



Elastic's FY27 Q2 Quarterly Partner Connect

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Elastic, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.



To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com



Explore More Resources:
carah.io/elasticresources



Join Events & Webinars:
carah.io/elasticevents



Discover Technology Solutions:
carah.io/elastic



Learn About Procurement:
carah.io/elasticcontracts



Connect With Our Team:
elastic@carahsoft.com
571-590-6810

The background is a solid blue color. It features several large, stylized, 3D geometric shapes in a lighter blue shade. These shapes are angular and layered, resembling architectural elements or abstract sculptures. They are positioned in the corners and along the edges of the slide, creating a modern and dynamic feel.

Thank you for joining us on **Elastic's FY27 Q2 Quarterly Partner Connect**

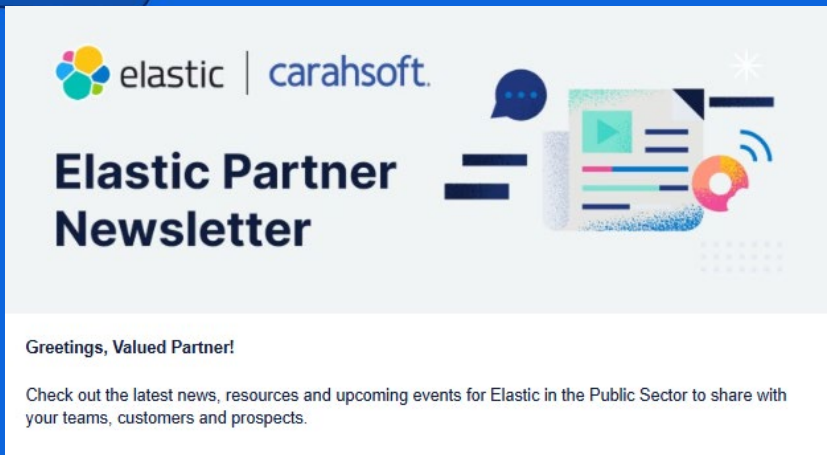
Welcome!

We will begin at the top of the hour.

About Carahsoft

Carahsoft is The Trusted Government IT Solutions Provider®, supporting Federal, State and Local Government and Education and Healthcare organizations with IT products, services and training through our partners and contracts.

Elastic Partner Newsletter



Here's a summary of four actionable takeaways for your organization:

- **Read:** Jesse Sladek's blog to learn more about his perspective on current market trends
- **Listen:** Sign up for the first iteration of the SOC Modernization Tour on September 24 in Chicago
- **Meet:** Schedule time with our Elastic experts to learn more about use cases for your IT team.
- **Learn:** Explore the launch of Elastic 9.5 in our latest blog post.

Agenda

<u>Session Time (ET)</u>	<u>Session Topic</u>	<u>Speaker</u>
3:00pm - 3:05pm ET	Welcome & Opening Remarks	Darryl Peek II
3:05pm - 3:15pm ET	Sales Update: Elastic Overview & Public Sector Update	Darryl Peek II
3:20pm - 3:30pm ET	Elastic & NVIDIA Updates	Rachel Wade
3:30pm - 3:40pm ET	Public Sector Channel Update: Partner Program & Partner Enablement	Darryl Peek II
3:35pm - 3:50pm ET	Solution Architecture Updates: Release 9.5	Thonda Taylor II
3:50pm - 4:00pm ET	Marketing Update: Partner Marketing Updates	Lauren Montross
4:00pm ET	Q&A & Closing Remarks	Darryl Peek II

Presenters



Darryl Peek II

VP, Channel Sales,
Global Public Sector



Rachael Wade

Global Tech Alliances Manager



Thonda Taylor II

Sr. Partner Solutions Architect,
Global Public Sector



Lauren Montross

Partner Marketing Manager,
Global Public Sector

Welcome and Overview

Darryl Peek II

VP, Partner Sales - US Public Sector



How to build AI-powered search with Elasticsearch [2 min live demo]

Search

Elasticsearch
in **2 minutes**



Public Sector Leadership Team

60+ Direct Sellers || 30+ Solution Architects || 9 Customer Engineers || 8 Channel Managers || 50+ Professional Services SMEs || 5+ Support Roles

Public Sector Leadership Team



Chris Townsend
VP, US Public Sector



Frank Garruzzo
Chief of Staff



Amy Moore
Exec Assistant



Jared Pane
Sr. Dir., Solution
Architecture



Faith Bateman
RVP, UKI Defense



Joe Winchell
Dir., Consulting



Jen Nowell
AVP, Civilian



Ryan Greenhill
Sr. Mgr., Inside Sales



Chris Radcliffe
Sr. Dir. Legal Counsel



Sean MacKirdy
AVP, Nat Sec



Darryl Peek II
VP, Partner Sales



Lawrence Butler
Capture Executive



David Stroth
AVP, SLED



Katharine Gannon
Dir. Sales
Development



Dave Erickson
GAM, AI



Mark Boschier
RVP, Pub Sec
UKI



Patrick Hoge
Dir., Customer
Architecture



John Harmon
GAM, Security

Meet Elastic — The Search AI Company

Elastic helps everyone transform data into **answers, actions, and outcomes** with Search AI.



Founded in
2012



5B+
downloads



3,000+
employees



Used by over **54%**
of the Fortune 500



40+
Countries with employees



Publicly traded under
ESTC in the NYSE

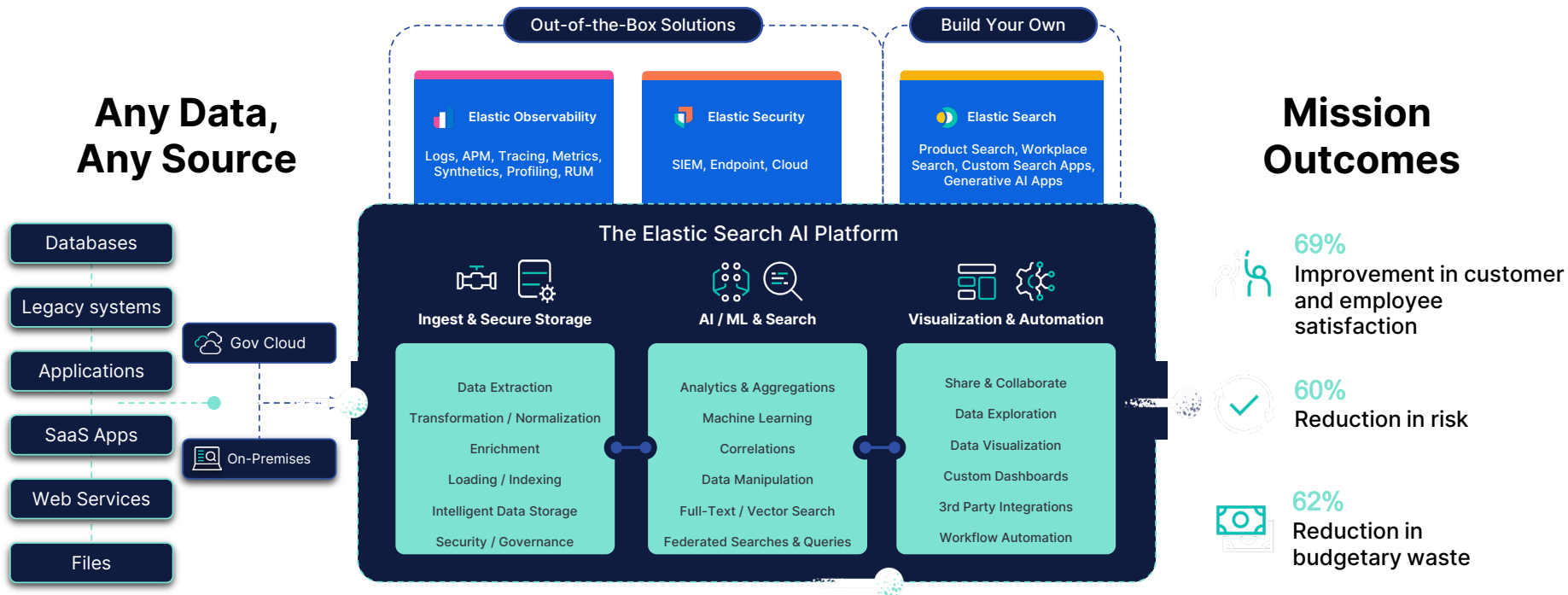


1,500+
Partners globally



300+
Turnkey integrations

Many mission use cases, One **Search AI** platform



**Validated by
third-party research*

Across public cloud, hybrid cloud, and on-premises deployments

One platform, three solutions, one copy of the data



Search

Search AI, RAG and agentic retrieval over agency content — FOIA, case files, knowledge bases, code, sensor and mission data.

Vector, hybrid and lexical retrieval in one engine



Observability

Logs, metrics, traces and profiling for mission systems — with AI-assisted triage to cut MTTR on the systems citizens actually touch.

Prometheus / PromQL support and OpenTelemetry native



Security

SIEM, endpoint and cloud security on the same data — detections, AI-driven investigation and an agentic SOC posture.

Analytics, EDR and detection engineering in one console

Elasticsearch — the data layer underneath all three

Ingest once. No duplicate pipelines, no duplicate storage, no duplicate license for the same log. Services attached is where the margin lives.

Two demands, inside hard security boundaries



Rapid AI innovation

- Mission teams want retrieval-augmented and agentic AI in production now, not in a FY28 roadmap
- The blocker is rarely the model — it is getting governed, current, permissioned data to it
- Search is the layer that makes agency data usable by an LLM



Platform consolidation

- Budgets are flat to down; tool sprawl across SIEM, log analytics and APM is the first line item under review
- Consolidating Search, Observability and Security onto one data layer removes duplicate ingest and duplicate licenses
- Every consolidation conversation is a services and migration conversation for you

The constraint that decides the deal: data sovereignty. If the platform cannot run in their enclave, at their impact level, under their control, the AI conversation ends.

What shipped that you can sell this quarter

Workflows — GA

Automation across the platform, generally available in 9.4. Turns **detection and response runbooks into repeatable, sellable engineering work.**

Agent Builder updates

Build and govern agents against agency data. **This is the practical on-ramp for 'we need agentic AI' requests.**

Prometheus / PromQL support

Existing Prometheus users keep their queries and dashboards. Removes the single biggest objection in observability displacement. **We already standardized on Prometheus and Grafana turns that from a wall into a starting point.**

LogsDB storage efficiency

Materially smaller log footprint on high-cardinality data. **This is your TCO argument, quantified.**

Data stream lifecycle

A short JSON policy moves aging indices to searchable snapshots on object storage automatically — **hot performance, archive economics.**

LLM observability

Monitor self-hosted model performance, cost and behavior. **Agencies standing up sovereign AI need this and rarely have it.**

Deploy where the mission requires — the real differentiator

1

FedRAMP authorized cloud

AWS Moderate and High environments for agencies that want a managed service without leaving the boundary.

2

Self-managed on-prem

Full control, agency-run, on agency hardware — including classified and disconnected networks.

3

Air-gapped and edge

Deployments with no outbound connectivity, including tactical and forward-deployed footprints.

4

Hyperscaler and marketplace

Run alongside AWS and Google Cloud public sector environments, including distributed and sovereign cloud offerings.

Ask this early

- What impact level does this data live at today?
- Is there an outbound connectivity path, or is this disconnected?
- Who owns the ATO, and when does it get re-reviewed?
- Is there an existing marketplace or contract vehicle we should transact through?

Deployment fit is a qualification question, not an implementation detail. Ask it in the first meeting.

The ecosystem you can co-sell into

**AWS**

Marketplace transactability and public sector co-sell motions for agencies buying through cloud vehicles.

**NVIDIA**

GPU-accelerated AI search. Joint public sector go-to-market and demo assets available now.

**Google Cloud**

Including Google Distributed Cloud for sovereign and disconnected deployments.

**Gigamon**

Deep network telemetry into Elastic for AI-driven threat hunting without decryption overhead.

**Tines****tines**

Automation and orchestration paired with Elastic detections for SOC modernization.

**Deductive AI**

Joint work on faster resolution of production incidents in complex environments.

**Corelight****corelight**

Zeek network evidence, ECS-formatted, into Elastic Security with prebuilt dashboards and detections.

**Axonius****AXONIUS**

Unified asset inventory indexed into Elastic as lookup context for every investigation.

**Red Hat****Red Hat**

Full-stack OpenShift observability: cluster, container, and application telemetry unified in one platform.

If you already hold a practice around any of these, there is a joint play available — ask your partner manager to scope it with the alliance team.

Used by more than 50% of the Fortune 500 enterprises

TECHNOLOGY	FINANCE	TELCO	CONSUMER	HEALTHCARE	PUBLIC SECTOR	AUTOMOTIVE	RETAIL
							
							
							
							
							
							

Trusted Across Public Sector

Defense	National Security	Federal	State & Local	Education
				
				
				
				

02

Sales Overview

Where the public sector money is moving in FY26 — and the five plays converting it

- The mandates and deadlines creating urgency right now
- Five plays, with the discovery questions that qualify each
- The fiscal calendar you should be selling against

Four forces creating funded urgency right now



M-26-14: Federal logging requirements

Agencies are under renewed direction to improve log collection, retention and visibility. Logging mandates are budget-creating events — they convert 'someday' into 'this fiscal year.'



CISA reference architecture and Zero Trust

New architectural guidance means gap analyses, then procurement. Agencies need help mapping current state to required state.



Post-quantum cryptography readiness

Long-horizon planning is starting now. Inventory and visibility come first — you cannot migrate what you cannot see.

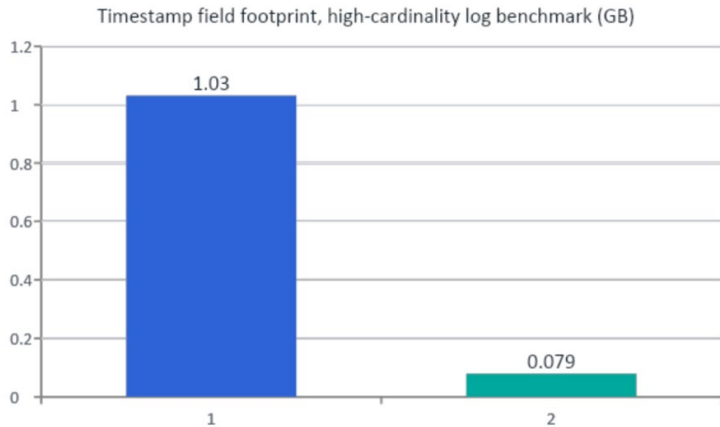


Sovereign AI adoption pressure

Every agency has an AI directive and a data problem. The data problem is where we win, and where your services attach.

Every one of these is a compliance clock — and compliance clocks are how federal deals move before a fiscal year ends.

Mandates raise data volume. Architecture lowers the cost.



Internal Elastic 9.5 benchmark on a single high-cardinality field. Directional, not a customer guarantee — validate against the customer's own data.

Storage is the objection

When an agency is told to log more, the first pushback is the bill. Lead with footprint, not features.

Tiering does the rest

A short lifecycle policy moves aging data to searchable snapshots on object storage — still searchable, dramatically cheaper to hold.

Consolidation compounds it

One ingest pipeline feeding security and observability removes a duplicate license and a duplicate copy of the same data.

Where you make money

Sizing, migration, pipeline engineering and detection content. The savings fund your services.

Five plays converting in public sector right now

1

SIEM consolidation and displacement

Trigger: incumbent SIEM renewal 6-12 months out

Incumbent SIEM renewals are the largest single pool of addressable spend. Attack on ingest economics, detection quality and analyst experience.

2

Observability consolidation

Trigger: a modernization or cloud migration program

Replace three or four monitoring tools with one platform on the same data as security. PromQL support removes the migration objection.

3

Log tiering and TCO rescue

Trigger: budget pressure or an unplanned log overage

The customer is already drowning in log costs. Re-architect retention rather than replace the whole stack. Fast, low-risk, high-trust entry point.

4

Metrics upsell into logging accounts

Trigger: any existing Elastic logging customer

For accounts already running Elastic for logs, adding metrics is expansion without a cold start — resale margin plus services plus recurring managed services.

5

Search AI and agentic retrieval

Trigger: a named AI initiative or a stalled LLM pilot

The agency has an AI mandate and no governed data layer. Start with retrieval over a single high-value corpus, then expand.

Play 4 is the highest-return use of your next 30 days — the accounts already exist in your base.

So if you hear.....

KEY COMPETITORS BY SOLUTION

Enterprise Search



Observability



Security/SIEM



Think ...  elastic

Metrics upsell: expansion revenue without a cold start

Why this one first

- The account is already yours — no new logo, no new procurement relationship
- The data pipeline and the deployment already exist
- The consolidation value that wins the customer is the same value that grows your revenue
- Updated metrics pricing for Elastic Observability makes the math easier to present

Asset: 'Upsell with Elastic Metrics' — Seismic Partner Salesroom

1

Resale margin

Incremental license on an existing, warm account.

2

High-margin services

Instrumentation, dashboard build-out, SLO definition and alert tuning.

3

Recurring managed services

Monitoring the monitoring — an annuity, not a one-time project.

4

Follow-on security attach

The natural runway into the SIEM conversation.

This week: book a metrics conversation in every Elastic logging account you hold.

Discovery that separates a real deal from a demo request



Mission and mandate

- What requirement or directive is forcing this change, and what is the date attached to it?
- What happens to this program if nothing changes for 12 months?
- Who signs off that the requirement has been met?



Money and vehicle

- Is this funded, or are we building the justification together?
- Which contract vehicle or marketplace will this transact through?
- When does the incumbent contract renew?



Data and environment

- How much data per day, and how long must you retain it?
- What impact level and what enclave?
- What tools are ingesting this same data today?

If you cannot answer the vehicle question, you do not have a Q1 deal — you have a Q3 deal. Register it anyway, then go find the vehicle.

Sell against the calendar, not against the quarter

Now — Sept 30

Federal fiscal year end

Expiring-funds conversations, add-on capacity, renewals pulled forward. Anything already scoped should be closing here.

Oct — Dec

New fiscal year starts

New-start programs, but funding under continuing resolution rules can delay new procurements. Pursue expansions and existing vehicles first.

Jan — Mar

Budget clarity

Full-year appropriations conversations. Best window for new architectures and multi-year commitments.

Year-round

SLED cycles

State and local fiscal years mostly turn July 1. Education buys against academic calendars. Different rhythm — plan separately.

Planning assumption: expect procurement friction around the turn of the calendar year. Pull what you can into the current window and build first-quarter pipeline now.

Thank you!



NVIDIA Partnership Update

Rachael Wade

Global Tech Alliances Manager



elastic

| The Search
AI Company



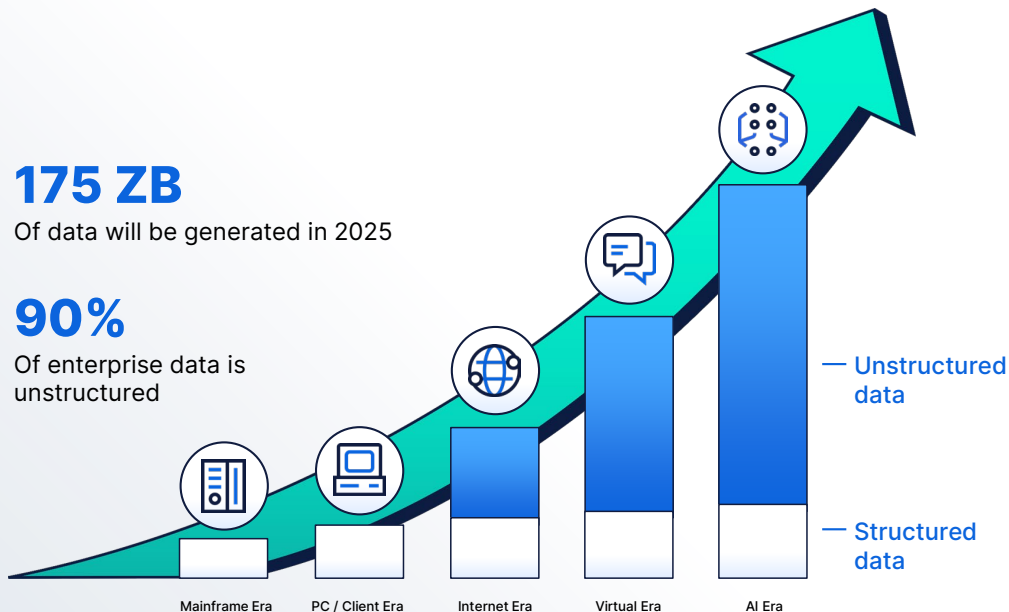
The Proliferation of Unstructured Data

175 ZB

Of data will be generated in 2025

90%

Of enterprise data is unstructured



The Data Explosion

Logs, document, emails, images, and code repositories. This data holds the most valuable context for your business.

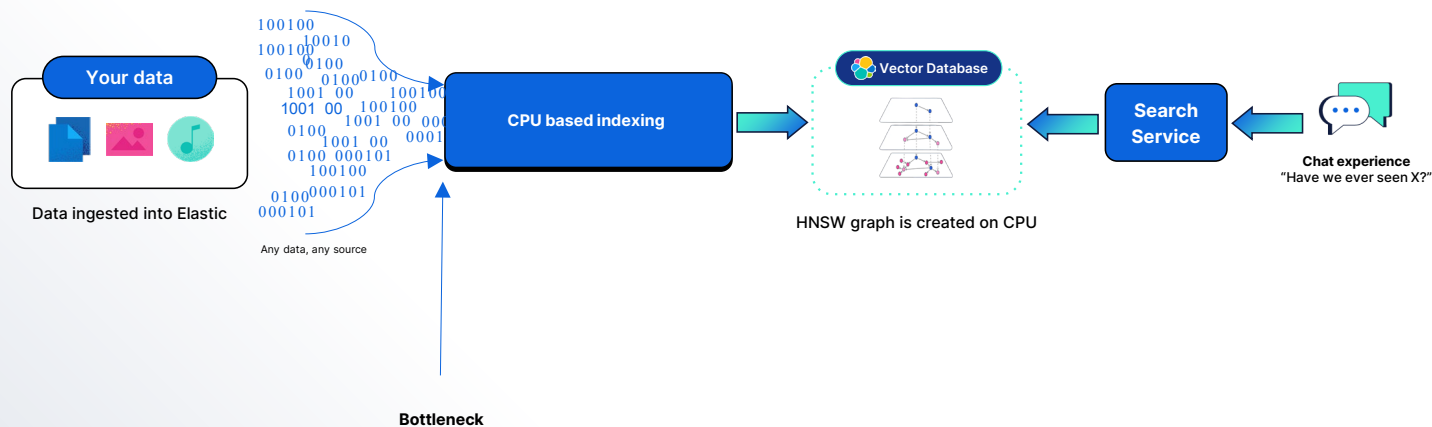
The Real-Time Challenge

Making sense of this data historically required slow batch processing. Today's applications demand instantaneous retrieval and semantic understanding.

Agentic Requirements

AI agents cannot function on raw text. They require unstructured data to be converted into vector embeddings and indexed for sub-second similarity search.

The Challenge of Indexing Enterprise Data at Scale



Search remains fast and accurate

The HNSW graph within the Elastic vector DB created upon data ingest is optimized for CPU workloads executing with accuracy and speed when searching.

CPU-based indexing can't keep pace with enterprise data growth



Traditional scaling approaches to add more CPU nodes result in exponential infrastructure costs

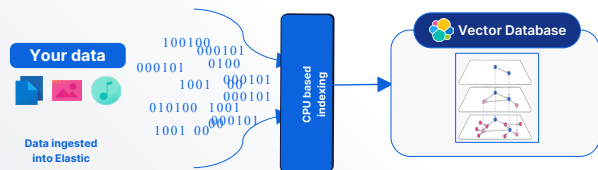


TTV becomes a barrier

As data volume grows, ingestion time increases as well as the infrastructure spend.

Elastic GPU Accelerated with NVIDIA cuVS

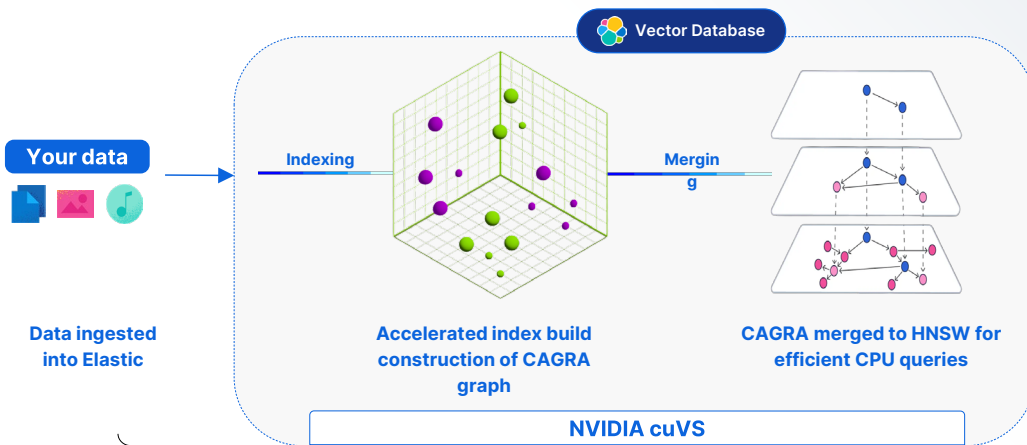
Indexing on the CPU



Graph construction is the most compute-intensive indexing operation

Elastic GPU Indexing Accelerated with NVIDIA cuVS

GPU acceleration for indexing, CPU for queries



7x decrease in force-merge latency

12x improvement in indexing throughput

Target industries for Elastic **vector** search

WHERE THE PLAY LANDS + TARGET SEGMENTS



Software & Technology

ISVs and SaaS teams embedding search, RAG, and agents into their products.



e-Commerce

Product discovery, personalization, and ranking across large catalogs.



Telecommunications

AI assistants and retrieval over massive operational and customer data.



Government

Investigation workflows across records, case files, and intelligence data.



Energy & Utilities

Streaming sensor and transaction data, usage analytics at massive scale.



Financial Services

Knowledge discovery, research, and compliance across unstructured documents.

Same data problem across all segments

Each of these industries sits on **large volumes of proprietary, unstructured data** spread across many systems, with AI initiatives that depend on making it retrievable. Regulated and sovereign requirements are standard.

Elastic is usually **already in the building**, through free and open Elasticsearch, observability, or security. The play expands a footprint instead of opening a cold door.

WHO MOVES THE DEAL

CHAMPION

Engineering Lead; Head of Search; Head of Platform

A win for them: **one unified retrieval platform**, glue code gone, costs that scale predictably.

INFLUENCER

App Developer; ML Engineer; Data Engineer

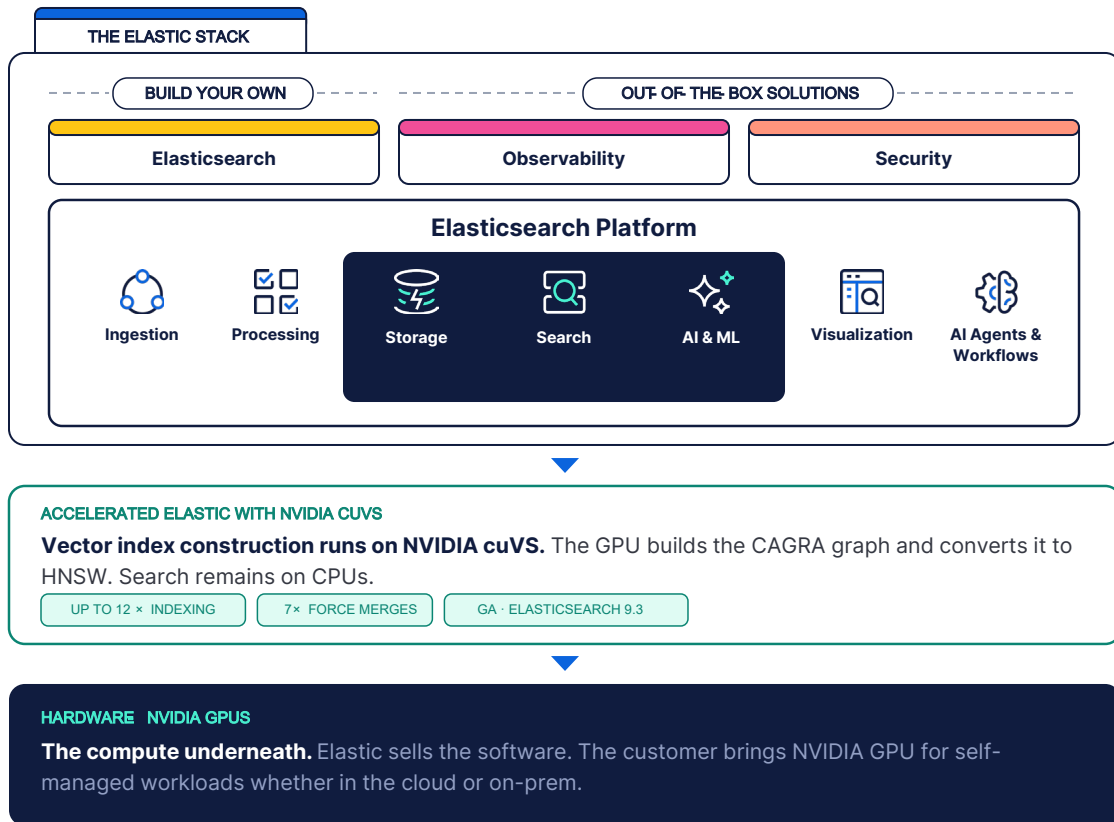
A win for them: retrieval that **works at speed and scale**, transparent debugging, more time shipping product.

ECONOMIC BUYER

CTO; CIO ; VP Engineering; VP Product

A win for them: **clear ROI**, fewer systems to maintain, a platform that grows with the AI roadmap.

Elastic + NVIDIA Joint Value Prop



Accelerating enterprise AI at scale

Elastic GPU-accelerated search with NVIDIA cuVS delivers **12x faster indexing speeds** and **7x improvement in force-merge latency**, enabling enterprise-scale AI deployments and a faster path from POC to production.

FOR THE CHAMPION

Index build SLAs **met with ease**. Ingest and search stop fighting for CPU, offloading the unused resources for better improved search latency.

FOR THE DEVELOPER

Zero pipeline rewrite. Same APIs, same index format, same queries. The GPU takes the expensive step invisibly.

FOR THE ECONOMIC BUYER

The GPU investment shows return on ROI on a production workload with lower ~78% lower TCO and faster path from POC to production.

Thank you!



Channel & Alliances Updates

Darryl Peek II

VP, Channel Sales - Global Public Sector





Darryl E. Peek II
VP,
US Public Sector Partner Sales



Mark Phillips
Director, AMER/USPS Partner SAs



Vicky Wells
Director, Global Partner Marketing

Resell Partners



Dave Henley
USPS Partner Manager

Territory Central/West - Manage Resellers / MSPs



Mark Vanweezendonk
USPS Partner Manager (Acting)

Territory CIV - Manage Resellers / SIs



Avonne Thompson
USPS Partner Manager

Territory IC - Manage Resellers / SIs

FSI & Strategic Partners



Sara French
USPS Partner Manager

Federal / SLED FSI Partners



Amie Stariha
USPS Partner Manager

Territory Public Sector - Manage Resellers / SIs

Hyperscalers



Hollie Anderson
USPS Partner Manager

US Pub Sec Hyperscalers
and Key Strategic Partners

Channel Overlays



Lawrence Butler
Capture Executive



Lauren Montross
Partner Marketing Exec



Peter Gignac
Partner Solution Architect



Thonda Taylor II
Partner Solution Architect



Mark Vanweezendonk
Inside Channel Manager



Hailey Gibbons
Sales Enablement

Four ways partners make money with Elastic

1

Resell and distribution

Transact Elastic through the vehicles your customers already hold. Margin on license, plus the relationship stays yours.

2

Services and integration

Sizing, migration, pipeline engineering, detection content, dashboard and SLO build-out. The largest revenue pool for most of our partners.

3

Managed services

Run it for them. Recurring, high-retention revenue on top of the platform — especially in agencies short on operators.

4

Systems integration and prime contracts

Embed Elastic in a program of record or task order. Longer cycle, largest deal size, strongest lock-in.

Most of our strongest public sector partners run three of the four. If you only resell, you are leaving the majority of the deal value on the table.

Deal registration: the one thing to take away from today

What registration gets you

- Protection on the opportunity you sourced
- A named Elastic seller and solutions architect on the pursuit with you
- Visibility that unlocks field resources — value engineering, executive sponsorship, demo and lab support
- Credit that determines your standing, incentives and investment in the next planning cycle

1

Register early

At first qualified conversation — not when the quote is ready. Late registration is where protection gets contested.

2

Give us real detail

Agency, program, use case, estimated value, timing and vehicle. Thin registrations get slow answers.

3

Work the joint pursuit

Bring your Elastic counterpart into the account meeting. Registered-and-silent is not a strategy.

4

Keep it current

Update timing and value as the deal moves.

Your partner manager will send the link and walk your team through submission this week.

Enablement: get your team accredited, not just briefed



Sales

- Solution positioning across Search, Observability and Security
- Play-by-play battlecards and objection handling
- Public sector value messaging and TCO framing



Sales engineering

- Security SE accreditation: hands-on SIEM, detection engine and AI labs
- Demo environments and guided lab access
- Architecture and sizing guidance for regulated environments



Delivery and practice

- Migration and pipeline engineering patterns
- Detection content and dashboard build-out
- Joint technical workshops — security, AI security, and Zero Trust

Seismic Partner Salesroom

Your self-service library: play guides, upsell assets, competitive positioning and the latest release content. If you cannot find what you need there, tell your partner manager — we are actively rebuilding the public sector content set.

Where to meet customers with us — next 60 days

Aug 27

Tines Gov Builder Connect

Reston, VA

CPE-eligible, hands-on. Elastic-sponsored. Good for SOC modernization conversations.

Sept 8

Billington CyberSecurity Summit

Washington, D.C.

Our highest-priority event of the quarter. Senior federal cyber leadership in one room.

Sept 15

Cyber Defense Breakfast

Washington, D.C.

Executive-level federal security audience with on-site media presence.

Sept 17

Leadership Connect

Washington, D.C.

Evening executive networking — bring the customer you want in front of our leadership.

Late Sept

SLED conferences

Multiple

State CIO and higher-education audiences — the right venue for SLED-focused practices.

Oct 6

FSI virtual enablement

Virtual

Deep-dive session for systems integrator teams building Elastic into programs.

The Billington ask: every partner books at least two customer meetings around the summit — tell us who you are targeting and we will help set them.

Joint marketing: what we will build with you

1

Joint campaigns and webinars

Co-branded demand generation against a named use case — threat hunting, log consolidation, AI search. We bring the content and the audience; you bring the account list.

2

Customer case studies and win stories

Every significant joint win is a candidate for a public case study. Your logo, your delivery, our platform — credible proof for the next agency.

3

Thought leadership

Joint papers and blogs on the topics agencies are being told to solve: Zero Trust architecture, post-quantum readiness, agentic SOC.

4

Executive briefings

Get your customer in front of Elastic executives and product leadership. This is a closing tool, not a courtesy meeting — use it on real deals.

Bring us a customer who will go on record and we will invest behind it — interviews, speaking slots, media and campaign support.

Your next 90 days — what good looks like

First 30 days

- Register every qualified opportunity in your pipeline today
- Pull your list of Elastic logging accounts and book metrics conversations
- Book two customer meetings around Billington
- Name your accreditation candidates

By 60 days

- Complete sales and SE accreditation for your core team
- Run one joint campaign or webinar with us against a named account list
- Bring one customer forward for a case study or TEI interview

By 90 days

- A repeatable services offer attached to at least one play
- A joint account plan with your partner manager covering your top five agencies
- First-quarter pipeline built and registered, not just forecast

Everything on this slide is something your partner manager can help you start before the end of this week.

Thank you

We are investing in your success because mission outcomes get delivered through you, not around you.

- Register your qualified deals this week
- Book two customer meetings for Billington
- Name your accreditation candidates
- Bring us one customer willing to go on record

Darryl Peek II

VP, Partner Sales — U.S. Public Sector, Elastic

Your partner manager is your fastest path to everything in this deck.

Registration links, enablement scheduling and joint planning start there.

Elastic FY27 Q2 Quarterly Partner Connect | August 25, 2026 | Partner-shareable

USPS Solutions Architecture Update

Thonda Taylor II

Sr. Partner Solutions Architect



What's New in Elastic 9.5

First release of FY27 · Security · Observability · Platform · Search

Security

Sentinel Migration*

[TP] KQL to ES|QL, 97% translated

Attack Discovery*

[GA] Rebuilt on skills

Rule Change History

[GA] Diff + rollback, all tiers

Detection Rule Skills

[GA] Coverage gaps, noisy rules

Alert Triage

[EXP] Per-rule pre-triage

Observability

Prometheus + PromQL*

[GA] Full stack now live

Managed Integrations

[GA] 200+ agentless, no collector

AWS Metrics Quickstart

[GA] 40 alerts, 8 SLOs OOB

Migration Tooling*

[TP] Grafana + Datadog to Kibana

APM Dependencies

[GA] Rebuilt service analysis

Platform

Columnar Mode*

[TP] 3.5x storage efficiency

Cases as Data

[GA] Analytics indices + skill

Case Templates

[GA] 200 per space, MSSP-ready

AutoOps Insight API

[GA] GovCloud in September

Workflow Triggers*

[GA] Case + alert event-driven

Search + Agents

Vector Database*

[GA] New Serverless project,
VectorDB index mode

ES|QL Federation

[EM] Query S3 Parquet in place

Agent Observability*

[GA] Traces, tokens, rounds

Agent HITL Controls

[GA] Approval gates on tools

Context Engine

[SOON] Meridian, 9.6 roadmap

9.5 Mapped to Federal Priorities

Every major 9.5 capability maps to an active federal requirement.



M-26-14

CEM + THIRF

Prometheus + PromQL GA

CEM: metrics + logs in one

Columnar Mode [TP]

THIRF: 3.5x retention economics

Managed Integrations GA

200+ sources, no collector

ES|QL Data Federation

Query S3 archives in place

Sentinel Rule Migration

Consolidate onto one SIEM



Zero Trust

Visibility & Analytics Pillar

FedRAMP High on ECH

CUI, ZTA workloads

FIPS 140-3 full-stack

Sept 2026 deadline

Rule Change History GA

NIST change management

Entity Resolution

One identity profile

AutoOps in GovCloud

Insight API, September



Agentic AI

AI-Driven SOC + Mission Ops

Attack Discovery Skills

Agentic triage out of box

Detection Rule Skills

Closes coverage gaps

Alert Triage Workflow

Verdict + rationale [EXP]

Agent HITL Controls

AI proposes, analyst approves

Workflows + Agent Builder

Meets M-26-14 Level 4

ElasticsearchAgentsDiscoverDashboardsWorkflowsMachine LearningData management

New workflowUnsaved changes

JSON Schema

```
name: New workflow
version: "1"
name: Daily Joke
description: Generates a joke using AI every day at 9am UTC and posts it to the Slack
enabled: false
description: This is a new workflow
triggers:
  - type: manual
    inputs:
      - name: message
        type: string
        default: "hello world"
  - type: scheduled@
    with:
      rrule: DAILY
      interval: 1
      tzid: UTC
      byhour:
        - 9
      byminute:
        - 0
steps:
  - name: hello_world_step
    type: console
  - name: generate_joke
    type: ai.prompt@
    with:
      message: "{{ inputs.message }}"
      prompt: Tell me a joke. Respond with only the joke text - no preamble, no explanation, no commentary.
      connector-id: < Anthropic Claude Sonnet 4.5 Anthropic-Claude-Sonnet-4-5
  - name: post_joke_to_slack
    type: slack2.sendMessage@
    with:
      channel: C08HV4TMJDT
      text: "{{ steps.generate_joke.output }}"
      connector-id: < my-slack-workspace my-slack-workspace
```

5 of 5AcceptDecline

No validation errors

Accept AllDecline All

Daily Joke Generator to SlackElastic AI Agent

2 tools responded >

I found two Slack connectors. Let me also look up the AI connector and find the jokes channel ID.

2 tools responded >

Found the #jokes channel (ID: C08HV4TMJDT). Now let me check for AI connectors and generate the workflow:

1 tool responded >

I have everything I need. Now let me generate the workflow:

1 tool responded >

Here's your daily joke workflow 🎉

Daily Joke+23 -11

```
name: New workflow
version: "1"
name: Daily Joke
description: Generates a joke using AI every day at 9am UTC and posts it to the Slack
enabled: false
description: This is a new workflow
triggers:
  - type: manual
    connector-id: < my-slack-workspace my-slack-workspace
```

Show 30 more lines

Daily JokePreview

1 trigger and 2 steps

Here's what was built:

- **Trigger:** Runs every day at 9:00 AM UTC
- **Step 1** - generate_joke : Uses ai.prompt with Anthropic Claude Sonnet 4.5 — prompts the model to return only the joke, no preamble
- **Step 2** - post_joke_to_slack : Sends the raw joke text to your #jokes channel (C08HV4TMJDT) via my-slack-workspace

The workflow is currently disabled — enable it when you're ready to start the daily laughs! Want me to run it once now to test it?

   45s

Attachment added: Off for workflow 'Daily Joke'

Attachment added:

Ask anything

Anthropic Claude Sonnet 4.6



Home



Discover



Dashboards



Rules



Detections



Workflows



Agents

Attack
discovery

More



Workflows

Workflows

Template library

Executions

Template Library

Experimental



Contribute a template

Search templates

Security

All categories

17

AI agent

3

Case management

2

Detection

3

Enrichment

2

Hunting

1

Integration

1

Response

9

Root cause analysis

1

Search

2

Threat intelligence

2

Utility

1



Browser Extension Daily Reputation Check

Daily ES|QL hunt for rarely-seen Chromium browser extensions using Elastic Defend .crx file events on...

hunting response



Hash Threat Check (VirusTotal)

Check a file hash (MD5, SHA-1, or SHA-256) against the VirusTotal database and produce a human-...

detection enrichment threat-intel



Mark Alert as Acknowledged

Set the status of a detection alert to "acknowledged" via the Security Detection Engine...

response



Create Slack Channel

Create a new Slack channel (public or private) via the Slack v2 API. Useful as a building block for...

integration



IP Reputation Check (AbuseIPDB)

Assess the reputation of an IP address using AbuseIPDB and enrich the result with geolocation...

enrichment threat-intel



Remediate Behavior - Windows Script File

On a Malicious Behavior Prevention alert or a daily schedule, find Windows behavior alerts involving...

response

Partner Plays + 90-Day Action Plan

Three plays. Three moves. Every public sector account has at least one open door.

Partner Plays

DISPLACEMENT: Replace the incumbent

Splunk rule + dashboard migration GA. Dashboard CLI covers Datadog + Grafana. M-26-14 creates urgency.

[Splunk / Datadog / Grafana](#) · [Rule migration GA](#) · [M-26-14 urgency](#)

SERVICES: Scope the engagement

Logging maturity assessment. FedRAMP High ATO. Workflow + Skills implementation.

[M-26-14 assessment](#) · [FedRAMP High ATO](#) · [Workflows + Skills](#)

EXPANSION: Grow the contract

30x faster than Prometheus. 2.6x more efficient. <50% cost of Datadog. M-26-14 retention justifies storage spend.

[30x Prometheus](#) · [<50% Datadog](#) · [FedRAMP High + FIPS](#)

90-Day Action Plan

Days 1–30: Open mandate conversations

- Brief every ECH account on FedRAMP High
- Flag M-26-14 logging gaps from renewal lists
- Demo Splunk rule migration tool for customers

Days 31–60: Scope the first engagement

- Run an M-26-14 maturity assessment
- Co-design one Attack Discovery workflow
- Get SE/SA trained on GA Security Skills

Days 61–90: Lead renewals with math

- Update TCO with performance/cost benchmarks
- Brief on Dell AI Factory + NVIDIA cuVS

Questions?

Thonda Taylor II

Solution Architect | Partner Channels

Contact Information

thonda.taylorii@elastic.co

Technical Enablement Offerings:

`school` Workshops for your teams

`model_training` Demo Training

`gps_fixed` Technical Positioning

`edit` Whiteboarding

`architecture` Elastic Architectures

Thank you!



US Public Sector Marketing Update

Lauren Montross

Partner Marketing Manager, US Public Sector



elastic

| The Search
AI Company

What's on the agenda?

- Global Partner Events
 - Regional Partner Events
- Billington Cybersecurity Summit
- Advocate Marketing & Partner Blogs

FY27 Global Events at a Glance

Elastic ON

- Sept. 23
ElasticON Bengaluru
- Oct. 8
ElasticON NYC
- Oct. 20
ElasticON Amsterdam

- Nov. 4
ElasticON SF

- Feb. 25
ElasticON London
- Mar. 23
ElasticON Singapore
- ElasticON PubSec DC

3PC

- June 1-3
Gartner Security Risk Mgmt Summit
- Jun. 29 - Jul. 2
AI Engineer World's Fair

- Aug. 1-6
Black Hat U.S.

- Nov. 9-12
KubeCon NA
- Nov. 17-20
Microsoft Ignite
- (Nov. 30 - Dec. 4
AWS re:Invent

- Mar. 15-18
KubeCon EMEA
- Apr. 5-8
RSA Conference
- GTC Nvidia
- Google Cloud

May-July

August - October

November - January

February - April

Q1

Q2

Q3

Q4

Q2FY27 USPS Partner Marketing

Aug 2026

- **8/1-8/6:** Black Hat
- **8/4:** WWT SLED NE Team Dinner NYC
- **8/4-8/6:** USMC / GAI 3-Day AI Workshop at Marine Corps Base Hawaii
- **8/5:** GDIT Reception at Black Hat
- **8/9-8/12:** DoDIIS 2026
- **8/10:** Happy Hour with Norseman at DoDIIS
- **8/11-8/13:** DHITS 2026
- **8/11:** Elastic Hands On Workshop
 - Registrations
- **8/17-8/20:** TechNet Augusta
- **8/19:** Happy Hour with ECS at TechNet Augusta
- **8/19:** Epoch Event
- **8/24-8/26:** DAFITC
- **8/25-8/26:** NVIDIA AI Advisor Workshop (NVIDIA HQ, Santa Clara, CA)
- **8/25:** Gigamon & Elastic Threat Hunting Webinar
- **8/25:** GPS/Elastic Durham Bulls Baseball Game
- **8/27:** Tines Builder Connect

Sept 2026

- **9/1:** 2nd Annual Optiv + ClearShark Drive an Impact Charity Golf Tournament
- **9/3:** FSI Baseball Suite: Orioles VS Red Sox at Camden Yards
- **9/3:** Automating ATO & RMF Webinar with Elastic and Tines
- **9/8-9/10:** Billington
- **9/8:** Peak Cyber Symposium
- **9/10:** GovJam
- **9/12:** R4's 6th Annual Charity Event
- **9/15-9/16:** AWS Imagine
- **9/18:** Service to the Citizen Awards
- **9/19:** Iron Bow Charity Golf Tournament
- **9/20-9/24:** TribalNet
- **9/21:** Honoring the Green Golf Tournament
- **9/22:** DOT & FAA Cyber Symposium
- **9/22:** INL Cyber Day with Impres
- **9/23:** US Cyber Challenge Awards Dinner
- **9/24:** Colossal Busy Season Sponsorship
- **9/29-10/2:** EDUCAUSE

Oct 2026

- **10/1:** RIVA's 17th Annual Staying Connected Charity Event
- **10/2:** Effectual Golf Tournament (AWS)
- **10/3:** PMIWDC 2026 Annual Conference - Keynote Panel Invite
- **10/5:** V3Gate Charity Golf Tournament
- **10/12-10/14:** AUSA Annual Meeting + Expo
- **10/13:** Security Workshop with SWISH and Carahsoft
- **10/16:** 22 for You with Colossal
- **10/20:** Open Source Tech Summit
- **10/21:** Elastic at Dell's Innovation Summit
- **10/22:** Nebraska Public Sector Cybersecurity & AI Summit
- **10/26-10/29:** AFCEA Indo Pacific

Elastic Engagement at Billington Cybersecurity Summit

Walter E. Washington Convention Center

September 8-10, 2026

Exhibit Details:

- Generative AI Partner
- Booth #311



Speaking Sessions:

1. Tuesday 9/8: **Mainstage Fireside Chat “Data as a Warfighting Advantage: Operationalizing the Digital Battlefield”** (Cameron Stanley, Chief Digital and Artificial Intelligence Officer, Department of War and Chris Townsend, Elastic)
2. Tuesday 9/8: **Mainstage General Session Panel — The Future of Cyber Warfare** (Moderator: Lieutenant General (Retired) Stephen Fogarty, Senior Executive Advisor, Booz Allen, John Garstka, Director, Cyber Warfare, OUSW A&S, Department of War, Dave Carroll, Vice President, Cyber Capability Engineering and Strategy, Sean MacKirdy, AVP, National Security, Elastic)
3. Wednesday 9/9: **Breakout Session Panel C4 — Building a Modern Malware Analysis Workflow: Tools, Automation & Rapid Triage** (Moderator: Gerald “Jerry” Mazur, Senior Advisor, Cyber Intelligence, Peraton, Rain Baker, Senior Incident Response Specialist, Nightwing, Adam Maddock, Section Chief, Cyber Division, FBI, John Harmon, GVP, Cyber Solutions, Elastic)

Ancillary Events:

1. Bytes, Burgers & Brews: Unwind After Billington
 - a. The Capital Burger, 1005 7th St NW, Washington, DC 20001
 - b. [Landing Page](#)

Better Together: Customer Stories & Blog Post

Customer Stories:

- Do you have customer stories to highlight?
- Customer references can help *drive revenue* and *close deals quicker*
- Elastic Contact: Michelle Gardner, Sr. Director of Customer Insights and Advocate Marketing

Partner Blogs:

- Do you have a blog that you plan to post?
- Elastic Contacts: Leanne Link, Sr. Manager, Product Marketing; Alexia Russell, Sr. Director, Global Public Relations

Thank you!



Q&A

Carahsoft Contact Information

Questions? Please reach out.



Kris Helweg

Sales Team Lead

571-662-3263

Kris.Helweg@carahsoft.com



Thank you!

