cymulate

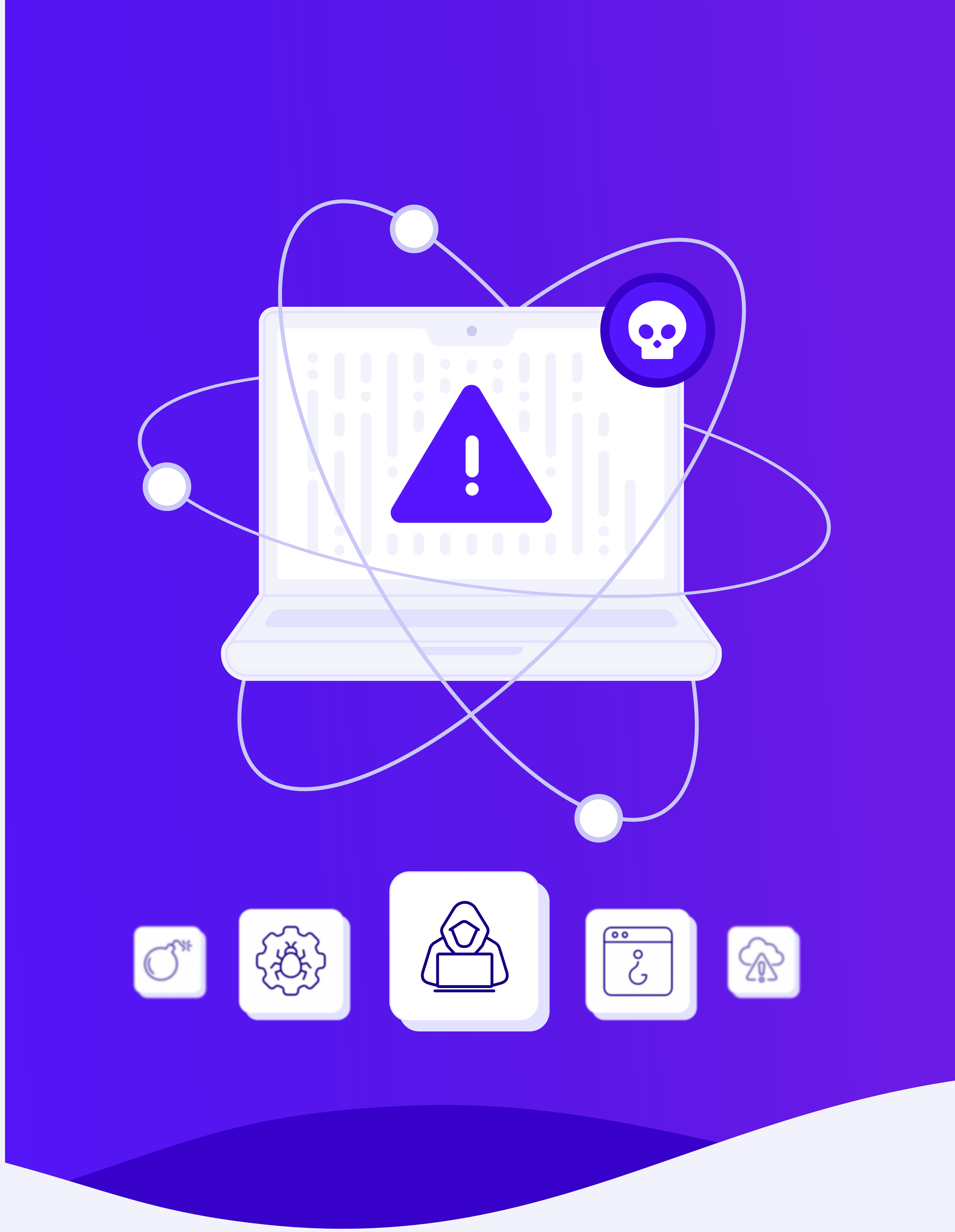
Buyer's Guide to Exposure Management

How to Spend Your Budget Wisely to Harden Defenses Against Real-World Threats

A shift in cybersecurity from managing vulnerabilities and validating exposure to full continuous threat exposure management (CTEM) is well underway. Gartner says that organizations that adopt a full CTEM strategy are three times less likely to suffer a breach.

What's driving this change? Threats to your environment move fast and evolve quickly. Your attack surface has expanded more than you may realize because of the proliferation of cloud and ephemeral architectures. Being reactive is no longer acceptable.

Exposure management is about focusing on your organization's biggest cyber weaknesses and rallying teams to address issues before attackers exploit them. By adding real-world context to your exposure data, you and your teams get faster, smarter and more efficient security outcomes.



According to Gartner, by 2028 organizations enriching Security Operations Center (SOC) data with exposure information will enhance threat evaluation and accelerate incident response, reducing the frequency and impact of cyberattacks by 50%. (Transform SecOps via Proactive Exposure Management and Threat Defense, May 2025)

Exposure management may seem like the natural evolution from vulnerability management and exposure validation, but there's nuance to this shift in three key ways:

1. Exposure management offers a more **targeted approach** to addressing threats that can harm your environment
2. Unlike previous processes, exposure management provides more **actionable steps** for remediating issues
3. Instead of operating in siloes, exposure management allows for more **cross-functional involvement and accountability**, making the practice more impactful across an entire security organization

If you've received budget approval to seek an exposure management solution, it's important to spend it wisely. The time to consider point solutions that only address part of your issues has passed.

There's now opportunity to achieve your objectives and proactively reduce your exposure risk. We'll walk through what you'll need to consider so your budget is well-spent.

Three Primary Considerations for Unified Exposure Management

There are many critical features and capabilities within exposure management, but when you boil it down, there are three primary considerations that must be in play for any buyer:

01 Unified, Multisource Discovery Data

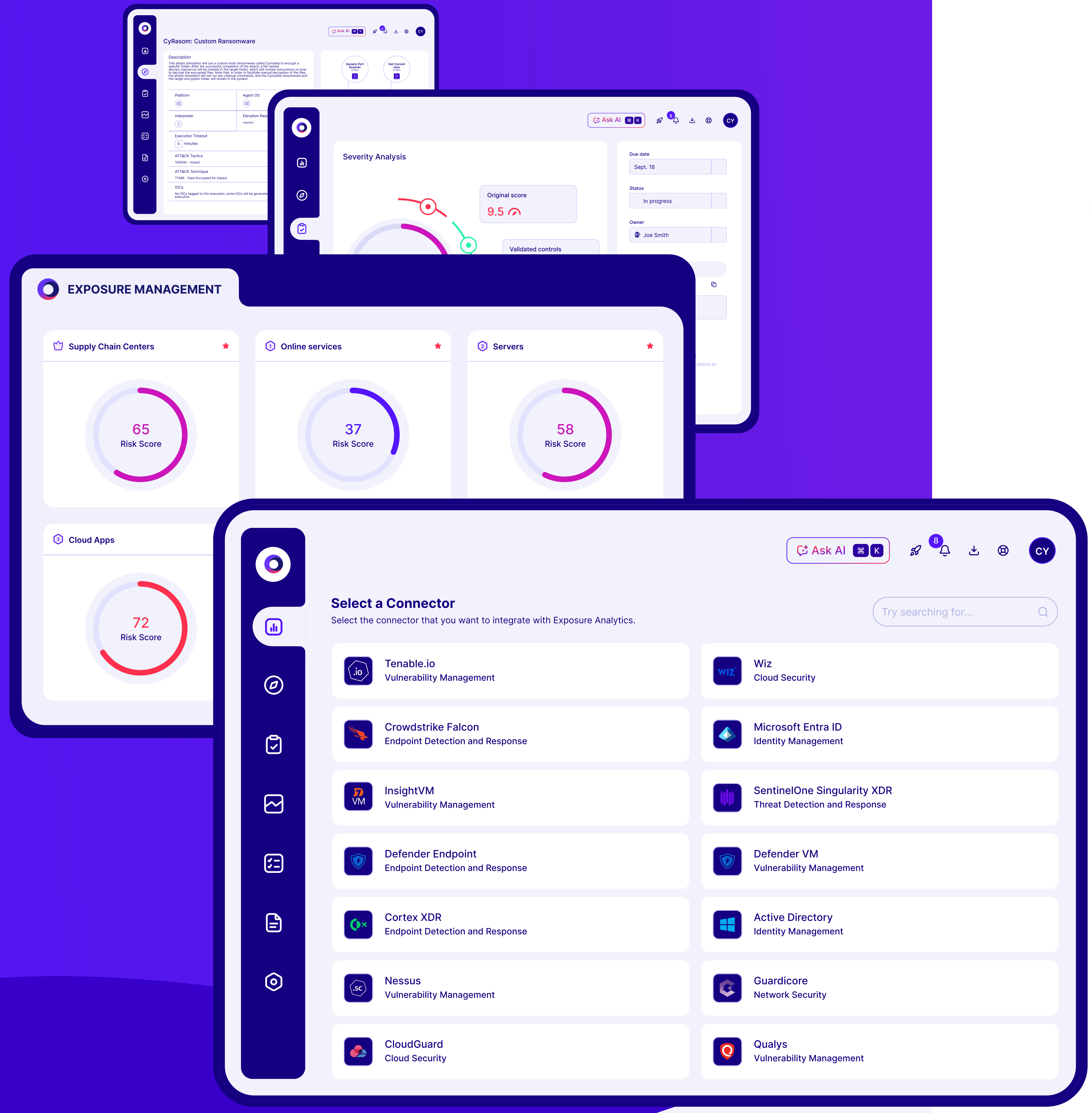
A unified view of exposure management demands a unified view of validated exposure. Anything less won't cut it.

Any security vendor that can discover a CVE or misconfiguration can (and will) call themselves an exposure management solution. However, native discovery, nor a list of findings, can qualify a solution as CTEM.

The real purpose of CTEM is to break down siloes and align teams on security gaps with the biggest potential impact. Some solutions may highlight a single area of concern (such as cloud, application, network, identity, data) but CTEM brings all these security posture management concepts together.

02 Native Validation and Proof of Exploitation Capabilities

Exposure management demands more than just discovery. You need to consider the view of the attacker to know what can be reached and exploited. Validation is thus essential in creating a new, proactive culture around securing your environment. Migrating away from the find-fix process inherent in vulnerability management-only strategies is critical.



Select a Connector

Select the connector that you want to integrate with Exposure Analytics.

Try searching for...

Tenable.io
Vulnerability Management

Wiz
Cloud Security

Crowdstrike Falcon
Endpoint Detection and Response

Microsoft Entra ID
Identity Management

InsightVM
Vulnerability Management

SentinelOne Singularity XDR
Threat Detection and Response

Defender Endpoint
Endpoint Detection and Response

Defender VM
Vulnerability Management

Cortex XDR
Endpoint Detection and Response

Active Directory
Identity Management

Nessus
Vulnerability Management

Guardicore
Network Security

CloudGuard
Cloud Security

Qualys
Vulnerability Management

03 A Unified Platform Experience

To truly adopt the full-scope strategy around exposure management, multiple points in the CTEM lifecycle (scope, discover, prioritize, validate, mobilize) must be addressed by the same solution. This requires a platform approach.

Prioritizing what matters, validating with real threats, mobilizing with confidence and making the process continuous should be where you're focusing your resources. Any offering that only offers part of this picture is a point solution and may not represent your best option to keep your organizational exposure and risk minimized.

What to Seek in an Exposure Management Platform

If you spread your CTEM efforts around a few different solutions, you're not only leaving yourself open to gaps but you're also not getting the most out of your budget.

Here's what you should seek when considering spending on exposure management:

Consolidated view of exposure.

Integrate exposure discovery results with a single view of weaknesses and assets at risk.

Continuous, automated threat exposure validation.

Prove your resilience to threats with validation of current defenses. Your solution should allow you to understand the impact and blast radius of each threat. You should be able to answer: "If an exposure is exploited, what systems are at risk?"

It should also afford you the chance to optimize controls and take immediate action to build resilience through prevention and detection. Prioritize validated risks and exposures. Not all exposures require the same level of attention. A solution should allow you to focus urgent remediation where it's needed by filtering out the exposures where you have effective prevention and detection.

An exposure management solution should stack rank exposures based on:

- Proven threat prevention and detection for the exposure exploited
- Threat intelligence and what it means for your organization (i.e. "Is there a known exploit? Has it been used on active threats? Is it a current threat?")
- Asset information and business context of effected assets

Business alignment and performance metrics.

Ensure your platform provides data-driven risk evaluation to justify security investments and articulate impact to leadership. Measure the state of threat resilience with trending to demonstrate performance trends.

Decision-Making Checklist

As a buyer, refer to this actionable checklist so you can evaluate solutions and select what works best for you.

Category	What to Look For
☑ ***Comprehensive Asset Visibility***	Vendor agnostic approach to discover and aggregate cloud, endpoints, IoT, hybrid environments
☑ ***Attack Simulation + Exposure Analysis***	Combines offensive testing with asset data to validate controls and exposures
☑ ***Mitigation options***	Provides actionable and automated options to mitigate the exposure with control optimization – improved prevention and detection
☑ ***Context + Exploitability***	Go beyond static scores and prioritize based on real exploitation likelihood
☑ ***Ease of Use + Deployment***	Lightweight agents, cloud-native, fast onboarding, access to training, low maintenance
☑ ***Integration + Workflow Support***	Works with SIEM, SOAR, ticketing, enables collaboration + automation
☑ ***Business-Aligned Reporting***	Presents actionable risk metrics and evidence to both technical teams + executives
☑ ***Continuous Validation Loop***	Supports ongoing simulation, control testing and posture tracking beyond infrequent scans

5 Key Steps for Implementing Unified Exposure Management

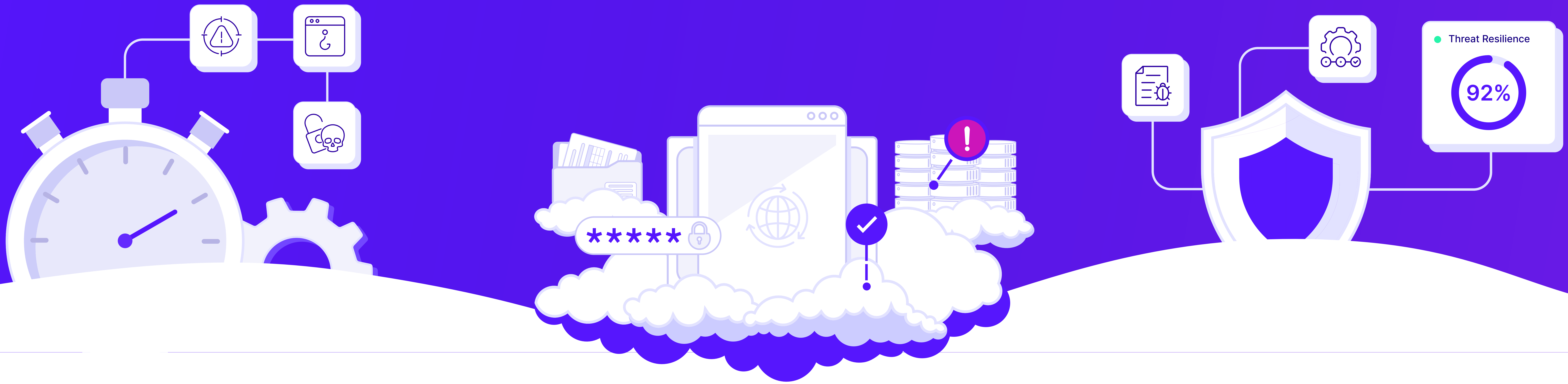
Spending the money on your unified exposure management platform is just the beginning. Once you've made your selection, getting the most out of your investment is your next important mission. Follow these key steps to ensure you've implemented your new platform correctly:

01 Know your attack surface

Map all assets, including on-prem, cloud, remote endpoints, shadow IT, APIs and more. Utilize automated discovery, continuous mapping and asset criticality tagging for the use functionality of existing platforms and choosing the best of breed for gaps in discovery.

02 Expose risk in context

Emphasize on whether the platform can evaluate real risk, not just vulnerability counts. Look for contextual layering with threat intelligence, asset value and exploitability. The platform should offer help via attack simulations mapped to your actual infrastructure so you can address actual exposures instead of theoretical ones.



03 Prioritize what matters most

Focus remediation efforts on exposures for critical assets or business impact. Tie exposures to active threat relevance and business asset risk.

04 Remediate with validation

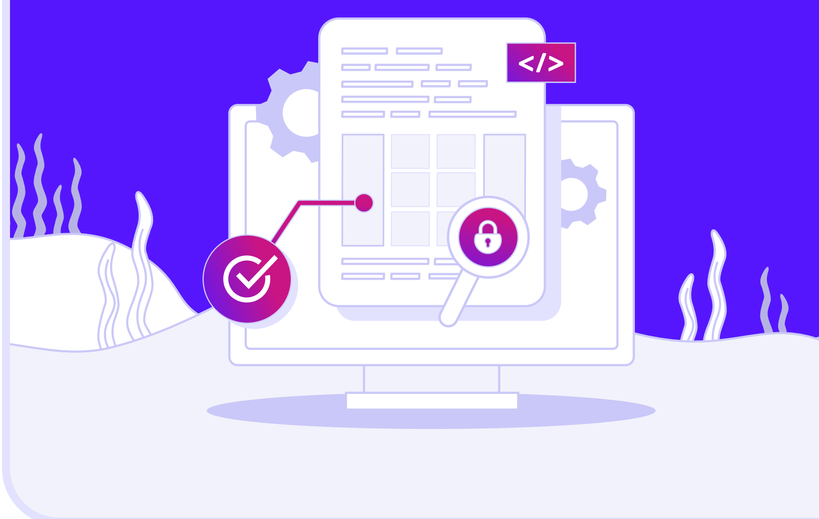
Ensure remediation efforts work by performing re-tests, tracking controls and monitoring status. Continuously simulate attacks to confirm fixes are effective and defenses are hardened.

05 Continuously monitor and improve

Exposure is dynamic. Build routines and processes to monitor new threats, re-validate controls and track posture improvements over time.

Research, Test and Evaluate. Buy with Confidence.

Smart unified exposure management means seeing your environment clearly, testing defenses continuously and prioritizing what counts.



Sign up for a demo of the Cymulate Exposure Management Platform

Start Your Live Demo

Don’t just buy exposure management. Invest in resilience and smarter security posture. Set up a pilot or demo of the platform you’re considering, run your own tests, build a C-suite friendly dashboard and you’re well on your way to buying with confidence.

Cymulate is here to help. By integrating with exposure discovery tools, Cymulate Exposure Management brings together exposure assessment and validation to focus security teams on what’s truly exploitable and improve their threat resilience.

By putting threat resilience at the heart of your CTEM strategy, you can:

- **Integrate** into existing security stack to collect assets and exposure
- **Identify** testable exposures by exploitation techniques and APT groups
- **Analyze** the risk factors influencing the severity including security control effectiveness, business context and threat intelligence
- **Score** exposures based on contextual data
- **Prioritize** by focusing on your most critical exposures

About Cymulate

Cymulate is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to prove, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. Cymulate integrates with assessment tools and continuously tests defenses against the full kill chain of attack techniques providing cybersecurity teams with the automation and insights to prove and optimize threat resilience; accelerate detection engineering; drive continuous threat exposure management; and measure and baseline security posture. Prove the threat. Improve resilience. For more information, visit www.cymulate.com.