SYNERCOMM

Continuous Attack Surface Management - CASM®

Continuous Attack Surface Management is the new Managed Vulnerability Scanning

Let's face it, every security team, audit department, and IT group could use a little extra help. Project loads continue to increase, fires need to be put out, vulnerabilities and attack methods keep changing, and too often the most basic processes fail first. CASM® takes the guesswork out of security by automating asset discovery and monitoring while still assessing risk with expert analysts.

Out with the old...

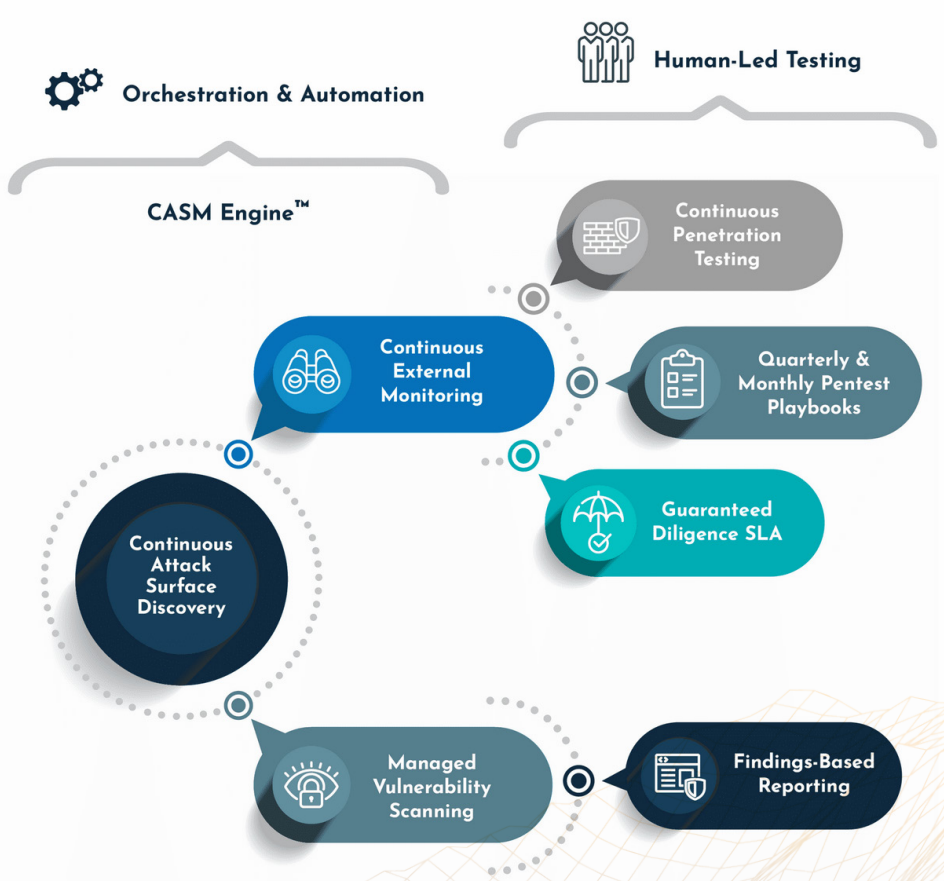
Shortly after the first vulnerability scanner was created, managed vulnerability scanning services quickly followed. The concept was simple, organizations hire a managed security services provider (MSSP) to scan their IP ranges and report all potential vulnerabilities. 20 years later, these basic services remain largely unchanged, and their value is long gone.

In with the new...

Vulnerability scanning is critically important, but it must be done right. The rate of change has never been higher, and your security partner must keep up. Gartner® defines External Attack Surface Management as delivering monitoring, asset discovery, analysis, prioritization of risks and vulnerabilities, and remediation. CASM® checks all these boxes and adds continuous coverage through automation.

How it Works

- Continuous monitoring of external assets
- Automatic discovery of new public-facing systems
- Discovery of shadow IT and under-managed systems
- Provides an inventory of public systems and services
- Vulnerability scanning of your entire external attack surface
- Continuous monitoring of DNS, SSL, and email-based risks
- Continuous monitoring of online reputational risks
- Validated findings: no false positives



Take it to the next level with Continuous Penetration Testing!

With CASM, you benefit from having a team of expert penetration testers (ethical hackers) continually building and improving new tools for scanning and assessing systems. This same reputable team helps design and build our CASM Engine scanners, and they help analyze the data produced by our monitors. Along with a baseline penetration test, CASM monitoring is at the core of SynerComm's Continuous Penetration Testing subscriptions. When you require deeper testing and additional validation, SynerComm leads in both point-in-time and continuous penetration testing. Our tool stands out compared to managed vulnerability scanning because it automatically discovers and monitors dynamic cloud assets, reducing the burden of upkeep on IT teams.

Organizations that benefit most:

Find accidental exposures (aka "I thought that we shut down these old instances")

Find high risk exposures (aka "That shouldn't be public facing")

Full external inventory of assets, risks, and confirmed vulnerabilities (findings)

Quickly validate changes and remediation efforts

Hands on or hands off, your choice: actively use the dashboard throughout your daily risk management activities or only be notified when risk changes.

Change alerts: stay ahead of attackers with fast detection of changes in your attack surface

Hosting breakdown: see a complete breakdown of where your assets are hosted, across all providers

Partner with SynerComm to test the security of your internet exposed assets year-round.

SYNERCOMM