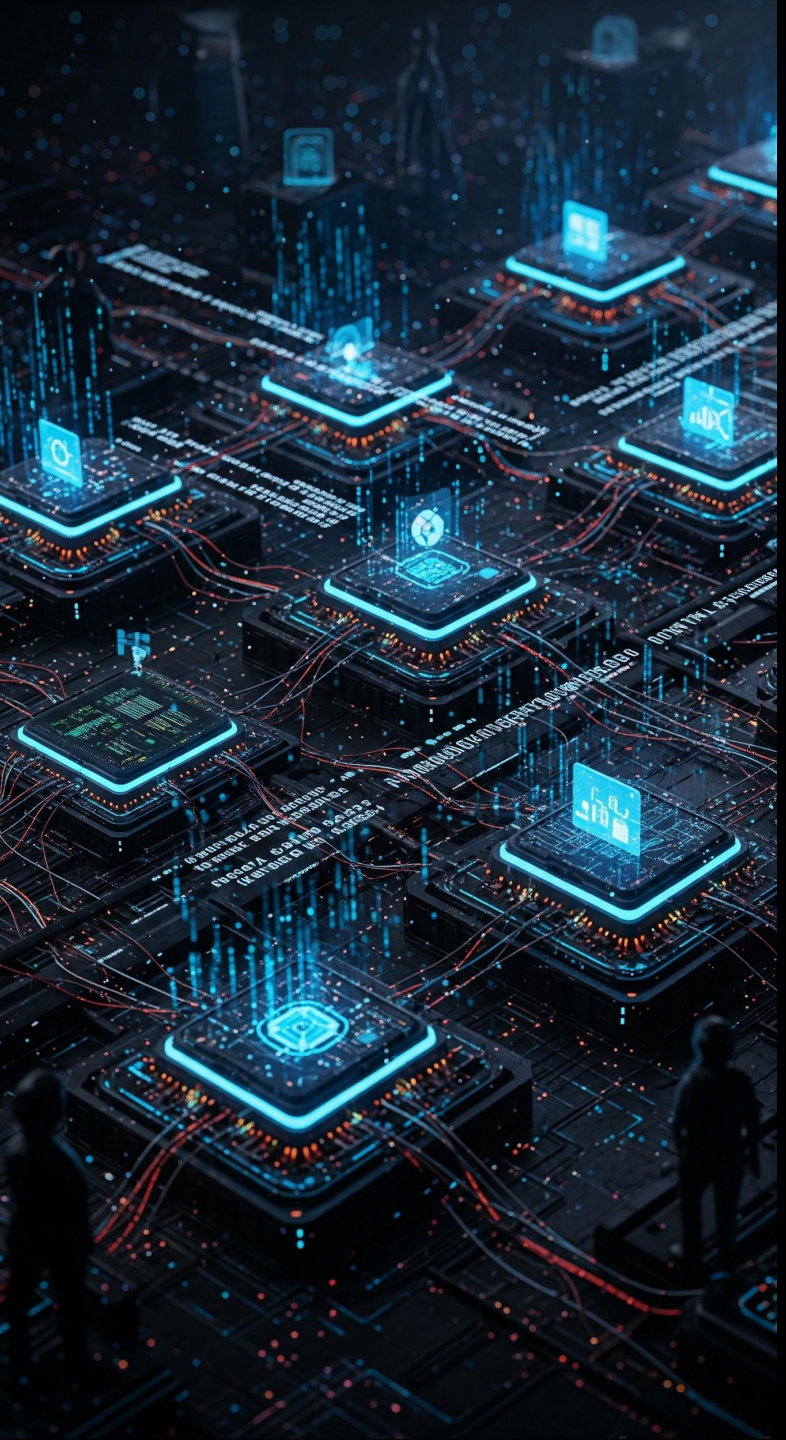


narf

Ranger.ai, into an Agentic AI Age

July 2025 Investor Update

Steve Bassi, CEO and Founder
Michael Locasto, CTO
John Herring, Executive Chairman

Disclaimer

The content of information contained in these slides and any accompanying verbal presentation (together, the “Presentation”) has not been approved by an authorised person within the meaning of the Financial Services and Markets Act 2000 (“FSMA”). Reliance upon this Presentation for the purpose of engaging in any investment activity may expose an individual to a significant risk of losing all of the property or other assets invested. If any person is in any doubt as to the contents of this Presentation, they should seek independent advice from a person who is authorised for the purposes of FSMA and who specialises in advising in investments of this kind. This Presentation is being made available for information purposes only. This Presentation has been prepared by, and is the sole responsibility of, the directors of NARF plc (the “Company”). Those directors have taken all reasonable care to ensure that the facts stated herein are true to the best of their knowledge, information and belief. This Presentation does not constitute, or form part of, any offer or invitation to sell or issue, or any solicitation of any offer to purchase or subscribe for, any shares in the Company nor shall it or any part of it, or the fact of its distribution, form the basis of, or be relied upon in connection with, or act as any inducement to enter in America (or any of its territories or possessions) (together, the “US”), Canada, Japan, Australia, the Republic of South Africa, or the Republic of Ireland, or to any corporation, partnership or other entity created or organised under the laws thereof, or in any other country outside the United Kingdom where such distribution may lead to a breach of any legal or regulatory requirement. The recipients should inform themselves about and observe any such requirements or relationship. The Company’s ordinary shares have not been, and are not expected to be, registered under the United States Securities Act 1933, as amended, (the “US Securities Act”) or under the securities laws of any other jurisdiction, and are not being offered or sold, directly or indirectly, within or into the US, Canada, Japan, Australia, the Republic of South Africa or the Republic of Ireland or to, or for the account or benefit of, any US persons or any national, citizen or resident of the US, Canada, Japan, Australia, the Republic of South Africa or the Republic of Ireland, unless such offer or sale would qualify for an exemption from registration under the US Securities Act and/or any other applicable securities laws. This Presentation or documents referred to in it contain forward-looking statements. These statements relate to the future prospects, developments and business strategies of the Company and its subsidiaries (the “Group”). Forward-looking statements are identified by the use of such terms as “believe”, “could”, “envisage”, “estimate”, “potential”, “intend”, “may”, “plan”, “will” or the negative of those, variations or comparable expressions, including references to assumptions. The forward-looking statements contained in this Presentation are based on current expectations and are subject to risks and uncertainties that could cause actual results to differ materially from those expressed or implied by those statements. If one or more of these risks or uncertainties materialises, or if underlying assumptions prove incorrect, the Group’s actual results may vary materially from those expected, estimated or projected. Given these risks and uncertainties, no reliance should be placed on such forward looking statements. These forward-looking statements speak only as at the date of this Presentation. No undertaking, representation, warranty or other assurance, express or implied, is made or given by or on behalf of the Company, Strand Hanson or any of their respective directors, officers, partners, employees or advisers or any other person as to the accuracy or the completeness of the information or opinions contained herein and to the extent permitted by law no responsibility or liability is accepted by any of them for any such information or opinions. In particular, no undertaking, representation, warranty or other assurance, express or implied, is given as to the achievement or reasonableness of any management estimates and forecasts. Notwithstanding the aforesaid, nothing in this paragraph shall exclude liability for any representation or warranty made fraudulently. Liability for such statements and information is expressly disclaimed by the Company directors. verified by footnotes. Liability for such statements is expressly disclaimed by the Company directors.

Agenda

- Open Source Software is critical infrastructure, total investment: $9T
- How do companies consume OSS, why it is critical.
- Meet the product team
- What is ranger.ai: 1.0, initial customers
- Current, Agentic AI release
- Future Agentic Roadmap
- GTM, launching lead generation, freemium model

narf

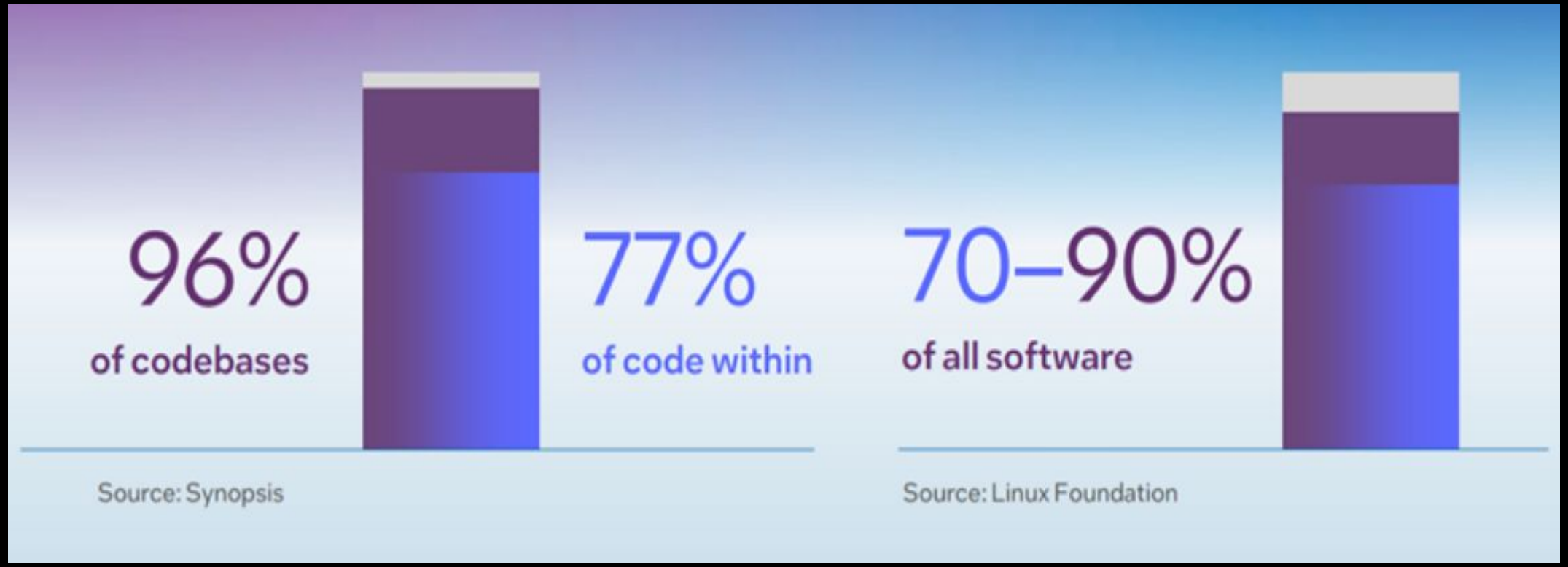
Entrepreneurship

Open Source Software: The $9 Trillion Resource Companies Take for Granted

Many companies build their businesses on open source software, code that would cost firms $8.8 trillion to create from scratch if it weren't freely available. Research by **Frank Nagle** and colleagues puts a value on an economic necessity that will require investment to meet demand.


Featuring Frank Nagle and Manuel Hoffmann. By Rachel Layne on March 22, 2024.

pervasive.

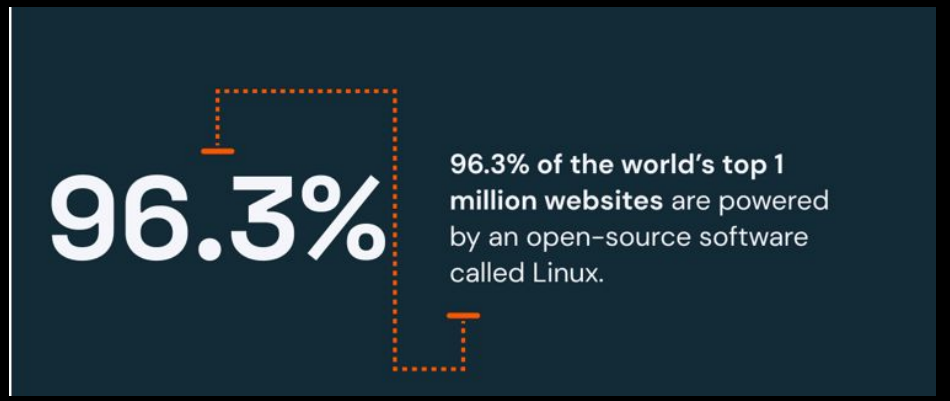


In 2011, Marc Andreessen declared ***"software is eating the world."*** Turns out that open source is **pervasive** in the DNA of that software eating the world.

narf

Open source consumption has exploded, with estimates placing downloads at over 6.6 trillion in 2024.

TL;DR people are building on OSS infrastructure that is moving fast with contributions from all of the planet.



narf

Open-source software is the software wiring of the modern world. It's built into nearly every product and service — from mobile apps to cloud platforms — just like electrical wiring is built into your home. Developers and companies simply 'plug in' their applications, much like plugging in appliances.

Few ask: Who installed that wiring? Was it maintained? Is it safe?

This invisible infrastructure powers everything — and yet the people behind it are often unknown, unvetted, and unmonitored. That's a massive, overlooked risk.

Reducing risk at relentless pace of OSS.

Contributors: The Human Layer

Millions of developers worldwide across various time zones
Volunteer, corporate-backed, and anonymous participants
Highly distributed - no central governance
Varying levels of trust, skill and intent

Projects: The Building Blocks

Hosted on public platforms (e.g., GitHub, GitLab)
Includes libraries, tools, frameworks, runtimes
Widely reused across government and commercial applications
Often maintained by 1-3 people (or sometime no one)

Updates: The Velocity

Constantly changing - new versions, forks, patches
Tens of thousands of commits daily
Dependencies evolve without notification

narf

Refresh of attacks from March 2024

WIRED

WIRED SECURITY POLITICS GEAR BACKCHANNEL BUSINESS SCIENCE CULTURE IDEAS MERCH SIGN IN

BY ANDY GREENBERG AND MATT BURGESS SECURITY APR 3, 2024 9:54 AM

The Mystery of 'Jia Tan,' the XZ Backdoor Mastermind

The thwarted XZ Utils supply chain attack was years in the making. Now, clues suggest nation-state hackers were behind the persona that inserted the malicious code.

Black Hat News Omdia Cybersecurity

DARKREADING

XZ Utils Backdoor Implanted in Carefully Executed, Multiyear Supply Chain Attack

Had a Microsoft developer not spotted the malware when he did, the outcome could have been much worse.

The Economist

Menu Weekly edition The world in brief Search

Science and technology | Hacking the internet

A stealth attack came close to compromising the world's computers

The cyber-scare shows why the internet's crowdsourced code is vulnerable

The Guardian

TechScape: How one man stopped a potentially massive cyber-attack - by accident

The New York Times

THE SHIFT

Did One Guy Just Stop a Huge Cyberattack?

A Microsoft engineer noticed something was off on a piece of software he worked on. He soon discovered someone was probably trying to gain access to computers all over the world.

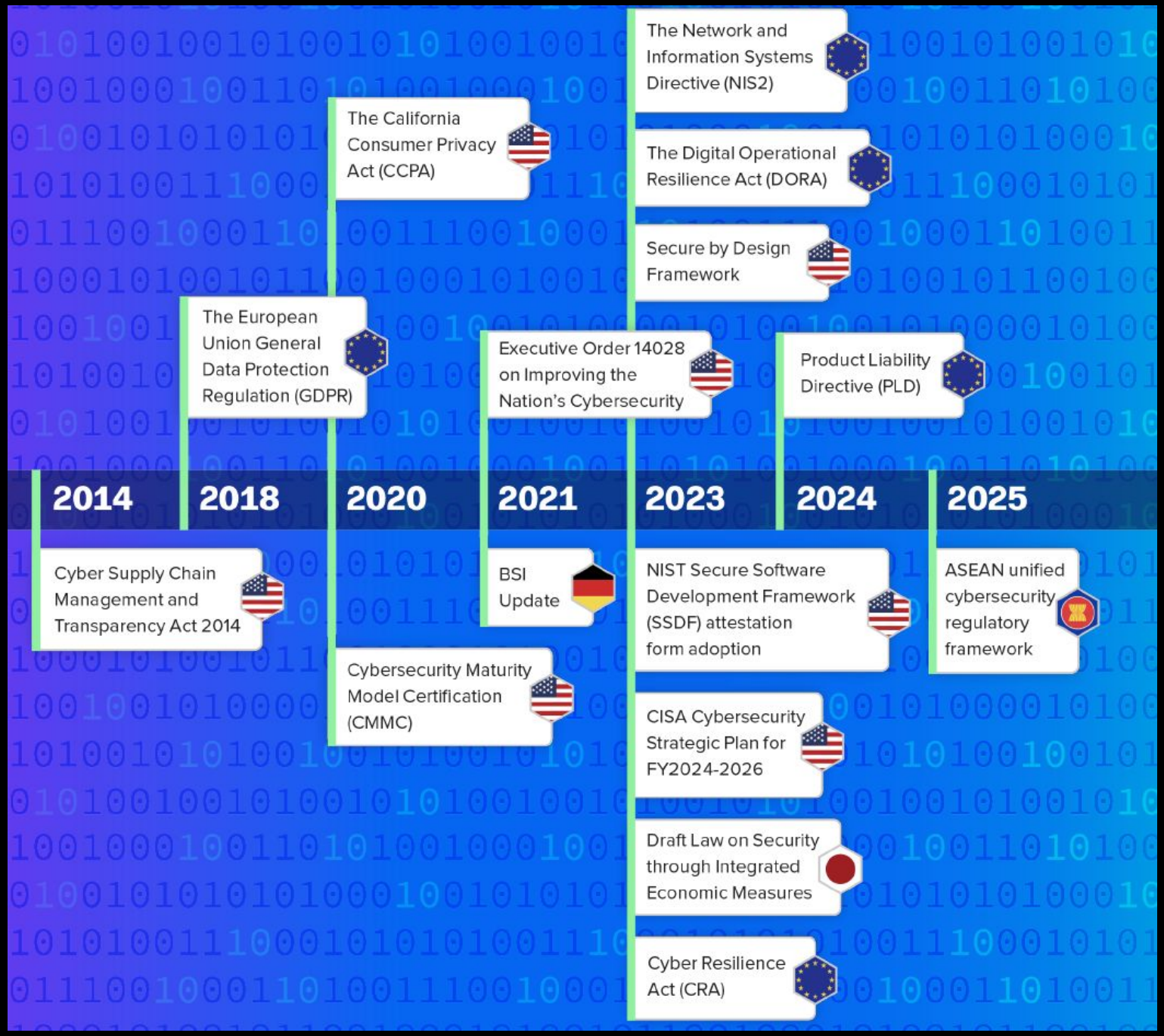
narf

and Accelerating…

narf

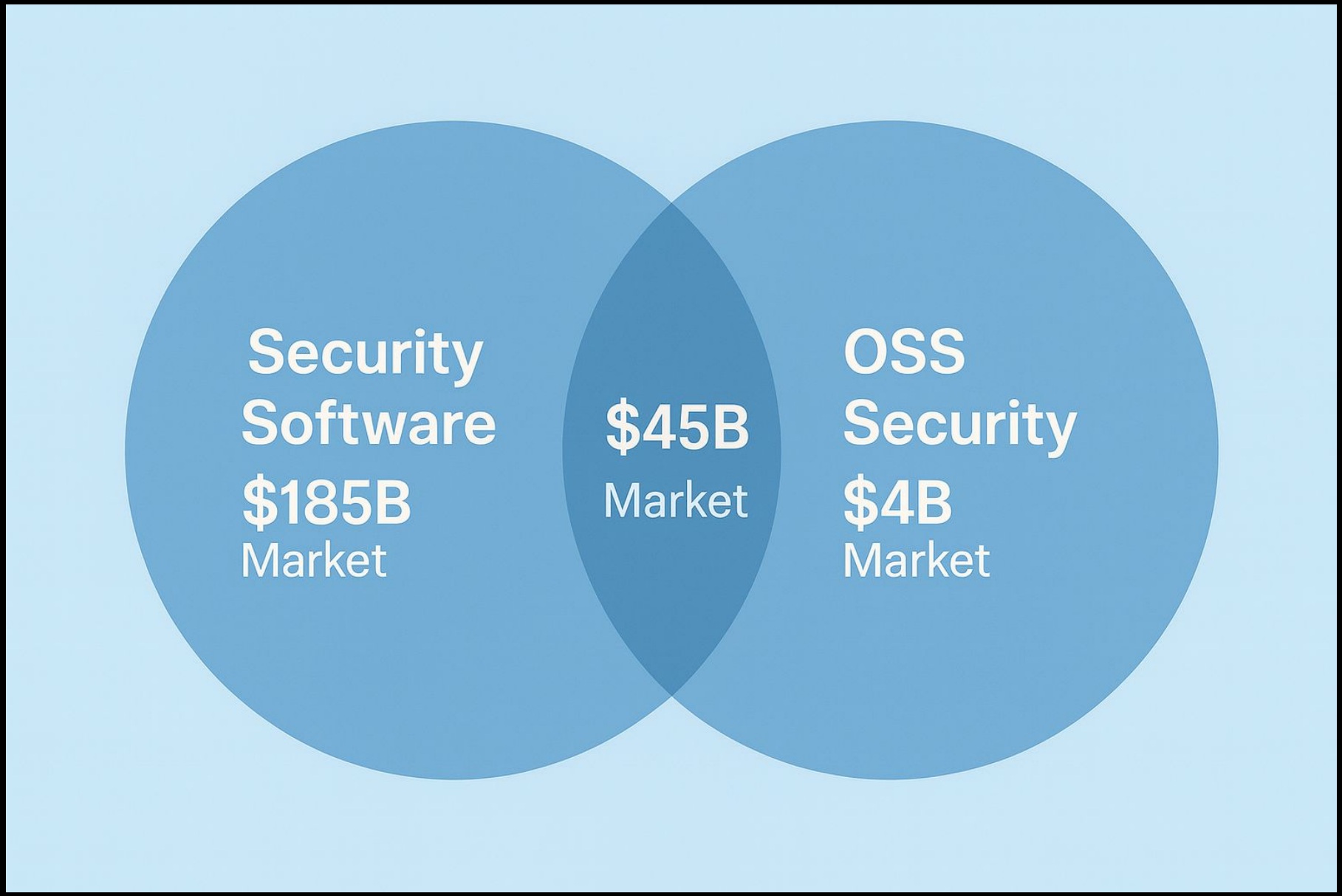
Regulatory …acceleration

- Regulatory security requirements still accelerating
- Sign Governments are realizing that OSS is critical infrastructure
- No regulatory pass by using open source
- EU Software vendors are now liable for bad software, including OSS
- How do you de-risk leveraging that $9T OSS investment?



narf

Significant Market Opportunity



narf

Ranger.ai Product Team

Dr. Michael E. Locasto
CTO and R&D Tsar behind Ranger and other recent DARPA wins.

Dr. Sean Carrick
Senior Security Research, responsible for AI application on binary security vulnerabilities.

Greg Roussas, MS Computer Science
Lead developer, AI & Agentic solutions for Open Source Security.

Stuart Nagy-Kato
Sr Product Development Manager for Ranger.ai.

narf

OSS is Now Enterprise Critical Infrastructure

- Deployed as software containers that run in clouds handling:
  - Financial transactions and markets
  - Critical customer data
  - Classified information
  - Life-or-death military systems

- Used with underappreciation of resources required to manage risks of this *free* software:
  - Developer geographic origin and data sovereignty
  - Backdoors in the source code, its dependencies
  - Innocent security vulnerabilities introduced by varying developer quality/attention
  - Support and mitigation of exploitation during an attack

narf

Our AI Ethos:

Harness Agentic AI's ability to recognize, automate, and scale Narf's human security expertise and workflows for our customers who want to continue to *safely* leverage the $9T investment already made into building on OSS.

narf

Ranger 1.0 to Ranger.ai

Ranger 1.0 leveraged $4M+ DARPA funding to build capability. USAF validated the is real, and valuable and 1.0 is being taken to market now. However, 1.0 needs Agentic DNA to *extend and scale its value beyond Government customers.* Along the way we've experienced the value of Agentic AI, reframing our ambition based on encouraging initial customers:

- From a scanner to a suite of AI agents that can *adapt* and *scale* to vast OSS infrastructure
- From esoteric data on developer habits to timely, actionable fixes for defenders
- To comprehensively addressing the problem of making OSS safer to build on

What We Hear from Our Initial Customers

“ No one else in the industry is background checking developers who make source contributions to the software we rely on to deliver our cluster services – big risk on a huge revenue driver for us”

- US Air Force (USAF) - Platform One
  - Repository of record for ‘safe’ OSS distribution Military & Contractor applications
  - Must maintain daily security vigilance across ~6000 OSS software projects
  - OSS software projects have a global mix of developers, poorly understood
  - Limited security staff attention (~30 persons) does not scale to 6000 OSS projects
  - Security patches are slow, manual, and likely incomplete giving attackers *time*

- A Large Government and Commercial IT Services and System Integrator
  - Billions in USG contracts for secure cluster operations, delivered with OSS
  - Additional multi-million dollar contracts for customized software on OSS bedrock
  - Narf’s Agentic platform scales to meet their challenges, timelines
  - Partnership to deliver millions more in joint, strategic, OSS onshoring efforts

narf

What is Ranger: Narf's Agentic AI Security Platform

- The Agentic AI Platform for OSS security operations
    - Scale past bespoke human security expertise with continuous Agentic AI vigilance
    - Identify vulnerable software containers missed by traditional approaches
    - AI remediation of vulnerable containers *specific to customer environments*
- A data capture platform surrounding customer environments, pain points
- A sales conduit:
    - Partner system integrators capture onshoring OSS work
    - Services revenue for agentic/human partnership remediating vulnerabilities in Customer Environments

narf

Roadmap and Initial Customers

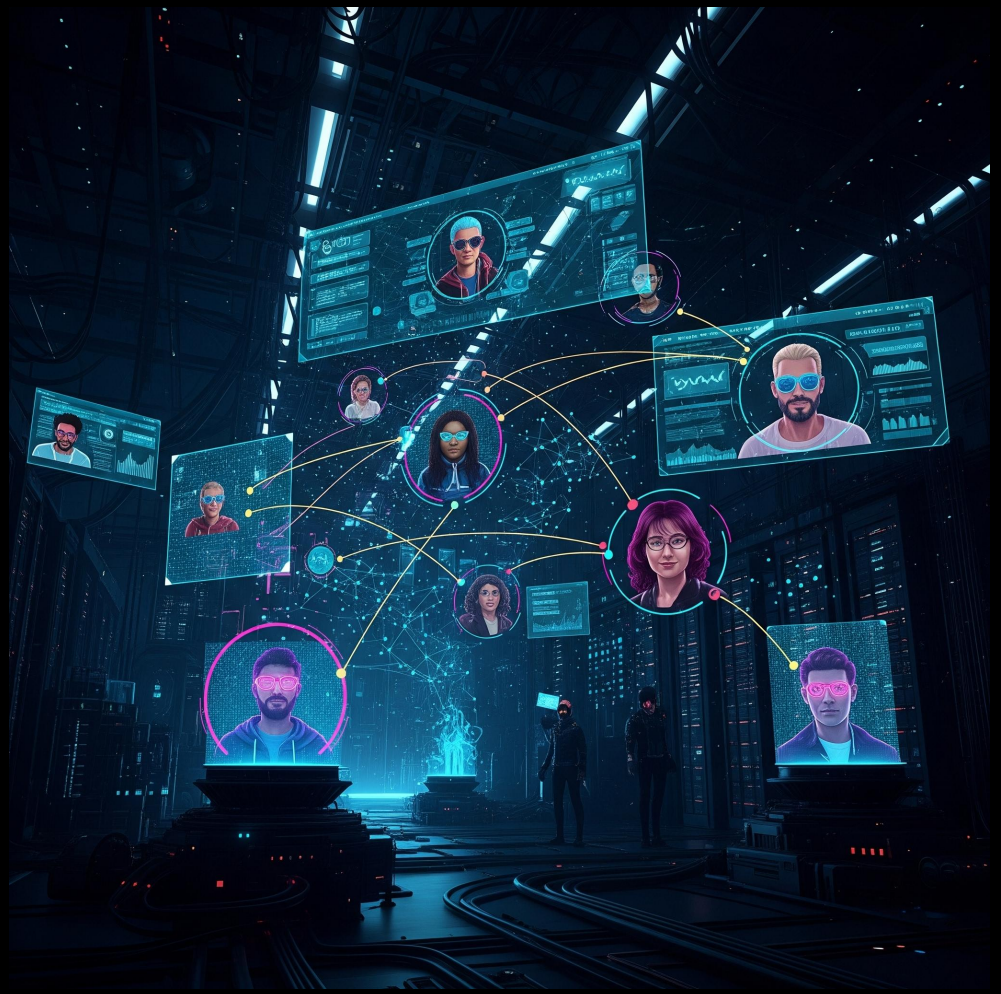
- 2 Launch Customers
  - USAF
  - A major system integrator with $B USD in federal compute cluster contracts
- We expect to announce contracts in Q4:
  - New spending bill and FY25 YE money are being spent in Sep-Oct timeframe.
  - Government spending unusually weird
  - Both launch customers dependent on these cycles
- Six/low-seven figure budgets submitted to launch customers:
  - Platform access
  - Narf security team, paired with our Agentic AI flows
  - Design partner status on expanding Agentic AI platform additions

narf

The Power of Agentic: Infrastructure Project Dynamics

- Constantly health checks on critical projects:
  - Allows identification of interventions for national security
  - What is the national strategic reserve of OSS developers?

- Customer impact to date:
  - Identification and tracking of key projects, health
  - Notification on critical infrastructure maintenance being abandoned
  - Support plans for replacing abandonware

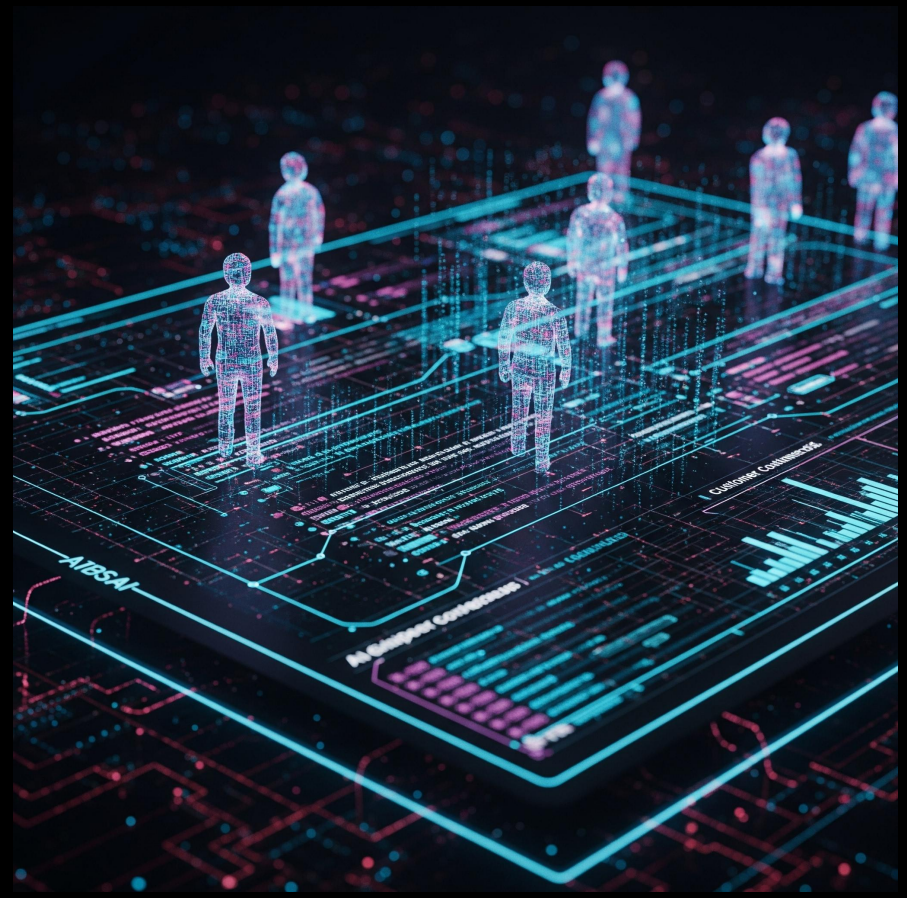


narf

The Power of Agentic: Developer Background Checks

- Constantly monitors developers delivering critical code:
  - Educational background
  - Company employment, association
  - Are devs qualified to be writing any critical code in customers eyes?

- Customer impact to date:
  - Passed on potential security vulnerabilities in customer containers
  - Highlighted critical infrastructure components maintained by sanctioned adversaries
  - AI reconstruction of critical human developer resumes, beginnings of a national strategic reserve of OSS capability



narf

Power of Agentic: Realtime Source Security Reviews

- Uses advanced models to review open source code contributions
- Understands security issues and their potential impact to customer environments
- Can review source code at speed, scale (100K+ commits day) impossible for humans
- Impact to date:
  - 20K recent software contributions agentically vetted
  - 750 introduce security issues likely in customer environments
  - Agenticly generated patches for issues, Narf staff tailoring for customer impact

narf

Future Roadmap: Selected Milestones

Generally:

- All roads are Agentic
- Near term: focus on Ideal Customer Profile and Delivering Agentic Workflows that obviate expensive technical humans, software security engineers
- Long term: capture and scale human security engineering expertise into agentic workflows, building data asset

Q4 2025: Initial 2 customers onboarded to Agentic Vigilance.
Q1 2026: Freemium model release, Agentic vigilance for your cluster. Acceleration in commercial lead generation.
Q2 2026: Customer Tailored Agentic Remediation Services delivered to very large cluster operators.
H2 2026: System integrator partnerships, Government funded Agentic rewrites, maintenance of critical OSS onshoring efforts.
H1 2027: Agentic training, delivery, from 3rd party expert security humans.

narf

#!/bin/thanks

Get in touch:

steve.bassi@narfindustries.com
jh@narfgroup.com

narf