carahsoft.

ARMIS®
from ServiceNow

¢2Ǉ мл ¢KǞyƎă ú2 /2yãǞŘŜǊ ² KŜy /K22ăǞyƎ l· /èōŜǊ 9ȄǇ2ădzǊŜ a l·yl·ƎŜYŜyǘ ó/9 a ú к /¢9 a {2fdzǘǞ2Y

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider®** supporting a broad portfolio of industry-leading technologies and a wide range of contract vehicles.

As the **Master Government Aggregator®**, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Armis, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/ArmisResources

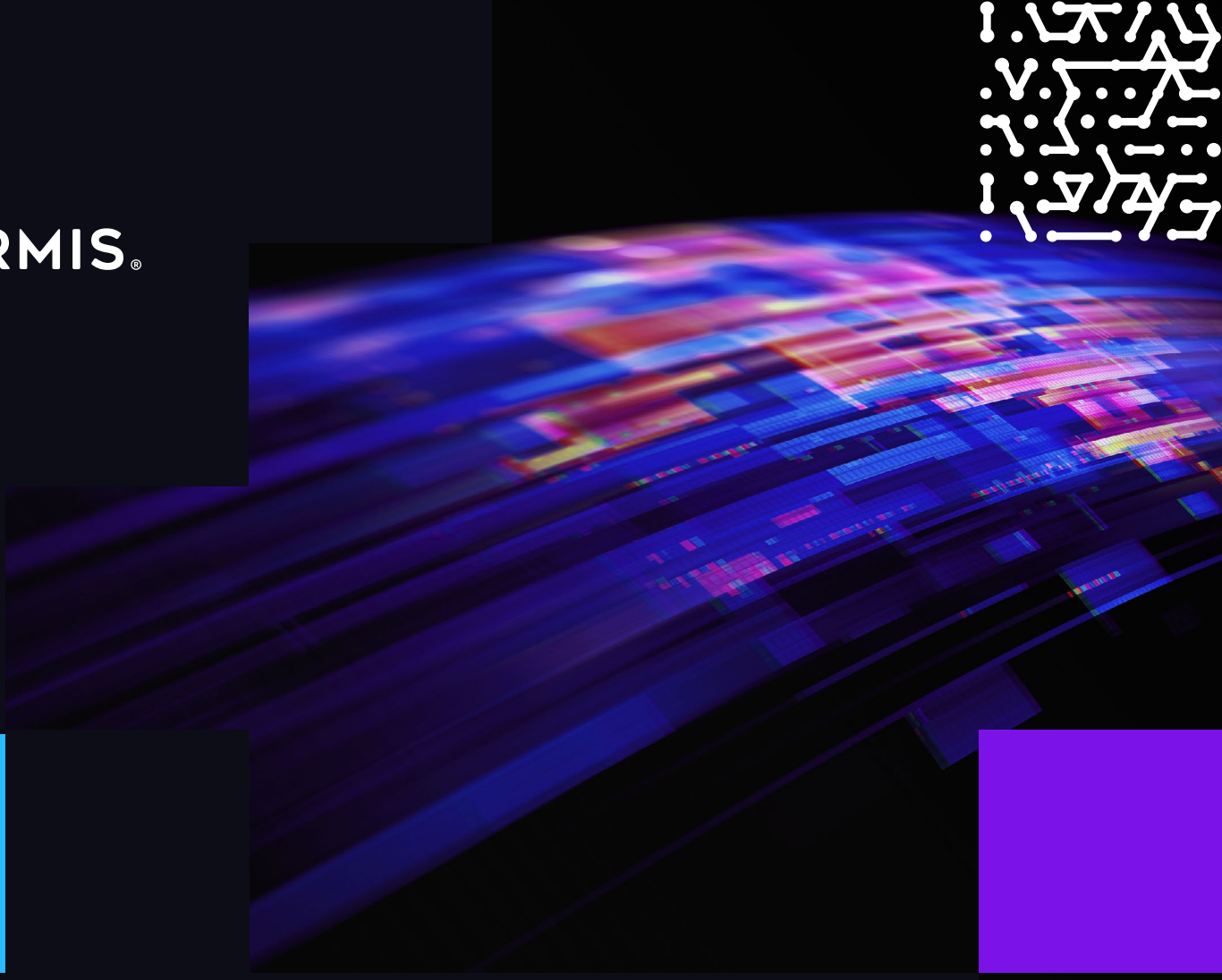
Join Events & Webinars:
carah.io/ArmisEvents

Discover Technology Solutions:
carah.io/ArmisCMMC

Learn About Procurement:
carah.io/ArmisContracts

Connect With Our Team:
Armis@carahsoft.com
888-662-2724

ARMIS®



SOLUTION BRIEF

Top 10 Things to Consider When Choosing a Cyber Exposure Management (CEM) / CTEM Solution

© Copyright Armis 2025

Executive Summary

As security practitioners, we know one thing for certain: cyber risk is no longer something we track in spreadsheets or manage with once-a-quarter scans. It's dynamic. It's real-time. And it's spreading across every connected asset in the organization, from traditional IT to the production floor, the clinic, the cloud, and everything in between.

It's not enough to just have "visibility" anymore. We need context. We need prioritization based on real threats. And most of all, we need actionability, because identifying exposure without a path to remediation just leads to more alert fatigue and risk acceptance.

The Cyber Exposure Management (CEM) and Continuous Threat Exposure Management (CTEM) approach is gaining momentum because it delivers a proactive, continuous way to understand where risk lives in an environment, how it can be exploited, and what to do about it.

But not all platforms that claim to offer CTEM or exposure management are built for today's enterprise, and definitely not for tomorrow's threat landscape.

At Armis, we work with some of the largest and most complex organizations in the world to protect every connected asset and close security gaps before they become headlines. This brief outlines the top 10 things we believe every organization must consider when selecting a CEM/CTEM solution.

© Copyright Armis 2025

1. Complete Asset Visibility Across the Entire Environment

Security starts with knowing what you have. In most environments, that's easier said than done. Shadow IT, BYOD, legacy devices, rogue access points, third-party systems are all part of the attack surface.

A CTEM platform should give you real-time visibility into every connected device and asset; even those you can't install agents on. That includes IT & OT systems, IoT sensors, unmanaged medical equipment, logical environments and cloud-based workloads. Without full visibility, you're flying blind.

Key requirement: Real-time discovery of every asset, with deep detail on device type, location, function, and status.

2. Business Contextualization of Assets and Risks

Not all vulnerabilities matter equally. A missing patch on a dormant laptop isn't the same as a known exploit on a device controlling a chemical process. Yet too many tools treat them the same.

We recommend a solution that ties asset data to business function and operational criticality. Whether it's a patient monitoring system or a robotic arm on the assembly line, you need to understand what the asset does, what it touches, and what happens if it goes down.

Key requirement: Real-time discovery of every asset, with deep detail on device type, location, function, and status.

© Copyright Armis 2025

3. Real-Time Threat Intelligence and Exploitability Correlation

A long list of CVEs doesn't help unless you know which ones are being exploited, and more specifically, what is relevant to your environment.

Your CTEM solution should correlate live threat intelligence with your asset inventory to surface which threats are active, which are targeting your industry, and where those exposures exist in your environment.

Key requirement: Built-in, continuously updated threat intel mapped directly to your environment and prioritized by exploitability.

4. Continuous, Risk-Based Vulnerability Prioritization

Vulnerability management can't be about finding everything. It has to be about fixing what matters. And that requires intelligent prioritization.

You need a system that uses machine learning, behavioral analysis, and threat telemetry to prioritize where to act first. Prioritization should be based not just on CVSS scores, but also asset criticality, exploitability, network exposure, and business impact.

Key requirement: Real-world risk scoring that evolves with your environment and shows you which issues need fixing now, and which can wait.

© Copyright Armis 2025

5. Contextualization and Use of AI to Preempt Attacks

It's not enough to react to what's happening now. You need to understand how attackers might move through your environment next. That's where AI and predictive modeling become game-changers.

A modern CTEM platform should apply AI to contextually assess your environment and identify likely attack paths, provide early warning capabilities, detect anomalies, and flag combinations of risk that could lead to a breach.

Key requirement: AI-powered exposure analysis that can simulate attack paths, provide early warnings of threats, predict lateral movement, and preemptively surface combinations of risk.

6. Support for Specialized Environments

Most exposure management tools were built for IT, and break down when applied to specialized environments. If you operate in manufacturing, healthcare, energy, logistics, or smart buildings, your attack surface is filled with non-traditional, often unmanaged systems.

You need a platform that understands industrial, medical and even proprietary protocols, doesn't require agents, can detect dormant assets, and protects safety-critical assets while maintaining operational resiliency.

Key requirement: Purpose-built CTEM/CEM that acts as part of the "domain expert team", for highly specialized systems.

© Copyright Armis 2025

7. Automated Exposure Remediation Workflows

Once you've identified exposure, the next step must be remediation; and doing that manually across thousands of assets and multiple teams just doesn't scale.

Look for a platform that integrates with your ticketing systems (like ServiceNow), patching tools, and firewalls and compensating controls, so you can automate response based on asset risk and policy.

Key requirement: Integration with CMMS, ITSM and remediation tools to automatically open, assign, and track (with evidence) resolution of high-risk issues.

8. Attack Path and Blast Radius Analysis

You can't assess risk in isolation. It's about understanding how an attacker could pivot from one exposed system to another, and what the downstream impact could be.

Your CEM/CTEM solution should visualize the attack chain, simulate lateral movement, and highlight the "blast radius" of a compromised device so you can prioritize controls that break the lateral progression of an attack.

Key requirement: Attack path simulation and blast radius visualization across hybrid environments.

© Copyright Armis 2025

9. Integration with Security and IT Ecosystems

Your CEM/CTEM solution must plug into the tech stack you already use. Whether it's your SIEM, SOAR, EDR, or identity systems, you need exposure data to collaborate with eachother and be actionable across platforms.

Look for open APIs, prebuilt integrations, and connectors that make it easy to share context, enrich telemetry, and accelerate triage.

Key requirement: Deep integration with security stack; not another silo.

10. Scalability, Speed, and SimplicityAnalysis

The best tool is the one your team can actually use. A CEM/CTEM platform needs to deploy quickly, scale effortlessly, and deliver insights without a PhD in threat modeling.

That means deployment methodologies that offer you the freedom to choose on-premises or SaaS, intuitive dashboards, templates and automated updates that don't require constant tuning or human intervention.

Key requirement: Cloud-native, enterprise-grade platform that scales globally and delivers value in days, not months.

© Copyright Armis 2025

Checklist: Top 10 Considerations for a CEM/CTEM Solution

01 Complete asset visibility across all environments

02 Business context mapping and operational impact awareness

03 Real-time threat intelligence tied to active vulnerabilities

04 Continuous, risk-based vulnerability prioritization

05 Contextualization and AI-driven preemptive attack modeling

06 Native support for specialized systems

07 Automated remediation workflows and ITSM integration

08 Attack path and blast radius analysis

09 Integration with security, IT, and cloud ecosystems

10 Cloud-native delivery with speed, scale, and simplicity

© Copyright Armis 2025

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo