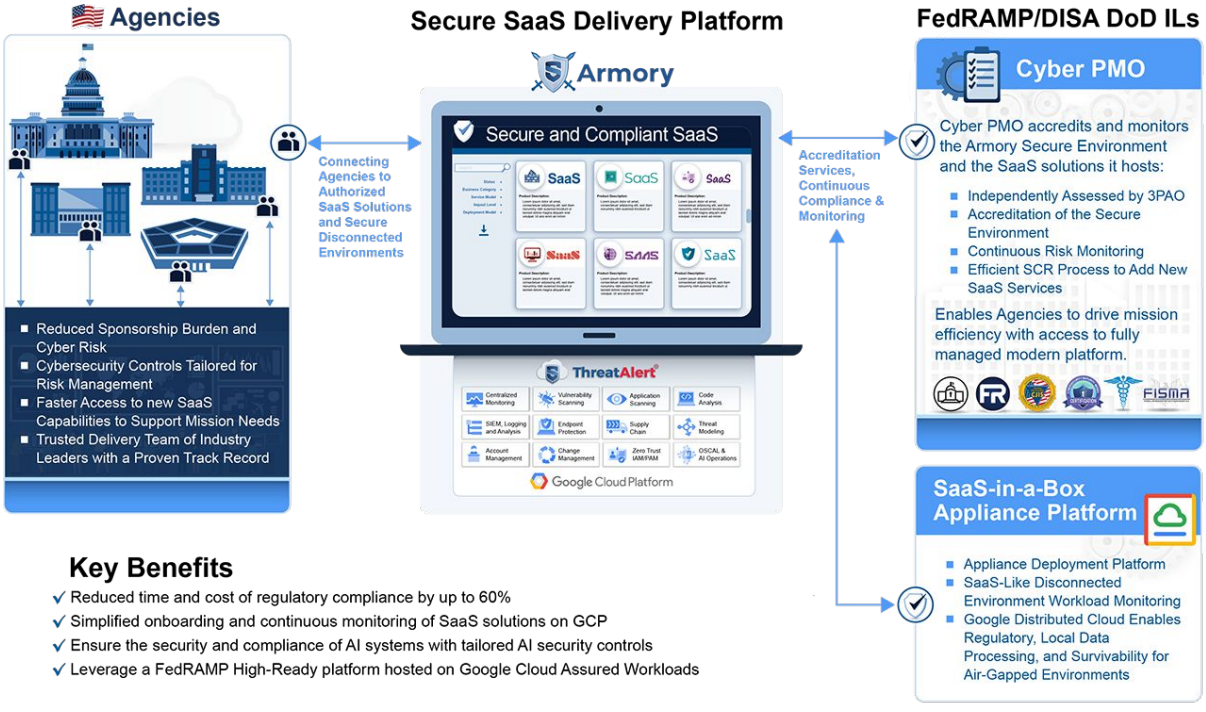
Product Management: Armory Plus

Created Many New Versions of Armory Infographics

Versions of original vectors created to visually communicate Armory deployment models and Armory's role in serving government agencies.

- *All vector art, with multiple versions created for GP in the fall to support various engagement opportunities.*
- *Some of the content is re-use, some is new.*





Key Benefits

- ✓ Reduced time and cost of regulatory compliance by up to 60%
- ✓ Simplified onboarding and continuous monitoring of SaaS solutions on GCP
- ✓ Ensure the security and compliance of AI systems with tailored AI security controls
- ✓ Leverage a FedRAMP High-Ready platform hosted on Google Cloud Assured Workloads

More Armory Illustrations that Help Communicate Complex Concepts

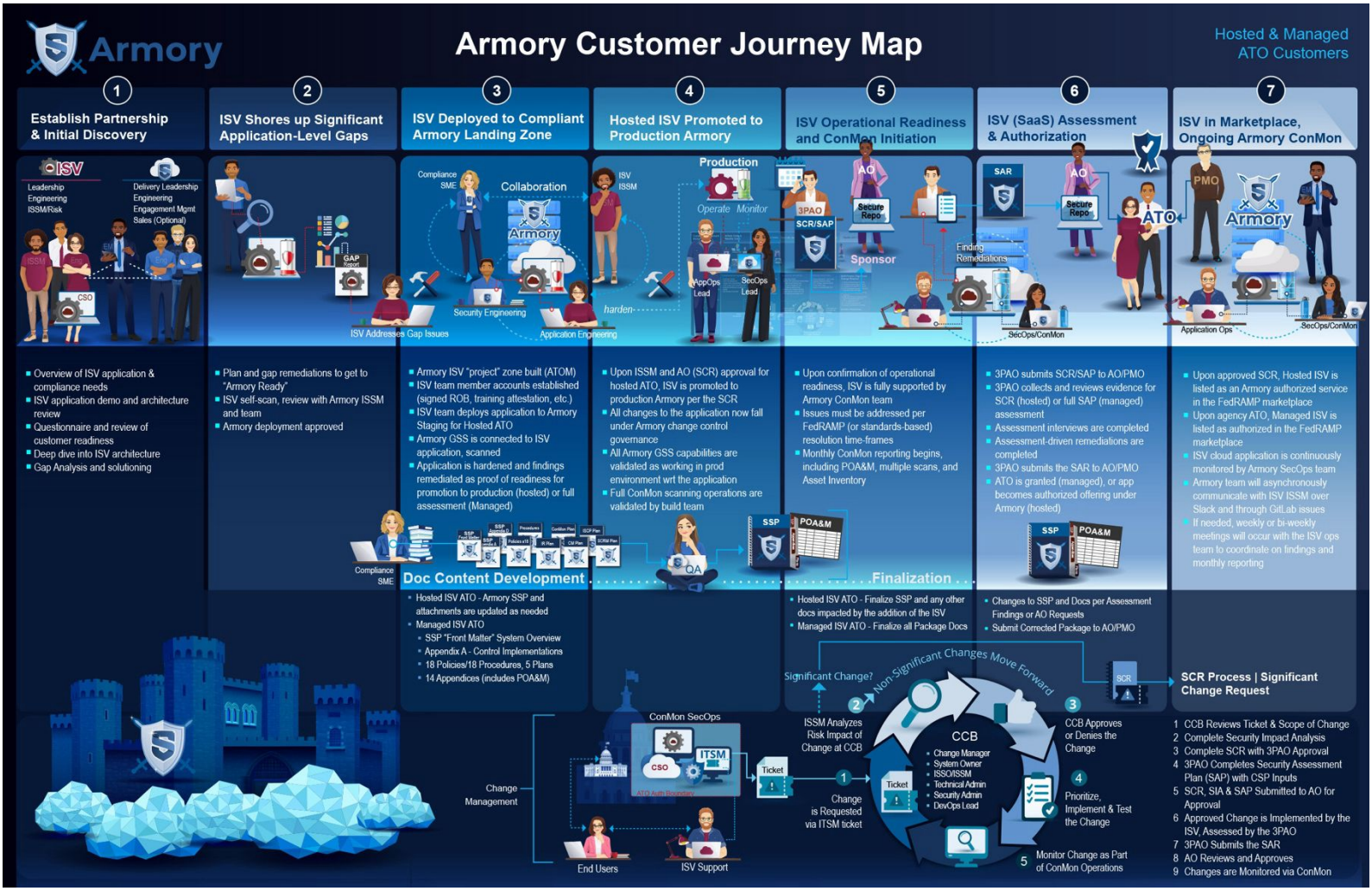
I illustrated this vector image to show how machine-driven system evaluations (e.g. query driven assessments) are architected.

This glowing Armory logo is actually a complex vector illustration that I created for one of the white paper covers.

Revised Armory Customer Journey Map

Made updates to the draft of the Armory customer journey map based on evolving FedRAMP and Armory variables.

- *Journey Map is a key artifact of product managers and UX architects.*
- *Created a combined Hosted/Managed map – we may want to break these out.*
- Image at the bottom was illustrated as well

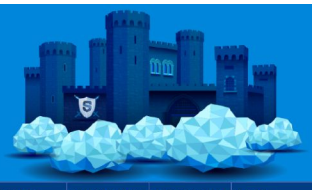


Created a Strategic Armory/TSW Product Roadmap

Built a prioritized product roadmap to highlight priority strategic capabilities we need to be considering.

- *This has Epic level, strategic capabilities vs the "feature backlog" roadmaps*
- *We are missing the boat in thinking our only competitors are other services orgs as security products are expanding their compliance management capabilities.*
- Our dev folks have discussed having no guidance as to feature prioritization.

Armory/ThreatAlert Working Roadmap



For the purposes of this roadmap, "ThreatAlert" means the whole tech stack - The dashboards, scripts, playbooks, connections, and connected commercial tools that work together for the purpose of establishing, maintaining, and monitoring solutions to adhere to regulatory cybersecurity standards

Epic	General Capability	Description	Value/Benefit (Who Cares and Why?)	Q1 2026	Q2 2026	Q3 2026	Q4 2026	Q1+Q2 2027	Q3+Q4 2027	2028+
Risk Management App Front-End GUI Designed for Efficiency, Clarity, and Error Prevention	(Obfuscating GitLab at least 1 layer below being "the" layer) Design Risk Management Application Front-end - this is DESIGN only, no build	*Using Focus Groups (Analysts and ISSMs), finalize a design for a Risk Management Application Front-end (between the user and GitLab).*	*Improved UX especially for analysts, ISSMs and compliance managers, reduced training time/need to learn our complicated way of using GitLab, improved compliance, etc. GitLab is an ITSM tool built to track trouble tickets - not designed to support complex risk management, incident response and robust compliance operations. We've figured out how to make GitLab to a lot of things, but the more we establish "workarounds" that push the limits of the GitLab interface, the less user friendly it becomes. We are digging a hole.*	x	x					
Risk Management App Front-End GUI Designed for Efficiency, Clarity, and Error Prevention	Build Beta Version of TBD Risk Management Application Front-end/GUI	*First version of the to-be SecOps Management application "smart GUI", whose elements are structured specifically to guide users to make better risk-based decisions without requiring them to search for instructions. moves GitLab one layer below.*	*This will significantly improve the usability and as a result, effectiveness and perceived value of our threatAlert tool - translating what currently exists in rules and playbooks into a (mostly) machine-guided human experience.*			x				
Risk Management App Front-End GUI Designed for Efficiency, Clarity, and Error Prevention	Deploy/GA Release of Risk Management Application Front-end/GUI	*First version of the to-be SecOps Management application "smart GUI", whose elements are structured specifically to guide users to make better risk-based decisions without requiring them to search for instructions. moves GitLab one layer below.*	*This will significantly improve the usability and as a result, effectiveness and perceived value of our threatAlert tool - translating what currently exists in rules and playbooks into a (mostly) machine-guided human experience.*				x			
Multitenancy	Establish Multitenant Deployment Architecture	*Establish a true multi-tenant solution for ThreatAlert and the Armory where Armory tenant data (or customer tenant data) and reports can be viewed and reported on uniquely.*	*Enable functional and extensible SecOps and significantly reduce the LOE for onboarding and supporting Managed Armory customers. In addition, once we have this model architected, it's a model that can be sold directly to government agencies wanting to run their own multi-tenant SecOps. (Currently, to support Armory tenants (including managed ATOs who need operations and reports that reflect only the information about their system), the POA&M and reports have to be manually edited to remove data about other systems.*	x	x					
Multitenancy	Build Beta Version of TBD Multi-tenance version of Armory for testing	*First version of the to-be multi-tenant architecture where the data and status of all "tenant" systems (hosted and managed) can be viewed uniquely, without touching the information about other tenants.*	*I believe this will become a sticking point for the government - especially DOD - and should be a priority item. Even for hosted tenants, we should have the ability to view their system data (vulnerability data, scan data, inventory data, POA&M data, future compliance validation data, etc.)*			x				
Multitenancy	GA Release of TBD Multi-tenance version of Armory for testing	*Releasable version of the to-be multi-tenant architecture where the data and status of all "tenant" systems (hosted and managed) can be viewed uniquely, without touching the information about other tenants.*	*I believe this will become a sticking point for the government - especially DOD - and should be a priority item. Even for hosted tenants, we should have the ability to view their system data (vulnerability data, scan data, inventory data, POA&M data, future compliance validation data, etc.)*				x			
ATOM Front End ("Productized ATOM)	Establish a GUI-driven ATOM/system deployment application front-end	*Anywhere we are using CLI, we might consider something less raw that actually guides users*	*(I see this as lower priority as this is one of the last things any external user would need to be able to do)*				x			
ATOM Front End ("Productized ATOM)	Beta release/testing of the GUI-driven ATOM	*Anywhere we are using CLI, we might consider something less raw that actually guides users*	*Puts the machine more in charge, reduces human error, protects against missed steps, etc.*					x		
ATOM Front End ("Productized ATOM)	GA Release of the GUI-driven ATOM	*Anywhere we are using CLI, we might consider something less raw that actually guides users*	*Puts the machine more in charge, reduces human error, protects against missed steps, etc.*						x	
Customer Feedback Portal	Establish customer input portal and formalize a feature priorization process	*Establish a public-facing portal (could also have an in-boundary portal) to give users an easy way to share feedback.*	*This can be combined with a bug bounty input portal - giving our customers a lower friction way to share their ideas or issues. They can always enter a system specific request, but it would be better to have a broader review of issues since features one customer wants are often things others also want.*	x						
Make Playbooks Easily Exportable	Make playbooks exportable in Word or PDF format as a first step	*Currently, there is no real training or manual to help our SecOps and security engineers understand our tooling. This is a step-1 (in what needs to be a multi-step journey) toward translating the gold buried within out "application" to a format better designed for human consumption.*	*Online guidance and content is excellent and needs to remain/exist, but isn't a great primary approach to supporting new users struggling to use our tooling. Lots of studies show a significant decline in cognition for things read online versus on paper. It's just a fact - as much as we'd like for digital content to be all we need. For heady subject matter and complex instructions, jumping around through links and wading through complex playbooks isn't the ideal for human users. In addition, Markdown is literally a different language, with unique syntax - increasing the cognitive load even more, and reducing the chances that users will find and understand what they need. .*	x						
"Smart" Playbooks - giving users complete set of actions per use cases (GUI or Artifact Output)	Build a model (possibly AI) to better leverage playbooks - that can query all playbooks and return a complete guide for common use cases in actionable format	*Currently, users must navigate pages of content and follow multiple links, requiring them to synthesize large amounts of information.*	*Money saved directly (less training needed) and indirectly (less re-work, fewer mistakes, more efficient SecOps team). Also, increased customer satisfaction. Improved customer experience. Reduced LOE required for new employee onboarding. Reduced user-error created problems.*		x					
Flexible "Service Bus" Tool Connector Platform (e.g. API Bus :))	Architect/Design a more robust connector platform that makes tool or capability plug-and-play more feasible	*Establish a modernized version of a Service Bus that makes plug and play for specific commercial tooling and/or capability modules easier and faster.*	*There is tremendous value in removing dependencies on any specific commercial tool, and establishing a construct that cares less about specific tools and more about ingesting or collaborating with various types of commercial tools or capabilities as a part of a flexible "GSS" stack. This can reduce the cost of delivery, remove barriers related to competitor conflicts, remove vendor lock-in, and better evolve within the broader cybersecurity landscape.*	x						
Flexible "Service Bus" Tool Connector Platform (e.g. API Bus :))	Build a more robust connector platform that makes tool or capability plug-and-play more feasible	*Establish a modernized version of a Service Bus that makes plug and play for specific commercial tooling and/or capability modules easier and faster.*	*There is tremendous value in removing dependencies on any specific commercial tool, and establishing a construct that cares less about specific tools and more about ingesting or collaborating with various types of commercial tools or capabilities as a part of a flexible "GSS" stack. This can reduce the cost of delivery, remove barriers related to competitor conflicts, remove vendor lock-in, and better evolve within the broader cybersecurity landscape.*		x					
Flexible "Service Bus" Tool Connector Platform (e.g. API Bus :))	Deploy a more robust connector platform that makes tool or capability plug-and-play more feasible	*Establish a modernized version of a Service Bus that makes plug and play for specific commercial tooling and/or capability modules easier and faster.*	*There is tremendous value in removing dependencies on any specific commercial tool, and establishing a construct that cares less about specific tools and more about ingesting or collaborating with various types of commercial tools or capabilities as a part of a flexible "GSS" stack. This can reduce the cost of delivery, remove barriers related to competitor conflicts, remove vendor lock-in, and better evolve within the broader cybersecurity landscape.*			x				
Machine Compliance Status Verification (ASA - Automated Security Analyst)	A machine-executable verification of compliance posture	*This is already in the works with early versions of "ASA"*	*This kind of capability is fundamental to FedRAMP 20x and future-proofing our approach to risk management and compliance*	x						
Machine ConMon Report Creation (Customer Friendly)	Not sure where we are with this - Customer friendly, professional, intuitive report	*This is already in the works I believe…*		x						

Slack Canvas to Track the Roadmap

I have created a Slack Canvas for the strategic roadmap in the stackArmor internal Armory Slack channel to encourage team collaboration on the roadmap! (Above is the header image for the roadmap Slack canvas - presentation matters!!!)

Roadmap | Summarized, Epic Level Prioritization

(This doesn't yet contain the latest RFC requirements - but contains critical capabilities to help future-proof our offering in a strategic manner - addressing issues that will increasingly limit our ability to scale and succeed including critical security (multi-tenancy), usability and vendor lock-in issues.)

Epic	General Capability	Description	Value/Benefit (Who Cares and Why?)	Priority
Risk Management App Front-End GUI Designed for Efficiency, Clarity, and Error Prevention	**(Obfuscating GitLab at least 1 layer below being "the" layer)** **Design Risk Management Application Front-end**	*Using Focus Groups (Analysts and ISSMs), finalize a design for a Risk Management Application Front-end (between the user and GitLab) - then build iteratively getting user feedback throughout.*	*Improved UX especially for analysts, ISSMs and compliance managers, reduced training time/need to learn our complicated way of using GitLab, improved compliance, etc. GitLab is an ITSM tool built to track trouble tickets - not designed to support complex risk management, incident response and robust compliance operations. We've figured out how to make GitLab to a lot of things, but the more we establish "workarounds" that push the limits of the GitLab interface, the less user friendly it becomes.*	**1**
Multitenancy	**Establish Multitenant Deployment Architecture**	*Establish a true multi-tenant solution for ThreatAlert and the Armory where Armory tenant data (or customer tenant data) and reports can be viewed and reported on uniquely.*	*Enable functional and extensible SecOps and significantly reduce the LOE for onboarding and supporting Managed Armory customers. In addition, once we have this model architected, it's a model that can be sold directly to government agencies wanting to run their own multi-tenant SecOps. (Currently, to support Armory tenants, including managed ATOs who need operations and reports that reflect only the information about their system, the POA&M and reports have to be manually edited to remove data about other systems. I believe this will become a sticking point for the government - especially DOD - and should be a priority item. Even for hosted tenants, we should have the ability to view their system data (vulnerability data, scan data, inventory data, POA&M data, future compliance validation data, etc.)*	**1**
Customer Feedback Portal	**Establish customer input portal and formalize a feature priorization process**	*Establish a public-facing portal (could also have an in-boundary portal) to give users an easy way to share feedback.*	*This can be combined with a bug bounty input portal - giving our customers a lower friction way to share their ideas or issues. They can always enter a system specific request, but it would be better to have a broader review of issues since features one customer wants are often things others also want.*	**1**
Make Playbooks Easily Exportable	**Make playbooks exportable in Word or PDF format as a first step**	*Currently, there is no real training or manual to help our SecOps and security engineers understand our tooling. This is a step-1 (in what needs to be a multi-step journey) toward translating the gold buried within out "application" to a format better designed for human consumption.*	*Online guidance and content is excellent and needs to remain/exist, but isn't a great primary approach to supporting new users strugglint to use our tooling. Lots of studies show a significant decline in cognition for things read online versus on paper. It's just a fact - as much as we'd like for digital content to be all we need. For heady subject matter and complex instructions, jumping around through links and wading through complex playbooks isn't the ideal for human users. In addition, Markdown is literally a different language, with unique syntax - increasing the cognitive load even more, and reducing the chances that users will find and understand what they need.*	**1**
Flexible "Service Bus" Tool Connector Platform (e.g. API Bus :))	**Architect/Design a more robust connector platform that makes tool or capability plug-and-play more feasible**	*Establish a modernized verison of a Service Bus that makes plug and play for specific commercial tooling and/or capability modules easier and faster.*	*There is tremendous value in removing dependencies on any specific commercial tool, and establishing a construct that cares less about specific tools and more about ingesting or collaborating with various types of commercial tools or capabilities as a part of a flexible "GSS" stack. This can reduce the cost of delivery, remove barriers related to competitor conflicts, remove vendor lock-in, and better evolve within the broader cybersecurity landscape.*	**1**
Machine Compliance Status Verification (ASA - Automated Security Analyst)	**A machine-executable verification of compliance posture**	*This is already in the works with early versions of "ASA"*	*This kind of capability is fundamental to FedRAMP 20x and future-proofing our approach to risk management and compliance*	**1**
Machine ConMon Report Creation (Customer Friendly)	**Not sure where we are with this - Customer friendly, professional, intuitive report to replace weekly and monthly SecOps manual reports**	*Need SecOps reports designed for ISSMs and humans who aren't necessarily spending all day in our tool stack (they have lots of other responsibilities)*	*Machine-generated dashboards or reports are low-hanging fruit, since we already have all of the data needed. Working with analysts we can create actual reports that summarize the most critical information instead of expecting customer teams to wade through GitLab alone and synthesize the data themselves. This would be a huge win, and add significant perceived value (and stickiness) to our customer base - as well as being a great sales tool to convince prospective customers that we make it "easy".*	**1**
"Smart" Playbooks - giving users complete set of actions per use cases (GUI or Artifact Output)	**Build a model (possibly AI) to better leverage playbooks - that can query all playbooks and return a complete guide for common use cases in actionable format**	*Currently, users must navigate pages of content and follow multiple links, requiring them to synthesize large amounts of information.*	*Money saved directly (less training needed) and indirectly (less re-work, fewer mistakes, more efficient SecOps team). Also, Increased customer satisfaction. Improved customer experience. Reduced LOE required for new employee onboarding. Reduced user-error created problems.*	**2**
ATOM Front End ("Productized ATOM)	**Establish a GUI-driven ATOM/system deployment application front-end**	*Anywhere we are using CLI, we might consider something less raw that actually guides users*	*(I see this as lower priority as this is one of the last things any external user would need to be able to do) - Puts the machine more in charge, reduces human error, protects against missed steps, etc.*	**3**

Pitched a Strategic Approach to Product Management

Built on my original strategic product management plan - presented on product management to stack/Tyto leadership to try to get everyone invested and on the same page.

- *Re-visited mission, vision, resourcing, and path forward*
- *Updated my SWOT analysis from the original (standard for strategic plan)*
- Established "what's next" since original plans were shelved
- Clarified Project Management v Engineering Management v Product Management to try to fix these being conflated

Pitch for Strategic Approach to Product Management Continued…

Where We Are Today - Do We Have a "Product"?

We have designed and developed a growing suite of modules, all with specific purposes, capabilities, feature backlogs, and release dates. We are reliant on having the latest version of this specific suite of modules, in addition to a stack of commercial tools, to deliver cybersecurity engineering and compliance services to our customers – so we do have a product. It doesn't have to be commercially available or offered externally as a product to be a product per se. So in this way, YES, we have a product – and at this point, it comes in 3-ish flavors. And while our product users are primarily internal, they are increasingly external as customers want more autonomy and flexibility to manage their systems with our "product." This is our product (or product suite):

ThreatAlert® Armory Armory 20x

- **Threat Alert Platform** – Products + Services
  - **ThreatAlert Security Workbench** (TSW)
    - **TSR** (ThreatAlert Se
    - **TST** (ThreatAlert Se
    - **TCS** (ThreatAlert Co

Further, with 20x, we've rapidly increased the speed with which we "product" – making it increasingly difficult to support if we don't ac

1/27/26

" Overview Draft

stackArmor — A TYTO ATHENE COMPANY

ThreatAlert® Security Workbench | Cybersecurity Management Platform

Dashboard | Security Lens | ConMon Lens

ATOM - ATO Machine | ISV Secure Environment Establishment

TCS - Container Scanner | Container Hardening

TSR - Serverless Relay | Automated SecComms

TST - Security Toolbox | ConMon Reporting & Artifact Generation

ThreatAlert GitLab — ITSM — GitLab

TSW | Security Workbench — GSS — Customer Application — ISV SaaS

ThreatAlert

Armory Brand Guide (We Do Have One)

Product Core Messaging

What? — The Armory is a purpose-built General Support System (GSS) and managed services offering that lowers the barrier to entry to FedRAMP and other regulatory compliance standards for Cloud Service Providers (CSPs) – especially those that are smaller or have emergent technology solutions and need a path to serve the federal market. It provides all the compliance, documentation, audit and architecture support to get CSP systems Authorized to Operate (ATO).

Why? — The Armory was built to bring software solutions to the federal government with lower cost and lower management effort and CSPS and agencies - while maintaining the integrity of the risk posture and compliance operations of cloud solutions.

How? — The Armory does this through the machine-aided generation of an accredited environment (using ATOM for Google) and deployment boundary architected for zero trust and furnished with a feature-rich tech stack of expertly deployed state-of-the-art cybersecurity tools. The tools stack includes commercial off-the-shelf (COTS) solutions selected and configured to meet specific NIST 800-53 cybersecurity controls. stackArmor's proprietary ThreatAlert tooling then extends the capabilities of COTS tools by orchestrating security operations and findings management (FML), as well as providing additional automations around container scanning (TST), multi-cloud relays from SIEM solutions to Armory Alerts (with additional support for incidents) - (TSR), and ConMon reporting/FedRAMP program ConMon artifact generation. Ultimately with The Armory, customer cloud CSPs or government off-the-shelf (GOTS) cloud solutions are able to be monitored, assessed and maintained to FedRAMP, DOD IL, FISMA, CMMC, and other regulatory standards.

For Whom? — The Armory paves the road to compliance for commercial CSPs that don't have the experience or resources to navigate the FedRAMP process - and therefore are missing out on the opportunity to serve federal agencies in meeting their missions.

What's in it for Customers? — Built on top of Google Cloud Platform, this future-defining solution provides coverage for roughly 60% of FedRAMP baseline controls for federal agencies and CSPs, leveraging various degrees of automation and machine-driven findings management to act as a force multiplier for security operations teams. The remaining 40% of controls, including documentation package development and audit support, is further delivered by stackArmor expert services and SME reach-back - for 100% control support coverage. Combined with stackArmor's SME services, The Armory customers receive significant support for 100% of the controls in the FedRAMP baseline, allowing CSPs to focus instead on their application and customers.

Armory Product Positioning

Competitive Differentiators:

- First (& Only) High Google Accelerator Platform
- Armory is an evolved solution based on 12+ years of lessons learned deploying ThreatAlert on AWS
- Turn Key Program (To Be Capability)
- User Friendly ConMon Management UI (To Be Capability)

Core Capabilities:

- Access Control | Account Management
- Threat Modeling
- Continuous Monitoring
- Vulnerability Scanning
- SIEM, Logging and Analysis
- Container Hardening
- Endpoint Protection
- Supply Chain
- Zero Trust

Core Benefits:

Core Personality:

Armory is the Easy Accelerator with future proofing Tech Chops

Armory is the answer the government and tech community have been looking for, being at the forefront of building an automation and machine-driven platform on which GRC operations will continue to improve in the ease with which they are delivered AND the breadth and depth with which they solve critical cybersecurity and compliance conundrums of yesterday.

Imagery and Visual Aesthetic:

Crisp & Clean - concise and to the point images
Digital Energy/Movement - images that reflect

Key User Profiles (Internal & External):

- Architects
- Security analysts
- Security engineers
- ISSM

Secondary User Profiles

- Assessors
- PMO
- Agency AOs

Armory Customer Journey Map

Hosted & Managed ATO Customers

1. Establish Partnership & Initial Discovery
2. ISV Shores up Significant Application-Level Gaps
3. ISV Deployed to Compliant Armory Landing Zone
4. Hosted ISV Promoted to Production Armory
5. ISV Operational Readiness and ConMon Initiation
6. ISV (SaaS) Assessment & Authorization
7. ISV in Marketplace, Ongoing Armory ConMon

Armory Offering Today: SWOT Analysis

Original presentation: Oct 1, 2024
Current presentation: Oct 2, 2025
Red – new
~~Strikethrough~~ – no longer true

STRENGTHS

- Tons of experience with compliance, FedRAMP, the PMO, 3PAOs, and Engineering
- Significant experience delivery ConMon services
- Reputation as leaders in this industry
- Phenomenal engineering skills and commitment to build the right solution (Added some new automations)
- Excitement over the future prospects
- ~~Existing, waiting customer ISVs~~ – we have customers!
- No real GCP competitors
- 20x Pilot participants, with some early wins in the things 20x is looking for

WEAKNESSES

- No Sponsor
- Lack of GCP experience – unknowns of building a new product with new tech (don't know what we don't know)
- Lack of experience being a product company (can't be managed like billable services engagements)
- Lack of recent experience building/running a compliance program as an authorized vendor (not like other stackArmor engagements)
- Limited team resources, ~~no ISSM, no PM~~ no test team or ARB, no formal strategic roadmap, many resources are task switching
- Loss of Asa
- Communication gap between what we do and how others/the PMO perceive what we do

S W SWOT ANALYSIS T O

THREATS

- ~~Backlog of PMO, 3PAOs and other variables that impact promised delivery timelines~~
- Unknowns of ~~Rev 5~~ future and 20x assessment standards
- Significant (ongoing) disruptive FedRAMP changes
- Multiple competitors across other clouds – and our competitors are also now focused on automation…
- ~~Pending~~ Election (DOGE) – induces caution in spending
- Current economic environment
- Lack of buy-in from ISVs that want their logo in the marketplace

OPPORTUNITIES

- Noone is great at CX in this arena, so we could make that a differentiator (if we put intention into it)
- AI – being on the ground floor means we can design and build what customers want and need!!
- "Automation" for many non-tech controls (e.g. IR, PS, IR, AT) would be a big differentiator and close a gap
- Being first to market with the GCP cloud plus targeted marketing could result in a ~~really big~~ win
- ~~OSCAL~~ Automation – our component approach and 20x POC automations makes us a leader

1/27/26

The information contained in this presentation is proprietary to stackArmor, Inc and should not be distributed or shared without stackArmor's written permission.

9

Pitch for Strategic Approach to Product Management Continued…

Industry Trends or Known Pain Points

Things that will help inform strategic decisions…

- Automation and machine-driven capabilities for anything that can be automated is going to be key to survival
- Architecturally, hyper-converged "appliance" model solutions are being replaced with de-coupled API/service and query-based models where capabilities are initiated and content accessed on the fly as needed
- Analysts are missing issues (missing POA&M item
- to failure to fully leverage the capabilities
- Customers (ISSMs and Operators) have asked for
- sessions to figure out playbooks – where our valu
- Customers want options in security tools (e.g. Git
- Employees have repeatedly asked for more traini
- newer tech (which an intuitive "product" would h
- Customers frequently ask for specific compliance

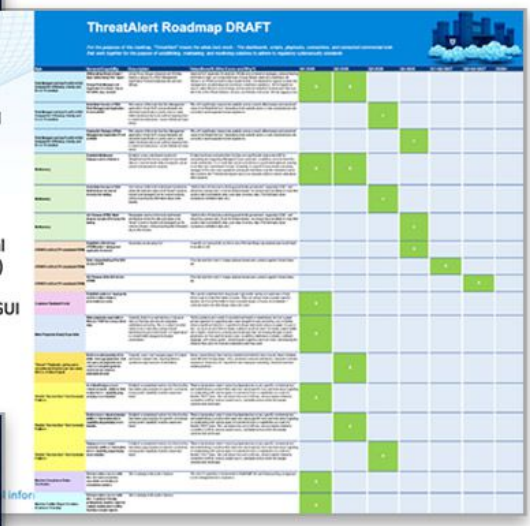
Output: *(other issues?)*

January 27, 2026 Proprietary and confidential information of stackArmor

Roadmap Epics to Consider

(I am aware some of these have been on the radar, or exist in early draft versions)

- Risk Management App Front-End GUI Designed for Efficiency, Clarity, and Error Prevention (to address GitLab usability)
- Multitenancy Architecture
- ATOM Front End ("Productized" ATOM with an intuitive Turbotax-like GUI)
- Establish customer feature request/input portal (with a review board and prioritization process)
- Make Playbooks Easily Exportable (using AI?)
- "Smart" Playbooks – Guidance is Baked into a GUI
- Flexible "Service Bus" Tool Connector Platform
- Machine Compliance Status Verification
- Machine ConMon Report Creation (Customer Friendly)



What's Next?

- Agree to some "intentional" actions to shift to a product mindset where the "what" (product strategy and UX) matter as much as the "how" (tactical and engineering brilliance)
- Schedule blue-sky brainstorming meeting(s) to discuss (and eventually prioritize) key strategic features?
- Establish a product management recurring (monthly) innovation meeting to track progress against plans and coordinate against our mission – identifying single topics per meeting as well to review architectural plans: e.g. architecture to support current (muti-tenant) customers, architecture for increased interoperability (removing dependencies), architecture for future automations and AI, architecture for scalability, architecture for usability, etc.
- ?

January 27, 2026 Proprietary and confidential information of stackArmor

Questions?

Thank You

www.stackarmor.com

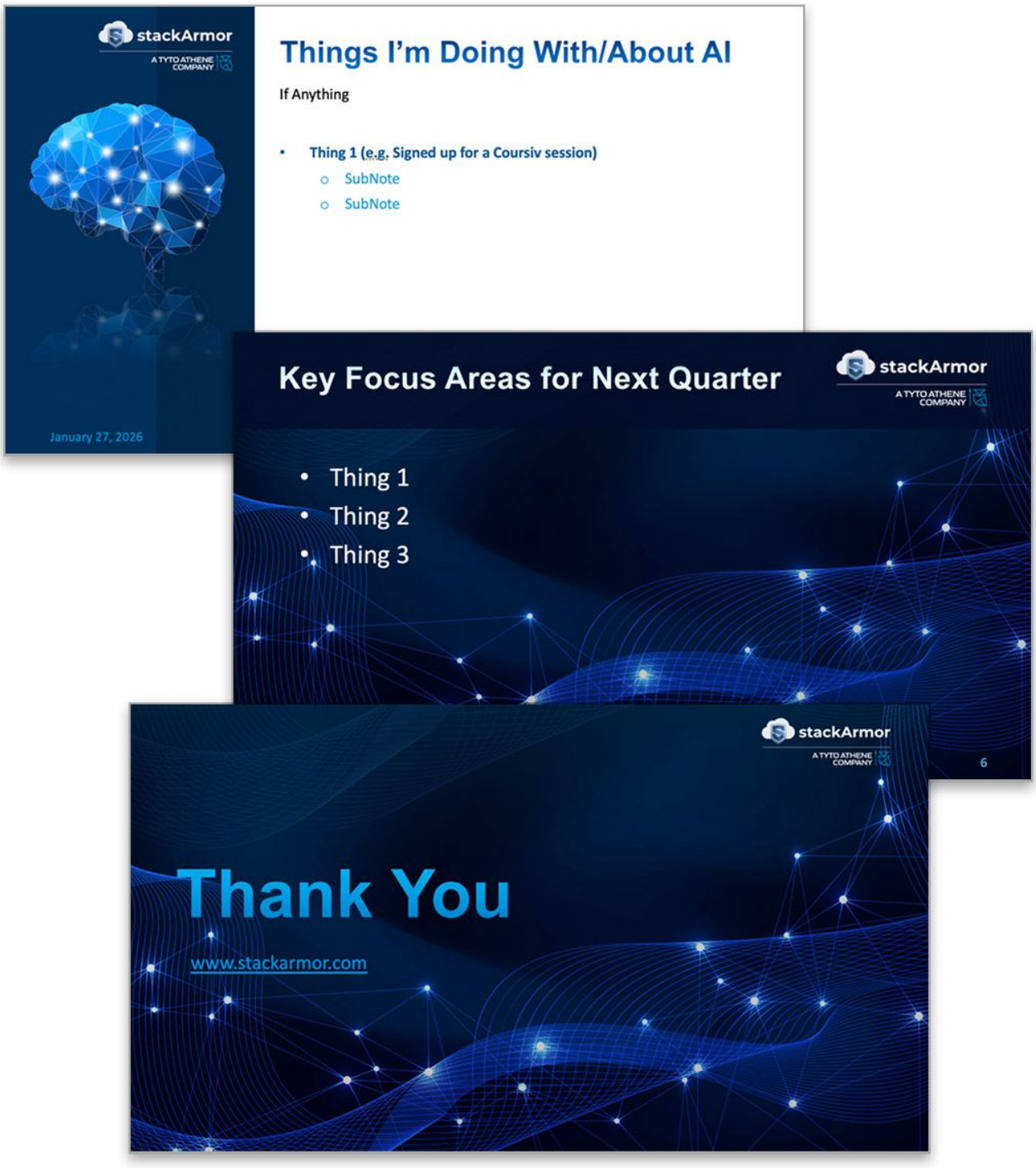
Engagement Management Leadership

Culture of Accountability - Created EM QPR with Reporting Template

To build and model a culture of accountability focused on CX - I established a quarterly program review for the EM team.

- *Held our first QPR in September.*
- *Will hold our next QPR in February.*

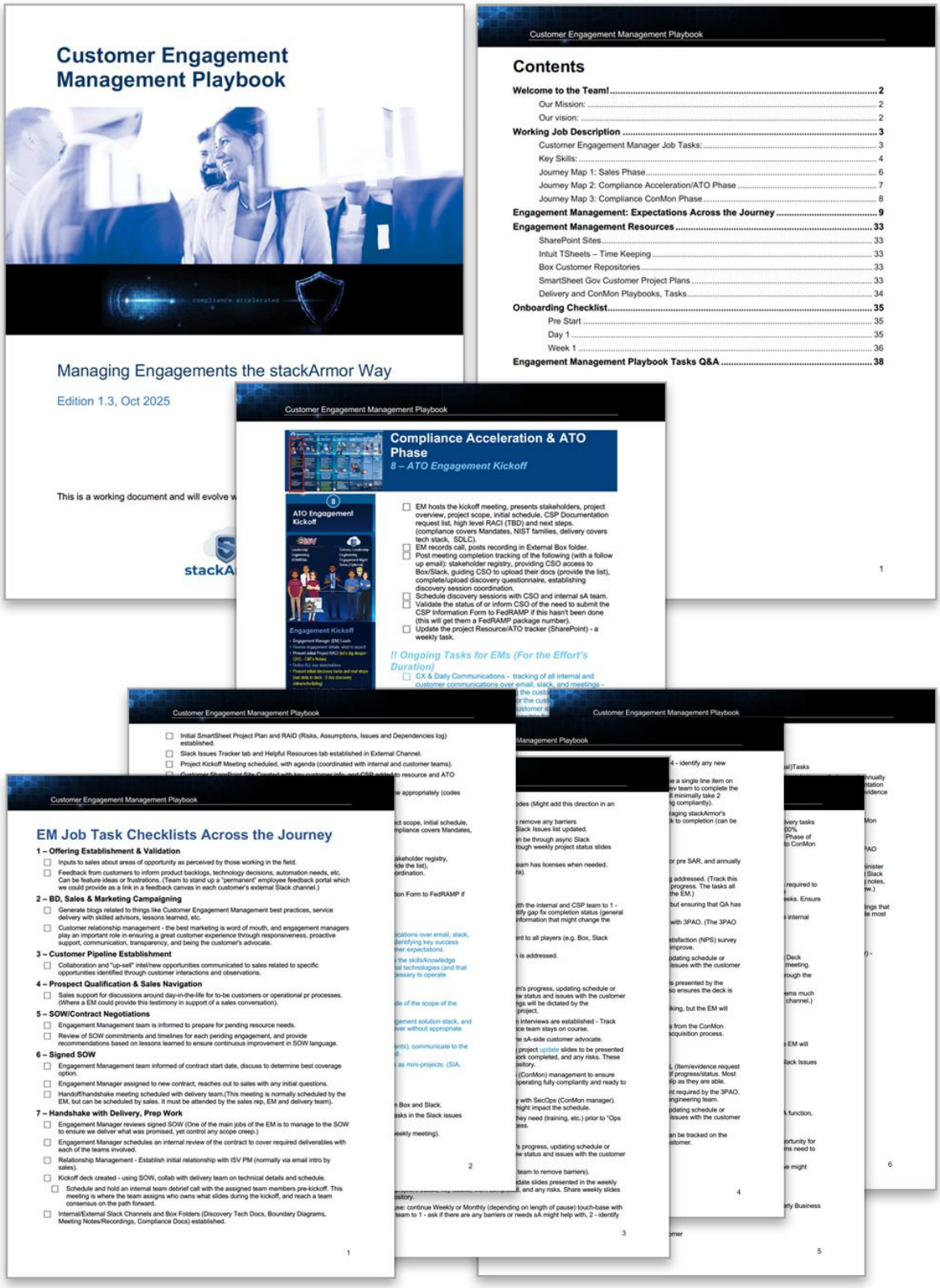
EM Quarterly Program Review Continued…



Revised the Engagement Management Playbook

Revised the Engagement Management Playbook I authored to switch tasks to checklists, adding an appendix that lists all checklists across each phase in an engagement.

- *The playbook is a foundation for onboarding, training, job description creation, cross-team collaboration and role clarification.*
- *This has provided structure and standardization to the EM role.*
- *Current version is located on the CX/EX Intranet Site.*



Supported Gecko as “sA Assessment Lead” Through 3PAO Assessments

Took on the lion’s share of the work quarterbacking the 3PAO assessment, which has been quite chaotic - has provided great insights into ways we can improve.

- I became the translator between engineering and EIT with our first trial of AI-collected evidence. (image below is just one of many communications I drove to help pave the way)
- This has been a particularly challenging engagement, with team members - many of whom are less than cooperative.
- So far, I believe we’ve salvaged our relationship with the customer - fingers crossed.

Example of many communications between me and all parties involved in the assessment:

Technical Evidence

Gecko Robotics, Oct 24, 2025

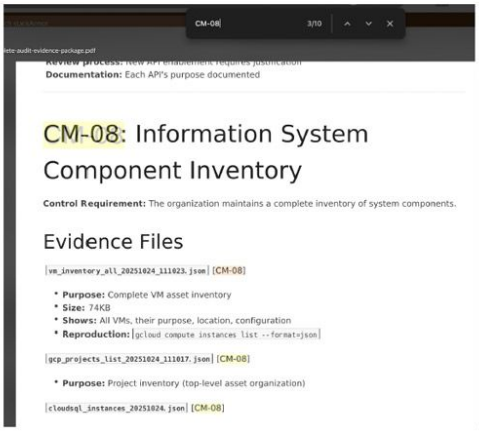
The engineering team has gathered evidence and made it available in an automated fashion using an API – which should make it easier to review. Everything the team needs to review this evidence is laid out in the attached pdf file that is in the Ext CSP-Evidence Box folder:

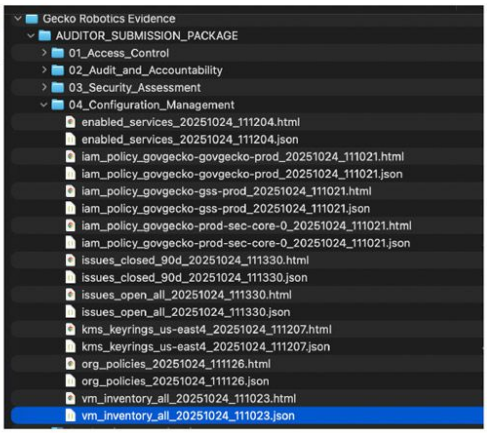
govgecko-complete-audit-evidence-package.pdf

All the evidence findings can be viewed using crtl+f/cmd+f search in the pdf on mac or on chrome (any browser) on windows. It has all been automated via the API from gecko gitlab/gcp. The jsons were also converted to html for most of the items so they can be viewed in a browser with timestamps. The webpage can also be searched as well if the team would rather not view json files.

Example:

As an example, doing a control search the CM-08 allows the team to see the json/html evidence files or html which can be clicked to review the evidence.





Let me know if you have any questions or issues, and we would be happy to jump on a quick call to make sure you’ve got everything you need!

Sarah

Supported Gecko (and Qanapi) as Primary EM

Provided white glove advisory support to both, but more for Gecko, investing to help expand our work with them.

- Produced FastPass Justification paper with content from team
- This doc was to help Gecko address a finding with EIT, and attempt to prevent the need for additional tooling changes (e.g. Yubikey)

Created Architecture Justification Paper for Gecko

Provided white glove advisory support to Gecko, investing to help expand our work with them.

- Produced GCP Isolation paper with content from the team to help get approval on their solution architecture for their “AO” (BPMI)

gecko robotics

GCP

GCP Isolation & Separation Architecture Justification for Authorizing Official (AO)

GCP Isolation & Separation Architecture Justification

Introduction and Purpose

This document provides a security-based justification that the Google Cloud Platform (GCP) hosting environment—configured under Assured Workloads and aligned to DoD Impact Level 4 (IL4) requirements—meets the relevant isolation and separation requirements in NN-801 Cloud Computing Security Requirements Guide and the DoD Cloud Computing SRG v1 Release 5 (v1R5), section 5.2.2.3, without the need for dedicated physical infrastructure.

Summary Position

- Physical separation is not required for Impact Level 4 (IL4) systems per DoD CC SRG v1R5 5.2.2.3; logical, virtualized, hardware-enforced separation is acceptable.
- GCP Assured Workloads and Google’s software-defined community cloud model are already DISA-authorized at IL5, demonstrating stronger separation controls than IL4 requires.
- GCP’s technical implementation (confidential computing, secure boot, vTPMs, NAP, VPC SC, hypervisor isolation, microarchitectural mitigations) provides stronger security guarantees than physical separation alone.
- Sole-tenant nodes are available as an option, but they add cost and operational complexity and are not required for IL4.

Applicable Requirements

DoD CC SRG v1R5 (2024)

5.2.2.3 (Physical Separation Requirements): IL4 systems may leverage multi-tenant cloud infrastructure when separated via NSA-approved virtualization and isolation mechanisms. Only IL6/NSS systems require dedicated hosting or physical isolation.

NN-801 Cloud Enclosure

Requires logical tenant isolation, robust hypervisor security, boundary protection, continuous monitoring, and incident response integration. Does not mandate physical separation for non-NSS workloads.

Google Cloud IL4/IL5 Provisional Authorization

GCP’s IL5 PA demonstrates that DISA has already validated GCP’s isolation, virtualization, and community cloud model at the higher assurance level (IL5).

GCP Isolation & Separation Architecture Justification

GCP Isolation and Security: Technical Implementation Overview

These IL5-validated controls exceed requirements for IL4.

Virtualization & Hardware-Rooted Isolation

- Google-designed KVM-based hypervisor with hardened security modules.
- Memory isolation enforced in hardware (Intel VT-x/AMD-V) preventing cross-tenant memory leakage.
- Microarchitectural protections against Spectre, Meltdown, L1TF, MDS, Retbleed.

Cryptographic Isolation

- Per-resource encryption keys, CMEK, and CSEK support.
- Full-stack encryption: at-rest, in-transit, inter-service RPC.

vTPM, Secure Boot, and Workload Integrity

- Verified Boot ensures signed, validated host firmware and OS.
- vTPM provides per-VM integrity measurements.

Network Isolation

- SDN fabric (Andromeda) ensures tenant routing isolation.
- VPC Service Controls provide software-defined boundaries and anti-exfiltration protections.

Assured Workloads:

- Enforces U.S.-only personnel, region lock, and DoD IL4/IL5 requirements.
- Software-Defined Community Cloud segmentation.

Why Physical Separation Is Not Required for IL4

- DoD CC SRG explicitly permits multi-tenant infrastructure at IL4 when NSA-approved isolation is used—already validated at IL5 for GCP.
- IL4 system processes no NSS data, so IL6-level physical separation triggers do not apply.

3

GCP Isolation & Separation Architecture Justification

Alternate (Optional) Solution: Sole-Tenant Node Mitigation

If used, Google’s Sole-Tenant Node configuration introduces the following pros and cons.

- Provides single-tenant physical hosts.
- Adds 40–70%+ cost.
- Increases operational overhead.
- Reduces elasticity/autoscaling.

Conclusion / Recommendation to AO

Based on DoD and NN-801 criteria, GCP’s IL5-authorized isolation architecture fully satisfies IL4 requirements without requiring physical separation. The system benefits from hardware-rooted integrity, advanced SDN isolation, and Assured Workloads boundaries.

Recommendation

The recommended path forward is to approve continued operation in current IL4 configuration. This decision is done knowing that sole-tenant nodes may be used if agency-specific policy requires, but they are not required by DoD SRG.

References

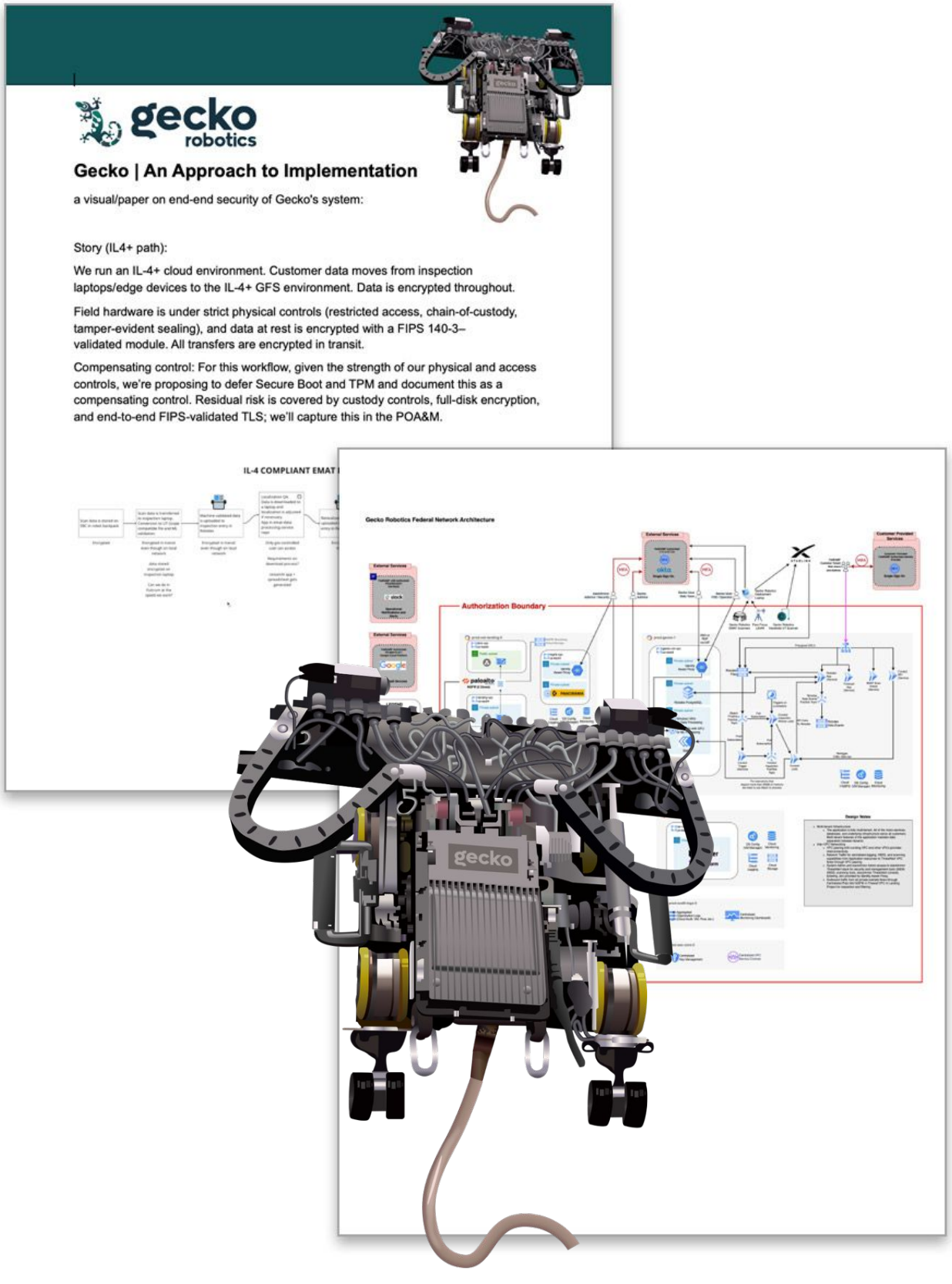
- DoD Cloud Computing SRG v1R5: https://public.cyber.mil/dccs/dccs-documents/
- GCP Assured Workloads: https://cloud.google.com/assured-workloads
- GCP Security Infrastructure Design: https://cloud.google.com/security/infrastructure/design
- Shielded VMs: https://cloud.google.com/compute/shielded-vm
- Encryption by Default: https://cloud.google.com/security/encryption-by-default
- VPC Service Controls: https://cloud.google.com/vpc-service-controls
- Sole-Tenant Nodes: https://cloud.google.com/compute/docs/nodes/sole-tenant-nodes

4

Produced Architecture Implementation Paper for Gecko

Provided white glove advisory support to Gecko, investing to help expand our work with them.

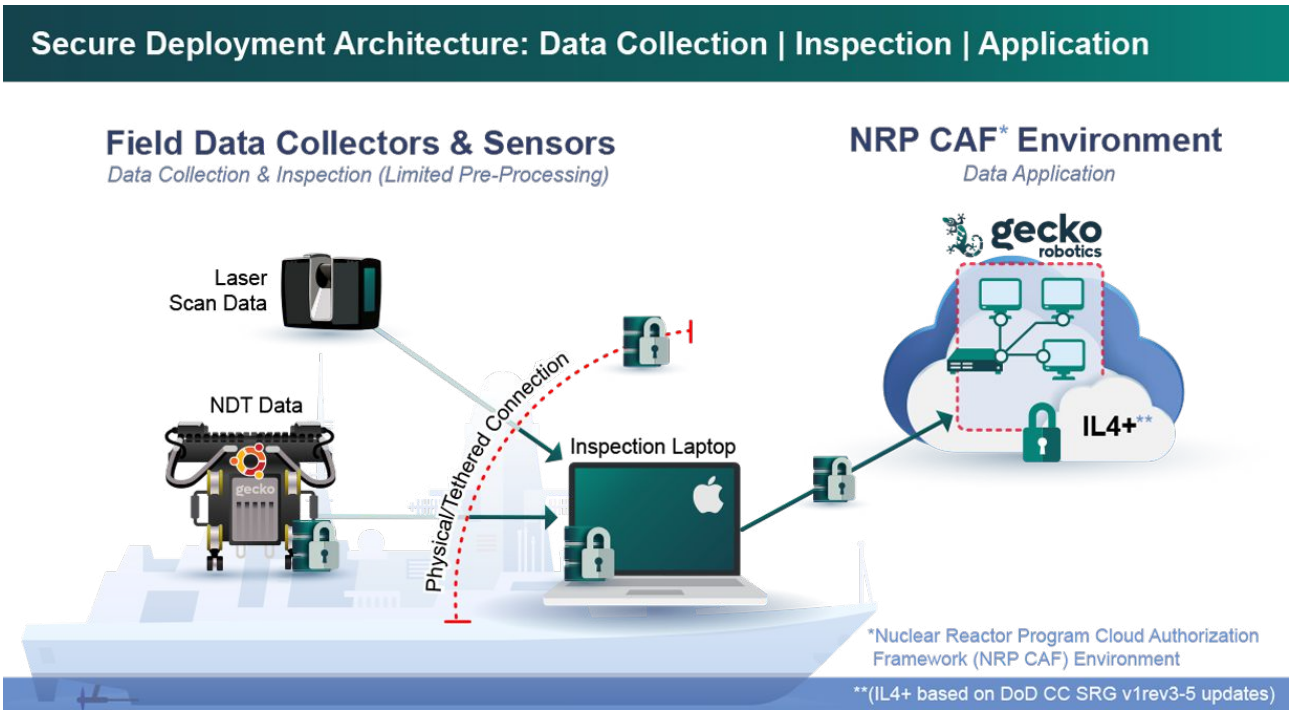
- To support their exchanges with BPMI, put together this paper to articulate their architecture.
- Illustrated their robot as a CX “plussing” opportunity



Produced IoT vs Boundary Illustration for Gecko

Illustrated a specific concept for Gecko to help them communicate clearly how IoT devices are outside of the boundary.

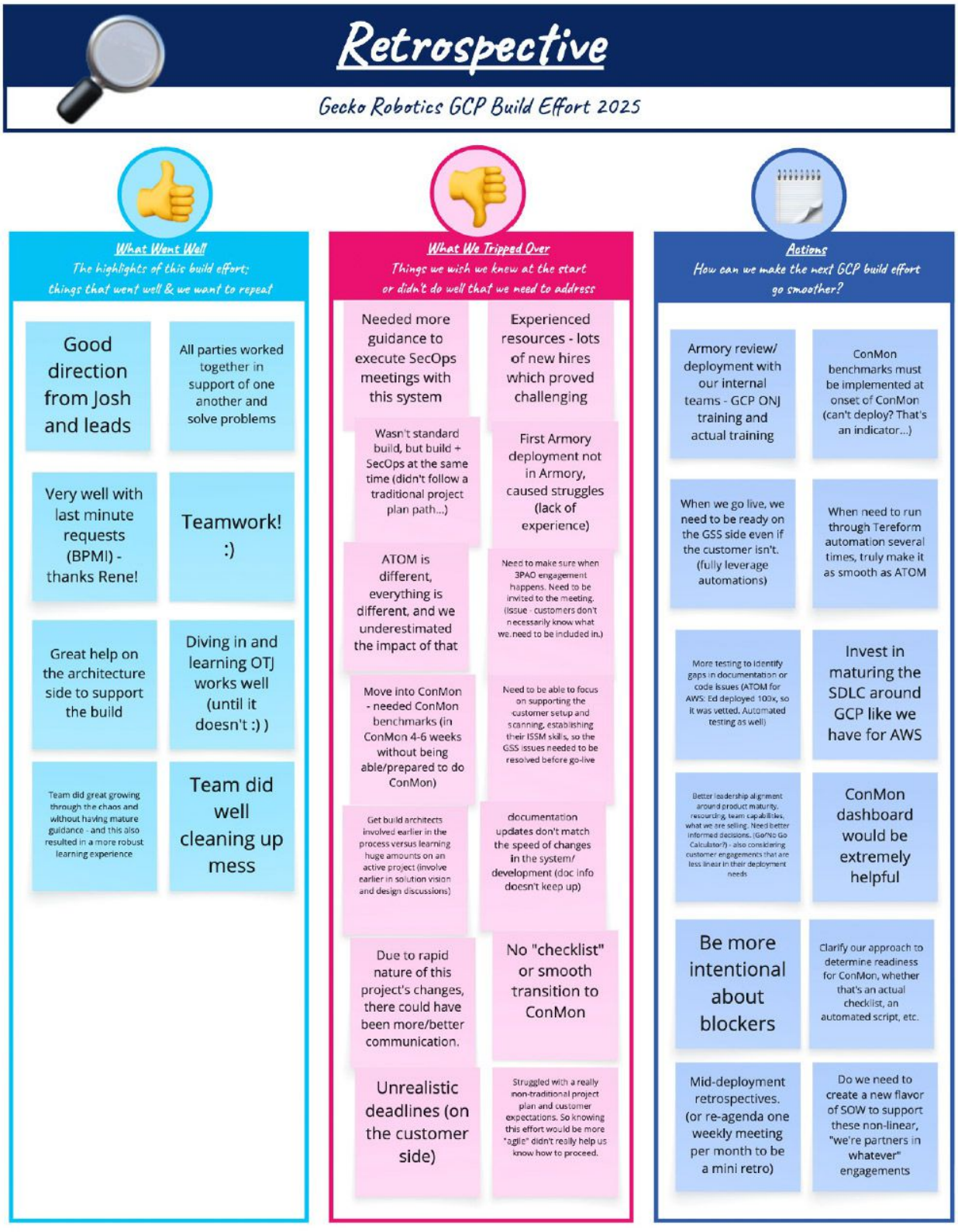
- Gecko was having difficulty getting their potential sponsor to understand how the various sensors and IoT devices fit into the broader secure boundary
- The illustration helped them get their sponsor to a “yes”!



Held Critical Retrospective on Gecko post Build Phase (with Interactive Miro Board)

Taught myself Miro, and used it to create an interactive retrospective board used with the team to identify lessons learned.

- Gecko is a project that is unfortunately defined by lessons we must learn and not repeat.
- This approach worked great, and allowed us to generate action items that are still being implemented.



Customer/User/Employee Experience

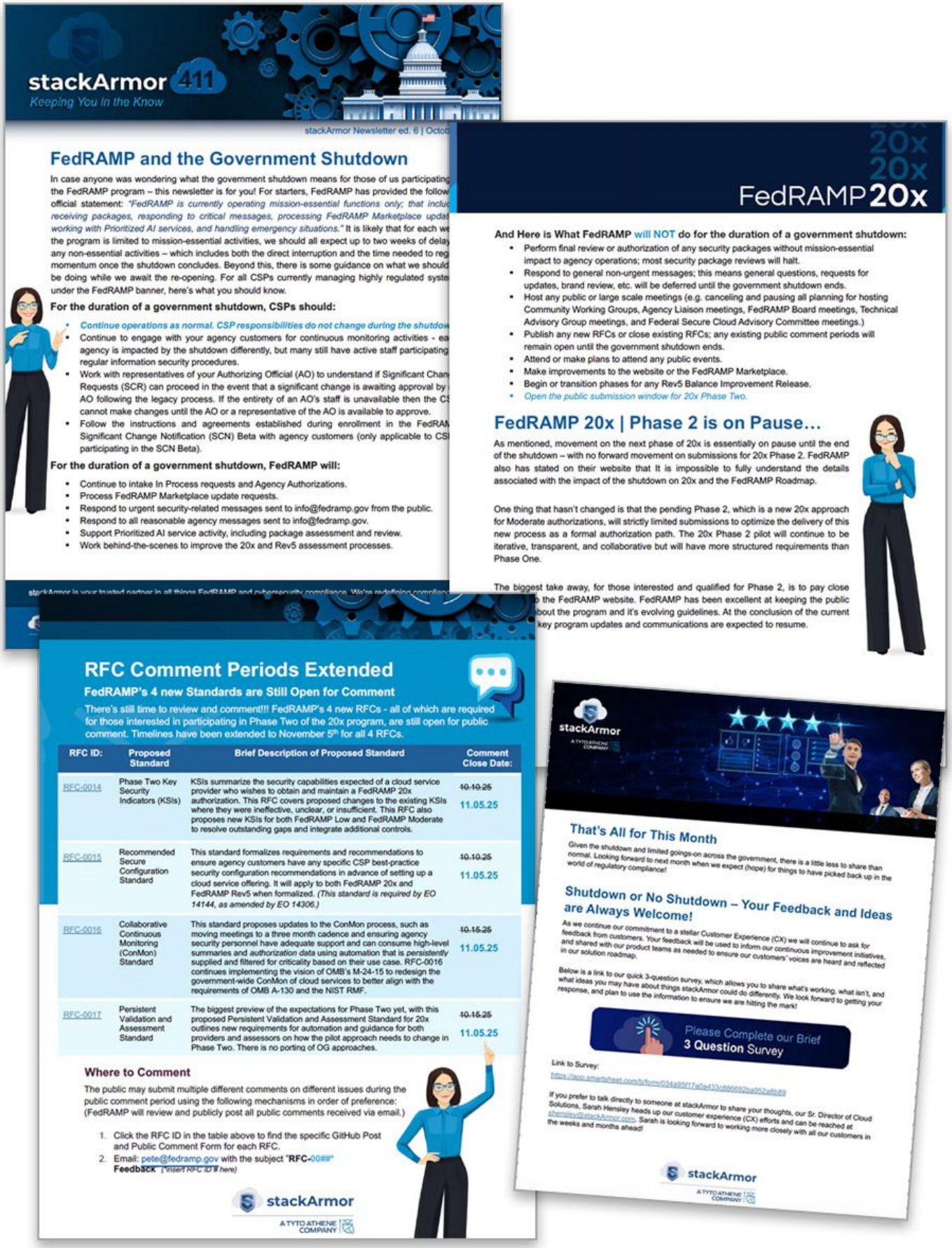
Took Initiative to Create a Delighful CX Through a Monthly Customer Newsletter

To continue my commitment to increasing our value/stickiness, I stuck with our monthly newsletter - authoring, editing, designing, and fully producing it each month.

- *I generated or selected/collaboratively edited content.*
- *Worked with Tyto to also expand our audience to a **HubSpot** library…*
- *Created many custom illustrations each month.*
- *Received a request in the fall by a customer that wanted to subscribe - **an indication that it is valuable and making an impact!!!***

September 2025 Newsletter

October 2025 Newsletter



stackArmor 411
Keeping You in the Know

stackArmor Newsletter ed. 6 | Octob

FedRAMP and the Government Shutdown

In case anyone was wondering what the government shutdown means for those of us participating the FedRAMP program – this newsletter is for you! For starters, FedRAMP has provided the follow official statement: *"FedRAMP is currently operating mission-essential functions only; that inclu receiving packages, responding to critical messages, processing FedRAMP Marketplace updat working with Prioritized AI services, and handling emergency situations."* It is likely that for each we the program is limited to mission-essential activities, we should all expect up to two weeks of delay any non-essential activities – which includes both the direct interruption and the time needed to reg momentum once the shutdown concludes. Beyond this, there is some guidance on what we should be doing while we await the re-opening. For all CSPs currently managing highly regulated syste under the FedRAMP banner, here's what you should know.

For the duration of a government shutdown, CSPs should:

- *Continue operations as normal. CSP responsibilities do not change during the shutdow*
- Continue to engage with your agency customers for continuous monitoring activities - ea agency is impacted by the shutdown differently, but many still have active staff participating regular information security procedures.
- Work with representatives of your Authorizing Official (AO) to understand if Significant Chan Requests (SCR) can proceed in the event that a significant change is awaiting approval by AO following the legacy process. If the entirety of an AO's staff is unavailable then the CS cannot make changes until the AO or a representative of the AO is available to approve.
- Follow the instructions and agreements established during enrollment in the FedRA Significant Change Notification (SCN) Beta with agency customers (only applicable to CS participating in the SCN Beta).

For the duration of a government shutdown, FedRAMP will:

- Continue to intake In Process requests and Agency Authorizations.
- Process FedRAMP Marketplace update requests.
- Respond to urgent security-related messages sent to info@fedramp.gov from the public.
- Respond to all reasonable agency messages sent to info@fedramp.gov.
- Support Prioritized AI service activity, including package assessment and review.
- Work behind-the-scenes to improve the 20x and Rev5 assessment processes.

FedRAMP 20x

And Here is What FedRAMP will NOT do for the duration of a government shutdown:

- Perform final review or authorization of any security packages without mission-essential impact to agency operations; most security package reviews will halt.
- Respond to general non-urgent messages; this means general questions, requests for updates, brand review, etc. will be deferred until the government shutdown ends.
- Host any public or large scale meetings (e.g. canceling and pausing all planning for hosting Community Working Groups, Agency Liaison meetings, FedRAMP Board meetings, Technical Advisory Group meetings, and Federal Secure Cloud Advisory Committee meetings.)
- Publish any new RFCs or close existing RFCs; any existing public comment periods will remain open until the government shutdown ends.
- Attend or make plans to attend any public events.
- Make improvements to the website or the FedRAMP Marketplace.
- Begin or transition phases for any Rev5 Balance Improvement Release.
- *Open the public submission window for 20x Phase Two.*

FedRAMP 20x | Phase 2 is on Pause…

As mentioned, movement on the next phase of 20x is essentially on pause until the end of the shutdown – with no forward movement on submissions for 20x Phase 2. FedRAMP also has stated on their website that It is impossible to fully understand the details associated with the impact of the shutdown on 20x and the FedRAMP Roadmap.

One thing that hasn't changed is that the pending Phase 2, which is a new 20x approach for Moderate authorizations, will strictly limited submissions to optimize the delivery of this new process as a formal authorization path. The 20x Phase 2 pilot will continue to be iterative, transparent, and collaborative but will have more structured requirements than Phase One.

The biggest take away, for those interested and qualified for Phase 2, is to pay close the FedRAMP website. FedRAMP has been excellent at keeping the public bout the program and it's evolving guidelines. At the conclusion of the current key program updates and communications are expected to resume.

RFC Comment Periods Extended

FedRAMP's 4 new Standards are Still Open for Comment

There's still time to review and comment!!! FedRAMP's 4 new RFCs - all of which are required for those interested in participating in Phase Two of the 20x program, are still open for public comment. Timelines have been extended to November 5th for all 4 RFCs.

RFC ID:	Proposed Standard	Brief Description of Proposed Standard	Comment Close Date:
RFC-0014	Phase Two Key Security Indicators (KSIs)	KSIs summarize the security capabilities expected of a cloud service provider who wishes to obtain and maintain a FedRAMP 20x authorization. This RFC covers proposed changes to the existing KSIs where they were ineffective, unclear, or insufficient. This RFC also proposes new KSIs for both FedRAMP Low and FedRAMP Moderate to resolve outstanding gaps and integrate additional controls.	~~10.10.25~~ 11.05.25
RFC-0015	Recommended Secure Configuration Standard	This standard formalizes requirements and recommendations to ensure agency customers have any specific CSP best-practice security configuration recommendations in advance of setting up a cloud service offering. It will apply to both FedRAMP 20x and FedRAMP Rev5 when formalized. *(This standard is required by EO 14144, as amended by EO 14306.)*	~~10.10.25~~ 11.05.25
RFC-0016	Collaborative Continuous Monitoring (ConMon) Standard	This standard proposes updates to the ConMon process, such as moving meetings to a three month cadence and ensuring agency security personnel have adequate support and can consume high-level summaries and *authorization data* using automation that is *persistently* supplied and filtered for criticality based on their use case. RFC-0016 continues implementing the vision of OMB's M-24-15 to redesign the government-wide ConMon of cloud services to better align with the requirements of OMB A-130 and the NIST RMF.	~~10.15.25~~ 11.05.25
RFC-0017	Persistent Validation and Assessment Standard	The biggest preview of the expectations for Phase Two yet, with this proposed Persistent Validation and Assessment Standard for 20x outlines new requirements for automation and guidance for both providers and assessors on how the pilot approach needs to change in Phase Two. There is no porting of OG approaches.	~~10.15.25~~ 11.05.25

Where to Comment

The public may submit multiple different comments on different issues during the public comment period using the following mechanisms in order of preference: (FedRAMP will review and publicly post all public comments received via email.)

1. Click the RFC ID in the table above to find the specific GitHub Post and Public Comment Form for each RFC.
2. Email: pete@fedramp.gov with the subject "**RFC-**00##" **Feedback** *(* insert RFC ID # here)*

stackArmor
A TYTO ATHENE COMPANY

stackArmor
A TYTO ATHENE COMPANY

That's All for This Month

Given the shutdown and limited goings-on across the government, there is a little less to share than normal. Looking forward to next month when we expect (hope) for things to have picked back up in the world of regulatory compliance!

Shutdown or No Shutdown – Your Feedback and Ideas are Always Welcome!

As we continue our commitment to a stellar Customer Experience (CX) we will continue to ask for feedback from customers. Your feedback will be used to inform our continuous improvement initiatives, and shared with our product teams as needed to ensure our customers' voices are heard and reflected in our solution roadmap.

Below is a link to our quick 3-question survey, which allows you to share what's working, what isn't, and what ideas you may have about things stackArmor could do differently. We look forward to getting your response, and plan to use the information to ensure we are hitting the mark!

Please Complete our Brief **3 Question** Survey

Link to Survey:
https://app.smartsheet.com/b/form/034a95f17a0a433c886692baf952a8b8

If you prefer to talk directly to someone at stackArmor to share your thoughts, our Sr. Director of Cloud Solutions, Sarah Hensley heads up our customer experience (CX) efforts and can be reached at shensley@stackArmor.com. Sarah is looking forward to working more closely with all our customers in the weeks and months ahead!

stackArmor
A TYTO ATHENE COMPANY

November/December 2025 Newsletter

stackArmor 411
Keeping You in the Know

stackArmor Newsletter ed. 7 | November/December 2025

Things are Happening in the World of Compliance!

As we approach the holidays, the team at stackArmor wanted to share one last 2025 newsletter. Since the last edition, the government shutdown that paused many FedRAMP program activities has ended, and some exciting things have been happening with stackArmor's Armory offering.

1 Armory 20x — *The Armory20x ATO Accelerator on Google Cloud has been **Authorized** as part of the FedRAMP 20x Pilot Program (Phase 1).*

2 Armory — *The Armory FedRAMP High Rev 5 Accelerator on Google Cloud is now **In Process** in the marketplace.*

A Lesson in the Importance of Acting with Integrity in Compliance Program Operations

Adhering to FedRAMP and DoD IL compliance standards for systems that are processing federal data under a government-issued Authorization to Operate (ATO) isn't just about taking the necessary steps to pass audits. Lest anyone has lost sight of the programs' key objectives - protecting federal data - the recent indictment of a government contractor for intentionally misleading agencies (and 3PAOs) about matters of compliance should serve as a stark "cold splash of water to the face" reminder.

Danielle Hillmer, a former senior compliance manager from Virginia has been charged by the Justice Department with major government fraud, wire fraud, and obstructing federal audits. According to FedScoop, she has been accused of carrying out a "multi-year scheme to mislead agencies over a government contractor's compliance with security controls." Specifically, she allegedly ***concealed the cloud service offering's noncompliance with FedRAMP security controls*** and the DoD's RMF by deceptively claiming security controls were in place (per the SSP) all while knowing they weren't.

So here's the thing. There is simply no win in this kind of deceptive behavior. Even if the deceptive practices hadn't been caught, what good is passing a cybersecurity audit while having your system positioned perfectly to make the ten o-clock news for losing millions of customer records or leaking critical national security information? In this case, the cost carries the possibility of **20+ years in prison**. This is a good reminder that having an authorized system isn't just about passing audits - it's about doing the right thing, protecting government data, mitigating risk, and doing it with transparency to accurately represent the security and risk posture of a system for its government users.

stackArmor — A TYTO ATHENE COMPANY — www.stackarmor.com

20x 20x FedRAMP 20x

FedRAMP 20x | Phase 2 Updates

As FedRAMP 20x got back into the swing of things following the government shutdown, Phase 2 initiatives are back in motion! That said, FedRAMP has shared that most CSPs wanting a 20x Moderate authorization must wait until the Phase 2 Pilot systems have paved the way for a more standardized approach, when the process is simpler and critical third-party tools are more widely available.

Further, unlike Phase 1 which allowed any interested CSP to submit a package, Phase 2 is NOT open to the public. Only CSPs who submitted a complete package during Phase 1 that was not rejected or withdrawn are eligible to apply for the Phase 2 Pilot. Of the 23 CSPs that meet this criterion (which includes stackArmor's Armory 20x), FedRAMP is targeting approximately 10 Moderate pilot authorizations to participate in Phase 2 (3 of which have already been selected!). This is based on an understanding that even many systems that obtained a 20x Low authorization under Phase 1 won't be able to meet all of the requirements and timelines outlined for Phase 2. The FedRAMP website has more details about the application (and pilot proposal) process.

Finally, Phase 2 is actually being broken up into 2 sub-phases or Cohorts. Cohort 1 in December resulted in the selection of the first 3 participants with Cohort 2 following in January.

Phase 2: Cohort 1 Participants Already Selected

As previously mentioned, there are 3 CSPs that have already gone through the application and proposal review process and been selected to participate in Phase 2! The first 3 CSP participants include:

- Confluent Cloud for Government
- Meridian LMS
- Paramify Cloud

Phase 2: Cohort 2 Coming in January 2026

Beginning January 5th, applications will be accepted for the remaining 7 CSP slots for Phase 2.

Date	FedRAMP 20x Phase 2 Milestones
Nov 18, 2025	Phase 2 pilot authorization requirement and other criteria are finalized and published
Dec 1 - Dec 5, 2025	Cohort 1 application period, up to 3 cloud services selected
[illegible]	Cohort 2 application period, up to 7 cloud services selected
[illegible]	[illegible] for Cohort 1

There's a New POA&M Template

FedRAMP Releases Version 3.0 of the Official POA&M Template

Anyone supporting FedRAMP authorized systems is undoubtedly familiar with the Plan of Action and Milestones (POA&M) - a templated artifact required by FedRAMP (as well as other compliance standards) to track risk remediation and mitigation activities for system findings.

According to the official "Record of Changes" tab in this new version, the changes include the addition of an Instructions Tab, the consolidation of reporting fields, and the simplification of input requirements. A couple changes of note:

- There is a new PL-2 Findings tab used to capture documentation deficiencies in the SSP and related attachments
- A few columns, including Planned Milestones, Milestone Changes, and Auto Approve, appear to have been removed from the new template

As stackArmor works through all of the changes, the team will also be working to update our automations to support this new template wherever it is possible to do so. In the meantime, system ISSMs will need to pay careful attention to the new POA&M to ensure it is accurately completed as a part of the monthly reporting requirements.

POA&M

stackArmor — A TYTO ATHENE COMPANY

2025 FORUM IT100 AWARD WINNER

CONGRATULATIONS!

JOHANN DETTWEILER
CISO
STACKARMOR, A TYTO ATHENE COMPANY

Johann Dettweiler Named to the 2025 FORUM IT100 List

While we often include insights FROM our CISO, this edition includes a shout out TO our CISO!

We are proud to share that Johann Dettweiler, our amazing CISO, has been named a 2025 FORUM IT100 Award recipient. The FORUM IT100 recognizes dynamic leaders who drive [illegible] advancement across government and federal technology through cutting-[illegible] innovation, and a commitment to giving back to the broader Federal [illegible]

While most of our customers have likely met Jo[illegible] across the industry for pioneering technical [illegible] spearheaded stackArmor's FedRAMP 20x pilot [illegible] compliance evidence, advanced DoD Zero Trust [illegible] platform, and championed AI governance align[illegible] challenging outdated compliance models while re[illegible]

"Johann's passion for innovation and his ability to [illegible] approach cybersecurity and compliance," GP Pal, [illegible] technical, designing compliance-as-code framework[illegible] that materially reduce operational burden while stren[illegible] helped equip the public sector to better protect sensitiv[illegible]

In addition to his technical leadership, Johann is a trust[illegible] technology ecosystem, consistently sharing expertise to [illegible] recognition by FORUM underscores stackArmor's comm[illegible] cybersecurity solutions that enable CSPs ad governme[illegible] compromising security or compliance. We are proud and [illegible]

stackArmor — A TYTO ATHENE COMPANY

stackArmor

One Last 2025 Call for Feedback and Ideas!

Please Complete our Brief 3 Question Survey

Wishing everyone the Happiest of holidays from your team at stackArmor!

Maintained End-to-End stackArmor Journey Maps

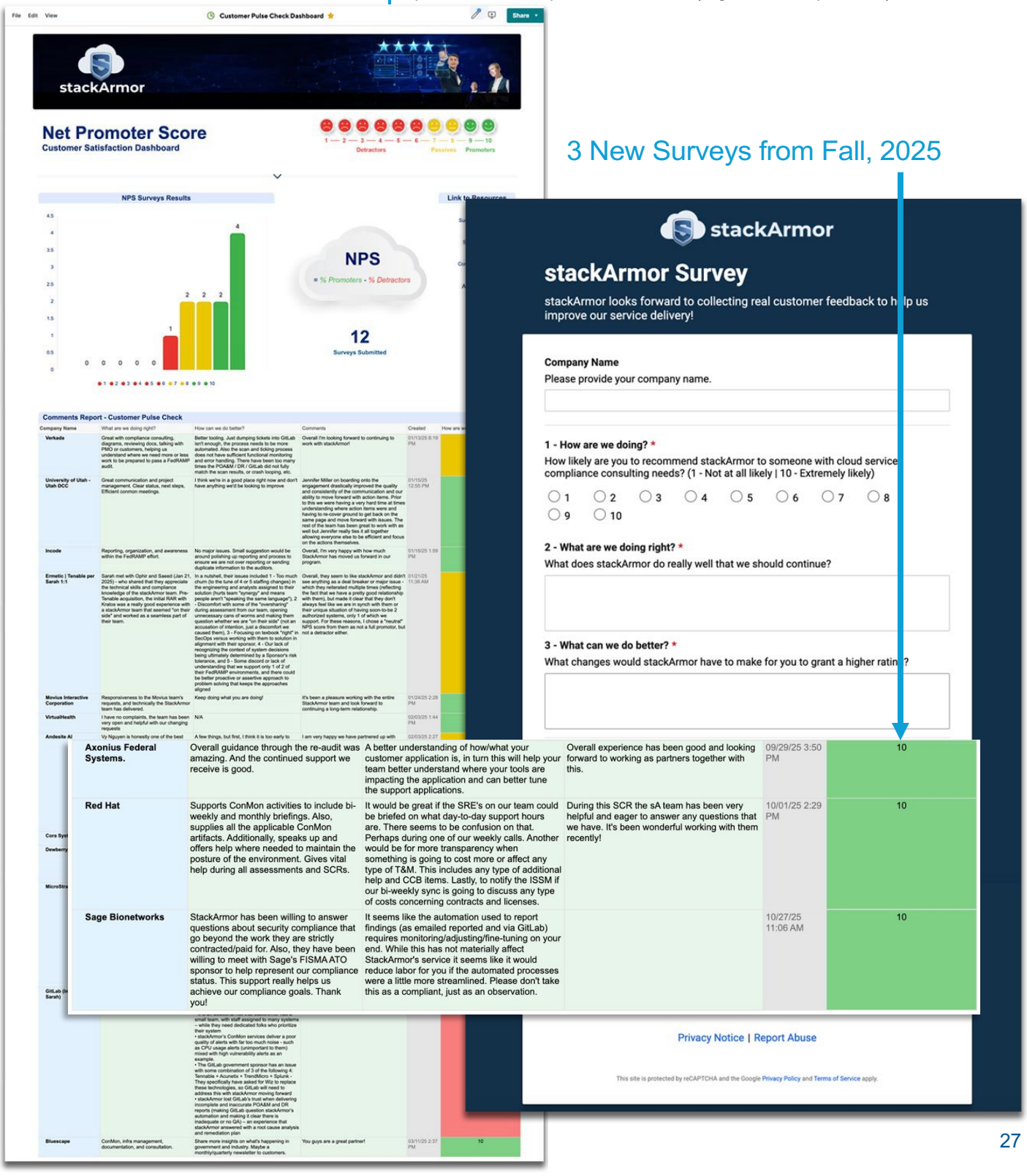
Updated all 3 Customer Journey Maps throughout the year (and fall)

- *These were originally created prior to August, then maintained and updated.*
- *Maps enable clear definition of roles/responsibility across teams, and activities all customers and team members can expect*
- *All journey maps are available on the CX/CI Intranet site.*

Continued CX Program with NPS-Based Customer Satisfaction Tracking

Updated our process to include an ask to customers to submit a survey annually, and after the build phase. (Average NPS is 9.1, which is excellent)

- *Axonius and Red Hat and Sage all provided us NPS scores of 10 in the fall! (Props to the EM team for this - none were mine ☺)*
- *Each Newsletter contains a link and call to action re: the survey.*
- *Program continues to inform new feature request tickets and product roadmap considerations (e.g. Wiz incorporation)*



Marketing & Content Development

Created Multiple Ad Mocks When the Marketing Agency Couldn't Hit the Mark

Even though I'm not official marketing, I was able to create much of the original messaging and the actual ad mocks used to create an ad campaign.

- *After multiple tries, a professional marketing agency was struggling to give us what we needed or wanted.*
- GP, Gabriela and I brainstormed, and decided the quickest way to get what we wanted was for me to translate our concepts into ad mocks.
- I took that and ran with it to get some "draft" ads - doing the heavy lifting of getting the basic imagery concepts and content correct (it's now in marketing's hands to do the fun work and re-create these in a high-res "polished" format ☺ - which I'm more than capable of doing… but ran out of bandwidth.

Produced Polished, Professional White Papers x2

Translated Johann's raw text into a high-quality artifacts, doing copy editing, copy creation, original illustrations, and design.

- *Took a plain text file, edited for clarity, designed and formatted for information chunking, and created all graphics to augment the words.*

Future of Compliance White Paper

Compliance-as-Code

Instead of writing prose implementation statements and manually gathering evidence for each control, stackArmor defines each requirement as a code artifact (i.e. a control). As the project documentation explains, rather than stating *"all GCP compute disks are encrypted with CMKs (Customer-Managed Keys)"* in a document and later proving it via ad-hoc checks, the team directly encodes this rule as an automated control with an associated query. For example, within Armory20x there is a control named "**gcp_compute_disk_encrypted_with_cmk**[8]". Each control includes the following:

- Descriptive title;
- Explanation of the requirement the control is designed to validate; and
- A reference to a SQL query.
  - For this control, the query checks every Google Cloud disk for a CMK encryption key.

In this example, the query (written in HCL/SQL within a module (mod)) selects all GCP disks and flags any disk that is in a "READY" state but lacking a KMS key as an "alarm" (meaning the resource is in a non-compliant state). By running this query continuously or on-demand, the system can instantly identify if any cloud disk violates the encryption requirement, and it provides a machine-readable result in JSON that identifies the state ("ok" or "alarm" with a reason) for each resource.

This small example illustrates the broader methodology:

> Every control is expressed as a structured query that returns a pass/fail status along with evidence details.

In addition, because the controls and benchmarks are defined declaratively

Metadata and Structure

The query-based controls are not just raw scripts; they carry metadata and are organized logically. Each control includes tags (for example, indicating the service area, severity, or mapping to compliance framework IDs) to assist with filtering and reporting. Controls are grouped into benchmarks which are hierarchically arranged sets that correspond to portions of the compliance framework.

In the Armory20x mod, controls are grouped under benchmarks for each KSI grouping or "family", which roll up into an overall FedRAMP 20x KSI benchmark. This hierarchy ensures the results can be viewed at multiple levels: you can see an overall compliance summary, each KSI domain's status, each individual KSI control check, and even drill down to the underlying evidence for a failing control.

Figure 2: Structure of 20x Benchmark > KSI Family/Group Benchmarks > Controls > Implementation Evidence

The output of a benchmark run is a structured JSON document that contains all this information:

- Summaries of how many controls passed or failed; and

ting ambiguity; it provides concrete "show me" program, the Armory20x repository included the eliverables"[9]. stackArmor believes this level of demonstrate its approach to the pilot program.

6

Rapid, Continuous Monitoring

The query-driven approach has many advantages including accuracy, speed and frequency. Automated controls execute in seconds, even when run as part of a large suite of dozens or hundreds of checks. This means an entire FedRAMP KSI assessment can be performed on demand or even scheduled to run continuously (e.g. nightly or whenever infrastructure changes).

The stackArmor team integrates these checks into its
Dashboard, which provides an interactive view of KSI co
stackArmor shares an example Armory20x KSI Compli
highlights the information and datapoints in a visual re

System stakeholders (security engineers, auditors, and
any time to see the up-to-date compliance posture,
yearly audit reports. Because the checks are automate
feedback loop. If a configuration drifts out of compli
immediately, reducing the window of vulnerability. Thi
with modern DevSecOps and Continuous Monitorin
controls are constantly enforced and verified.

As an overall benefit to security, this approach is inherently more resilient against tampering than traditional document-based evidence. Because results are drawn directly from live system queries and recorded in machine-readable formats, there is no opportunity to hand-pick screenshots or redact inconvenient details. The queries themselves are transparent, repeatable, and source-controlled, ensuring that
the evidence reflects actual syste

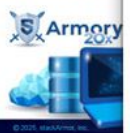
Eliminating Ambiguity and Manual Effort

From a process standpoint, query-based compliance s
time. stackArmor's philosophy is to **source-control comp**
been the domain of manually documented implement
much manual interpretation as reasonably possible.

By encoding the intent of each control in an unambi
subjective interpretation or error during an assessment
written policy is implemented; they can directly see
themselves). The use of open standards and tooling (S
transparent and extensible. Anyone (with appropriate a
to understand exactly what is being checked and ho
automation and facilitates collaboration.

For example - third-party assessors can suggest impro
assessment process. Once trust in the queries is establi
pull static artifacts from the environment. The queries a

*stackArmor's query-based methodology transforms co
heavy exercise into a proactive, data-driven discipline.*



[8] stackarmor.github.io/armory-20x-public/

© 2025, stackArmor, Inc.

Implementation in stackArmor's Armor

To illustrate how this methodology works in practi
implementation for the FedRAMP 20x pilot. The Armo
a comprehensive set of automated controls covering
controls are developed as a mod (module) and relea
public[11]. The repository's structure reflects the differe
supporting data. Summarized below are the key compo
of controls included.

- Core Cloud Infrastructure (Google Cloud Plat
  foundational cloud resources meet security req

  For example, controls verify disk encrypti
  configurations, log settings, etc., focusing on te

  These GCP-specific controls are defined with t
  This allows stackArmor to automatically enforce
  services (storage, compute, networking) and re
- Identity and Access Management (IAM) | The s
  Identity platform which manages user authent
  stackArmor integrated the Okta Security Tech
  benchmark within the mod[13]. Controls in the di
  accordance with DoD's STIG hardening guideli

  For instance, one the controls in this mod check
  for all users, a critical security indicator for identi
  query approach can extend to third-party Sa
  compliance guides like STIGs.

[11] stackArmor/armory-20x-public: Publicly accessible FedRAMP 20x pilot pr
[12] Okta's new Security Technical Implementation Guide (STIG) | Okta Secur
[13] At the time of the pilot, not every Okta STIG item was fully automatable, c
but the framework is in place to expand this coverage.

- DevSecOps and IT Service Management (ITSM) | Armory20x leverages a Git platform for code repositories and ITSM for change control, tickets, etc. The mod defines controls for the ITSM to ensure security and compliance in code and operational processes. These include checks on repository settings, branch protections, as well as operational metrics (e.g., ensuring security processes or approvals are in place for changes). Because some FedRAMP KSI requirements pertain to organizational processes (like incident response, configuration management, etc.), the ITSM controls help gather evidence of those processes (e.g., verifying if security issues are tracked and resolved within defined timeframes). By querying the ITSM's API for project settings and issue data, the system provides objective evidence for security objectives that have traditionally proven very difficult to automate.
- Vulnerability Management and Scanning[14] | To address controls related to system vulnerabilities and secure configurations, the Armory20x implementation leverages powerful network vulnerability scanning results. In addition, a custom plugin was developed to retrieve scan findings and configuration checks. As an example:
  - One control pulls data on whether servers have Federal Information Processing Standards (FIPS) 140-3 compliant configurations (as required by FedRAMP crypto standards) by referencing the system's STIG compliance scan results.
  - Another ensures that scheduled vulnerability scans are running and up to date.

  By automating the ingestion of scanner output, the solution integrates traditional vulnerability management into the continuous compliance framework.
- Security Operations Platform (ThreatAlert® Security Workbench) | Finally, stackArmor's own ThreatAlert Security Workbench (TSW), an operational suite of services for continuous monitoring and security operations, is subject to compliance checks. The mod includes controls to ensure that the security operations tooling itself is functioning correctly and following best practices.

  For example, controls verify that the TSW's scheduled jobs (which perform tasks like generating inventory and POA&M, running benchmarks, etc.) are operational, and that any findings are being properly ingested and tracked in the system.

  This is an important aspect often overlooked: not only must the cloud and IT components be secure, but the monitoring apparatus must also be intact and compliant. By treating TSW as another component to be continuously verified, stackArmor adds confidence that the compliance monitoring pipeline has no blind spots.

The previously mentioned components are integrated under a top-level FedRAMP 20x KSIs benchmark "**fedramp20x-ksis**" which ties together the controls relevant to each KSI domain. In practice, running this benchmark executes every underlying query across the GCP, Okta, ITSM, Vuln Scanner, and TSW, then compiles the results. The output is both human-readable (viewable in the web dashboard) and machine-readable (JSON files) for traceability. The repository's public dashboard (via a hosted page) shows an overview of how each KSI category is doing, presenting green for compliant (OK), red for issues (alarms), etc., and descriptions of each check.

[14] For the 20x submission, the Nessus plugin and control set were minimal but are expected to grow, and similar integrations for other scanning tools and system telemetry sources will be developed as needed.

9

Future of Compliance White Paper Continued

Transparency and Collaboration

Because the entire set of controls and their results are open-sourced, 3PAOs, FedRAMP officials, and even peer organizations can inspect and even reuse the code. In fact, once a complete vetting has occurred, stackArmor plans to publish some of the components, like the Okta STIG, to the public, open-source Hub for consumption by other organizations. This community-driven aspect means organizations won't have to reinvent the wheel for each compliance framework, they can leverage and customize pre-built query libraries that represent industry consensus or best practice for meeting standards.

Results and Validation in the Pilot

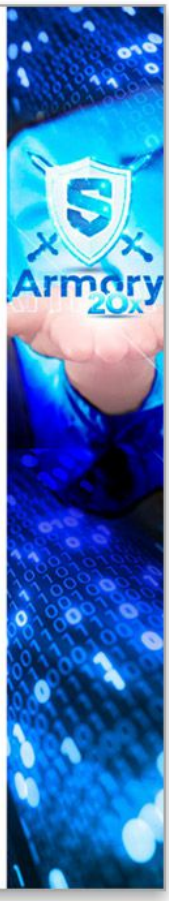
By the conclusion of the FedRAMP 20x Phase One pilot[15], stackArmor's Armory20x demonstrated a functioning model of continuous, query-based compliance for all required KSIs. The automated checks covered all ten KSI domains defined by FedRAMP, providing a one-stop, real-time view of the system's security posture. The final KSI assessment output consisted of the machine-readable results and a system declaration file, which together showed the system's compliance status without relying on extensive ancillary documentation. This was a significant departure from traditional FedRAMP packages that can consist of literally hundreds of pages of static documentation. Instead, Armory20x's evidence was largely in the form of data, queries and results that validated the status of each KSI.

An accredited Third-Party Assessment Organization (3PAO), Kratos, was engaged to evaluate the Armory20x system and its compliance deliverables. Over a series of collaborative reviews and validation exercises, the 3PAO scrutinized both the automated checks and the live environment. The timeline shows that initial KSI results were delivered by stackArmor on August 1, 2025, with updated results on August 6 after some iterations. By August 15, 2025, a final validation report was issued and was followed up with a formal 3PAO attestation for the FedRAMP 20x package on August 19, 2025. This attestation indicated that Kratos found the automated evidence credible and sufficient to meet the FedRAMP 20x Low requirements.

> *In other words, the query-based approach passed the test of a real-world audit.*

stackArmor will continue to update the repository as we address any findings and progress toward a full authorization. The repository will serve as a collaboration hub with the 3PAO and FedRAMP PMO, and it is publicly available to anyone who wishes to follow along in the process.

[15] August 19th, 2025



The Future is Automated, Continuous, and Data-Driven!

One of the most important outcomes of this pilot is the increased confidence in automation. By having a 3PAO validate the results, it set a precedent that automated, continuous controls can be trusted (given proper transparency and review) just like traditional evidence. StackArmor coined the term "**total equilibrium**" to describe our end goal; a state where:

> *Automation fully validates all KSIs and benchmark results stand alone without any additional artifacts.*

For stackArmor, the future is bright as we look to continue to establish trust in these repeatable, automated benchmarks, akin to how auditors develop trust in a repeatable process or tool. The pilot results suggest that this trust is achievable. Over time, as coverage is expanded and more controls are automated, the need for supplemental manual evidence should diminish further. Indeed, the Armory20x team plans to keep expanding the scope and depth of validations, integrating more cloud services and more controls, such that eventually a complete, fully automated information system assessment is possible.

The current state of the project demonstrates that:

1. A significant portion of security compliance checks can be automated with query-based controls, even across diverse technology stacks;
2. The outputs are understandable and useful to both technical teams and auditors; and
3. An authoritative reviewer (3PAO) was able to rely on this approach to provide a letter of attestation, indicating regulatory acceptance of the methodology.

These are promising signs for the future of compliance. Building on this foundation, we now look at potential future paths to broaden and generalize the query-based compliance methodology beyond this initial pilot.

The Compliance Fabric: Weaving Security Data into Actionable Intelligence

While stackArmor has taken a novel approach to implementing open-source technologies in the environment, the tools are publicly availa
its ability to gather telemetry data across
it into meaningful data points that tie ba

Every modern system produces a torrent
and telemetry. On their own, these sour
navigate, inconsistent in format, and imp
Most organizations struggle to reconcile
or operations.

Armory20x utilizes the query-based com
its foundation the system uses The Ar
leverages tools and services, custom-bu
vulnerability findings, security agent aler
outputs into a consistent schema. This
modules, including the Finding Lifecycl

FLM plays a critical role as the connec
compliance reporting. It ingests results
and container scanners, then manages fi
is tracked, updated, and remediated ac
to system resources and GitLab issues,
reducing administrative overhead. The
consistent, and ready for use in compliai

This woven fabric of normalized data is
information is exposed as SQL, stackArm
warehouses that reflect the live state of

- Analysts can correlate control im
- Compliance managers can instan
- Auditors can query live data dire

When FedRAMP 20x launched its p
infrastructure in place to ingest the
FedRAMP KSIs. As the KSIs continue to
as new frameworks such as DoD Zero T
Armory20x can trivially extend the exis
approach positions us to perfectly addre
evolving threat landscape.

Our ability to weave security and compli
stackArmor to lead the next generation
that enables Armory20x customers to
efficiently, and gain visibility at a depth

Future Directions: Expanding Query-Based Compliance

The success of the FedRAMP 20x pilot opens the door to extending the query-based compliance methodology to additional frameworks and deeper levels of assurance. A number of future developments are on the horizon for stackArmor.

- **Full FedRAMP Baseline Coverage:** The 20x pilot focused on a limited set of KSIs (essentially a subset of controls for FedRAMP Low). A logical next step is to expand automated checks to cover the entire FedRAMP baseline. In practice, this means creating queries for hundreds of controls, beyond the "critical indicators" in the pilot. Many baseline controls are procedural or policy-oriented, which has posed a challenge in the past, but stackArmor now has an established a pattern of developing plugins that can be utilized to query information from all running services within a system boundary and is confident its approach can address these challenges. The open-source community is already moving in this direction; for example, there are open-source compliance mods that map AWS configurations to NIST 800-53 Rev.5 and even provide benchmarks for FedRAMP Low and Moderate (Rev.4) controls. stackArmor's own mod utilized queries from the official GCP compliance mod, as well as custom queries based on the unique environmental configurations. The future path will involve integrating broader benchmarks and tailoring for specific environments, eventually achieving complete coverage of all FedRAMP baseline requirements through code. Reaching full coverage will also involve further development of plugins to expand the ability to query the Information Technology Service Management (ITSM) and other security services running in the environment (e.g., SIEM, FIM, etc.). While in development of full coverage, even partial automation of the baseline will drastically reduce the effort to achieve and maintain FedRAMP authorizations.
- **DoD Zero Trust Architecture Compliance:** The U.S. Department of Defense's Zero Trust Architecture (ZTA) strategy calls for a robust set of capabilities across multiple pillars (Identity, Device, Network, Application, Data, etc.) to eliminate implicit trust. Organizations aiming to comply with DoD Zero Trust guidelines face a broad and complex set of requirements, often outlined as capability roadmaps with numerous activities and checkpoints. A query-based methodology will be able to monitor Zero Trust adherence in real time.
  - For example, a library of checks corresponding to each of the DoD Zero Trust capabilities which will verify things like: all user accounts have MFA enabled and recent credential rotation (Identity pillar), all devices on the network are known and meet security baselines (Device pillar), all network traffic is passing through defined inspection points (Network pillar), sensitive data is encrypted at rest and in transit (Data pillar), and so on.

Many of these checks overlap with existing controls (indeed, Zero Trust is an amalgamation of best practices from various domains). With cloud-centric operations, it's feasible to query identity providers, endpoint management systems, network configurations, and application settings to gather evidence of Zero Trust controls. Future versions will allow organizations to maintain a Zero Trust compliance dashboard analogous to the KSI dashboard, showing their live status against each pillar's criteria. As DoD starts to require proof of Zero Trust implementations, having a ready-made set of queries to demonstrate compliance will be invaluable. stackArmor's Armory platform[16], which emphasizes zero-trust principles ("in-boundary" security services, per their FedRAMP marketplace listing), will extend its query mod to explicitly cover the DoD Zero Trust reference architecture. This will include mapping existing controls to the DoD's Zero Trust Capability Model and developing new and innovative controls to provide agencies with confidence that all Zero Trust measures are not only designed but continuously verified.

- **Automating DoD STIG Compliance Mapping:** Beyond higher-level frameworks like FedRAMP and Zero Trust, there is also the granular world of DISA Security Technical Implementation Guides (STIGs). STIGs are detailed checklists for securely configuring specific technologies (operating systems, databases, network devices, cloud services, etc.), required in both FedRAMP and DoD environments. Currently, STIG compliance is often checked via manual review or scanning tools like SCAP or Nessus. The query-based approach offers a path to automate STIG checks in a scalable way. Our pilot already took a step in this direction by incorporating the Okta STIG rules into their compliance mod, demonstrating that even SaaS configuration guides can be codified. Moving forward, stackArmor will develop additional plugins and controls for additional STIGs such as:
  - An Active Directory Domain STIG mod that queries settings to ensure password sharing for local admins is disallowed, or
  - A Kubernetes STIG mod that checks a cluster's configuration against the STIG requirements.

In cases where direct querying is difficult, integration with scanning tools will fill the gap. stackArmor's use of a scanning tool plugin to retrieve host compliance data (like FIPS 140-3 settings) is a good model from which we will build. Our roadmap includes expanding that to model cover all applicable STIG checks.

> *The environment's scanner runs periodically, and then the query framework picks up the results and merges them into the compliance dashboard.*

Automating STIG compliance would significantly ease the burden on DoD contractors and systems integrators who must harden systems according to these guides. It also ensures consistency, the same script is used to check the control every time, reducing human error. In essence, this approach brings the "security as code" ethos down to the configuration baseline level.

[16] See stackArmor's Zero Trust White Paper for The Armory

Future of Compliance White Paper Continued

In all these future paths, a common theme is standardization and sharing. As organizations build query sets for various frameworks, publishing them (where permissible) as open modules enables a network effect: improvements from one team benefit all, and auditors become familiar with a common set of automated controls. The technology underpinning our approach is flexible enough to adapt to multiple domains, boding well for multi-framework compliance unification.

Implications for Organizations Adopting the Methodology

The move toward query-based, continuous compliance has significant implications for how organizations manage security and audits:

Real-Time Visibility and Co

Perhaps the most immediate benefit
and security teams gain near real-tim
out about compliance drift during a
This aligns compliance with the agile
For auditors and risk managers, con
focus on trend analysis (are things i
point-in-time checks.

Improved Consistency and

Automation ensures that a control
eliminates the variance that can oc
different ways. It also virtually elimin

For example, if a script is checking
automation won't accidentally overl
something in a large spreadsheet.

Of course, the accuracy is only as go
of peer review and validation of the
The open-source nature of the stac
one can expect that widely used c
recognized by compliance bodies.

Reduced Audit Fatigue and Cost:

By automating evidence collection, organizations can dramatically reduce the manpower spent on preparing audit materials. Manual evidence gathering (screenshots, spreadsheets, lengthy narratives) can be replaced with automated reports and dashboards leading to large reductions in compliance efforts.

	Traditional Approach (Before)	Armory20x Query-Based Approach (After)
Time to Prepare Audit Package	~8-12 weeks of manual evidence gathering, screenshotting, and document compilation.	~2-3 weeks to configure automated checks and deliver machine-readable results. Evidence can be regenerated in minutes at any time thereafter.
Engineering Hours Consumed	1,000-1,500 hours annually across multiple teams.	400-600 initial investment to establish the query-based compliance structure. 100-200 annually after initial install with the majority invested in improving and evolving controls rather than gathering artifacts.
Audit Confidence	Moderate Evidence represents a point-in-time snapshot and is vulnerable to drift. Assessors must extrapolate whether findings remain true beyond the collection date.	High Evidence is drawn from live system queries, is source-controlled, and repeatable. Auditors can validate the automation itself, reducing ambiguity.
Likelihood of Findings/Delays	High Manual processes introduce errors and gaps; remediation cycles often extend authorization timelines.	Low Automated benchmarks consistently cover 100% of the environment, minimizing overlooked gaps and enabling rapid remediation prior to audit.
Net Impact		
• ~60-70% reduction in prep time for assessments. • ~50-60% fewer engineering hours consumed annually. • Higher confidence levels for both system owners and auditors, due to transparent, repeatable queries versus static, curated artifacts.		

Table 3: Metrics for Implementing Query-Based Approach

Broader Organizational Impact:

Embracing continuous, automated compliance can foster a culture change. Compliance is no longer a "fire drill" event every year but becomes part of daily operations. Developers and engineers can get immediate feedback if a deployment would break a compliance rule, akin to how unit tests flag code issues. This can drive a more proactive security posture, essentially baking compliance into the DevOps pipeline. Additionally, having a live compliance dashboard can improve communication with management and customers.

> *It's a powerful thing to be able to show a live compliance scorecard to stakeholders, increasing overall system trust.*

For the public sector and regulated industries, widespread adoption of these techniques will lead to what stackArmor envisions on their website:

> *An explosion in the number of authorized cloud services because the cost and time to achieve compliance drop dramatically*[19].

FedRAMP itself hopes to see a jump from a few hundred authorized services to thousands, and stackArmor's automation will be a key enabler of that growth.

Challenges and Considerations:

A middle-of-the-road view must acknowledge that automating all aspects will take time, technology and skilled engineering, and adopting this methodology requires investments. Some considerations are as follows.

- Organizations will need skilled personnel who can translate compliance requirements into queries, a blend of compliance knowledge and scripting/SQL ability. This includes a need to maintain the scripts as environments and regulations change.
- Some controls (especially in areas like personnel security, physical security, or policy) are inherently qualitative and will still require some amount of human judgment.
- The query-based approach will complement auditors, not fully replace them. Auditors will shift to validating the automation itself and focusing on the non-automatable gaps.
- Another consideration is tool integration: ensuring that the query tools are properly configured, secured, and fit into the organization's architecture (especially for on-premises or air-gapped systems, where internet access for plugins might be an issue to solve).

stackArmor's approach of building trust in the automated benchmarks is real-world, instructive example. Organizations adopting this approach should similarly plan to work closely with their internal or external auditors initially to gain buy-in. These challenges are surmountable but

idence, and
d to validate
cannot, but
(with many
is lowering,
ironments.

17

Conclusion

The "future of compliance" is unfolding now in initiatives like FedRAMP 20x, where code and data take center stage over paperwork and spreadsheets. stackArmor's Armory20x pilot has demonstrated that a query-based continuous validation methodology is not only feasible but highly effective for meeting rigorous security requirements. By representing controls as code and leveraging real-time cloud data, organizations can achieve a level of visibility and responsiveness in compliance that was previously out of reach. The technical foundation, using tools to bridge cloud APIs and compliance logic, provides a repeatable pattern that can extend to numerous frameworks, from FedRAMP baselines to DoD's emerging Zero Trust mandates and beyond.

This white paper examines how stackArmor has begun to implement this novel approach, the outcomes of its efforts so far, and the potential to further broaden the methodology to full control coverage and other domains such as STIGs. The analysis shows that moving to automated compliance is not about eliminating humans from the loop, but rather about empowering both engineers and auditors with better tools and real evidence. As the industry and government bodies gain more experience with automated audits, we can expect official standards to evolve in parallel.

stackArmor imagines a world where future compliance regimes will explicitly provide machine-readable control definitions and accept continuous audit feeds as evidence, evolving the compliance landscape as we know it. The future of compliance is one where automated checks and live evidence largely supplant static documents, where compliance status is continuously knowable, and where achieving authorization is faster and more transparent.

For IT professionals with audit and compliance duties, the implications are clear. It is time to treat compliance controls with the same discipline as software engineering: version-controlled, tested, and continuously executed. The query-based methodology offers a practical blueprint to do so, with proven success in a FedRAMP context. Adopting these practices can lead to more secure systems (since issues are caught sooner), as well as faster and cheaper audits. Moreover, when many organizations adopt this methodology, it has a cumulative benefit: a community of practice can share control queries and improvements, regulators become more comfortable with automated evidence, and the overall state of security compliance advances.

The journey has begun with the pioneering efforts of stackArmor's Armory20x and will continue to accelerate. Organizations that embrace this shift early will be well positioned to navigate the evolving landscape of security compliance, turning what was once a painful process into a streamlined, engineering-driven advantage.

This is the future, and all stakeholders are welcome to participate. In query, we trust. Come and see[19].

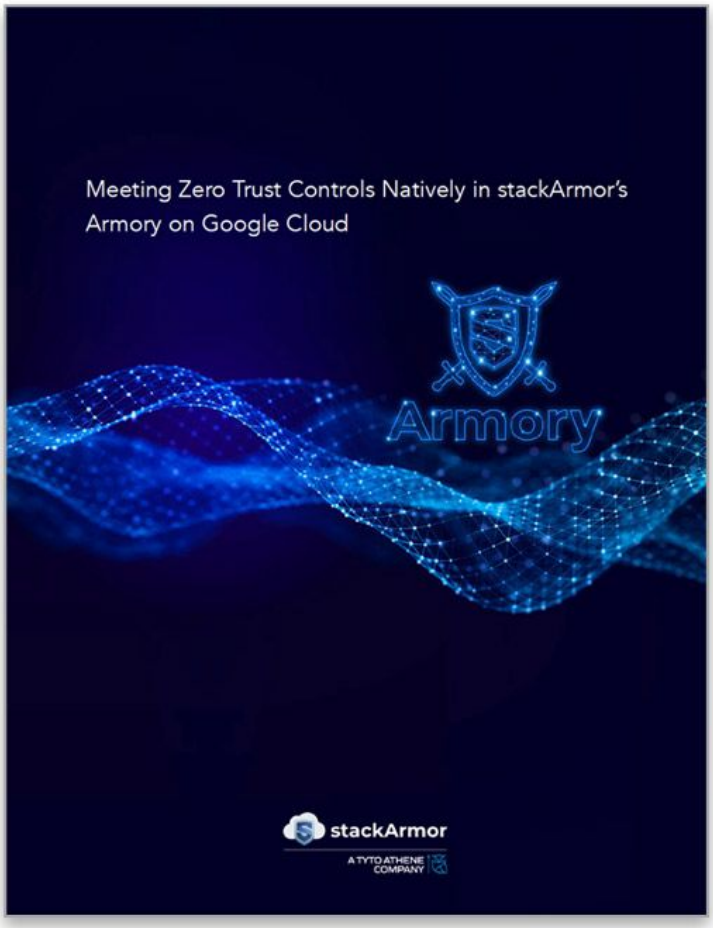
[19] stackArmor/armory-20x-public: Publicly accessible FedRAMP 20x pilot program submission for stackArmor's Armory 20x system

www.stackarmor.com/Armory

stackArmor
A TYTO ATHENE COMPANY

19

Armory ZTA White Paper



As cyber threats grow increasingly sophisticated and persistent, federal agencies and their partners must evolve their security postures to align with modern defense paradigms. The Department of Defense (DoD) Zero Trust Reference Architecture (ZTRA) v2.0 outlines a transformational shift away from perimeter-based defenses toward a "never trust, always verify" model that enforces least privilege, continuous validation, and policy-based enforcement across every aspect of the digital enterprise.

stackArmor's *The Armory* is a secure-by-design General Support System (GSS) purpose-built to streamline FedRAMP and DoD Impact Level (IL) authorizations for Independent Software Vendors (ISVs), and Mission workloads. Agencies are seeking accelerated and lower cost pathways to meeting mission needs in a secure and compliant manner. The cloud, security and compliance experts at stackArmor have developed the Armory on Google Cloud to incorporate zero-trust architecture elements that are validated by the implementation of zero-trust control overlays that are directly integrated into the architecture as opposed to being a "bolt-on." Our design is uniquely zero-trust native implementation.

This white paper provides an in-depth overview of The Armory's system architecture, as detailed in its System Security Plan (SSP), against the seven foundational pillars of the DoD's Zero Trust framework. The Armory™ not only meets but often exceeds the "optimal" capability tier envisioned by the DoD ZTRA, providing defense, federal customers and ISV partners with a secure, scalable foundation for mission-critical operations.

7 Pillars of Zero Trust

User
Securing, limiting, and enforcing person and non-person entities' system access.

Device
Continuous real-time authentication, inspection, assessment, and patching of devices.

Network/ Environment
Segment (both logically and physically), isolate, and control the network/environment (on premises and off-premises) with granular access and policy restrictions.

Applications & Workloads
Applications and workloads include tasks on systems or services on-premises, as well as applications or services running in a cloud environment.

Data
Clear understanding of an organization's data, applications, assets and services (CIaaS) is critical for a successful implementation of a ZT architecture.

Visibility & Analytics
Contextual details provide greater understanding of performance, behavior and actively baseline across other ZT Pillars. We have developed a unique zero-trust controls overlay dashboard to collect and present the continued zero-trust posture of the environment.

Automation & Orchestration
Automate manual security processes to take policy-based actions across the enterprise with speed and at scale.

User Pillar

The Armory's identity and access management
principles. It employs high-assurance user aut
800-63 IAL3/AAL3 requirements for FedRAMP
Identity-as-a-Service platform. This pillar was s
with DoD ZTRA guidance which requires enforc
least privilege access. ISVs deployed to The Ar

- **High-Assurance Identity Management:** provid
Cloud (GHC) as a centralized IdP for all user
authentication (MFA) and single sign-on (SSO) at
(AAL3). All administrative and security applic
SAML/LDAPS federation, ensuring unified id
environment. This meets DoD ZTRA's emphas
(person and non-person) for every access reque
- **Adaptive and Token-Based Authentication:** T
(aMFA) and Okta Verify tokens mean authentica
uses phishing-resistant factors (per AAL3). Har
provided through Okta FastPass or Yubico's Yubi
- **Privileged Access Controls:** The Armory strictly
privileged infrastructure users authenticate via
with Google's Identity Aware Proxy (IAP). This en
via a secure software-defined perimeter, tying n
user identity. Additionally, partners/customers
management planes or security functions of the
- **Least Privilege & Role-Based Access:** By design
only required resources. For example, each ten
to their own project/landing zone with role-base
projects and Virtual Private Clouds (VPCs) are g
flow authorizations. This reflects ZT principles of
and minimal implicit trust.
- **Continuous Identity Analytics:** After strong in
monitors real-time user behavior, incorporating U
(UEBA) to monitor anomalous account activity
actions) to ensure privileged users are perform
good rulesets.
- **Non-Person Entity (NPE) Identity Manageme**
treating service accounts and application identi
users and ensuring all machine-to-machi
authenticated, least-privilege service identities
auditable use). The Armory manages all machine
Google Cloud's Identity and Access Manageme
Service (KMS) services to ensure that both user a
in accordance with ZTA requirements.

The User pillar is key to controlling who and what has access within the sys
implements continuous identity monitoring which complements the secure
authorization (IA) capabilities implemented via Okta MFA and IAP. The system
adaptive authentication features fully for privileged users to dynamically adju
based on access required. In addition, Integrated identity analytics contin
session risk and aligns with DoD's goal of continuous validation of user trust.

All service accounts, APIs, and CI/CD pipelines use unique identities wit
protections and follow strict rotation and least privilege. NPE usage patter
monitored via the Security Information and Event Manager (SIEM) for any ri
for review upon detection.

Device Pillar

The Armory's architecture imposes tight control over devices that interact
especially for administrative access, with focus on ensuring a minimal level of c
to allowing device access. In addition, strong host-based protections are depl
control of what is allowed to run and on which devices this is allowed throug
authorization boundary. The system implements:

- **Secure Access for Administrator Devices:** The requirement that all privile
via Okta integrated with IAP means that administrator devices mus
conditional access policies (CAPs) in order to authenticate before reac
resource. This effectively acts as a DoD Comply-to-Connect mechani
authorized devices/users can form connections. Additionally, The Arm
Cloud's Identity-Aware Proxy (IAP) for admin console/VM access, ensuring t
sessions are brokered through an identity- and policy-aware service rather t
network access. All admin traffic traverses a controlled ingress (Cloud Load
and NGFW) and must be explicitly allowed, reducing the risk from
unauthorized devices.
- **Endpoint Posture Checking:** The system performs real-time posture
checking if an admin's laptop has up-to-date patches, a secure baseline, etc
access) for all privileged user devices used by system administrators. Th
continuously validates device health (OS patch level, antivirus stat
compliance) prior to and during privileged user sessions.

- **Endpoint Security on Servers:** Each server and workload instance in The Armory is treated as a hardened device. The system includes host-based security agents such as Trend Micro Deep Security (for anti-malware, HIDS/HIPS) and performs regular vulnerability scanning (Tenable Nessus) on VMs. These measures align with ZT device capabilities by ensuring that every compute instance is monitored for threats and kept in a known secure state. The SSP's inventory of update sources (e.g. for Trend Micro, Nessus, etc.) shows that The Armory maintains patch and signature updates for in-boundary software, contributing to continuous device (server) compliance.
- **Device Compliance Enforcement:** Although not explicitly a user endpoint control, the Armory enforces that no unmanaged or non-FedRAMP devices can persistently connect to its environment. By disallowing any persistent connections to external systems at lower assurance levels, the architecture implicitly requires that any device or system interfacing with the Armory meets equivalent security standards. This reflects a Zero Trust mindset of not trusting devices by default – only those from known, secure environments are permitted.

By design, The Armory requires the validation of all devices before allowing communication tunnels to be established, regardless of the privilege level of the user. By incorporating device posture checks and requiring that connecting are checked for compliance (patched OS, full disk encryption, FIPS-validated Trusted Platform Module (TPM), screen lock) before tunnel establishment. This aligns with DoD's *Continuous Compliance* mandate for devices.

Network & Environment Pillar

The Armory's network architecture is designed with strong segmentation, boundary control, and least-privilege connectivity, embodying core zero trust network concepts. Each tenant/ application environment is isolated, and all traffic, internal and external, is tightly governed by policy. This pillar shows comprehensive compliance with ZTRA guidance at an optimized level. The system minimizes implicit trust in the network by enforcing micro-segmentation, encryption in transit, and continuous monitoring of network traffic. Key highlights of security design within this pillar include the following.

- **Strong Segmentation of Enclaves:** The Armory uses a multi-tenant government-only cloud with VPCs and projects for each customer or application. Network access control and routing policies ensure each landing zone is completely segregated from others. In other words, there is no flat network – every application environment is a distinct segment with logically isolated subnets. This design contains any potential breach and maps to the ZT principle of micro-segmentation (down to the application/tenant level).
- **Default-Deny and Least-Privilege Traffic Policies:** All network traffic, both north-south and east-west, is subject to explicit policy whitelisting. The Armory employs Palo Alto Next-Generation Firewalls at the boundary and within a shared network hub to inspect and filter all system traffic. By policy, no traffic is allowed unless explicitly authorized. For example, even inter-service flows between components must be opened by rule, and any external inbound access (for user-facing apps) must traverse approved points. This approach aligns with DoD ZTRA's ideal that *no network traffic is implicitly trusted*. The system requires that all traffic must explicitly be allowed via traffic flow policies and whitelisting.
- **Identity-Aware Network Access:** The use of Google Cloud's Identity-Aware Proxy (IAP) integrated with load balancers means that network access to internal resources (like admin interfaces or SSH to VMs) requires user identity verification at the network layer. This tightly binds the network pillar with the user pillar – only authenticated, authorized requests get through. For privileged access, an admin's connection to a VM is not a direct network path but rather brokered by IAP and the firewall, ensuring the network never exposes listening ports unless the user is verified. This significantly reduces attack and exemplifies Zero Trust "authenticate before connect."
- **Encrypted Everywhere:** There is a significa
throughout the environment. Internal servic
Kubernetes clusters the guidance is to use
communication). All data in transit is enc
FedRAMP and DoD workloads, inside the
traffic within the cloud environment, it wo
zero trust tenets that the network is always
- **Egress Restrictions:** The Armory's environ
external systems. Outbound internet acces
only specific update sources and trusted
from known URLs over TLS). By preventing
data exfiltration and C2 channels. Any
anomaly. This whitelisting of external endp
where even outgoing traffic is governed by
- **Micro-Segmentation & Software-Defi**
segmentation at the workload or proc
communications between individual mic
achieved with VPC isolation. Allow lists ca
to further reduce the attack surface inside

The Armory takes a "trust no workload" stance, where even if an attacker compromises one workload, there is no pathway to freely reach others. Integrated log analysis has been established for key segments to enable better clarity and to support threat hunting. Security Engineers and Analysts are provided the tools needed to monitor and act against threats in near-real time.

The established trust zones are periodically reviewed and updated to ensure they align with real-world threat vectors and evolving threat landscapes. The goal is of the system design is to eliminate any "flat" subnet where numerous services can talk without checkpoints. This aligns with DoD's goal of *segmenting and isolating everything possible* to mitigate intrusions.

Application & Workload Pillar

The Armory's architecture implements a comprehensive Secure Software Development and Deployment Framework, providing security controls for applications and workloads from development through runtime. By delivering pre-hardened environments, integrated
erability management, The Armory addresses the
ar. The Armory implements:

application deployed on The Armory starts in a pre-
nitected GCP project/VPC with security controls and
and DoD Impact Level (IL) 5 baseline controls. These
ed IAM policies, network settings, logging, and
infrastructure-as-code through Terraform. Providing
ts inherit strong security from inception (least privilege
), reducing misconfiguration risk. This maps to the ZT
it secure configurations by default."

: StackArmor has built security into the software
ications. Notably, The Armory's ThreatAlert Container
th GitLab to scan container images for vulnerabilities
cked through a Findings Lifecycle Manager (FLM) in
e deployment. Additionally, static and dynamic code
lary, and infrastructure code is tested in a staging
motion. This end-to-end integration ensures that no
orough security checks, aligning with DoD's emphasis
secure development.

- **Continuous Vulnerability Management:** The Armory performs continuous scanning of running workloads and dependencies. It leverages tools like Tenable Nessus for vulnerability scanning and scans containers at least every 30 days (with a policy that no image older than 30 days, unscanned, should be in production). Any findings are handled per FedRAMP SI-2 (flaw remediation) processes in GitLab, which functions as the system's Information Technology Service Management (ITSM) platform. These practices ensure known vulnerabilities are quickly identified and patched, which is key to a Zero Trust workload posture (assuming workloads may be targeted, one must minimize their weaknesses at all times).
- **Runtime Threat Protection:** Workloads in The Armory are instrumented with security agents and monitored. The presence of host-based IDS/IPS, anti-malware (Trend Micro Deep Security), and file integrity monitoring on servers ensures that if an application process behaves maliciously, it can be detected or stopped. Moreover, all intra-cluster communications are encrypted (FIPS mode on hosts or via service mesh), preventing attackers from intercepting sensitive data between microservices. These controls embody DoD ZTRA's guidance that workloads should be secure, continuously monitored, and resilient to compromise.
- **Isolation and Least Privilege by Design:** Each application or customer workload is not only on a separate network but also deployed in its own GCP project with separate service accounts and access controls. Partners or developers cannot change security controls of the underlying GSS, and their privileges in their landing zone are limited. This ensures a clear tenant isolation

The Armory embodies the "secure-by-design" mindset. The stackArmor Architects and Engineers support partner applications onboarded to the system and provide them with guidelines to design their application architecture in a zero-trust manner as well. This includes building their app with strict role-based access internally, robust input validation (to prevent trusting any client data), and integrating with The Armory's centralized auth and logging. By propagating ZT principles into the application layer (not just the infrastructure), the overall system moves closer to a holistic zero trust implementation.

The system enforces that applications use cloud-managed identities and keys rather than static credentials. Google Cloud's Workload Identity Federation and KMS are leveraged so that VM instances, containers, and serverless functions each have a distinct, auditable identity and access only the secrets they require ensuring that all parts of The Armory are as secure as the next.

Through use of automated configuration scanning tools, the system ensures all workload configurations stay hardened at all times. Security Engineers work with ISVs to ensure their applications are secure not just during deployment, but throughout the system lifecycle and work with them to address any "drift" from these secure baselines as it is encountered.

Data Pillar

Data within The Armory is well-protected through a combination of strong encryption, access controls, and monitoring. The platform enforces Federal standards (FIPS 140-2/3, FedRAMP High, DoD IL5) for all data at rest and in transit, aligning with DoD's data pillar objectives to encrypt and strictly control data access. The architecture provides a solid foundation for data confidentiality and integrity (via encryption and separation), while also enabling availability through backups. The Armory demonstrates mature data security measures consistent with ZTRA guidance through:

- **Universal Encryption (Data-in-Transit & At-Rest):** The Armory implements end-to-end encryption for all data flows. All data in transit is encrypted with FIPS-validated cryptographic modules within the boundary, including internal service communications. For example, internal API calls or database connections use TLS; container orchestration traffic is encrypted via FIPS mode or service mesh. Externally, TLS 1.2+/HTTPS is enforced for user connections. Data at rest in databases and storage is also encrypted using FedRAMP-approved Google Cloud services native services with KMS customer-managed encryption keys (CMEKs). This comprehensive encryption strategy meets DoD's mandate to protect data everywhere, both "in motion" and "at rest" are covered, limiting exposure in case of interception or theft.
- **Strict Cryptographic Standards:** The Armory adheres to FIPS 140-2/3 compliance for all encryption mechanisms. Only cryptographic modules validated under FIPS 140 are permitted, and verification of module certificates via the NIST CMVP database before deployment is required. Non-compliant modules are prohibited. This ensures that data protection meets DoD and federal standards (no usage of weak or unapproved algorithms), achieving a high level of assurance in data confidentiality and integrity.
- **Data Segregation by Tenant:** Each customer's data resides in their dedicated project and storage, segregated from other tenants' data by design. Access to one tenant's data is not possible from another tenant's environment which is a critical consideration for multi-tenant zero trust, where one should assume no inherent trust even within a shared platform. All partner data and services are enclosed in their own landing zone. This strong data isolation aligns with the zero-trust principle of minimizing data access scope.
- **Backups and Resilience:** The Armory includes Contingency Planning and backup capabilities as a core service. Data is regularly backed up, and services are built with high availability. This means the integrity and availability of data are maintained even in adverse events, an important aspect since zero trust also considers ransomware or destructive attacks. In addition, continuous verification of the integrity of those backups is implemented. With backups in place, encrypted, protected and validated, the system provides assurances that data can be recovered if compromised.
- **Monitoring of Data Access:** All access to data stores (e.g., database queries, file access) is logged via Cloud Audit Logs and ingested into the SIEM. The SIEM alert use-cases include data deletion or access events, meaning the security team is alerted on unusual data access patterns.
- **Data Loss Prevention at Egress:** By virtue of the egress restrictions mentioned, the platform reduces risk of unauthorized data exfiltration. There are no open channels to send sensitive data out except those explicitly allowed, all of which are monitored. Additionally, the Palo Alto NGFWs at the boundary enable inspection of outgoing traffic (to detect, for example, large data transfers or known sensitive data patterns). These patterns enforce Data Loss Prevention (DLP).

Secure data by design is one of the key pillars of the system. Ensuring data is always encrypted, be it at rest, or in transit, is a hard requirement for ISVs deployed within the GSS. The use of CMEKs ensures that data owners always have direct control over their data. This empowers data owners to protect and control their sensitive data to meet their needs and ensures that all data within the system is trusted only to those users that have explicitly been granted privileges to that data.

Armory ZTA White Paper Continued

Automation & Orchestration Pillar

The Armory demonstrates a strong commitment to automation and orchestration, using infrastructure as code, continuous integration pipelines, and automated security responses in several areas. This pillar is well-addressed through the platform's ThreatAlert tooling and DevSecOps practices that automate monitoring, patching, and compliance tasks. The system implements the DoD's Zero Trust automation objectives via:

- **Infrastructure as Code (IaC) & Consistency:** The entire Armory environment (and customer landing zones) is deployed and managed via Terraform modules. Changes to configurations are tested in staging and require formal approval before production. This IaC approach ensures standardization and repeatability ensuring security controls are not manually applied ad hoc, but rather embedded in the templates. It also means the platform can rapidly instantiate secure environments or update configurations at scale, a key for orchestrating Zero Trust policies enterprise wide.
- **Automated Security Monitoring & Response:** The Armory's ThreatAlert(R) Security Workbench (TSW) provides real-time monitoring, and the platform includes automated alerting and responses to incidents. For example, when a potential security incident is detected, alerts are not only sent to personnel but can trigger automated actions. Additionally, Google Cloud's Monitoring/Alerting is configured as code (policy-as-code for alert definitions) and sends outputs to collaboration tools (GovSlack and GitLab issues) via the ThreatAlert(R) Serverless Relay (TSR). This integration means that the moment an alert fires, it is automatically routed to the Security Analyst team and logged for investigation, reducing response time and ensuring no alert is missed.
- **Continuous Compliance & Reporting:** StackArmor has integrated machine readable compliance artifacts using open standards like Markdown and Open Security Controls Assessment Language (OSCAL) tooling and detailed compliance reporting into the Armory's operations. The system's security controls and status are automatically tracked and can generate up-to-date security posture reports in near-real time. Automating compliance evidence collection and reporting is a significant orchestration benefit, aligning with DoD's push for continuous ATO processes. The system also automates key aspects of Continuous Monitoring requirements through scheduled and automated compliance tasks, Plan of Action and Milestones (POA&M) management, and automated vulnerability and compliance scan analysis.
- **Integrated DevSecOps Pipeline:** The development pipeline itself is orchestrated for security. With GitLab as the central platform, vulnerability scans, configuration scans, and ticketing are all tied together. For instance, when the ThreatAlert(R) Container Services (TCS) finds a vulnerability, it automatically creates or updates issues in GitLab (via the ThreatAlert(R) Findings Lifecycle Manager) for developers and engineers to address. The use of GitLab for change management and the Change Control Board process is tightly coupled with the automation (tickets, merge requests, etc., drive the promotion to production). This reduces human error and ensures that security steps cannot be skipped in the deployment process, essentially orchestrating security gates into the Continuous Integration/Continuous Delivery (CI/CD) workflow.
- **Orchestrated Network and Access Control:** The Armory uses automation in network and access realms too. Cloud configurations for logging, monitoring, and IAP are managed programmatically. Alert baselines are "managed as part of IaC". Service Control Policies and firewall rules are deployed through code templates for each project. This ensures that when a new project (landing zone) is created for a customer, all necessary ZT controls (network segmentation, IAM roles, logging sinks, etc.) are automatically instantiated without lag or omission. It shows a high level of orchestration, such that security is not reliant on manual setup.

Wherever possible, system architects leverage automation to enforce security updates across the environment. If a new baseline configuration is required (due to a discovered vulnerability or new hardening guideline), Terraform and scripts are utilized to push that change to all relevant cloud resources quickly. The revision history shows active updates (e.g., replacing insecure components, updating diagrams, etc.); having an automated method to do these ensures consistency. Integrated config management tools for live state further complement Terraform to maintain a consistent system state.

The culture of stackArmor has adopted the DoD Zero Trust Culture and it mandates its teams to trust and rely on automation to enforce security, rather than trying to bypass it. As technology evolves, the system evolves to further automate and enhance these processes, ensuring The Armory is a step ahead of nefarious actors.

Visibility & Analytics

The Armory excels in providing c
environment and leveraging analyti
logs from every layer; cloud infrast
applications into a centralized
dashboards and alerting. This pe
expectations that a zero-trust ente
measures the security posture" a
aspects that provide visibility into s

- **Centralized Logging and SIE**
centrally collected using Goog
the system SIEM. The Armory fu
OS logs, VPC flow logs, firewa
logs, vulnerability scanners, an
project. This comprehensive lo
events across all planes of th
cornerstone of Zero Trust, en
unseen.
- **Real-Time Alerting and Dashb**
real-time alerts and dashboar
Monitoring is set up with dashb
(managed via IaC) to detect
attempts, DoS patterns, susp
detections, and changes to criti
for attempted remote access f
account use, and potential r
automatically forwarded to the
for immediate triage. This cap
continuous monitoring and att
personnel have up-to-the-minut
- **Continuous Monitoring Oper**
monitored by the Armory Secu
Having dedicated analysts watch
alerts ensures that visibility lead
ITSM in-boundary for tracking
trail from detection to response
which allows for historical r
organizational commitment to c

the DoD ZT model calls for under the Visibility pillar, not just tooling, but people and processes actively engaged in using the telemetry.

- **Long-Term Data for Analytics:** The Armory configures log retention to align with federal guidelines – logs are kept for 30 months in object storage. This is important for forensic analysis and spotting slow-developing trends or repeated patterns over time. With extensive log
perform deep dives (e.g., searching if a newly discovered Indicator
appeared in the past) and machine learning models are trained on a larg
to improve anomaly detection. Retaining this volume of data shows
analytical capabilities of the monitoring team.
- **Single Pane of Glass –** stackArmor has created a proprietary application c
Workbench (TSW) to provide visualization of system state on an ong
provides dashboarding functionality that that maps the seven pillars and
each. Data Owners also have near-real time visibility into the running sy
their Continuous Monitoring requirements. Having such a dashboard
pillars, helps analysts and leadership alike quickly grasp security postu
overall situational awareness, which is key aim of the Visibility & Analytics
- **Periodic Red-Team Simulations:** To validate and improve visibility, regul
simulation exercises are conducted as part of continuous monitoring. Th
any blind spots exist in logging or if any malicious activity fails to trigger
utilizes lessons from these exercises to further tune the analytics. Over
and revalidation of the system automation helps to calibrate monitori
where any malicious or policy-violating action is noticed and responded

As seasoned security professionals, stackArmor understands that monitoring only provides value if that data is focused and actionable. The Armory was
gathered in the day-to-day operations of the system is consistently being e
to the right teams at the right times to act when action is needed.

Zero Trust Overlays Alignment

The DoD Zero Trust Overlays provide
adaptations of the Zero Trust principles, en
right controls in the right operational conte
naturally aligns with these overlays by co
compliant controls with mission-tailored Z

By leveraging capabilities such as identity
continuous monitoring via tamper-resistan
through NGFW and VPC Service Control
security posture that meets the overlay int
critical workloads. This alignment ensur
meets the baseline ZTA requirements bu
driven protections expected in high-assur

Conclusion

The Armory exemplifies a modern, zero-trust native implementation of the DoD Zero Trust Reference Architecture, weaving together secure user and device authentication, network micro-segmentation, encrypted workloads, continuous monitoring, and policy-driven automation into a cohesive and operationalized security fabric. Every element of the system, from its pre-hardened landing zones to its integrated ThreatAlert(R) Security Workbench, reflects the core tenets of "never trust, always verify" and "assume breach."

By unifying Identity-as-a-Service, FedRAMP-compliant cloud-native controls, and automated compliance orchestration under a single secure architecture, The Armory delivers a turn-key Zero Trust environment aligned with both FedRAMP and DoD cybersecurity expectations. Its design enables ISVs to rapidly deploy secure, resilient SaaS offerings within a trusted framework that meets the rigor of national security-grade standards.

With its foundational alignment to the DoD ZTRA and its commitment to continuous innovation, The Armory not only provides an effective blueprint for Zero Trust implementation, it sets a benchmark for the future of secure cloud service enablement across the federal landscape.

https://stackarmor.com/armory/

Created stack/Tyto Integrated Logo Mocks for GP

Upon being asked, created a number of integrated Tyto/stackArmor logos as original vector illustrations.

- *Created logos for both stackArmor and the Armory.*
- *Provided these to GP.*

GP Ask - Concept Logos that Blend Tyto with stackArmor

Designed Multiple Blog Header Graphics

Created multiple blog headers to align with blogs.

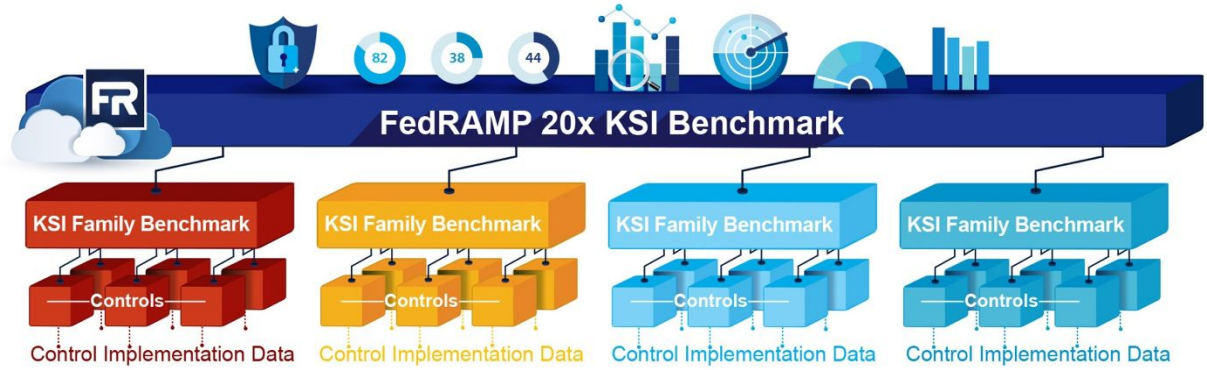
- Invested my own money in stock art subscription, showing my commitment.
- Created images using original illustrations combined with creative imagery collage techniques.

Blog Header Images Continued

Raised the Professionalism Bar by Creating Many Bespoke, Original Illustrations

Beyond any job description I was hired for, I've provided stackArmor with high quality graphics support without them needing to hire a graphics artist!

- *Johann provided most of the content for the blogs, while I added, edited, and formatted into publish-ready artifacts.*



Examples of Bespoke Vector Illustrations Continued

Step 1

Start with Secure-by-design deployment

Our security stack is built and deployed as code with security in mind: FIPS-validated crypto, centralized logging and monitoring, vulnerability and configuration management, backup/CP, boundary protection, and zero-trust overlays. All this is pre-baked into the stack and deployed via infrastructure-as-Code (IaC) to ensure secure, compliant configuration.

Step 3

Be FedRAMP Moderate Equivalent by design

ThreatAlert® is purpose-built to meet the DoD memo's requirements. When DIB customers are looking for a tried-and-true MSP that they can trust, you can provide all the necessary authorization and validation information to prove they are in good hands.

Step 5

GovRAMP without any translation

With Moderate-equivalent as your baseline, your evidence pack matches GovRAMP's model. You're not hand-waving reciprocity; you're aligning baselines and reusing testing artifacts.

Step 2

Instrument with ThreatAlert

Our Security Workbench automates the Continuous Monitoring (ConMon) processes and orchestrates the creation of deliverables (e.g., Plan of Action and Milestones (POA&M), system inventory, vulnerability reports, etc.) to ensure you are validation-ready at a moment's notice.

Step 4

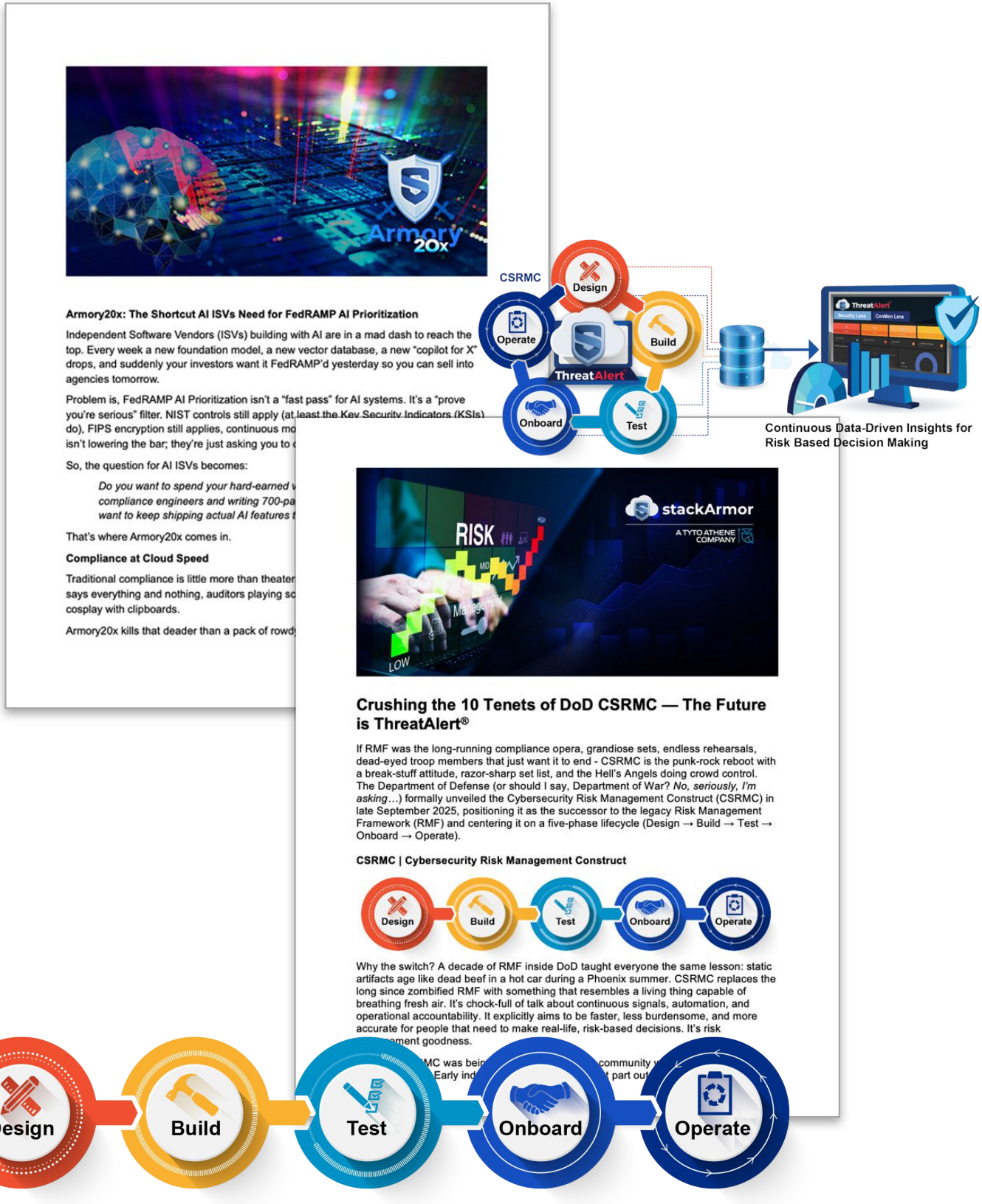
Map forward to IL4/IL5

Because the DISA Cloud SRG sits on top of FedRAMP, ThreatAlert also accounts for the SRG deltas (the + in FedRAMP+). This positions your organization to take advantage of the DISA Provisional Authorization (P-ATO) process and become widely available to DoD agency customers.

Visual and Textual Content Development for Blogs

Transformed many instances of raw text into polished blogs, each with multiple custom illustrations.

- *Johann provided most of the content for the blogs, while I added, edited, and formatted into publish-ready artifacts.*



Blogs Continued

DoD SRG's Silent Earthquake:

IL5 Moved to NSS-Land. Most of You Are Actually IL4 *(And That's Okay)*.

The Defense Information Systems Agency (DISA) has been pushing a number of Cloud Security Requirements Guide (SRG) updates in recent months. Since July 2025 we've seen:

- SRG V1R3 – dated July 02, 2025
- SRG V1R4 – dated August 13, 2025
- SRG V1R5 – dated September 03, 2025

Hey DISA, friendly request here - maybe gather everyone together and think about a roadmap of quarterly releases or an industry tow

While there's been a number of updates, in my c
far. The version number whispers "minor," but th
needs to understand the following:

Impact Level (IL) 5 is now explicitly a Nati
neighborhood, and that's not a place mos

The part hardly anyone is saying

Open the SRG, from version V1R3 through to th
IL levels, and it's unambiguous: IL5 is for unclas
Information (NSI). That's IL5. **Full stop.**

Beginning July 2, 2025: V1R3 introduced a singl

Impact Level	Baseline

Website Page Title:
Hey MSPs: Why FedRAMP Moderate Equivalency Beats Bare-Minimum CMMC

Meta Description:
With CMMC now in contracts, MSPs in the DIB face a choice: meet minimums or go further. Learn how FedRAMP Moderate Equivalency with ThreatAlert® delivers scalable compliance, faster onboarding, and future-proof security.

Slug:
msps-fedramp-moderate-equivalency-vs-cmmc

Implementing CMMC? Think FedRAMP Moderate Equivalent Instead.

Hey MSPs…You Should Aim Higher Than Bare-Minimum CMMC. Go Full FedRAMP Moderate Equivalent. Be Brave!

The Pentagon finally dropped the other shoe. With the Defense Federal Acquisition Regulation Supplement (DFARS) amendment now posted for public inspection, CMMC requirements officially land in DoD contracts on November 10, 2025.

Simply put, *the grace period is over! Procurement just turned into a cybersecurity filter. If you don't meet the level specified in the RFP, go home and slap yo' SSP - simple as that.*

FedRAMP Equivalency

1	2	3
100% coverage assessment of the FedRAMP Moderate baseline by a FedRAMP-recognized 3PAO.	A Body of Evidence (SSP, SAP, SAR, POA&M) available to the contractor and assessors.	DFARS 7012 report-ing and compliance activities baked in.

Blogs Continued

Let's Not "Blow up the RMF"

stackArmor's Query-Driven 20x Approach to Modernizing Compliance

IT security people, especially those people in Compliance, love drama. Every few years, somebody trots out a seemingly edgy but ultimately trite battle cry like, I don't know... *"Blow up the RMF!"*

As if we're all about to light the Risk Management around the ashes (has no one ever heard of the su honest, burning things down rarely fixes them. Th fossilized way we've been playing the compliance screenshots that are outdated the moment you ta are obsolete the second you zip them up.

Traditional Federal information system assessme

- Write 700 pages of "implementation stater only sometimes accurate.
- Have your highly skilled/paid engineers co a freshly minted, unskilled intern.
- Ship the whole mess to auditors and pray already outdated.

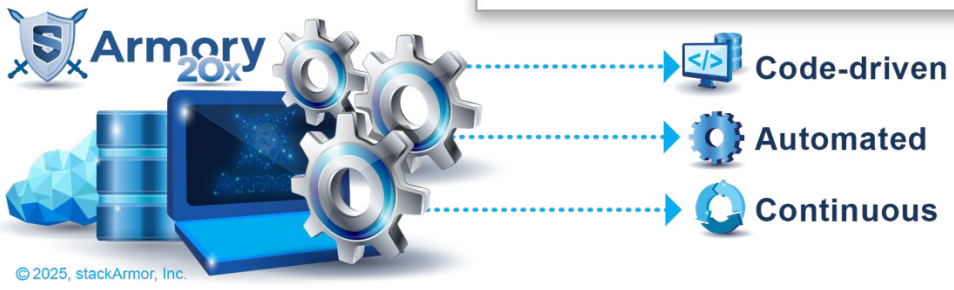
How to do FedRAMP the Wrong Way

A lovingly sarcastic field guide to burning time, money, and morale

Let's start with the myth that refuses to die: **FedRAMP ATOs take 18–24 months and cost $3–5M.**

If you follow the classic FedRAMP advisory playbook, sure. You'll spend months on a gap assessment, commission a reference architecture that looks gorgeous in PowerPoint, and then sink quarters into R&D trying to interpret every control like it's Renaissance poetry. *Damn it, what the hell is a Prince of Cats!?* Cue the consultant parade and the endless gap analyses. Cue roadmaps to hell. Cue the realization that you've made poor career choices. And the absolute worst - *cue the invoices*!!

1



Supported Tyto Sales with an Inscom “White Paper”

Worked with Tyto to create an Armory paper with content that speaks to a specific bulleted list of asks from a Government customer.

- *While this looks similar to others, the written content is nearly all completely new, requiring hours of research, analysis, and word smithing to get it right!*
- *Feedback was that this was VERY helpful!*

Created Another New Armory 2 Pager

Created yet another new 2 page glossy for GP to use at trade shows and sales/marketing highlighting the Armory offering. Used many graphics from the Inscom paper.

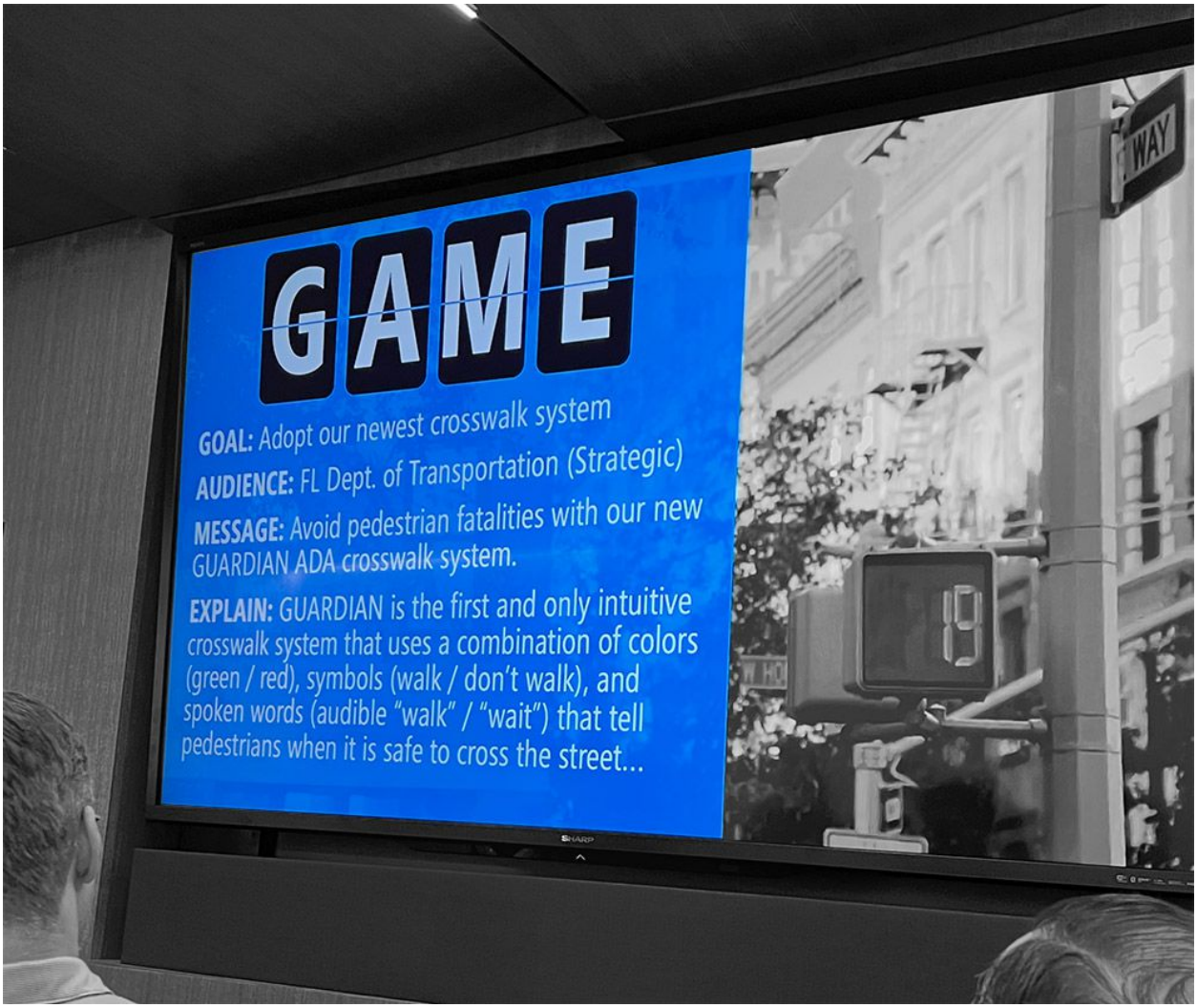
- *Because all illustrations are original and vector based, I can continue to create new versions of these kinds of glossies.*
- *Leveraged many illustrations from the Inscom "white paper," while much of the verbiage is different.*

Professional Growth

Attended Visual Storytelling Workshop

Thanks to Tyto, was able to attend a 2-day visual storytelling workshop in November where I learned some invaluable skills to deepen what I already know.

- *Material and approach was focused on proposal graphics, but the lessons were applicable to any/all graphics!*
- *Lots of focus on cognition, which was awesome (elephant vs rider)*



stackArmor

A TYTO ATHENE COMPANY

2025

AUG - DEC

Thank You!

Sarah Hensley

Annual Performance Report