Solution Overview

Cyber Asset Attack Surface Management (CAASM)

Know what's protected with Teneo's Cyber Asset Attack Surface Management (CAASM), powered by ThreatAware.

TENEO
OPENING MINDS

What is Cyber Asset Attack Surface Management (CAASM)?

Many organizations invest heavily in cybersecurity tools, yet still struggle to answer a simple question: Are we truly protected?

Teneo's Cyber Asset Attack Surface Management (CAASM) solution, powered by ThreatAware, helps organizations gain a trusted view of assets, security controls, and coverage across their environment. By connecting to existing security, IT, and cloud platforms, CAASM creates a single source of truth that helps identify gaps, validate controls, and highlight where protection may be missing.

Why It Matters

Security teams rely on a growing number of cybersecurity tools, yet disconnected systems, inconsistent data, and unknown assets continue to create blind spots across the attack surface. This makes it difficult to understand what's protected and where gaps exist.

Without clear visibility, risks can go unnoticed and security investments may not deliver the protection expected. Organizations can struggle to identify gaps, validate controls, and take action with confidence.

Common Challenges When Validating Security Controls:

Fragmented Visibility

No single, reliable source of truth across your attack surface, creating blind spots and gaps in protection.

Tool Sprawl

Too many disconnected tools increase complexity and make it harder to maintain consistent coverage.

Unknown Assets

Unmanaged and undiscovered devices create hidden gaps in coverage and increase exposure.

Untrusted Data

Inconsistent and conflicting data makes it difficult to identify gaps, maintain compliance, and act with confidence.

Control Gaps

No clear way to confirm that security controls are deployed and working as intended.

Operational Overhead

Significant time spent manually pulling data from multiple tools increases effort and slows response.

Without a trusted view of assets and security controls, organizations lack the clarity needed to identify gaps, reduce risk, and strengthen their security posture.

How Teneo Helps

Reducing risk across your attack surface is not about adding more tools; it's about gaining clarity, validating what's working, and ensuring your existing controls are protecting the assets they should, consistently and at scale.

With Teneo's CAASM solution, security teams can:

- Gain a full and accurate view of all assets, with no blind spots
- Detect missing or misconfigured controls before they can be exploited
- Ensure security controls are deployed, operational, and protecting the right assets
- Focus effort where it matters most, using accurate and trusted data
- Eliminate time spent reconciling data across multiple tools
- Ensure audit and compliance readiness with accurate, trusted asset data

Over time, this approach helps organizations gain confidence in what's protected, reduce exposure, and maximize the value of existing security investments.

Powered by ThreatAware.
Integrated Into Your Existing Ecosystem.

Teneo's Cyber Asset Attack Surface Management (CAASM) solution is powered by ThreatAware and integrates with your existing security and IT ecosystem.

By connecting to tools such as Microsoft Defender, CrowdStrike, ServiceNow, and AWS, the platform brings data together into a single, accurate view, helping teams identify gaps, validate controls, and reduce risk faster.

Key Platform Capabilities Include

- **Agentless API Integration:** Connect security and IT tools quickly without complex deployment or additional agents.
- **Accurate Asset Discovery:** Continuously identify known, unknown, and unmanaged devices across your environment.
- **Data Correlation and Normalization:** Bring together data from multiple tools to create a single, accurate, and trusted view.
- **Security Control Validation:** Confirm controls are deployed, operational, and protecting the assets they should.
- **Gap Identification and Coverage Analysis:** Identify missing controls, misconfigurations, and areas of increased exposure.
- **Real-Time Monitoring and Insight:** Maintain up-to-date visibility into asset health, control status, and coverage.

Ready to Get Started?

Whether you're looking to identify unknown assets, validate security coverage, improve compliance readiness, or strengthen cyber resilience, Teneo can help. **Book a demo today.**

StreamlineX

Cyber Asset Attack Surface Management (CAASM) is a cornerstone of StreamlineX. By centralizing visibility across assets, security controls, and coverage, it helps organizations identify gaps, validate protections, reduce risk, and maximize the value of existing security investments. This enables security teams to gain confidence in what's protected while strengthening cyber resilience and reducing operational complexity.

Learn more about StreamlineX

Purpose Beyond Profit

In working with Teneo, you are helping to improve the lives of a million children around the world. **Learn more**

About Teneo

Most Network and Security teams are overworked so making progress is a challenge. We securely connect users to their applications by combining leading technology with expert guidance. You stay in control, simplify your operations and keep ahead of the game.

Find out more at www.teneo.net.

UK
Teneo Ltd
20/21 Theale Lakes
Business Park
Moulden Way, Sulhamstead
RG7 4GB

T: +44 118 983 8600
F: +44 118 983 8633

France
Teneo France S.A.S.
43 47, Avenue de la Grande
Armée 75116
Paris
France

T: +33 1 55 51 30 38

USA
Teneo Inc.
44679 Endicott Drive,
Suite #355,
Ashburn,
VA 20147

T: +1 703 212 3220
F: +1 703 996 1118

Australia
Teneo Australia Pty Ltd
Level 11, 64 York Street
Sydney
NSW 2000

T: +61 2 8038 5021
F: +61 2 9012 0683