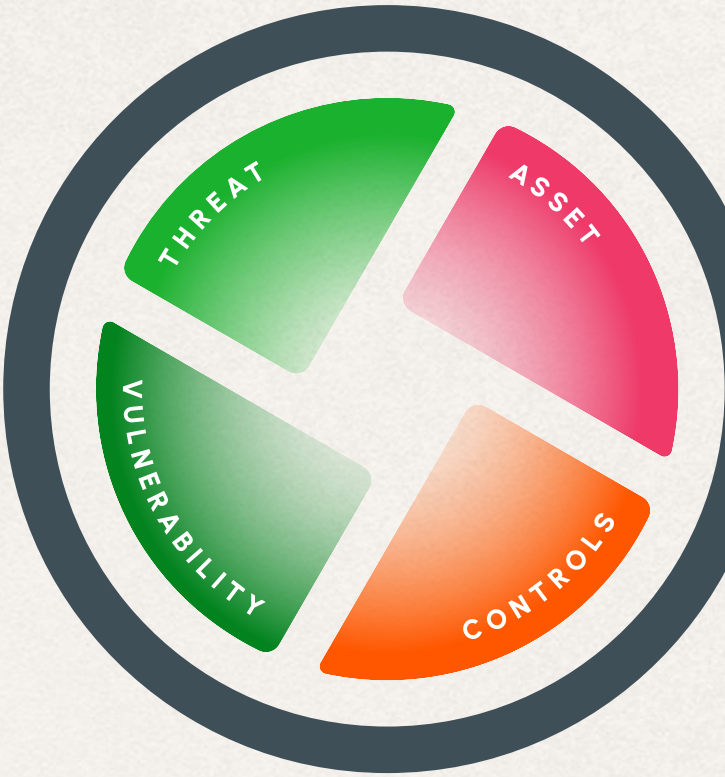
nagomi



Crossing the CAASM:
Managing Exposure Through a Lens of Control

ABSTRACT

Many security vendors label their solutions "exposure management" tools. Vulnerability and risk-based vulnerability management (VM/RBVM), CAASM, EAP, ASCA, and other emerging approaches all play a role – but enterprises need a way to pull the pieces together.

In this ebook we'll look at the current state and major misconceptions about exposure management and how you can add the missing pieces and perspective to transform the "acronym soup" of disparate tools (like RBVM, CCM, CAASM, and ASCA) into a proactive, automated practice for reducing risk, effort, and investment at the same time. The end goal: delivering the execution layer of CTEM, where visibility turns into action, and exposures are actually closed.

INTRODUCTION

Clearing up the Confusion: What Exposure Management Really Means

Ask ten security experts to define exposure management, and you might get ten different answers, and that's the heart of the problem. The industry is filled with misconceptions about managing exposures, starting with believing the terms "vulnerabilities," "exposures," and "risks" are interchangeable.

They aren't, and it's worth taking a minute to clarify the definitions:

- The term "vulnerability" refers to a flaw or weakness in a system, very often a known software bug that hasn't been patched
- "Exposure" refers to any vulnerability, misconfiguration, or security gap that a malicious actor could potenitally exploit to compromise an organization's digital assets
- "Risk" is what could happen when threat actors leverage exposures to exploit vulnerabilities – i.e., the likelihood and potential business impact considered of compromising that asset.

Unfortunately, most organizations still approach exposure management as an evolution of their vulnerability management (VM) programs, focusing on vulnerabilities as the primary type of exposure while giving other types less attention.

The narrative needs updating

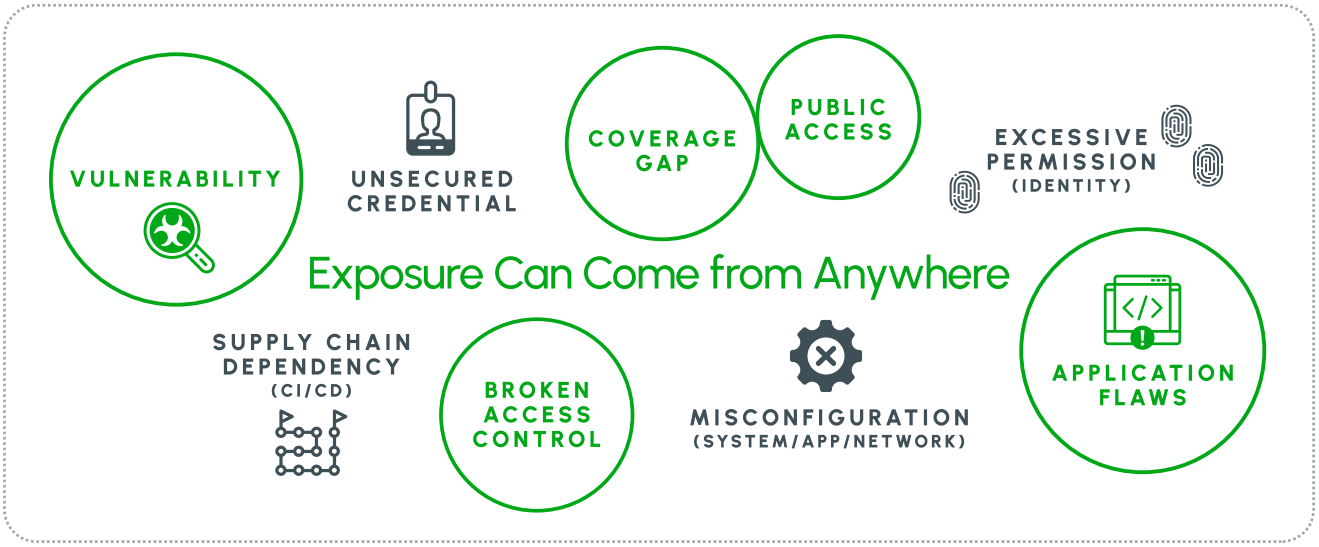
True exposure management is not about chasing every known and unknown vulnerability; this leads to wasting time on the wrong things and operating from a false sense of confidence. It's about understanding which exposures matter, why they matter, and how to fix them before attackers take advantage.

Developing this new understanding starts with deciding which tools and strategies update and improve your exposure management practice.

PART I

Pulling the Moving Pieces Together

Letting digital exposure fester within your attack surface leads to downtime, delays, fines for non-compliance, and nearly incalculable losses of data, productivity, and brand reputation and risk seems to come from everywhere.



AI MUDDIES THE WATERS

The rise of AI means there's even less time to find and defend exposures and a greater need to know what you have in place is working. Palo Alto Networks research shows the median time it takes an attacker to penetrate a network and access confidential data fell from nine days in 2022 to under 24 hours in nearly half of all cases in 2024.

CTEM Aims to Impose Order

Many different tools claim to mitigate exposure but CISOs need clearer understanding of the roles that each one plays, and a unifying strategy for making them work even better together.

Continuous Threat Exposure Management (CTEM) provides a framework, versus another point tool or collection of products, for managing risk.

CTEM scopes out a cycle of five ongoing steps, scoping, discovery, prioritization, validation, and mobilization to remediate digital exposure across your entire environment.

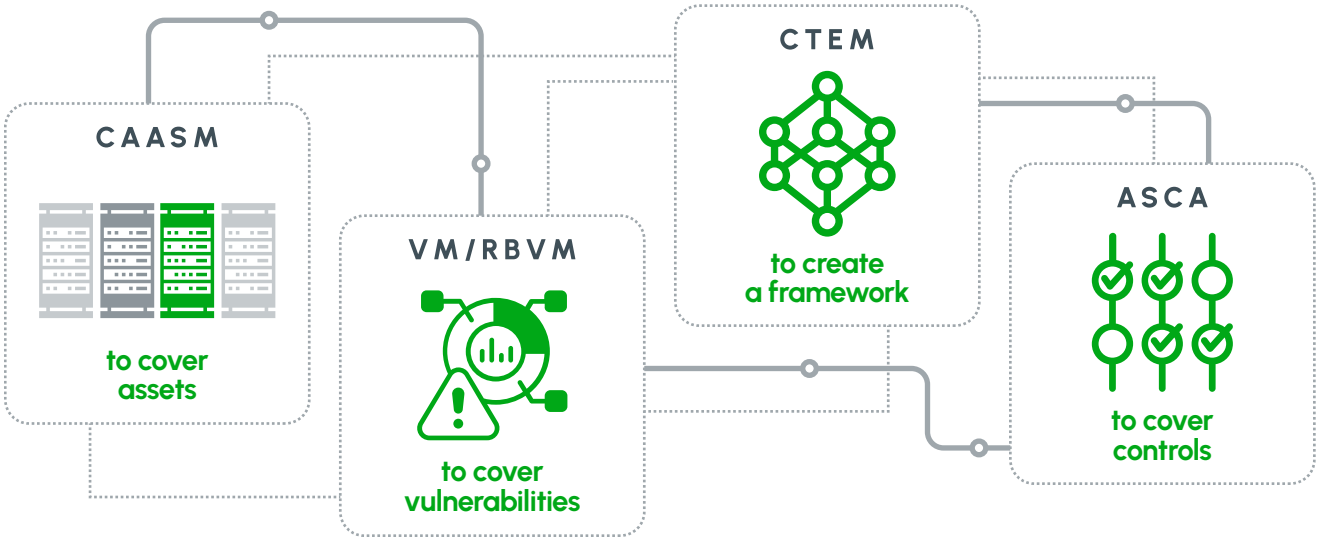
THE KEY WORD IS "FRAMEWORK"

The ongoing process prescribed by CTEM combines several traditional security tools and techniques–but it's not a perfect science. Coverage gaps may exist between tools, or solutions might overlap, and at the end of the day, the process lacks a vital, enabling perspective.

The CTEM umbrella covers:

- **Vulnerability management (VM),** the foundational step in managing exposure, that bombards security teams with too many tasks and too little context to help them prioritize and act.
- **Cyber Asset Attack Surface Management (CAASM)** CAASM that adds critical visibility by getting eyes on everything in your environment. CAASM delivers the asset piece, but only tells you what you have, not what you have that needs protecting.
- **Exposure assessment platforms (EAP)** go beyond scanning for vulnerabilities by introducing a risk-based approach to deciding what to fix first. They use asset and control context to prioritize vulnerabilities, but they stop short of treating control or coverage gaps themselves as exposures.
- **Automated Security Controls Assessment (ASCA)** that's coming to be viewed as the "engine" that drives CTEM.
- **Breach and attack surface (BAS)** or Adversarial Exposure Validation (AEV) vendors that also have begun aligning themselves with CTEM as a part of managing a company's attack surface and exploitable exposures.

Each approach delivers a vital perspective but, even when they operate collectively within a CTEM framework, all fail to answer the question: "What are we doing to mitigate risk, and is what we're doing effective?"



Not fully understanding what exposure management leads to focusing too narrowly on CVEs and asset inventories while ignoring the context needed to assess risk. Existing tools answer the first question, "Are we exposed?" but fail to the next one: "Are we protected?"

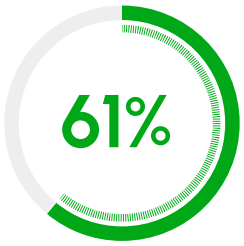
Over-emphasizing vulnerabilities and patching can also lead to under-utilization and even misconfigurations of other security controls.

ASCA introduces a controls perspective

ASCA operationalizes CTEM by continuously validating security controls, detecting misconfiguration or control drift, and helping prioritize and remediate exposure based on risk and available controls. By automating the assessment of security controls, ASCA:

- **Increases efficiency**, reducing the time it takes to manually evaluate controls
- **Improves the accuracy of security evaluations** by minimizing human effort—and error
- **Delivers real-time insight** through instantaneous feedback on security controls
- **Promotes scale** to handle growing volumes of data and streamline security operations

ASCA and CTEM deliver always-on coverage, continuous assessment and ongoing process and posture improvements. Together they enable new levels of protection that individual point tools and point-in-time (PIT) assessments don't deliver. To their credit, enterprise CISOs are investing to take full advantage:

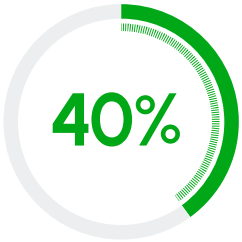


of security leaders have suffered a breach because of **failed or misconfigured controls** in the last 12 months.

SOURCE: GARTNER

By 2026, organizations that prioritize security investments based on continuous exposure management will be **3x less likely to suffer a breach**

By 2028, preemptive cyber solutions will have displaced at least



of solutions focused on traditional D&R methods

> "What's ***actually*** protecting us right now?"

> "What isn't and why?"

> "What's next?"

NAGOMI ADDS THE 'CONTROLS' PIECE

Security teams don't just need to see exposures, they need to understand whether controls are deployed correctly, enforced, and effective to mitigate the exposure. Only from this vantage point can your team answer:

- Are we protected?
- Do we need to patch, reconfigure, or just observe?
- Is our coverage improving or eroding over time?

Nagomi helps CISOs anchor exposure management around controls to turn static asset and vulnerability data into dynamic, prioritized action, automated, contextualized, and mapped to what matters to your business. Not just more visibility, but clarity you can defend.

"ARE WE PROTECTED?" REQUIRES A BROADER PERSPECTIVE

Tools like CAASM, RBVM, and other standard practices within traditional exposure management count assets, unearth CVEs, and might assign scores, but that only gets the SOC team so far. Misconfigurations, unmonitored assets, missing or unenforced security controls are the real conditions–and telltale signs–that theoretical vulnerabilities represent true exposures.

Without understanding how your defenses are deployed, enforced, and performing in the wild, the team misses half the picture. Today's patchworked solutions stop short of correlating and coalescing exposures, controls, and threat intelligence into a prioritized "hit list" and clear plan of action.

In the next section, we'll show how you can solve that problem by reframing exposure management to bridge that between "What threats are out there?" and "What really matters?"

PART II:

"Crossing the Chasm": 5 Steps to Transform and Modernize Exposure Management

The Starting Point: Rethink the "Old Way"

Begin taking exposure management to the next level by acknowledging what's broken and defining your own plan for upgrading to a modern approach. Nagomi recommends a five-step process:

				
STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
Broaden the scope of exposure management	**Build** a unifying intelligence engine	Add the critical missing perspective - **controls**	Get practical – **implement** your new strategies	**Automate** the entire process (where it makes sense)

STEP 1

Widen the Scope of EM: Go Beyond Patching Vulnerabilities

This may feel counter-intuitive and daunting, since there's no lack of vulnerabilities to patch now, but redefining exposure can make it easier to find, prioritize, and address your most dangerous threats. Start by broadening the scope of what exposure means to include other common vectors.

Taking a wider view and more expansive approach to managing exposures leads to finding, contextualizing, prioritizing, and where possible automatically mitigating, coverage gaps and misconfigured controls as well as known vulnerabilities.

STEP 2

Take a Unified Approach: More Complete and Continuous, Less Costly and Complex

The rise of AI means attacks can unfold in a fraction of the time, too fast for most organizations to detect and respond effectively. Eliminating exposures proactively takes away potential attack vectors, the only strategic path to avoiding risk.

Becoming more proactive means becoming more efficient, making exposure management work smarter, faster, and with greater autonomy. It does not mean adding more tools and expanding your own attack surface unless you verify gaps and dangerous blind spots.

UNIFIED INSIGHTS UNRAVEL COMPLEXITY

The missing link here isn't more "visibility", too many vulnerabilities already taunt analysts from their dashboards, it's a way to prioritize that avoids analyst burnout and promotes meaningful action. Consolidating data from multiple sources and perspectives paves the way for efficient operations and equips your teams to:

- Fully utilize security tools already in place
- Integrate, and prioritize threat and exposure insights and intelligence
- Prove and document progress

The unification of insight means adding a vital perspective most companies lack now.

STEP 3

Start Viewing Exposure through a New Lens: Controls

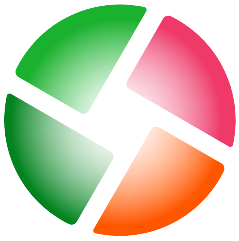
It's not enough to know an exposure exists. Security teams need to view it in the context of available controls to determine what needs to be done to mitigate risk, how, and in what order.

Viewing risk through the lens of your security controls brings multiple pieces into view and the complete picture into focus. That includes assets, threat actor intelligence, coverage gaps and misconfigurations. The aggregate view shows whether:

- Threat actors are actively exploiting exposures
- Their activity impacts critical assets
- Mitigating controls exist that can prevent the exposure from being exploited in your unique environment

THREAT ACTORS
Are we focused on the exposures being leveraged to target our industry?

VULNERABILITIES
Do we have exploitable vulnerabilities exposures?



ASSETS
Which assets matter most?

SECURITY CONTROLS
Are tools properly configured?
Are they doing what we expect them to do?

ATTACKERS ARE TARGETING CONTROLS

Without the perspective of available controls, security professionals waste time and effort patching the wrong things – and ignoring a critical attack vector. Taking a control-first approach becomes more important all the time because threat actors increasingly leverage misconfigurations and other avoidable gaps in controls to launch and conduct attacks.

[Controls are the new Number 1 attack vector]

Since the first denial of service (DoS) attack three decades ago, threat actors have been coming up with ways to take down or hijack security defenses to invade a business. Modern risks include missing, misconfigured, and unenforced or underutilized protections that create simple paths for attackers — open ports, excessive rights, and privilege escalation to name a few.

Most organizations can't correlate exposures with assets and correctly configured controls to see, verify, and document the existence of mitigating protections

Clarity vs. Visibility

Which exposures really matter?

Are our defenses working as intended?

What adjustments will truly reduce risk?

Here's where visibility comes into play. Most organizations lack visibility of their controls and the changes made by multiple administrators and risk- or policy-based solutions as time goes on. Viewing exposure through the lens of controls proves essential to building a complete, actionable view of risk and plan to address it.

Without a clear picture of your available controls, how they are configured and working together — and how they map to assets and exposures — your team struggles to prioritize patching, policy changes, and future investments. And CISOs will struggle to chart and demonstrate progress.

STEP 4

Get Practical: Operationalize CTEM

Nagomi recommends following a five-step process for assessing, prioritizing, mitigating, and reporting on risk on a continuous basis:

- Map controls to assets and threats
- Assess digital exposure
- Prioritize exposures in terms of their potential impact to your business
- Mobilize by determining the best path forward (patching, control tuning, accepting risk) in terms of controls as well as risk
- Maintain business-level dashboards and reporting to answer executive questions (like "Can this thing hurt us?" and "Are we patched?"), justify investments, and demonstrate success

STEP 5

Automate the Whole Cycle: Assess, Prioritize, Respond

Automation is crucial not only for patching but:

- Streamlining the entire process of assessing controls
- Mapping risk to your security environment
- Prioritizing and executing remediation efforts
- Reporting progress eliminating exposures
- Avoiding the slow, error-prone manual process , what takes customers weeks (and is outdated almost immediately) can be automated in near real time

Many tools now automate asset inventories and detection, but few can help with prioritization and tuning controls. Automating controls assessment — a critical function of ASCA — provides invaluable real-time perspective most companies lack. Or, attempt to create manually after-the-fact.

As we'll see in the next (and last) section, Nagomi's Control-Aware Defense platform automates the cross-correlation of exposures through gap detection, scoring, and reporting to slash analysis times — the time it takes your team to act — from days and weeks to hours and minutes and equips CISOs with the measurable board-level metrics they're increasingly asked to present.

PART III

Nagomi Control Rewrites the Book

Exposure management is too big a story to tell with spreadsheets. Done right, it's a coming of age story in which the hero saves your company's assets, employees, data, and brand reputation.

Nagomi Control, powered by Exposure lens serves as the execution layer for CTEM. It brings all the characters and plot lines together, consolidating, aggregating and correlating data about assets, risks, and controls in one easy place to deliver insights most organizations don't have now.

A Controls-First Approach Helps the Good Guys Win

Viewing assets, threats, and vulnerabilities through a control-first lens fills dangerous insight gaps at every stage and vector. A cohesive approach improves your security posture and operations so you can:

Optimize tools and unburden teams: A control-first approach promotes faster, smarter decisions about your defense stack. Reduce manual efforts, phase out redundant tools, and find impactful new ways to combine and integrate existing tools.

Automate prioritization and fast-track mobilization by determining the right remediation path. Nagomi moves exposure management beyond asset inventories and endless lists of CVEs so you can prioritize and proactively mitigate exposure based on your unique risk profile with a view to available and absent controls.

Operationalize CTEM. Use Nagomi's "exposure intelligence engine" to drive complete, continuous assessment and coverage that turns CTEM from a framework (read: nice idea) into a functioning practice that moves the needle on risk.

Equip CISOs to report ROI in board-level terms, linking exposures and potential impact to business to security investments and a steadily shrinking attack surface.

Achieve and accelerate proactive posture management by measuring, prioritizing and improving the way you deploy and enforce protections at all times.

Where do we have gaps?

Do we have a tool that does that?

Are controls working the way we thought or expected them to?

Give Your Heroes Superpowers

Ready to turn exposure management into mobilized risk reduction? See how Nagomi Control transforms CTEM from a framework into execution. **Request a demo today**.