ApexaiQ®

WHITE PAPER

Continuous Asset Assurance

An Executive Perspective on Moving Beyond Cisco Kenna to Continuous Assurance

A CEO White Paper by
Lokesh Aggarwal, Founder & CEO, ApexaiQ

Replace a retiring point product.
Upgrade to continuous assurance.

Executive Summary

Cisco is retiring Kenna Security on a fixed timeline, ending new sales, renewals, and ultimately support. For every Kenna customer, this is now a forced decision:

OPTION A

Swap one risk-based VM tool for another

OR

OPTION B (Recommended)

Step into an operating model built on continuous assurance

The Three-Imperative Model

Know Every Asset

Continuous Asset Assurance

Reduce Exposure

Exploitable Exposure Assurance

Prove Control

Proof of Control

ApexaiQ defines Kenna Displacement Assurance, the operating model for what comes next.

CORE THESIS

If Cisco is retiring Kenna, do not treat this as a tool swap. Use it to move from scanner-dependent triage to continuous assurance.

The Journey: From Kenna to Continuous Asset Assurance

Step 1: Recognize the Structural Shift

Kenna was designed as a scanner-fed prioritization engine more than a decade ago. **It answered one question well:** **"Of the findings we see, which matter most?"**

Meanwhile, your environment changed.

Cloud, SaaS, remote, OT/IoT, and shadow IT expanded the attack surface far beyond traditional scanner scope.

In that world, a product that cannot natively discover assets, cannot see unmanaged systems, and cannot verify remediation leaves structural gaps.

Step 2: See Why Kenna Customers Are Exposed

Kenna helped for a time. But several foundational design choices now translate directly into exposure. These are not just feature gaps, they are assurance failures.

No Native Asset Discovery

Depends entirely on external scanners. Assets outside scanner scope remain completely invisible.

No CAASM View

Cannot see unmanaged, shadow, or unagented assets across hybrid estates, cloud, OT/IoT remain dark.

No Estate-Level Hygiene Score

Produces risk scores for individual findings, not a simple posture grade for the full estate.

No Closed-Loop Remediation

Creates tickets but cannot prove fixes were applied or show that exposure actually shrank

Why Kenna Customers Need More Than a Like-for-Like Replacement

A forced migration should not preserve the structural limitations that made replacement necessary.

Preserves scanner blind spots

Unmanaged, unagented, and shadow assets may remain outside visibility.

Solves prioritization, not assurance

Ranking findings is not the same as proving control.

Recreates ticket-driven remediation fatigue

More prioritization may still produce larger queues, not less exposure.

Adds another point tool instead of reducing stack risk

Replacing one silo with another may increase complexity rather than simplify it.

✗ The question is not **"What replaces Kenna?"**
✓ It is **"What operating model should replace first-generation RBVM?"**

Kenna's retirement is not just a vendor change.
It is confirmation that first-generation RBVM has reached its limit.

Step 3: Three Imperatives for Kenna Displacement

01

Replace Scanner-Dependent Visibility with Continuous Asset Assurance

Know Every Asset You Are Accountable For

Move from "we know what our scanners see" to "we know every asset we are accountable for." Agentless discovery across endpoints, cloud, SaaS, OT/IoT, and shadow IT, with continuous detection of change and a unified inventory tying assets to exposures.

Key Capabilities:

- Endpoints & servers
- Cloud & SaaS assets
- OT / IoT devices
- Shadow IT & unmanaged systems

"Static inventories are insufficient. Continuous Asset Assurance is the foundation."

02

Reduce Exploitable Exposure, Not Just Findings

Machine-Speed Threats Require a Different Model

Kenna helped re-rank findings. Machine-speed threats require you to continuously shrink what can actually be exploited. That demands exploitability context, asset criticality, and risk-based remediation that closes real attack paths, not bigger ticket queues.

Key Capabilities:

- Exploitability context (KEV, EPSS)
- Asset criticality weighting
- Risk-based remediation paths
- Closed attack-path closure

"Patch everything was never a strategy. In a Kenna EOL world, it fails faster."

03

Make the Replacement Decision Provable

Prove You Remain in Control

The question is no longer only "Which tool do we buy next?" but "Can we show that the new model leaves us with fewer blind spots and less exposure?" Evidence that remediation occurred, exposure shrank, and the hygiene story is explainable to executives.

Key Capabilities:

- Evidence remediation occurred
- Show exposure shrank over time
- Executive-ready hygiene narrative
- Audit-ready artifact generation

"Evidence should be produced by controls, not assembled for audits."

Step 4: How ApexaiQ Wins the Displacement Decision

ApexaiQ was built around a simple principle

We know every asset | We know every material gap | And we can prove we are in control.

Native Agentless Discovery

Discovers hybrid environments including unmanaged and shadow assets often outside traditional scanner coverage.

ApexaIQ Cyber Hygiene IQ Score

A single cyber hygiene grade that executives can understand and track over time. Simple. Explainable. Provable.

Closed-Loop Remediation

Tracks from discovery to verification so exposure reduction is provable, not assumed. Control proven through operations.

Platform Consolidation

Collapses CAASM, VM, and hygiene into one SaaS subscription with documented ROI and attack surface reduction.

ApexaiQ vs Kenna Security, At a Glance

Capability	Kenna Security	ApexaiQ
Asset Discovery	Scanner-dependent	**Native agentless**
Shadow IT	Not visible	**Full visibility**
Hygiene Score	Finding-level score	**IQ Score 60–160**
Remediation Proof	Ticket creation only	**Closed-loop verification**
CAASM	Not included	**Native CAASM**
Deployment	Complex integration	**Weeks, agentless**

The Business Case: From Kenna Program Cost to Assurance ROI

Typical Kenna Program Costs

- Kenna licensing fees
- One or more enterprise scanners
- Integration & connector work
- Operational labor to maintain the stack

Mid-market programs:
$100K–$500K+/year combined

ApexaiQ Displacement ROI

- Eliminates separate discovery tools
- Reduces dependence on adjacent hygiene products
- Consolidates vendors, reduces integration overhead
- Proof of control = fewer audit preparation costs

Organizations can often reduce overlapping tool spend and operating effort by 30–50% through consolidation.

Fast, Low-Friction Migration:
Replace Kenna Without Losing a Step

01
Weeks 1-2

Assess

- ASSESS Inventory Kenna Weeks 1-2 integrations & scanner stack
- Map ticketing and remediation workflows
- Establish current asset counts
- Identify top exposed segments

Define baseline before migration begin

02
Weeks 3-6

Parallel Run

- Deploy ApexaiQ agentless alongside Kenna
- No agents to roll out, no scanners to replace
- Discover additional unmanaged & shadow assets
- Establish initial IQ Score baseline

Side-by-side: see what Kenna missed in days

03
Weeks 7-10

Cut Over

- Redirect ticketing & Weeks 7-10 exposure workflows to ApexaiQ
- Leave Kenna in read-only validation mode
- Validate ApexaiQ is driving remediation
- Confirm exposure is shrinking

Clean transition with zero visibility gap

04
Post cut-over

Optimize

- Retire redundant tools
- Tune IQ Score thresholds to risk appetite
- Institutionalize IQ Score & exposure review cadence
- Document ROI and consolidation savings

Continuous assurance as the new operating model.

Closing Perspective

Kenna's end of life marks the end of an era where risk-based VM alone was considered enough. The environment has moved on. Attackers move faster. Estates are more distributed. Boards expect clearer answers.

Kenna Displacement Assurance is not about reproducing yesterday's model with tomorrow's budget.

It is about using a forced migration to define the operating model for what comes next. **The question is no longer who replaces Kenna, but whether that replacement reduces blind spots and proves control.**

Our Commitment to Kenna Customers

End scanner-dependent blind spots

Native agentless discovery across your full hybrid estate

Shrink exploitable attack surface

Prioritized exposure reduction at machine speed

Turn VM into continuous assurance

Provable control that satisfies boards, auditors & regulators

APEXAiQ®

Scan to Book a Demo

https://www.apexaiq.com/kenna

ABOUT APEXAiQ

ApexaiQ® is a SaaS-based, agentless, continuous asset assurance platform that offers real-time visibility into IT risks. It automates remediation actions, providing a comprehensive view of asset health, vulnerabilities, and compliance through a single dashboard, enabling organizations to proactively manage their technology landscape and enhance security posture effectively. **ApexaiQ** prioritizes critical assets and those that may become critical, identifying patch needs continuously with enriched end-of-life and end-of-support data, warranties, and vulnerabilities; and providing a provable and reportable risk score.

For more information, contact ApexaiQ at apexaiq.com