nucleus

NUCLEUS CASE STUDY

Healthcare Enterprise Replaces Cisco Vulnerability Management (Kenna) with Nucleus

1 Customer Overview

About the Customer

A healthcare services organization operating across multiple affiliated entities had been running its vulnerability program on Cisco Vulnerability Management (Kenna).

The team faced a growing reality that functionality and integration momentum had stopped while the risk of running a core security workflow on an EOL product increased. They needed a Kenna replacement that preserved continuity while modernizing how risk gets prioritized, owned, routed, and measured.

Challenges

Since its acquisition by Cisco, Kenna's product advancement ground to a halt and connectors were being deprecated. In addition, the Kenna platform posed day-to-day limitations that forced manual workarounds and made the program difficult to scale. As a result, the organization chose to seek a modern platform with a clearer innovation path and stronger operational support.

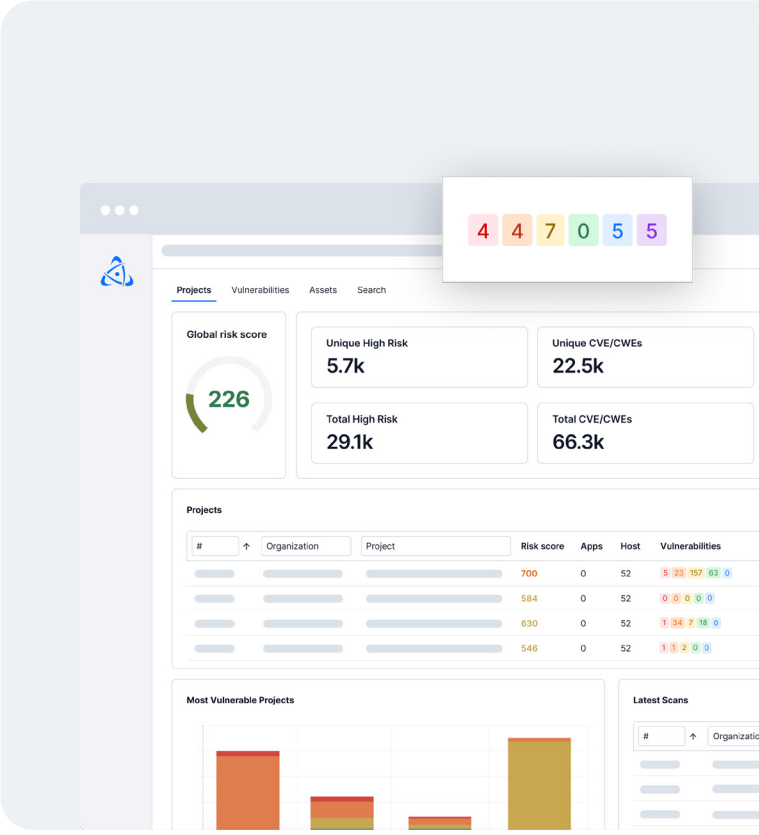
Outcomes

- Less than 30 days for initial migration.
- 99.8% reduction in the immediate do-now worklist (4,000+ backlog → 9 urgent, publicly exploitable exposures) using automated reprioritization filters.
- Replaced spreadsheet and calendar-driven processes with automation.

> "We were staring at 4,000 things in the backlog. Once we filtered to the existential threats with documented exploits, the do-now list dropped to nine."

2 Kenna Limitations

- Reporting capabilities were limited and required exporting data and rebuilding views in spreadsheets.
- Risk acceptance and exceptions were not time-bound by default, forcing manual tracking and reminders.
- Workflow automation was limited; changes were applied one vulnerability at a time rather than by reusable hierarchies and logic (asset group, OS, environment, metadata).
- Risk scoring and prioritization lacked transparency, creating a black-box effect when teams asked why something was ranked the way it was.
- The platform was limited to CVEs and did not support other exposure types (misconfigurations, compliance gaps, and non-CVE vulnerabilities).
- Enterprise governance was constrained, including segmentation and access controls for multi-entity structures, along with limited dashboards, trends, and metrics by team/group.



Kenna's prioritization was difficult to defend internally because it was hard to see and explain why an item was ranked the way it was. During evaluation, the customer highlighted the value of being able to understand what inputs drive prioritization, rather than relying on an opaque score.

> "It's not enough to say it's 'high risk.' We need to know what factors are pushing it up so we can make the case to the business."

nucleus

3 Implementation

Implementation: Kenna - Nucleus cutover

The implementation was anchored on a practical “definition of done:” replace Kenna for monthly reporting and day-to-day workflow, then expand.

STEP 1

Connector setup

1–2 days: The implementation team brought over credentials, verified access, started ingestion, and confirmed end-to-end data flow.

STEP 2

Recreate Kenna groupings and ownership logic

1 week: During the POV, it took less than a week for the customer, with Nucleus guidance, to replicate Kenna grouping logic into Nucleus automation rules.

STEP 3

Upgrade prioritization with Nucleus Insights

2 hours: After mirroring Kenna-style categorization, the team refined prioritization using Nucleus Insights threat rating + exploitability context

---

STEP 4

Reporting and dashboards

2 days: Nucleus includes a broad set of metrics out-of-the-box. Just a couple of days were required to recreate dashboards and views.

STEP 5

Expand coverage + automate governance

- Expand ingestion and context as needed (with the existing scanners).
- Implement time-bound exceptions with expiration and governance.
- Evolve routing: start with “who owns this asset,” then layer in finding-type routing (OS vs app-level) as needed.

4 Nucleus Advantages

Nucleus gave the customer a clear path from Kenna's legacy RBVM to unified exposure management. Instead of treating vulnerability management as CVE scoring and reporting, Nucleus unified vulnerabilities with broader exposure types and added workflow orchestration so remediation could run at enterprise scale.

Key capabilities and the value they delivered

Workflow orchestration:
End-to-end automation using rules that can be applied consistently across teams and asset populations. Expanding the scope from risk-based prioritization of "what to fix" into risk-based actions that accelerate "getting it fixed" for continuous exposure reduction at enterprise scale.

Rule-based exception handling:
Apply and expire exceptions by policy (asset group, environment, metadata), not one vulnerability at a time. Delivering governance that scales, with fewer missed renewals and eliminating error-prone spreadsheet-based reminders.

Dynamic asset grouping on ingest:
Automatically place new and changing assets into the right groups and hierarchies as data is ingested, including fast-changing cloud environments. This ensures that reporting and routing stay accurate even as the organization and environments change.

Reliable ownership and routing:
Assign risk owner dynamically using both asset context and finding type to identify the right team or user. This improves collaboration and trust across teams, increases remediation throughput, and reduces reassignments and stalled tickets.

Transparent risk scoring
Shows the inputs behind prioritization (threat signals, exploitability, and context) and supports customer-defined risk scores instead of relying on an opaque score. This reduces debate, speeds alignment, and strengthens remediation buy-in.

Bi-directional integrations:
Push findings into existing ticketing systems and keep status, ownership, and comments synchronized back to Nucleus so both systems stay aligned. Teams keep working where they already operate, leadership gets a single source of truth, and remediation progress stays accurate without manual updates.

True multitenancy:
Projects and asset-group-based access controls separate affiliated entities while maintaining centralized visibility and reporting. This creates clear boundaries for who can see and act on findings, while enabling consolidated measurement across the organization.

5 Looking Ahead

With Kenna replaced, the program can evolve from "risk-based lists" to continuous exposure operations:

- Expand beyond CVEs into a unified view of vulnerabilities, misconfigurations, and compliance gaps in the same operating cadence.
- Increase automation coverage so routing, exceptions, SLAs, and ticket updates run consistently across more teams and asset groups.
- Use trends and team-level metrics to improve accountability over time and to prove exposure reduction to leadership.

Request a Kenna → Nucleus Migration Assessment and Cutover Plan

We'll map your Kenna workflows, dashboards, SLAs, and connectors, and show how to run Nucleus in parallel until you're confident to cut over.

nucleus

Nucleus Security is the enterprise leader in unified vulnerability and exposure management, enabling organizations to prioritize and mitigate vulnerabilities faster, at scale. Delivering unmatched time to value, Nucleus automatically unifies and organizes data from all your security and business tools into a single pane of glass. With powerful dynamic automations, teams can effectively automate their vulnerability management program. As a FedRAMP authorized vendor, Nucleus Security is transforming how enterprises, federal agencies and defense contractors secure their digital assets and networks.

AUTODESK CBRE motorola DELTA DENTAL

www.nucleussec.com | hello@nucleussec.com

v1_01_26