navanta™

TECH-O-WEEN

2026



Mike Venaccio

SENIOR VP SECURITY ARCHITECTURE DEFENSE



Sean Corbin

SENIOR VP OF CLIENT OPERATIONS

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

AGENDA

- **Welcome and Introductions**
  MIKE VENACCIO & SEAN CORBIN
- **The Alchemy of Work: Engineering Agentic AI for the Real World**
  KAUMIL DALAL (WEST MONROE)
- **The Alchemy of the Breach**
  KEVIN BONG (GHOSTSCALE)
- **Alchemists in the Wild**
  NAVANTA CLIENT PANEL WITH DARREN BRIDGES
- **Inside the Laboratory**
  TOM HEARN
- **The Final Concoction**
  ERIC JONES, PATRICK RINSGRED, & STEPHEN MOSS
- **Close**
  MIKE VENACCIO & SEAN CORBIN

© 2026 Navanta™ All rights reserved. navanta.com



DEMYSTIFYING TECHNOLOGY.

CELEBRATING COMMUNITY FI & IT.

HAVING FUN.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

LOOKING BACK AT 2025

- The Art of the Possible with AI
- Microsoft Copilot, Under the Hood
- Brewing Up AI Innovation at RockPointBank
- Warding Off the AI Monsters
- From Haunted House to At Home with AI
- Name That Threat!

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com



“The Alchemists”

TURNING COMPLEXITY INTO CONFIDENCE

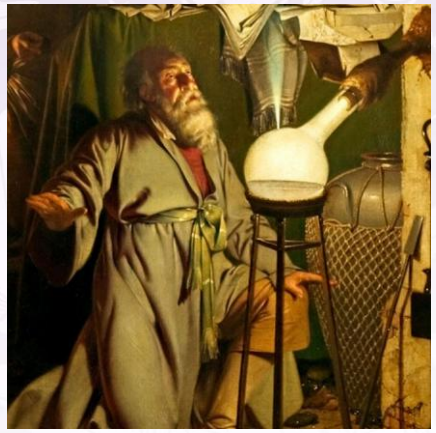
navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Alchemy is a process for turning the unknown into the usable.

© 2026 Navanta™ All rights reserved. navanta.com

Alchemy in Antiquity



Hennig Brand

1669, Hamburg

- Boiled down enormous quantities of urine, convinced its glow meant it held gold
- Found no gold. Found phosphorus, the first new element discovered since antiquity.
- Wrong about the goal. Right about something nobody knew to look for.



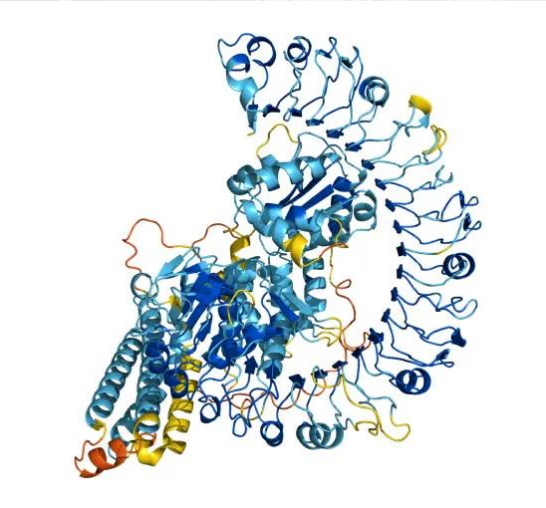
Jabir ibn Hayyan (Geber)

8th century, Arabia

- Invented distillation, crystallization, and evaporation, the lab techniques chemists still use today
- Never found gold. Found the method.
- "Alcohol" and "alkali" both come from his tradition

© 2026 Navanta™ All rights reserved. navanta.com

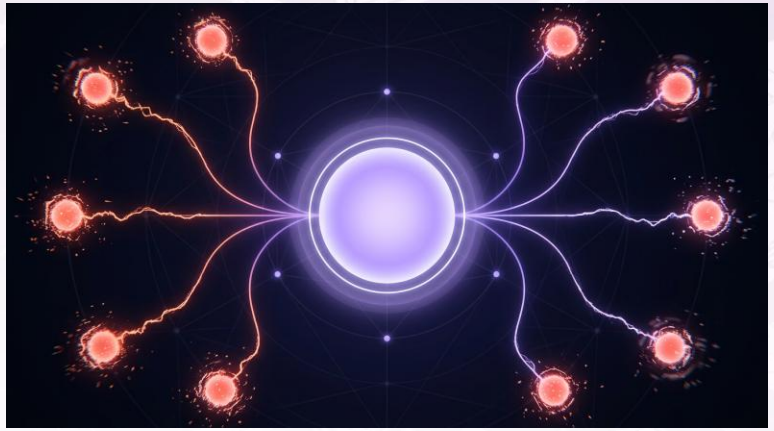
Modern Alchemy



AlphaFold

DeepMind, Nobel Prize in Chemistry 2024

- Predicts a protein's 3D shape from its raw sequence
- Now covers over 200 million proteins
- AI-designed drugs built on this method are already in human clinical trials



Quantum Error Correction

Quantum Computing

- Individual qubits are noisy and unreliable on their own, unusable raw material
- Combines many noisy qubits into one stable, trustworthy logical qubit

© 2026 Navanta™ All rights reserved. navanta.com

Your Alchemy Journey



The Exam Narrative

Translating for examiners

- Raw material: an examiner's evolving expectations, a regulatory framework still catching up to the pace of technology
- The method: turning a shifting external landscape into a clear, evidence-backed story
- The output: an examiner who leaves with real confidence in how the institution operates



The Briefing

Translating for leadership

- Raw material: the real promise of AI, buried inside a wall of technical detail
- The method: turning that information into one clear, confident recommendation
- The output: a system that moves forward with conviction

© 2026 Navanta™ All rights reserved. navanta.com

The Alchemy of Work: Engineering Agentic AI for the Real World





Kaumil Dalal

SR PARTNER, WEST MONROE

Lindsay Scarangello

MANAGING DIRECTOR, TECHNOLOGY & EXPERIENCE

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

west monroe

The AIchemy of Work

Engineering Agentic AI for the real world

Agenda

01 Opening Premise: The Alchemy

02 Agentic AI Trends

03 A practical architecture lens

04 Execution in the Real World

© 2026 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners' prior consent is prohibited.

West Monroe at-a-glance

We're tech-forward advisors who draw on decades of industry and private equity experience to create value quickly, innovate for the future, execute with precision, and lead in an AI-powered world.

Office Locations:

Chicago (HQ) | Los Angeles | New York | Boston
Seattle | Dallas | Minneapolis | San Francisco
Washington, D.C. | London | Costa Rica

Talent Hubs:

Denver | Orange County | Columbus
Pittsburgh | Chattanooga | Portland

WHAT WE DO



Artificial Intelligence

- AI Diligence in M&A
- AI-Powered Data Conversion
- Agentic Transformation
- AI-Enabled Software Engineering
- Integrating AI in Flexible, Secure Architecture
- Human + Agent workflow design
- Practical AI upskilling
- Change leadership for AI adoption



Mergers & Acquisitions

- Carveouts & Divestitures
- Portfolio Value Creation
- Post-Merger Integration
- Transaction Advisory



Operations

- Automation & Productivity
- Cost Reduction
- Outsourcing Advisory
- Supply Chain



Tech & Experience

- Data & Analytics
- Platforms
- Product & Experience
- Security & Cloud
- Software



Organization & People

- Organizational Design
- Organizational Change Management (OCM)
- HR Advisory
- Talent Strategy & Analytics

WHERE WE DO IT

Financial Services
Consumer & Industrial Products
Healthcare
High Tech & Software
Insurance
Life Sciences
Private Equity
Energy & Utilities

© 2026 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners' prior consent is prohibited.

West Monroe's Technology & Experience capabilities at a glance

CREATE VALUE THROUGH SOFTWARE PRODUCTS, INTEGRATIONS & AI AGENTS	TRANSFORM MARKETING, SALES AND SERVICE	UNLOCK THE VALUE OF DATA ASSETS	BUILD SECURE PLATFORMS & ORGANIZATIONS
Software Modernization	Marketing Strategy	Data Strategy & Monetization	Cybersecurity Strategy
Modern Integration Platform	Marketing Process & Technology	Data Governance	Technology Strategy & Enterprise Architecture
Intelligent Workplace	Service Strategy / Contact Center	Modern Data Platform	End User IT & Collaboration
Intelligent Products and AI Agents	Service Process & Technology	Data Migration	Governance, Risk & Compliance
Product Strategy, Design & Build	Sales Strategy	Analytics and AI Enablement	Cloud & Hosting Platforms
High Performing Product Organization	Sales Process & Technology	Rapid Insights	Infrastructure & Platform Remediation
M&A Advisory & Execution			

Platforms Expertise*

Microsoft 365, MuleSoft, aws, salesforce, Google Cloud Platform, Azure, ncino, servicenow, databricks, alteryx, Amazon Connect, celonis, GENESYS, Microsoft Power Platform, Microsoft 365 CoPilot

* Not an exhaustive list of platforms where West Monroe has technical experience and expertise

© 2025 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners' prior consent is prohibited.

WHERE AGENTS FIT IN

Agentic AI in the market

Internal Workflows

AI Changes how work gets done

Common Tools/Platforms:

Chatgpt

Claude Cowork

Microsoft Copilot

Google Gemini Enterprise

Measure:

- Cycle time
- Quality & Deflection
- Capacity or cost per case

Use Cases

- Operations workflows (Loan processing, Compliance)

Product AI

AI embedded in a product

Common Tools/Platforms:

AWS Bedrock

Microsoft AI Foundry

Google AI Platform

Measure:

- Feature Adoption
- Usage depth
- Win rate or retention

Use Cases

- Personalization (product cross sell)
- Agentic workflows

AI in SDLC

AI creates a capability

Common Tools/Platforms:

Claude

Codex

Github copilot

Code assist

Measure:

- Accepted output
- Velocity
- Time to market

Use Cases

- AI enabled SDLC
- R&D

© 2026 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners' prior consent is prohibited.

Platform Architecture: A component-based architecture built for agentic intelligence, scale and trust

Table Stakes

Competitive Moat

License to Operate

AI Intelligence

Turns Frontier AI into trusted Intelligence

- Model & Reasoning Infrastructure
- Prompt & Knowledge Adaptation

Agent Platform

Execution Layer turns AI into Workflow Action

- Agent Orchestration & Runtime
- Governed Extensibility
- Governed Interoperability
- Prompt & Output Engineering
- Tooling & Integration

Domain Intelligence

Makes AI Defensible

- Methodology & Learning
- AI Data Architecture
- Knowledge, Memory & RAG

AI Operations

Quality as a Continuous Flywheel

- Evaluation, Tracing, and Observability
- Usage and Metering, Billing and Unit Economics
- LLMOps and Quality Flywheel

Enterprise Trust

Regulated AI Governance

- Security, Guardrails, and Trust
- Governance & Compliance Posture
- Certification Roadmap

Platform Foundation

The Interoperability and data foundation that underpins the entire platform

Cloud Infrastructure & Scalability | Event-Driven Architecture | Enterprise Data & Open Standards | Shared Platform Services

© 2026 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners' prior consent is prohibited.

Technical Thread: Getting an employee onboarded for their first day

”Make sure Maya is ready to start next Monday in her new role as data analyst in Boston”

A natural-language objective with missing details, dependencies, sensitive data, and actions that change real systems

Facts To Confirm

Employment Status

Start Date

Location and Manager

Work to coordinate

Identity and Access

Device and Software

Orientation and Notifications

Boundaries to enforce

Role Policy

Budget and Approval

Audit Trail

© 2026 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners’ prior consent is prohibited.

DEMO

© 2026 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners' prior consent is prohibited.

Questions?

Lindsay Scarangello
Managing Director, Technology & Experience
lscarangello@westmonroe.com

Kaumil Dalal
Senior Partner, Technology & Experience
kdalal@westmonroe.com

© 2026 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners' prior consent is prohibited.

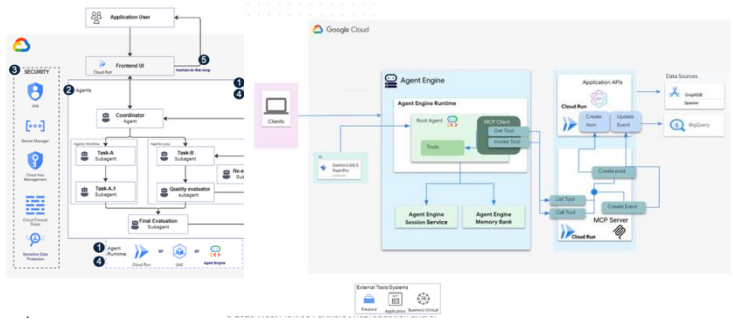
Appendix

© 2026 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners' prior consent is prohibited.

Large East Coast Utility

Agentic Use Cases on GCP

West Monroe is partnering with the Enterprise Data & Analytics organization is establishing a governed Agentic Platform on Google Cloud to securely scale AI across the enterprise. Rather than deploying isolated pilots, the 2026 program builds a centralized control plane with embedded guardrails, human-in-the-loop oversight, and standardized design patterns that allow domain teams to develop and operate agents safely and at scale. Through parallel platform foundation and POC acceleration workstreams, West Monroe is creating a repeatable pipeline from use case intake to MVP deployment: enabling measurable value realization, stronger governance, and the ability to introduce new models and capabilities without re-platforming or compromising compliance.



AN UNDENIABLY DIFFERENT APPROACH

We are employing a multi-disciplinary approach focusing on immediate value realization while building long-term infrastructure:

GCP Platform: We are designing and standing up a governed Agentic Platform on Google Cloud that enables agents to reason, act, and collaborate securely; without re-platforming for every new use case.

Rapid Use Case Development: In parallel, we are accelerating prioritized use cases through structured POC development; proving measurable value while shaping enterprise standards.

This approach enables a **centralized control plane with decentralized innovation**, where:

- Platform team owns runtime, guardrails, and observability
- Domain teams build and operate agents aligned to business outcomes
- New agentic use cases can be built out rapidly

AGENTIC USE CASES (In Development):

- **Contract Insights:** Identify and reduce value leakage between contracted terms and invoices, monitor contract compliance against regulations and specific company defined requirements.
- **Vehicle Idling:** Evaluate idling fines and videos against NYC law to make a recommendation to legal teams as to when they should pay vs dispute a case.

IMPACT:

- **First 40 cases disputed in court based on AI recommendation resulted in a win resulting in fine avoidance**

© 2025 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners' prior consent is prohibited.

Agentic capabilities become embedded across the underlying platform architecture to connect users, workflows, data, and systems

Agents operate across platform layers to observe context, reason over data, and execute governed actions

SENSE

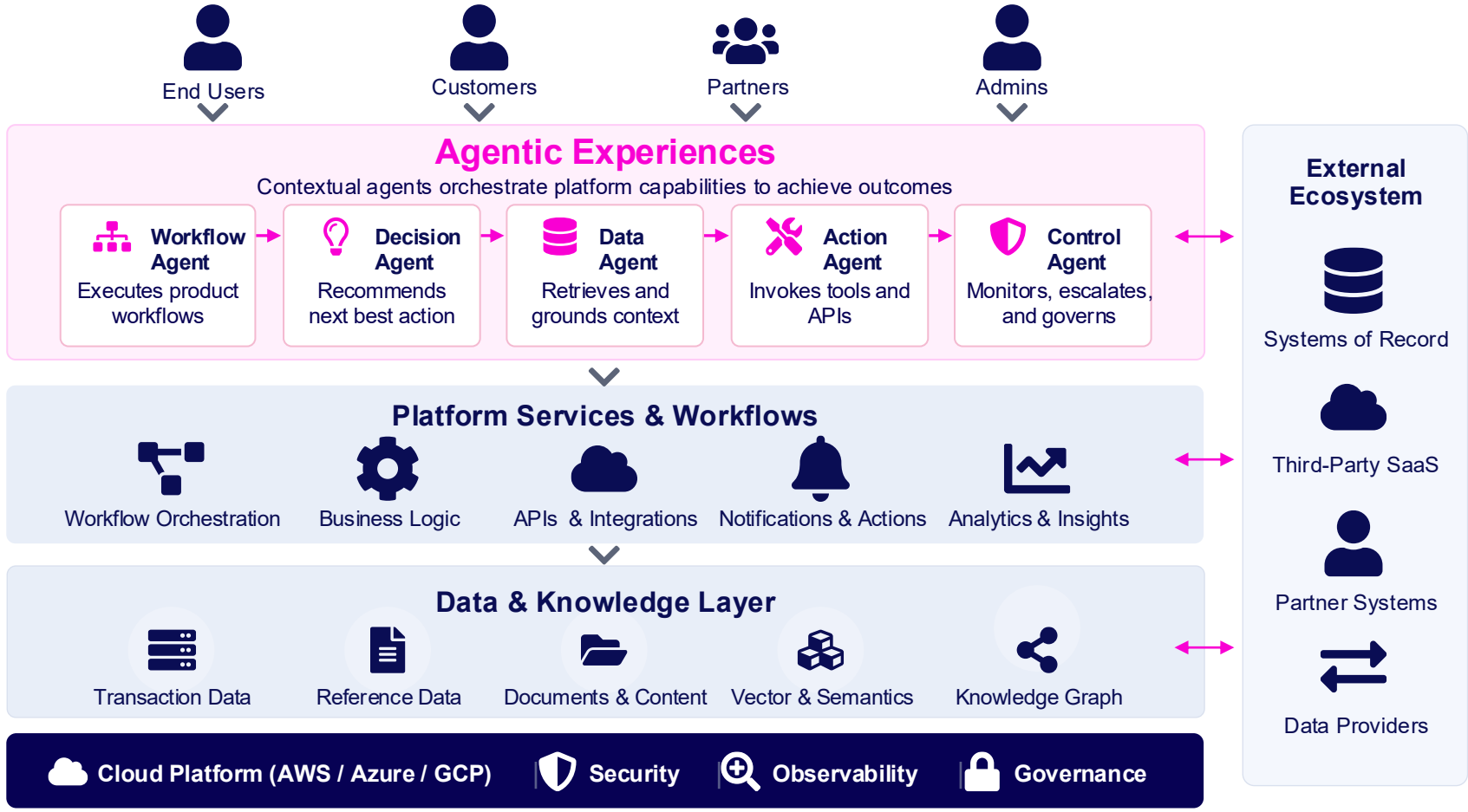
Agents continuously observe data, events, and interactions across the platform

DECIDE

Agents reason using models, knowledge, and business rules to determine the best action

ACT

Agents take action across systems, automate workflows, and deliver outcomes

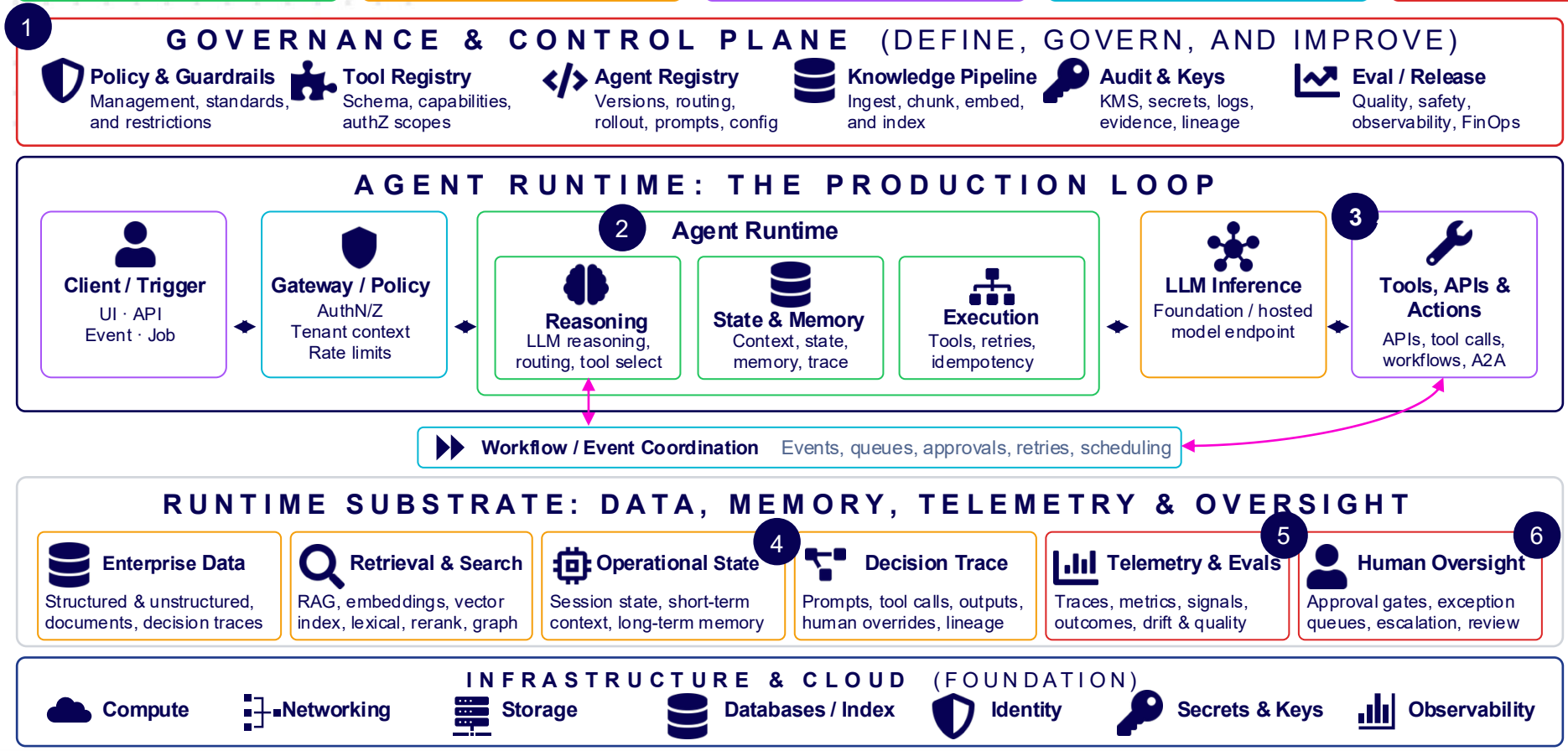


© 2026 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners' prior consent is prohibited.

Reference Agentic Architecture, including the Agent Runtime, Control Plane, Data & Reasoning, and Infrastructure

The agent loop is surrounded by policy, tool/auth control, data and memory, orchestration, and observability for safe, reliable operation

Agent Runtime | Data & Reasoning | Platform APIs & Eventing | Orchestration & Coordination | Governance & Control Plane | Infrastructure & Cloud



ARCHITECTURE PRINCIPLES

1. **Governance surrounds it**
   Policy, registry, audit, eval; surrounds and enables the system
2. **Agent is a loop**
   Repeats **(1)** observe **(2)** plan **(3)** act **(4)** evaluate **(5)** update until goal or stop
3. **Tools are contracted**
   Every external call has a schema, auth scope, idempotency boundary, and retry strategy
4. **Memory is layered**
   Short-term context, structured state, and long-term retrieval are distinct stores
5. **Telemetry closes the loop**
   Traces and evals feed continuous improvement, safety, and cost control
6. **Built for production**
   Deterministic execution, retries, idempotency, and human oversight enable reliable operation

© 2026 West Monroe Partners | Reproduction and/or distribution without West Monroe Partners' prior consent is prohibited.

The Alchemy of the Breach



Kevin Bong

DIRECTOR OF CYBERSECURITY
CONSULTING, GHOSTSCALE

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

THE ALCHEMY OF THE BREACH

KEVIN BONG - GHOSTSCALE

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

AGENDA

- Key Trends
- Extortion Incident
- Online Banking Attack
- Lessons Learned and Protection Strategies

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Today's Presenter



Kevin Bong

CISSP, CISA, PMP, GSE, GX-CS, GX-IA,
GX-IH, GPPA, GCFA, GAWN, CEH,
ISO 27001 LA, CMMC RP

DIRECTOR, GHOSTSCALE

Ghostscale is a cybersecurity professional services organization specializing in virtual Chief Information Security Officer (vCISO) and CISO advisory services, penetration testing, maturity assessments, threat simulations, digital forensics, and incident response.

© 2026 Navanta™ All rights reserved. navanta.com

Key Trends

© 2026 Navanta™ All rights reserved. navanta.com

KEY TRENDS

Migration to Cloud

- *Cloud is often more secure, but…*
- Identity becomes the gatekeeper
- Your traditional controls (antivirus, patching, firewalls) provide little protection against cloud attacks

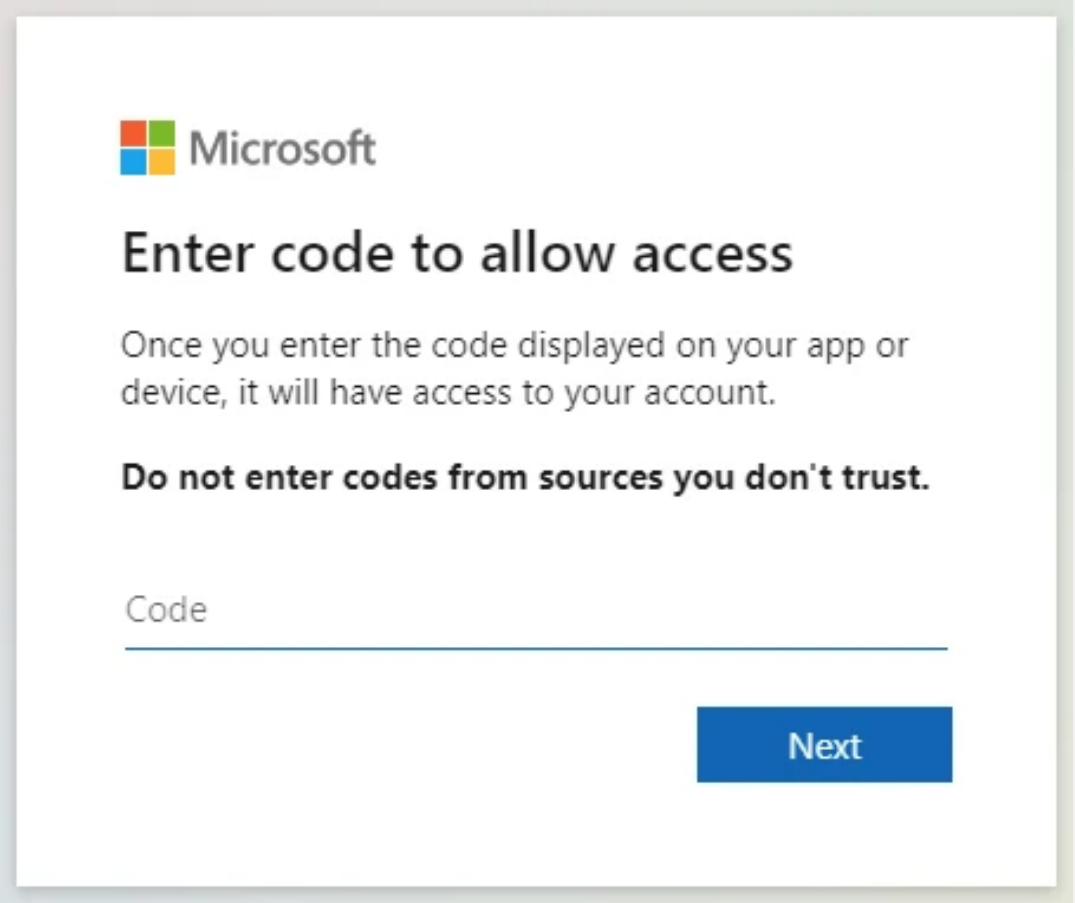


© 2026 Navanta™ All rights reserved. navanta.com

KEY TRENDS

Federated Identity (Single Sign-On)

- One identity accesses multiple services
- Sign-in prompt complexity causes mistakes
- Users experience “MFA Fatigue”

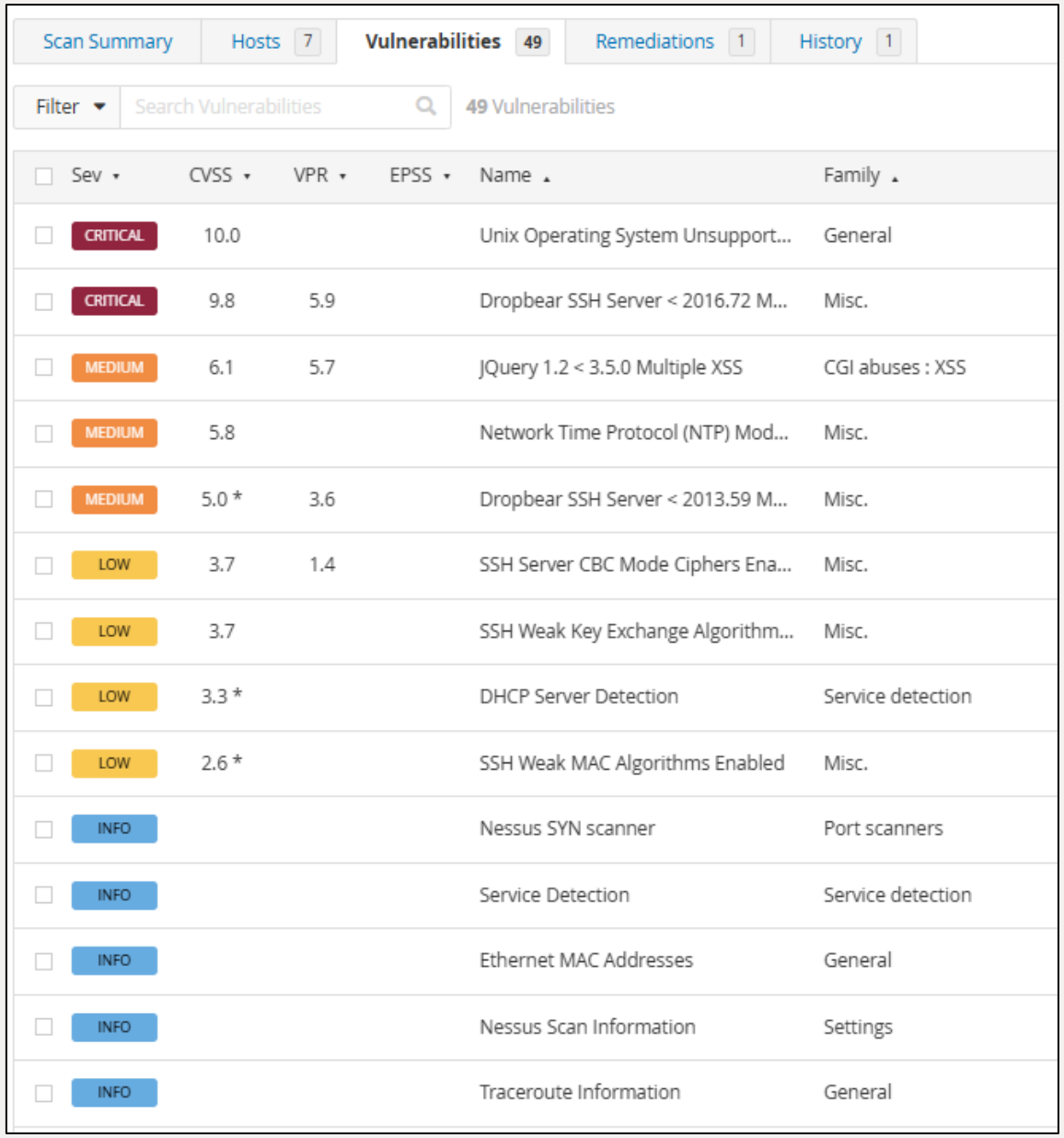


© 2026 Navanta™ All rights reserved. navanta.com

KEY TRENDS

AI-Enabled Attacks

- Accelerated vulnerability discovery
- Automated exploit development and testing
- Low effort/low technical barrier to sophisticated attacks



Scan Summary | Hosts 7 | **Vulnerabilities 49** | Remediations 1 | History 1

Filter | Search Vulnerabilities | 49 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family
CRITICAL	10.0			Unix Operating System Unsupport...	General
CRITICAL	9.8	5.9		Dropbear SSH Server < 2016.72 M...	Misc.
MEDIUM	6.1	5.7		JQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS
MEDIUM	5.8			Network Time Protocol (NTP) Mod...	Misc.
MEDIUM	5.0 *	3.6		Dropbear SSH Server < 2013.59 M...	Misc.
LOW	3.7	1.4		SSH Server CBC Mode Ciphers Ena...	Misc.
LOW	3.7			SSH Weak Key Exchange Algorithm...	Misc.
LOW	3.3 *			DHCP Server Detection	Service detection
LOW	2.6 *			SSH Weak MAC Algorithms Enabled	Misc.
INFO				Nessus SYN scanner	Port scanners
INFO				Service Detection	Service detection
INFO				Ethernet MAC Addresses	General
INFO				Nessus Scan Information	Settings
INFO				Traceroute Information	General

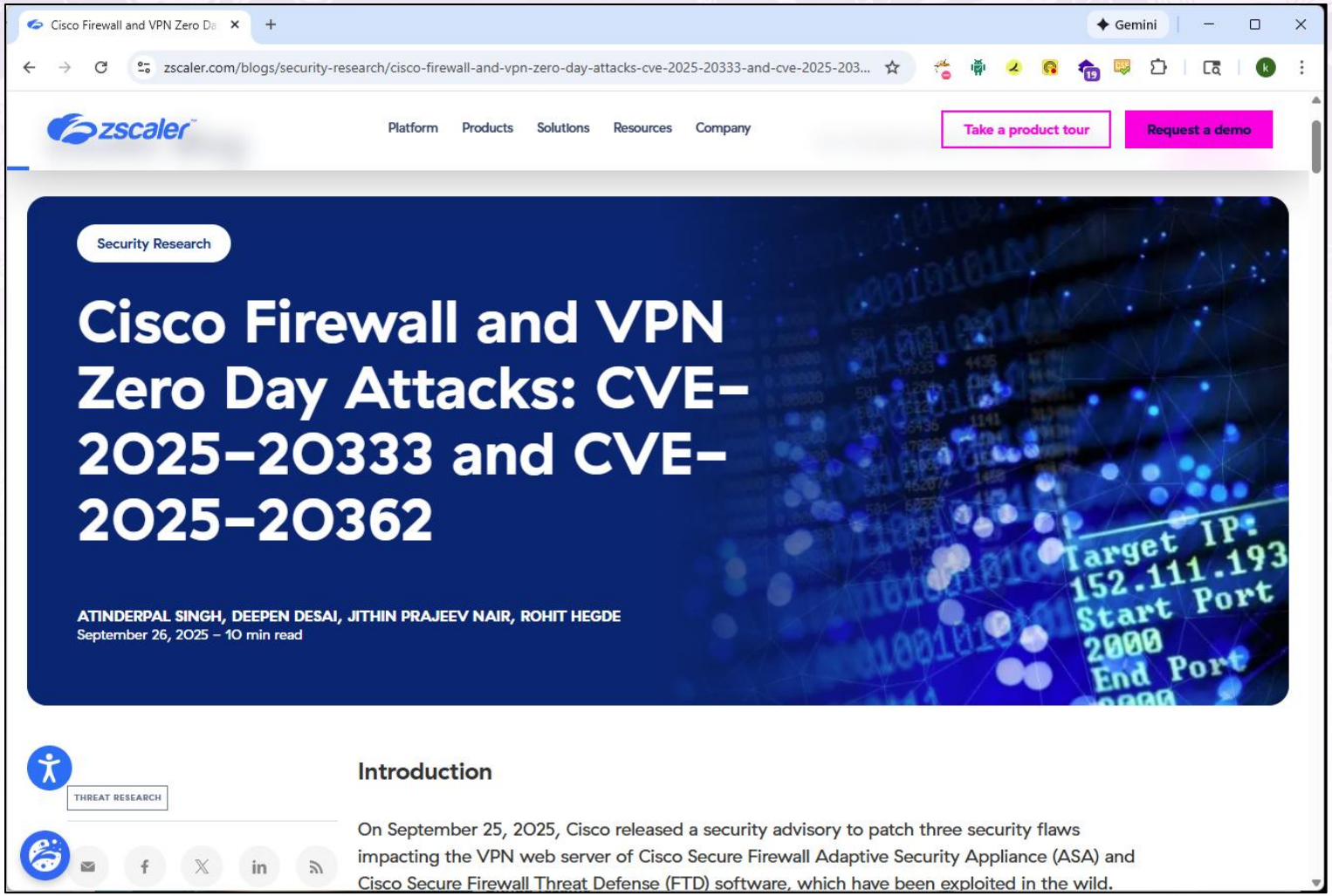
navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Extortion Incident

© 2026 Navanta™ All rights reserved. navanta.com

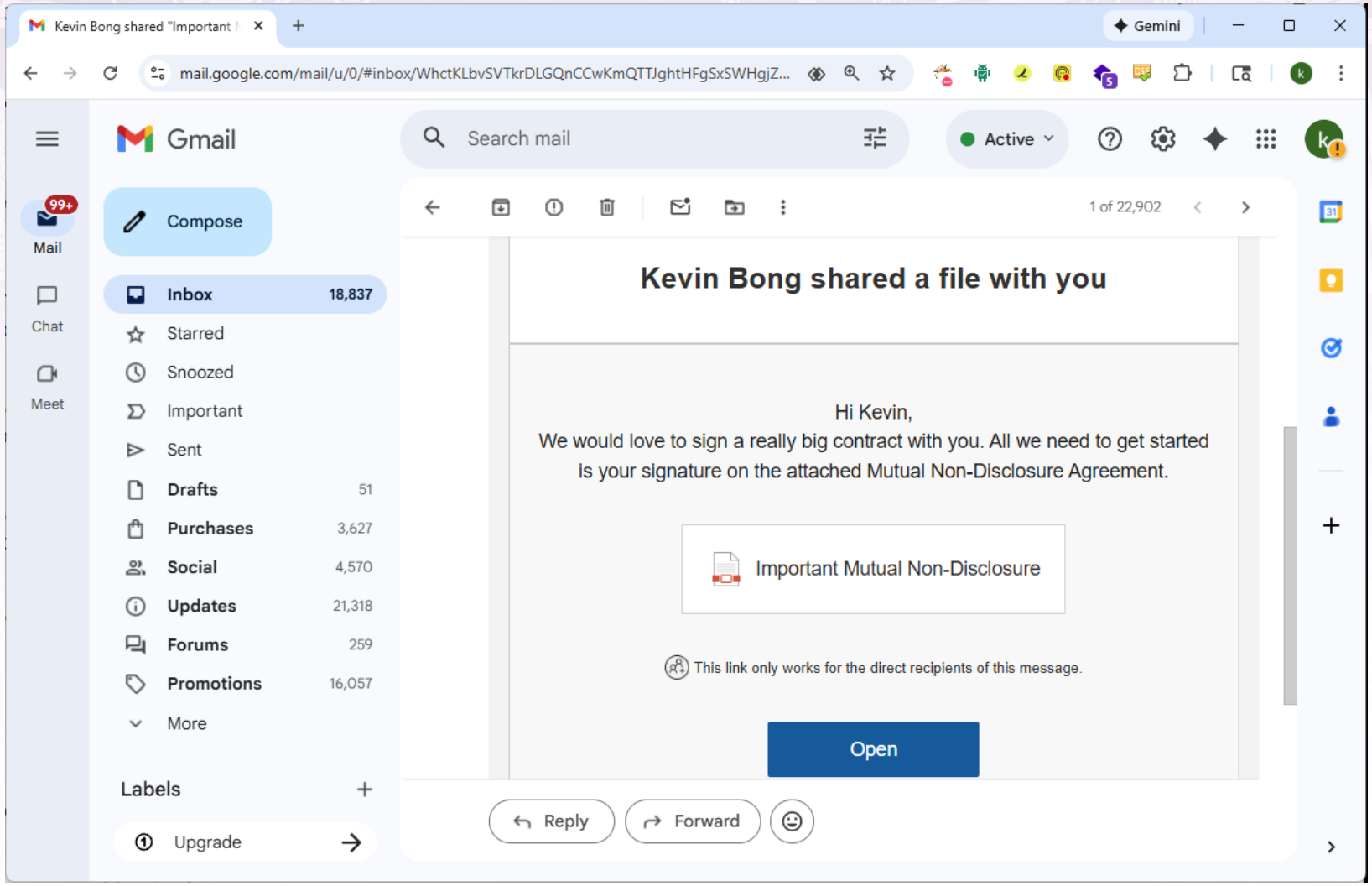
Resurgence of Public Vulnerabilities in Vendor Solutions



navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Increase in Successful Phishing/Account Takeover Attacks

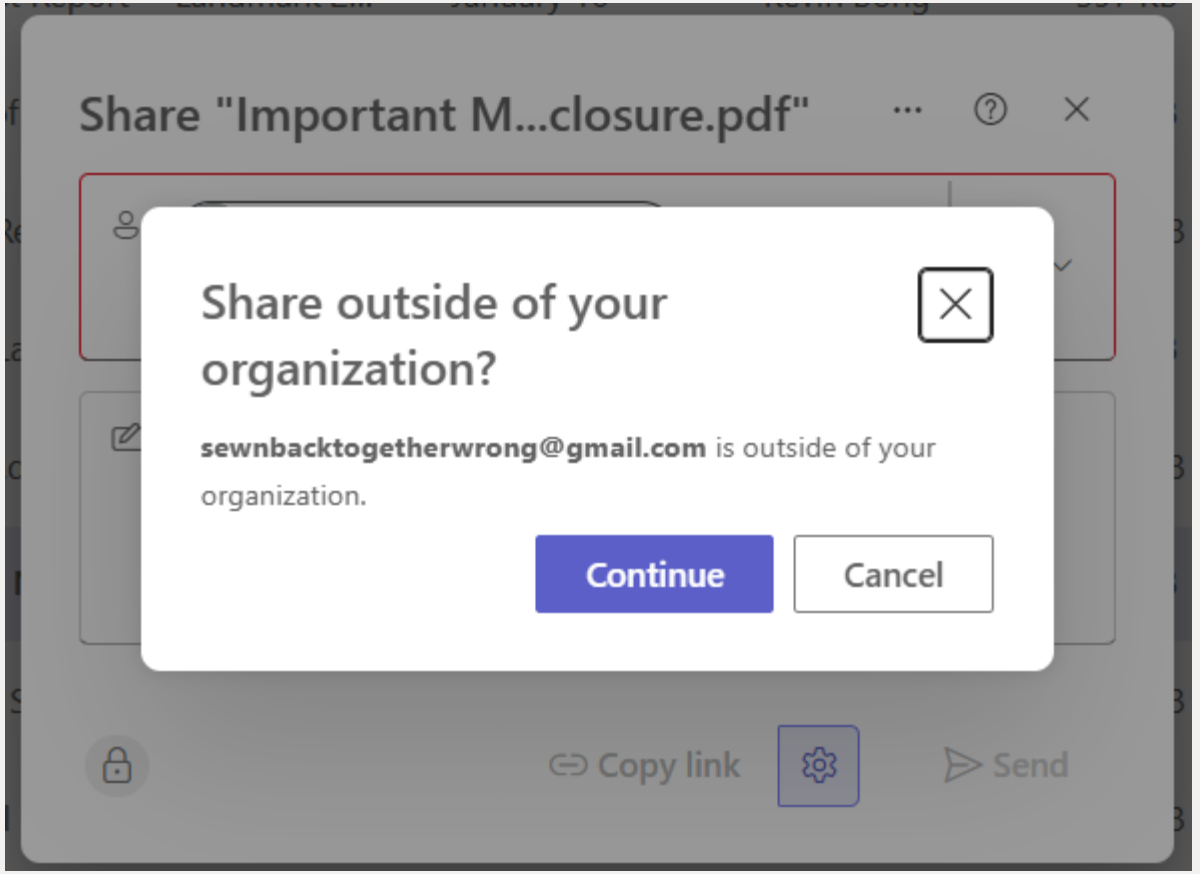


© 2026 Navanta™ All rights reserved. navanta.com

EXTORTION INCIDENT

They Don’t Look Like Nigerian Scammers

- Result of chained account takeover
- Comes from someone you trust
- May even be a legitimate “sharing” notification from M365



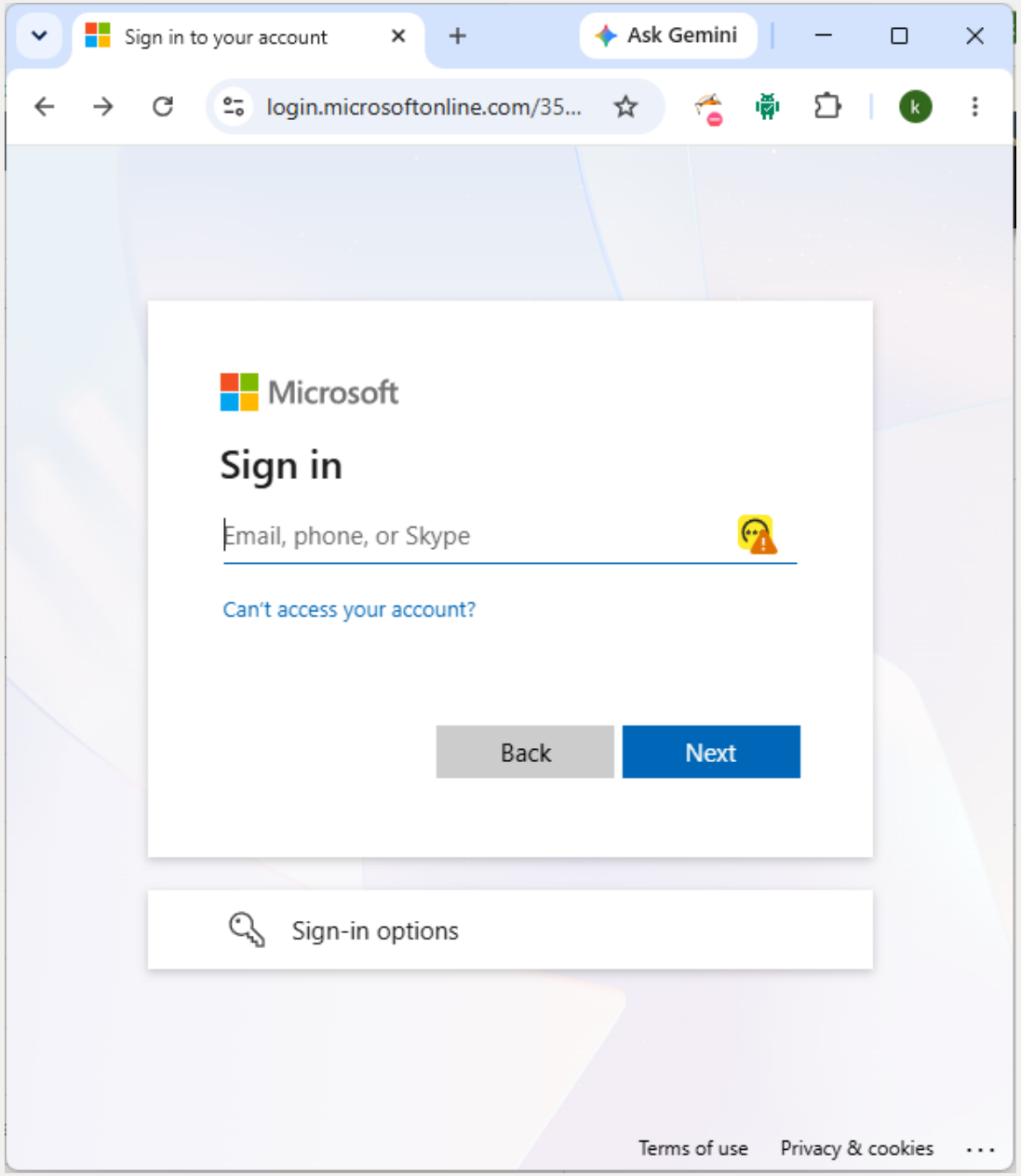
navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

EXTORTION INCIDENT

Gaining Access – MFA Bypass

- Adversary-in-the-middle phishing techniques
  - MFA Complexity
  - MFA Fatigue
- Persistent access
  - Interception of session tokens
  - Adding authentication methods
  - Enrolling trusted devices



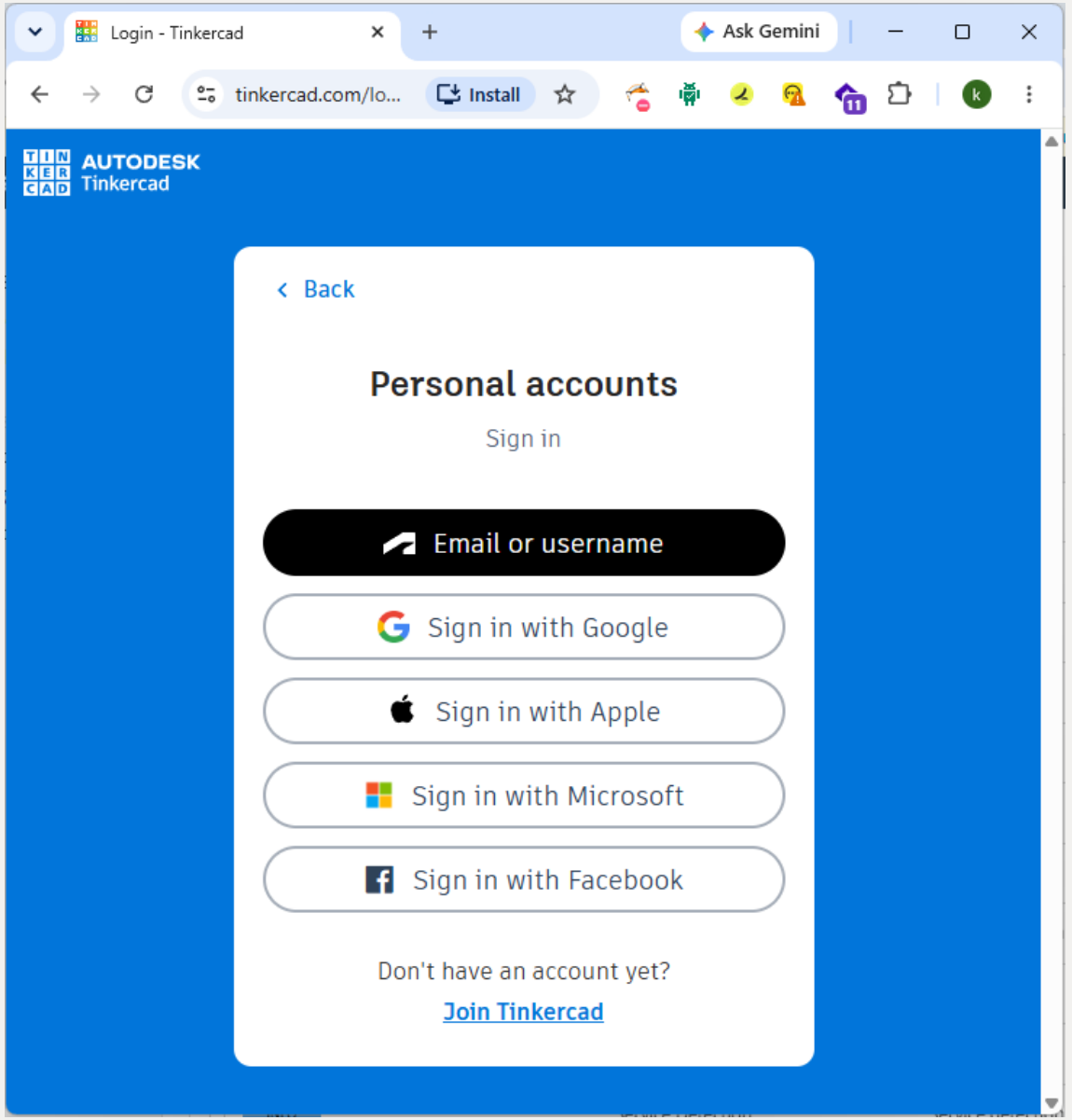
navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

EXTORTION INCIDENT

Abusing Single Sign-On

- *Single sign-on is generally more secure, but…*
- Increases the complexity of sign-in processes
- Creates habits that facilitate MFA fatigue
- A single compromise creates a wide blast radius



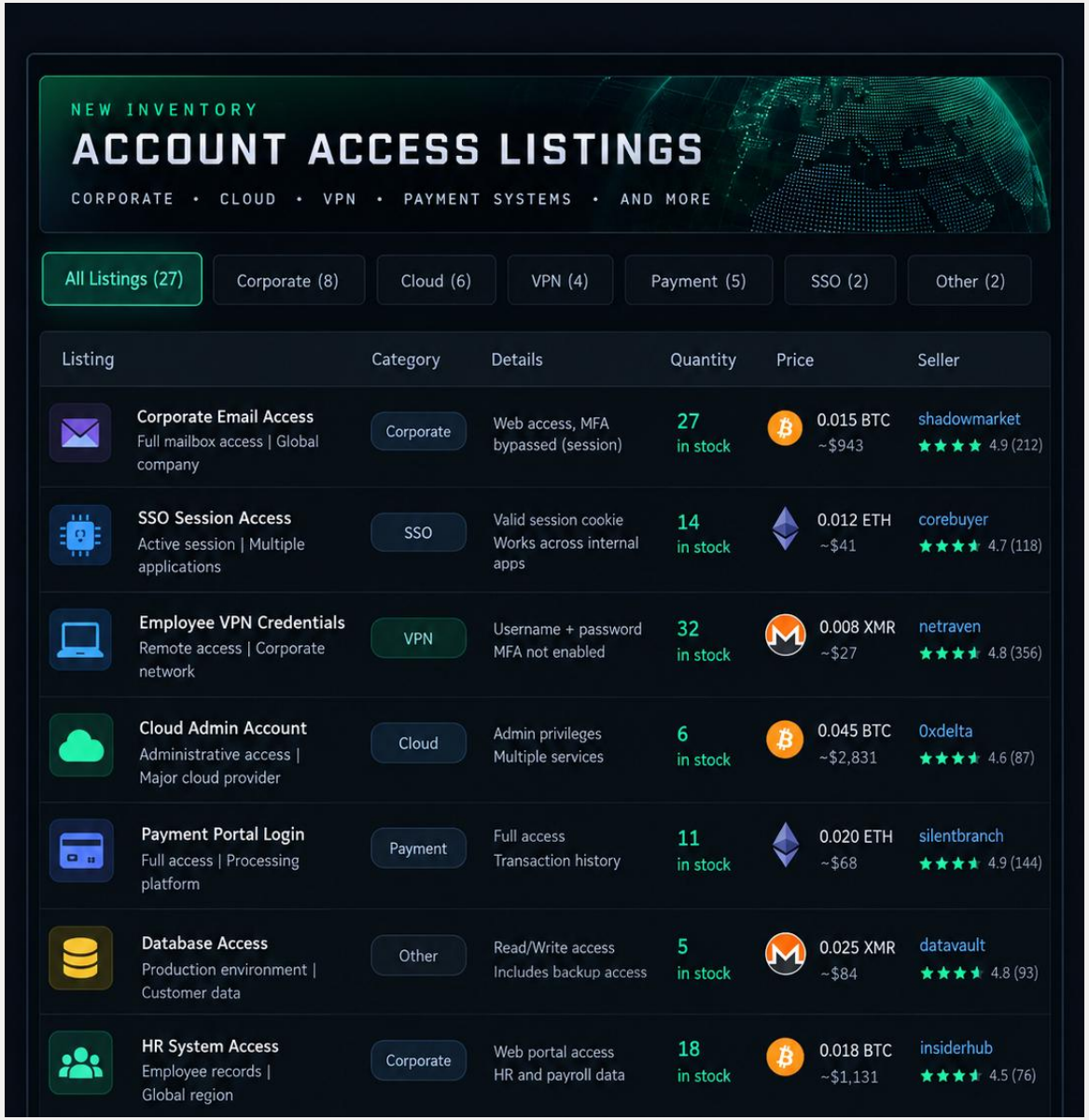
navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

EXTORTION INCIDENT

Account Compromise – What Now?

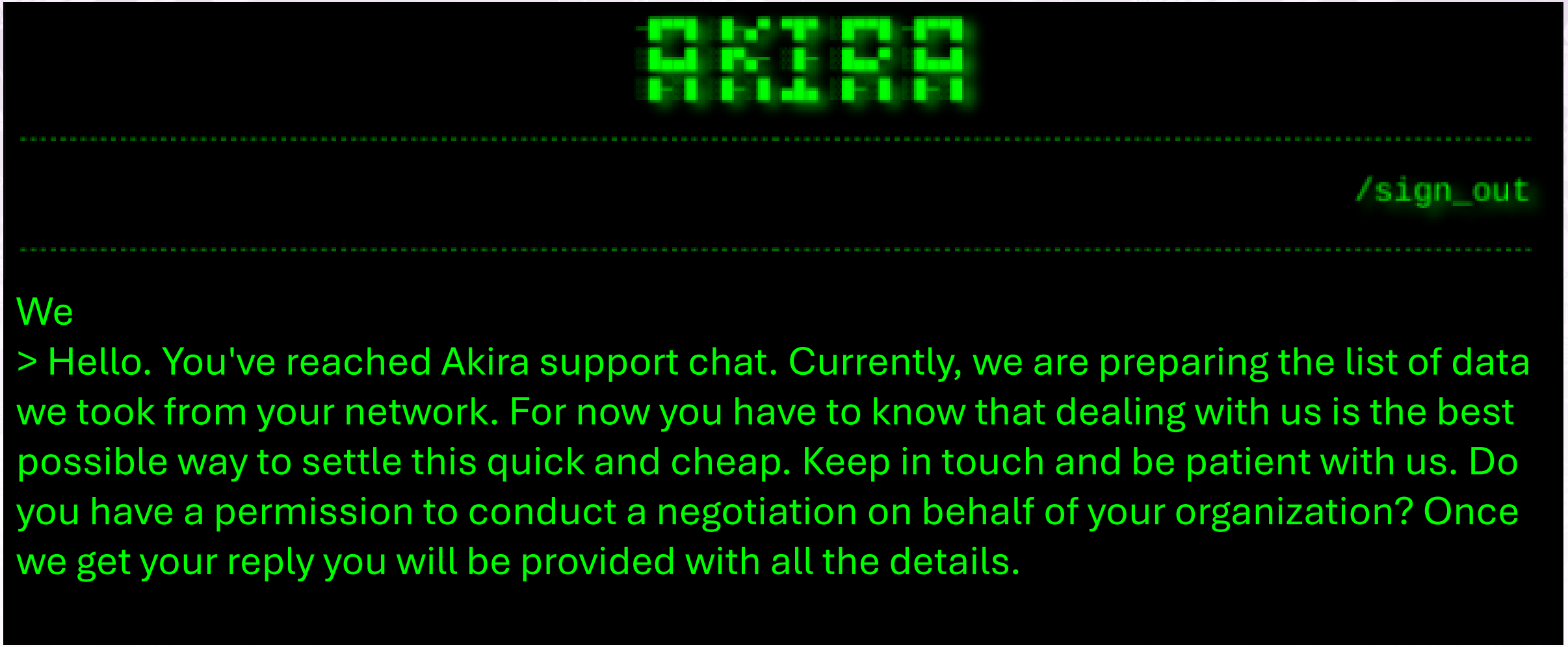
- Your compromised account is “handed off” or sold to another team or group
- This often creates a small window of time after the breach where you can minimize the impact... if you detect it early



navanta TECH-O-WEEN

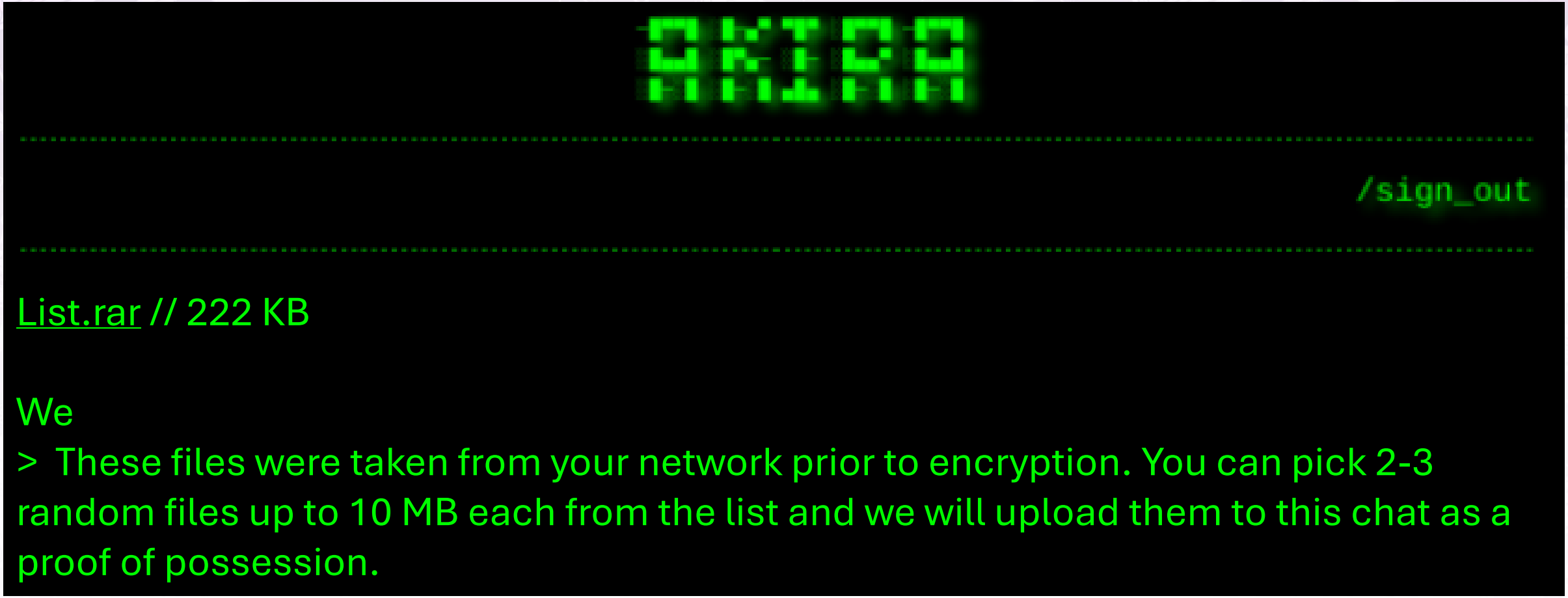
© 2026 Navanta™ All rights reserved. navanta.com

Please Join Our Chat…



© 2026 Navanta™ All rights reserved. navanta.com

Proof of Life



© 2026 Navanta™ All rights reserved. navanta.com

Menu of Services

We
> We're looking through your financial papers to come up with a reasonable demand to you. We offer:

1) full decryption assistance;
2) evidence of data removal;
3) security report on vulnerabilities we found;
4) guarantees not to publish or sell your data;
5) guarantees not to attack you in the future.

Let me know whether you're interested in a whole deal or in parts. This will affect the final price.

© 2026 Navanta™ All rights reserved. navanta.com

Leaks (Akira News Site)



© 2026 Navanta™ All rights reserved. navanta.com

Online Banking Attack

© 2026 Navanta™ All rights reserved. navanta.com

AI-Assisted Vulnerability Hunting

#	Host	URL	Method
94	https://www.chase.com	/	GET
137	https://reco.chase.com	/events/recoengine/public/aes/v2/mkt-aes/web/ccb/marketing/offer-mana...	GET
156	https://secure.chase.com	/web/auth/?treatment=chase	GET
403	https://secure.chase.com	/svc/wl/auth/public/v1/site/availability/list	POST
409	https://secure.chase.com	/auth/fcc/adaptive	POST
438	https://secure.chase.com	/auth/fcc/randomize	POST
439	https://secure.chase.com	/auth/fcc/login	POST

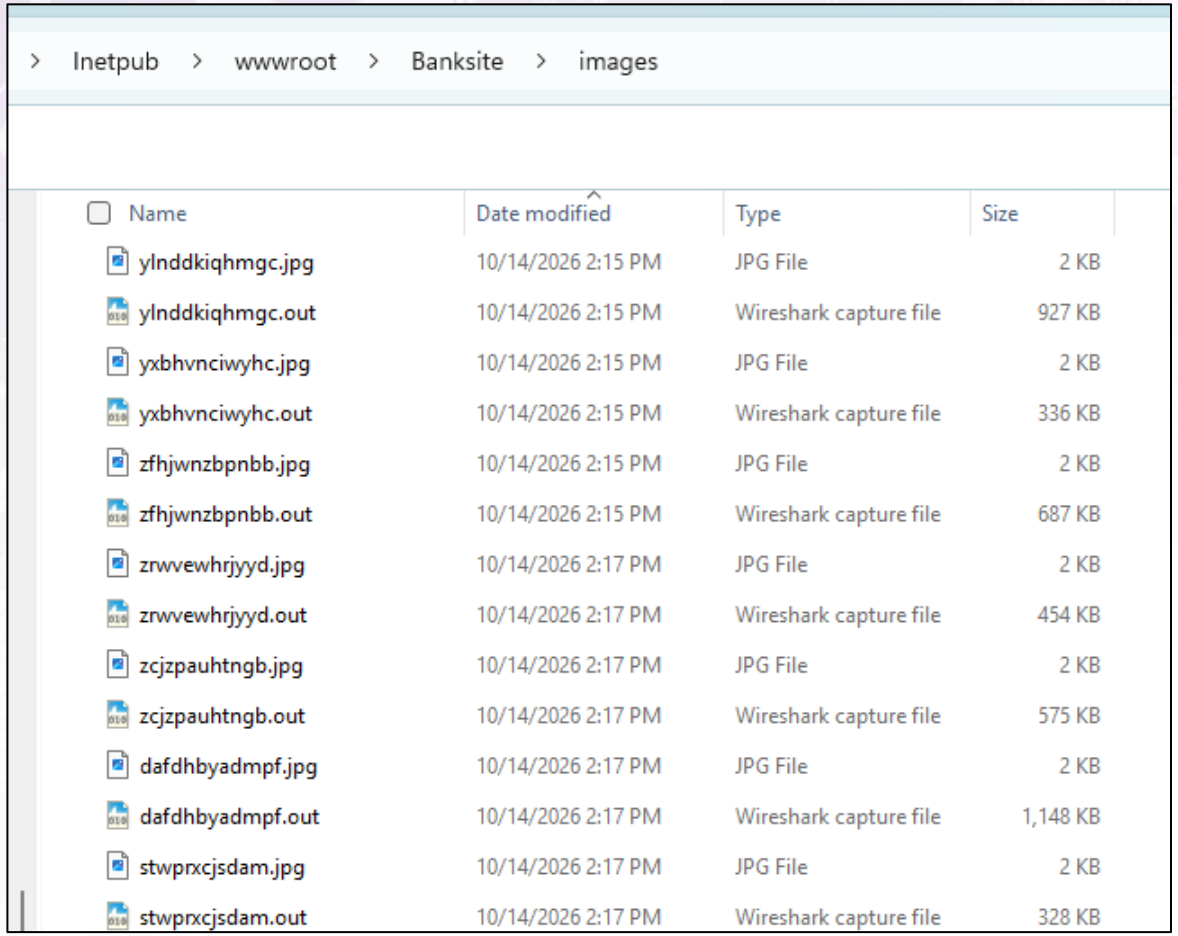
Request

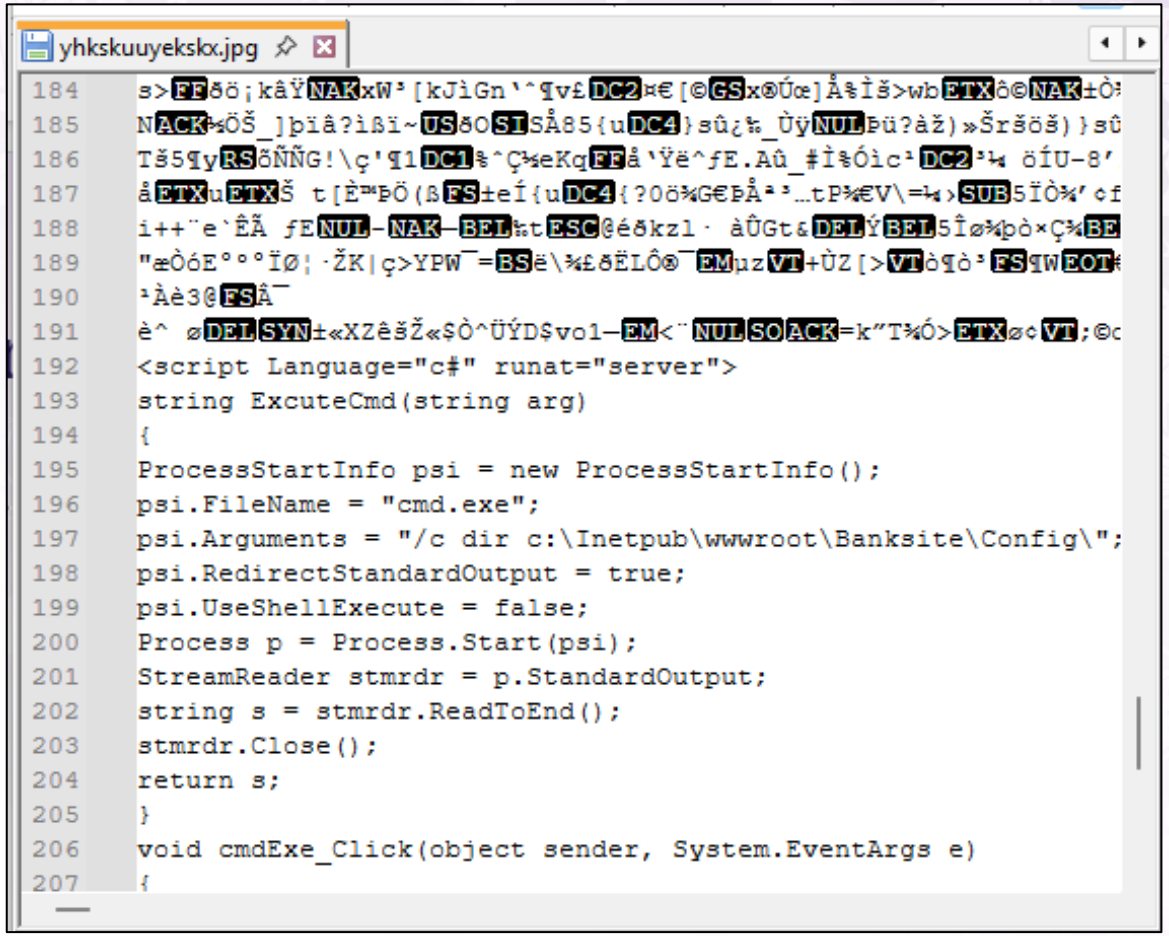
Pretty Raw Hex

```
POST /auth/fcc/login HTTP/2
Host: secure.chase.com
Cookie: AMCV_EA673DFC5A2F19060A495C9C@AdobeOrg=
1914845758|MCIDTS|17564|MCMID|09776816010760389084909184264306770648|MCAID|NONE|MCOPTOUT|isoptedout-false|
MCAAMLH||MCAAMB||MCCIDH||MCSYNCSOP|411-17568|vVersion|2.3.0|IsCustom|true; MortPrequalCampaignCookie=
SourceCode%3DOS0001%26iq_id%3D; _tmprememberme=0; store~logon~treatmentParameter=%22chase%22; PC_1_0=
locale%3Den_us%7C; dtCookie=
v_4_srv_27_sn_6BCB5A94DCB50E3F59C18A7BD130A489_perc_100000_ol_0_mul_1_app-3Ac0834ad25a3fd2c3_1_rcs-3Acss_0
; dps-pod-id=26EA; ig-ingress-cookie="33f702edf27198cf"; AKA_A2=A; akaalb_secure_chase_com=
~op=secure_chase_com_mw_lb:Secure-Secure26ea-us-east-2|~rv=52~m=Secure-Secure26ea-us-east-2:0|~os=90ae4da4
469d6bd8de4af73ca8e4badd~id=773100cc4fbaecdfcebc4a296170b1b9; dfs_E_5=000; v1st=B75C66BFB5D8CEE9; s_vi=
[CS]v1|B75C66BFB5D8CEE9-CD0564684B4C9CA1[CE]; dfs_E_1=0; dfs_E_8=13.0.0,135.0.1; dfs_E_4=4; dfs_E_6=01 -
02; dfs_F_6=cec95ba2f6521faef68beea3c024a4bacfc17b3dba001a692760f799834e2c99SFNcZg==; dfs_F_5=
f87b16ed3db8b841a10fb2de064c5b075dd22f1c0c9db4c71464350378e1ead6; dfs_F_7=
fcb3efe22bb89a52052044071f660175279bb9853d7489583db5bb6eb5ace2e8; RT=
"z=1&dm=secure.chase.com&si=50ed804e-8532-4887-b6cc-a6854c290d30&ss=mv8hdkrc&sl=1&tt=6y4&bcn=%2F%2F17de4c0
f.akstat.io%2F&ld=8p8"; store~logon~source=%22logon%22; store~logon~loginFailure=%22%22; dfs_E_7=
```


© 2026 Navanta™ All rights reserved. navanta.com

AI-Assisted Exploit Creation

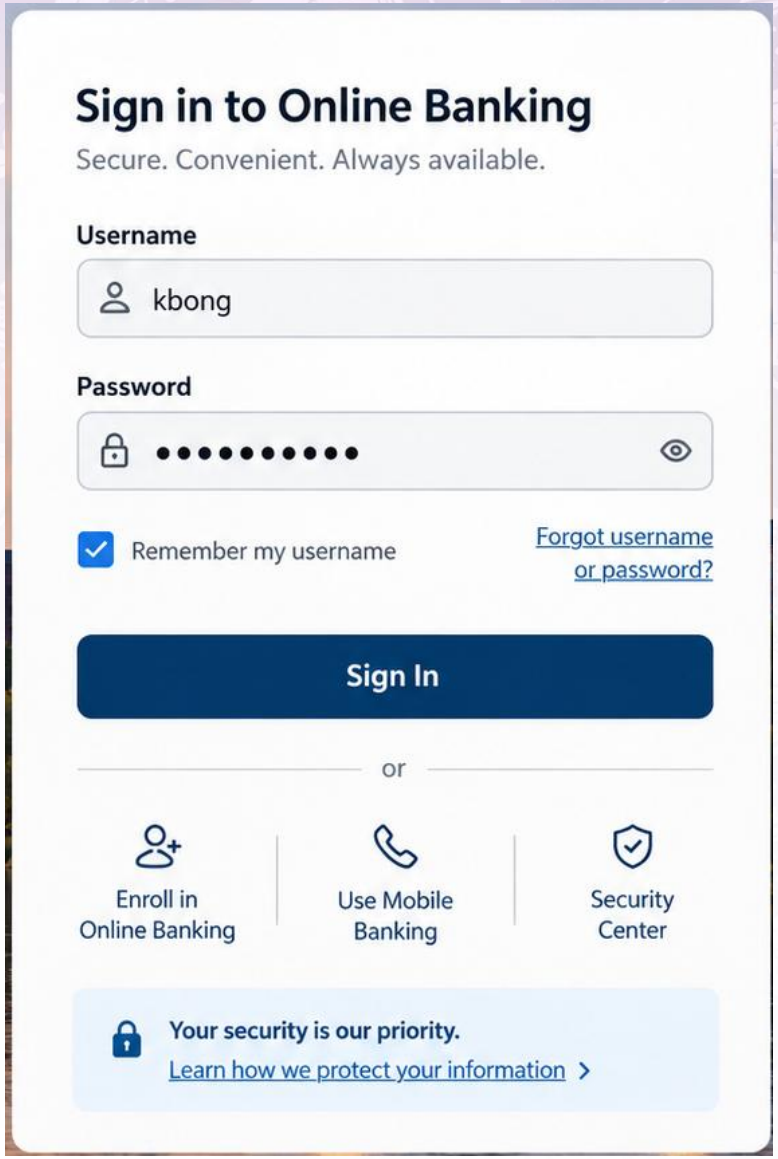




© 2026 Navanta™ All rights reserved. navanta.com

Low to Owned

- Typical online banking app, user login requires MFA
  - MFA is required to trust a device
  - Skips MFA if from a prior trusted device
- Risky actions require MFA again
  - Set up new bill pay payee
  - Instant link to Zelle or Venmo
  - Change your MFA method (between email, text, or authenticator app)



© 2026 Navanta™ All rights reserved. navanta.com

The Bad Guys Know More About Your App Than You Do

- The trusted device ID was NOT tied to a user ID
- Internal bank transfers did NOT require additional MFA
- Contact info changes did NOT require additional MFA

© 2026 Navanta™ All rights reserved. navanta.com

Steal Passwords… Do Evil… Profit

1. Get into one customer account using social engineering to bypass MFA
   - Use this to trust the threat actor's device
2. Steal other customer passwords through social engineering or credential stuffing
3. Log in to all accounts with stolen passwords (without MFA because the device is trusted)

© 2026 Navanta™ All rights reserved. navanta.com

Getting the Money Out

- If MFA method IS email
  - Change email address on contact info (no MFA required)
  - Link to Zelle or Venmo using MFA (take all the $$$)
- If MFA method is NOT email
  - Transfer funds to another compromised account within the bank
  - Transfer out from there with Zelle or Venmo

© 2026 Navanta™ All rights reserved. navanta.com

At Least We Have Good Logs, Right?

- API gateway provider expected narrow criteria in log requests and had a 3-day turnaround
- What seemed like detailed log entries… weren't

```
2024-02-02 14:30:15, 140.104.10.12, DevID KDSJG09D07FGJDFG2, UserID KevinMBong1, MFA Login Success
2024—02—02 14:31:22, 104.17.156.85, DevID 8THLA168KK09D08FM, UserID bigpackersfan, Login Success
```

- Good guys and bad guys all looked the same
  - Real customers were commonly using anonymizing VPNs
  - Automated access to multiple accounts from one source (e.g., QuickBooks, Rocket Money, Venmo)

© 2026 Navanta™ All rights reserved. navanta.com

Lessons Learned and Protection Strategies

© 2026 Navanta™ All rights reserved. navanta.com

Key Takeaways

Review your logs before you need them

- Retained for a minimum of 90 days, ideally for 1 year
- Readily accessible at the time of an incident
- Ensure the logs have the true source IP address of the external user
- Ensure they have necessary detail
  - MFA method used
  - Where MFA tokens were sent
- Check cloud platform defaults
  - Azure and AWS “bucket” logging is disabled by default

© 2026 Navanta™ All rights reserved. navanta.com

Key Takeaways

Monitor cloud and application logs for anomalies

- Centralize identity and SaaS logs
- Correlate activity across cloud applications
- Detect anomalous logins and sessions
- Alert on unusual data downloads
- Establish continuous monitoring and response
- Validate MSSP alerting and escalation

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Key Takeaways

Require phishing-resistant authentication methods

- Stop the use of phone and SMS text for MFA
- Enforce policies through Conditional Access
- Consider limiting employee logins to registered or compliant devices
- Extend protection to third-party access
- Block device-code authentication methods

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Key Takeaways

Test cybersecurity controls

- Internal and external penetration testing of corporate and cloud environments
- Web application penetration testing
- Atomic red team control validation
- Incident response exercises

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Get In Touch



Kevin Bong

DIRECTOR, GHOSTSCALE

262.378.1783
KEVIN.BONG@GHOSTSCALE.COM
WWW.GHOSTSCALE.COM

Ghostscale is a cybersecurity professional services organization specializing in virtual Chief Information Security Officer (vCISO) and CISO advisory services, penetration testing, maturity assessments, threat simulations, digital forensics, and incident response.

© 2026 Navanta™ All rights reserved. navanta.com

Thanks

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Alchemists in the Wild



Darren Bridges

GM ADVISORY & COMPLIANCE SERVICES

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Inside the Laboratory



Tom Hearn

SVP TECHNOLOGY,
COMMERCIAL AI LEAD

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Inside the Laboratory

© 2026 Navanta™ All rights reserved. navanta.com

AGENDA

Today’s tour

01

The blueprint

Why we built the environment before the product, and what discovery told us

02

The floor plan

Reference architecture, network zones, sizing, and build-versus-buy

03

The production line

Five phases, from a non-NPI pilot to confirmation-gated actions

04

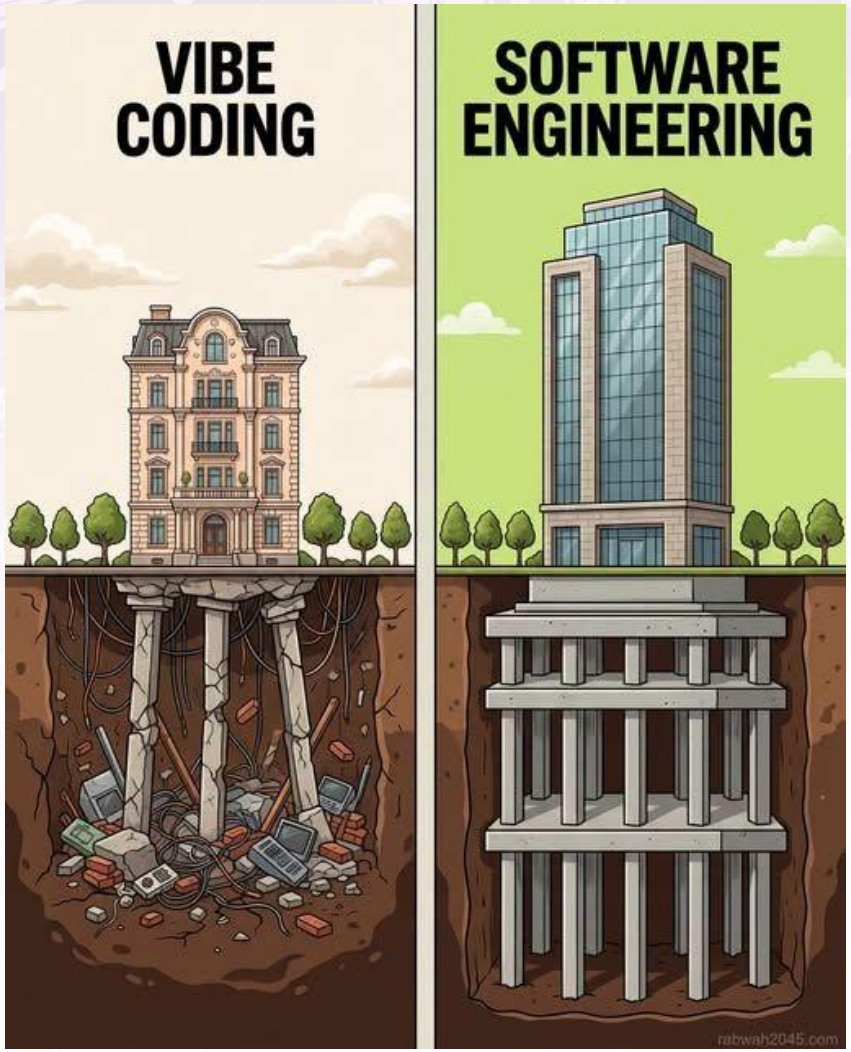
The lab notebook

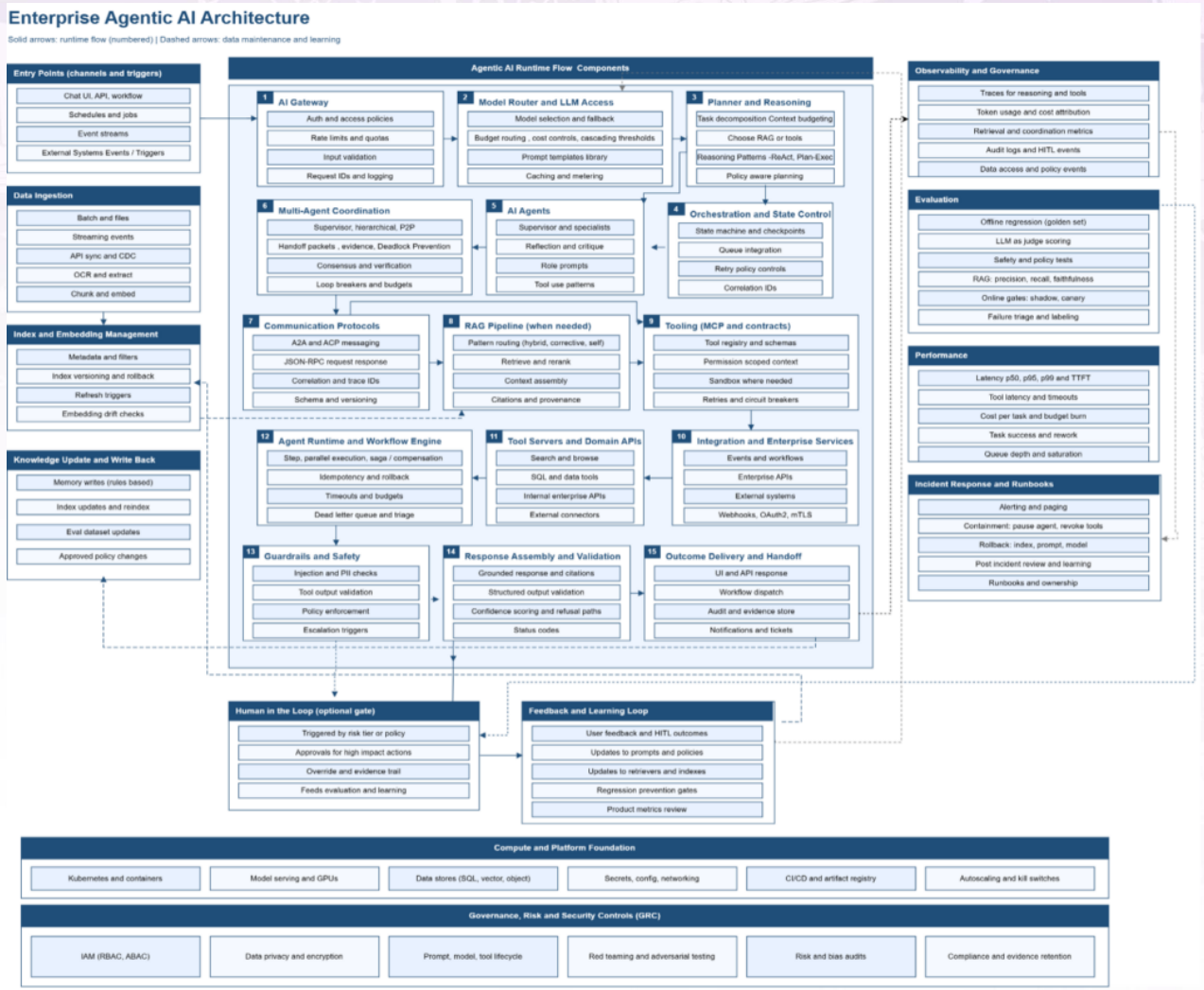
What is running, what went wrong, what we measure, and what is next

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

A brief level set on the reality of AI…





© 2026 Navanta™ All rights reserved. navanta.com

OUR FUNDAMENTALS

Four fundamentals behind everything we build

01

Built iteratively, with you

Small releases, shaped by heavy customer feedback. What we hear at each step re-ranks what we build next.

02

Outcomes, not a chat agent

Each product is measured by the work it completes and the time it returns. The interface serves the outcome.

03

End-to-end traceability

Every execution can be replayed from evidence, with timing captured at each step.

Request → **Who asked, and their role** → **Data pulled: where and what** → **Context at each call and turn** → **Outcome and decision** → **Human confirmation**

- Timestamped and recorded at every step, from the first request to the confirmed outcome

04

Identity follows the context

The agent works as the person, never with more access than that person has.

Signed-in user → **Role and tenant entitlements** → **Retrieval pre-filtered to what they may see** → **Agent context for turn** → **Cited answer or confirmed action**

↻ The same identity and role are enforced on every call and every turn, all the way to the data

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

THE IDEA

What we mean by an AI factory

01 Discover

Priorities come from discovery conversations, not planning meetings

02 Use it ourselves

Every capability runs on our own data and our own risk first

03 Pilot without NPI

Policy, procedure, and public data before customer records

04 Evidence gate

Security and governance review before customer data moves

05 Scale

One platform, many institutions, the same controls

↺ What we learn at every station feeds back and re-ranks the backlog.

A factory is the repeatable path, not any single product. Every capability passes the same stations.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

The Blueprint

Why we built the environment before the product

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

DESIGN COMMITMENTS

Decisions we made before writing code

01

Private by design

Runs on infrastructure we own and operate, with no public model in the path.

02

NPI minimization

NPI is processed from its system of record and retained only when needed, encrypted per institution. Early scope avoids NPI entirely.

03

People stay accountable

Where judgment matters, a person remains accountable for the outcome, and the record shows who it was.

04

What we put in writing

SOC-aligned control mapping, data-flow and network diagrams, BC/DR, encryption in transit and at rest, and access logging.

05

Earn the next step

Use it internally first, start with non-sensitive data, and move to institution data only when controls and evidence support it.

06

Deterministic where it counts

Matching and rules are deterministic. Models explain and draft; people decide.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

SEQUENCING

Why this order, and what sits underneath it

01

Policy and procedure RAG

Lowest governance friction. No customer data, no decisioning. Extends a capability we already run internally.

02

CRM-integrated agent

Integrations into 3rd party systems, API identity passing to agent context, and ease of use for an existing platform.

03

Accounting reconciliation

Best framed as one configuration of a general exception-review engine.

Priority 0: platform and governance. Not requested, but it consumes roughly 60% of capacity in Q4 and Q1.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

The Floor Plan

Architecture, zones, sizing, and the decisions behind them

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

DESIGN STANCE

Five principles that shaped the stack

01

One database until scale needed

Postgres gives relational, vector, full-text and a job queue until we move into Snowflake or others once required for interoperability.

02

Buy identity and others where we can

Avoiding over-engineering is a key tenant of our decision process. If it's proven, industry-recognized, and tested… we move forward without doing it ourselves.

03

Deterministic wherever possible

A matching decision a person can re-derive by hand is a control. One that cannot is a model risk.

04

Every dependency survives due diligence

A component choice is a subprocessor disclosure repeated across the client base.

05

Design seams, not abstractions

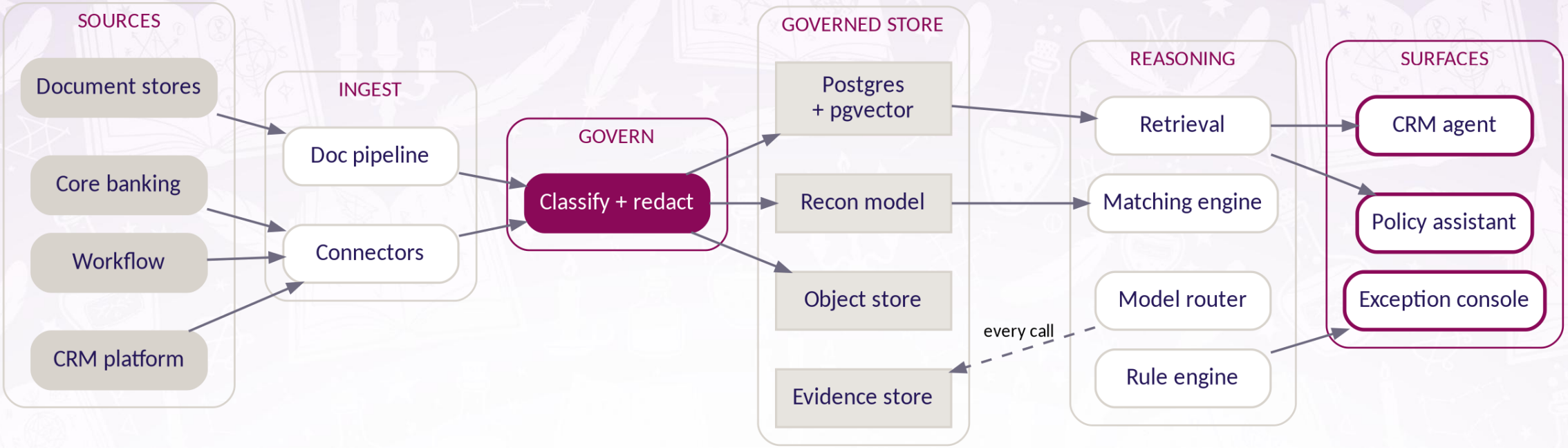
Five things must be swappable: parser, embedder, data platform, model provider, policy decision point.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

REFERENCE ARCHITECTURE

Five layers and a control plane that spans them



Authorization evaluates before retrieval. The audit record is written on every model call, without exception.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

WHY IT LOOKS THIS WAY

Five decisions inside the architecture

	Decision	Why we made it	What we accepted
1	**Classify and redact at ingest**	NPI is identified before anything is stored, embedded, or sent to a model	Every source passes the pipeline; onboarding is slower
2	**One database: Postgres + pgvector**	Access control becomes an ordinary SQL predicate; one system to secure and disclose	Fewer specialized vector features at very large scale
3	**Deterministic matching engine**	A match a person can re-derive by hand is a control, not a model risk	Fuzzy cases become explained exceptions, not auto-clears
4	**Model router from week one**	Models stay swappable; no single-model dependency	Every evaluation runs against more than one model
5	**Evidence on every model call**	The examiner record is first-party and complete	Storage and write cost on every request

Authorization evaluates before retrieval. Access is never checked after the answer is generated.

© 2026 Navanta™ All rights reserved. navanta.com

Target state: four enforced zones

ZONE 1
Edge / DMZ

- Reverse proxy and WAF
- Egress proxy
- No data at rest

FIREWALL · default deny · every allow rule logged and reviewed

ZONE 2
Application

- Policy assistant
- CRM agent
- Exception console
- Tool gateway
- Identity federation
- Authorization PDP

FIREWALL · default deny · every allow rule logged and reviewed

ZONE 3
Data and inference

Data	Inference · dedicated GPU
Postgres + pgvector	GPU inference 4 × H200
Object store	Model router
Evidence store	Matching engine

FIREWALL · default deny · every allow rule logged and reviewed

ZONE 4
Management / OOB

- Hypervisor management
- Backup
- Monitoring
- Jump host and BMC

© 2026 Navanta™ All rights reserved. navanta.com

SIZING AT 200 INSTITUTIONS

What the sizing model taught us

36 GB

vector index

4.2 million chunks, including graph structure

773 GB

source documents

3.4 million pages, three versions retained

14%

of one GPU node

annual inference throughput needed for the fleet

16×

concurrency headroom

232 available streams against 14 needed at peak

The AI is not what fills the array, and inference is not the bottleneck. Integration, entitlements, and evidence are.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

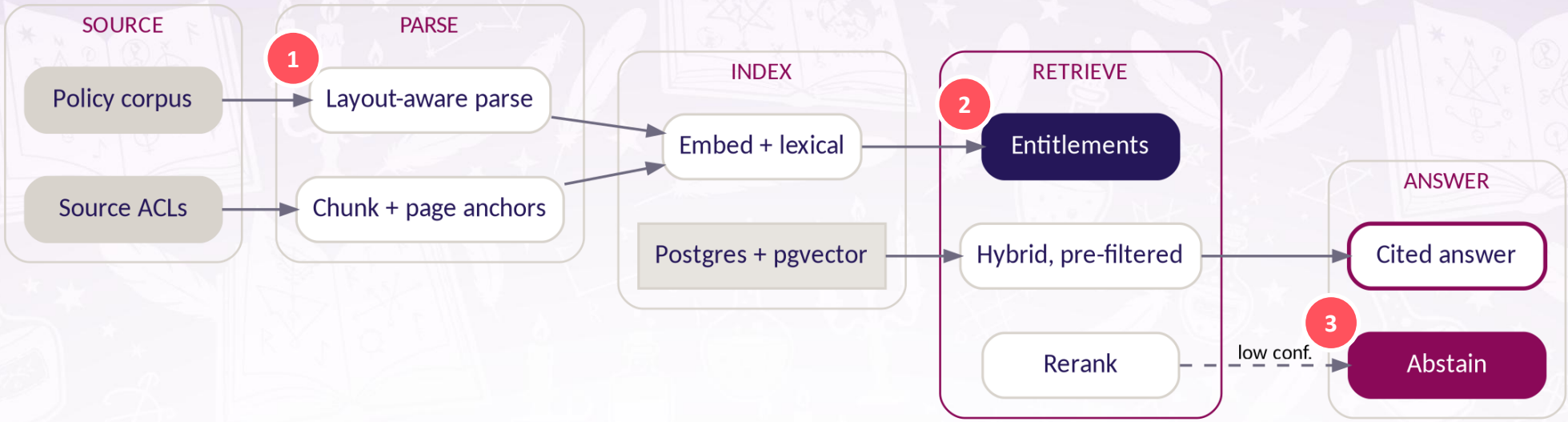
The Production Line

Five phases, one platform, each earning the next

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Phase 1 · Policy and procedure assistant



1 Layout-aware parsing

Citations point to the source paragraph. A parser that loses reading order produces confident, wrong citations.

2 Entitlements before retrieval

Hybrid search is pre-filtered by what the person asking may see. Never filtered after generation.

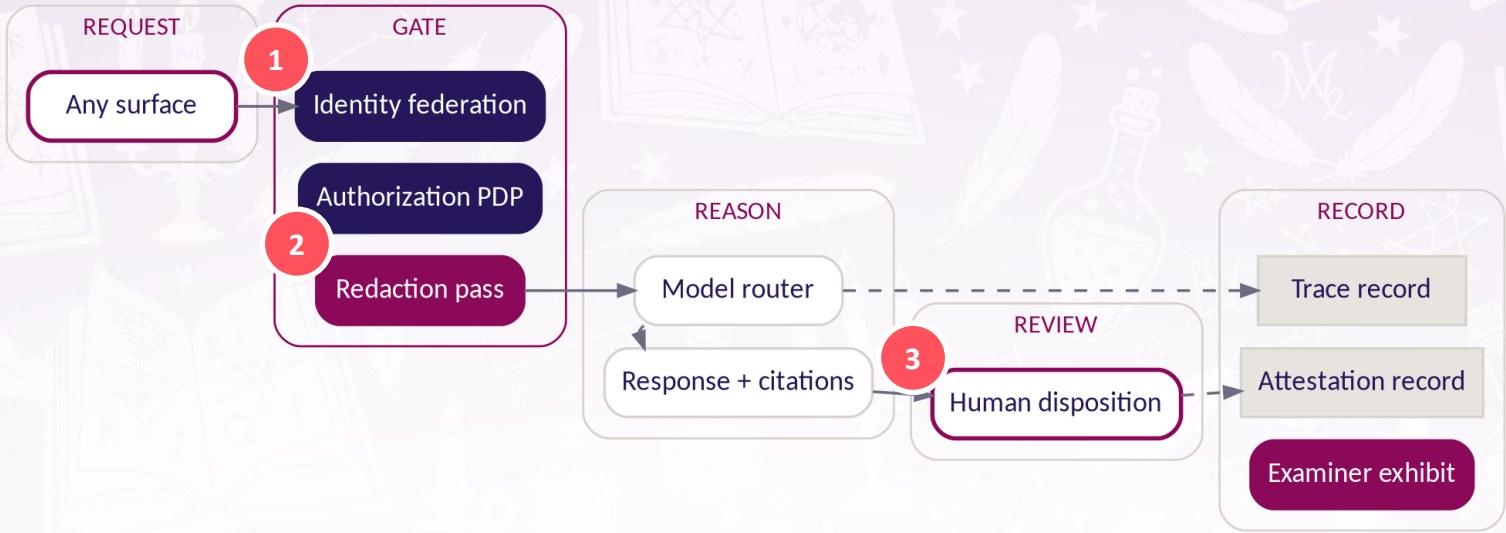
3 Abstain when unsure

Low-confidence retrieval routes to an abstention, not a fluent guess. A cited answer or no answer.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Phase 2 · Governance and the evidence record



1 Identity at the gate

Every request carries a named person through identity federation and a policy decision point, from any surface.

2 Redaction before the model

NPI is stripped before the model router sees the request, extending a capability we already run internally.

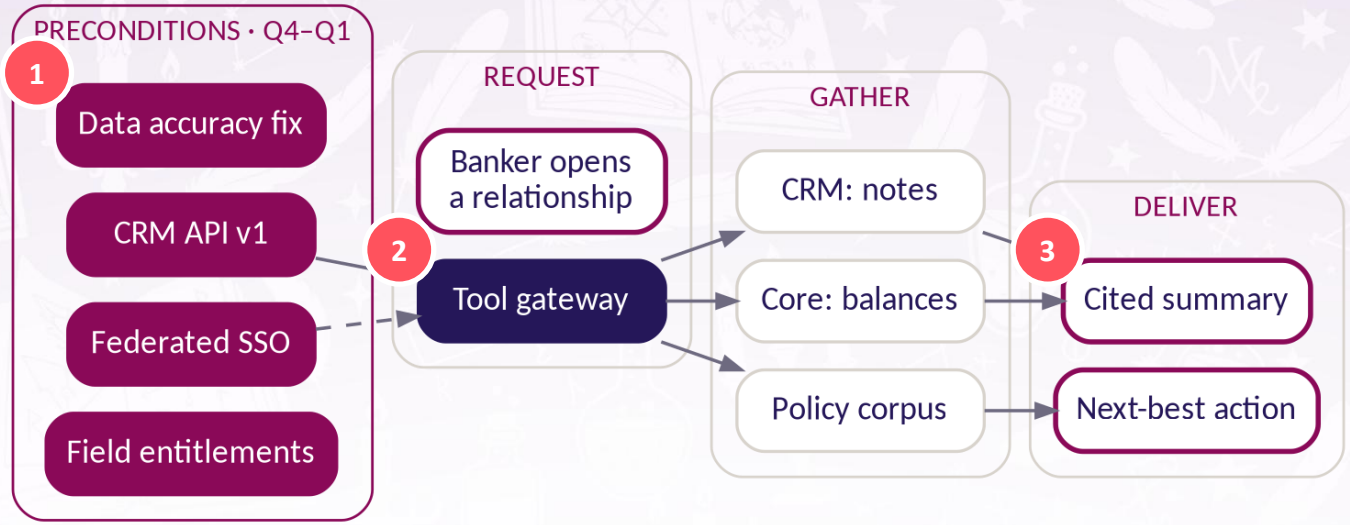
3 Evidence an examiner can use

Weights cannot be inspected, so validation is empirical: trace, human disposition, and attestation records.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Phase 3 · CRM agent, read-only



1 Preconditions first

Data accuracy, a CRM API, federated SSO, and field entitlements come before the agent does.

2 One tool gateway

Every system call passes one gateway with registration, authorization, and a kill switch. Read-only at launch.

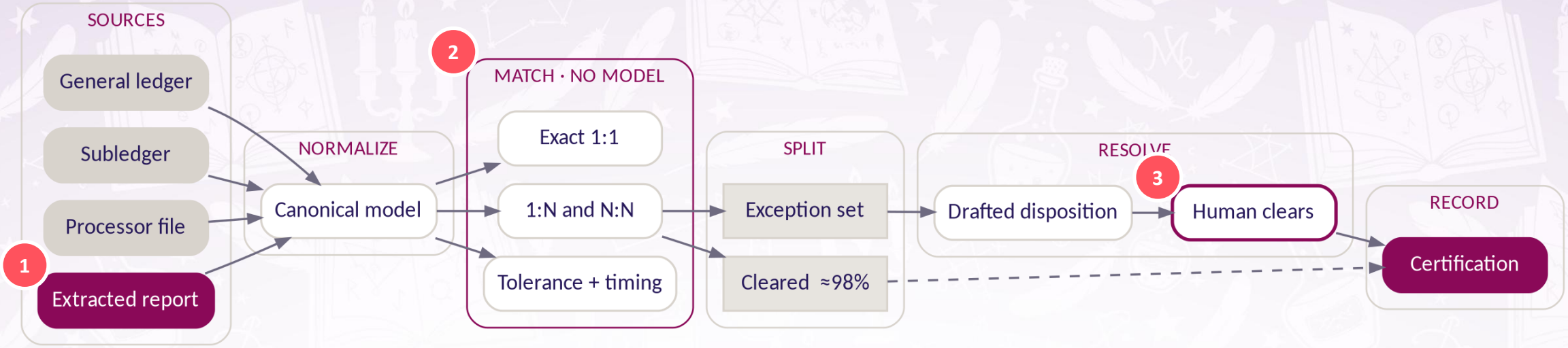
3 Cited summaries

Notes, balances, and policy content are gathered and cited, so a banker can see where each statement came from.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Phase 4 · Reconciliation as exception review



1 Reports become data

Where a report cannot be exported, it is extracted into the same canonical model as the ledger and processor files.

2 No model in matching

Exact, one-to-many, and tolerance rules are deterministic. A match a person can re-derive by hand is a control.

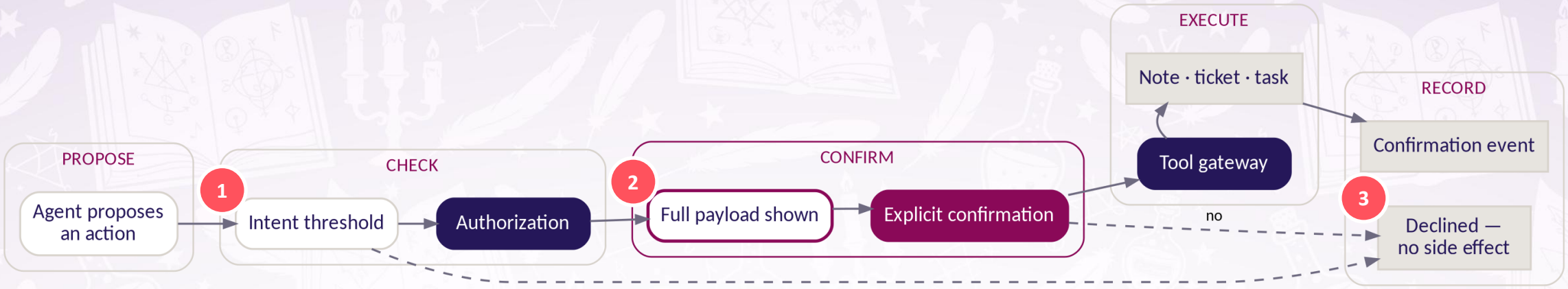
3 People clear exceptions

The model explains exceptions and drafts dispositions. A person clears them, and certification is recorded.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

Phase 5 · Confirmation-gated write actions



1 Check intent and authority

Below the intent threshold or outside the user's authority, nothing is proposed for execution.

2 Show the full payload

The person confirms the actual change, not a summary of it. Confirmation is explicit every time.

3 Fail closed, with a record

Every declined or failed path ends with no side effect and a record that it did so.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

The Lab Notebook

What is running, what went wrong, and what we measure

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

SUCCESSES

What is running in our own operation

IN USE

Ticket assistance

Fifteen years of our own support tickets became a recommendation engine for our service teams, scored on whether the resolution helped. Reduced time to resolution in tickets by 50%.

IN USE

Automated review pulls

System data assembles itself into the review materials relationship managers already present. No new interface to learn.

IN PLACE

Our own AI platform

An enterprise NVIDIA GPU platform in a Navanta data center, under our own development and supply-chain controls.

IN PLACE

Redaction, internally

Identifiers removed before data reaches a model, proven on our own workloads before it becomes a service.

READY TO DEMO

FDIC Call Report solution

Peer comparisons, trends, and outliers from public call report data. No NPI involved.

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

LESSONS LEARNED

Setbacks, and what we changed

What happened	What we learned	What we changed
Parsing, not retrieval, was the hard part	A parser that loses reading order produces confident, wrong citations	A parser bake-off, layout-aware parsing, page anchors, and citation tests
Data is the hard part	Synchronizing data across 10s of different source systems per customer is harder than it appears. Securing identity of access is even harder.	Agent controls and hard-coded software locking access to assets.
Platform work nobody requested	About 60% of early capacity goes to platform and governance	Planned as Priority 0 instead of discovered late
Speed of vibe-coded platforms	It's easy to make the products we are creating… until you ask them to show what occurred, with what data, with what context, and by whom.	Heavy focus on simplicity at first, with iterative additions to the platform as we progress. Encourage the team to slow down and focus on hard evidence.

© 2026 Navanta™ All rights reserved. navanta.com

MEASURABLE OUTCOMES

How we measure every capability

01 Citation fidelity

Does every answer resolve to the source paragraph it cites?

02 Abstention quality

When the corpus does not support an answer, does it decline rather than guess?

03 Retrieval quality

Golden-set evaluation runs in CI; a change that lowers a score does not ship.

04 Entitlement leakage

Adversarial multi-tenant tests. The only acceptable number is zero.

05 Evidence completeness

Every model call has a trace record; every human disposition has an attestation.

06 Time returned

Hours per task before and after, measured on the people doing the work.

© 2026 Navanta™ All rights reserved. navanta.com

The Final Concoction



Eric Jones

PRESIDENT & CEO



Patrick Rinsgred

CHIEF STRATEGY OFFICER



Stephen Moss

CHIEF OPERATING OFFICER

navanta TECH-O-WEEN

© 2026 Navanta™ All rights reserved. navanta.com

navanta™

TECH-O-WEEN

2026

navanta™

TECH-O-WEEN

2026




AI generated

navanta™

TECH-O-WEEN

2026