censys

The External Attack Surface Management Vendor Evaluation Checklist

Expand Your Tech Stack with Confidence

Introduction

As cyber attacks become more sophisticated, so too should the tools we use to prevent them.

External Attack Surface Management (EASM) has emerged as one such tool, becoming a critical part of the modern security tech stack. That's because, with an EASM solution, security teams can continuously detect and monitor exposures across their entire attack surface, and gain the visibility and scalability they need to stay ahead of advanced threats.

Of course, as with any tech, not all EASM solutions are created equal, which is why organizations ready to invest in EASM need to find a solution that's truly best-in-class, built on a foundation of superior data with the capabilities to meet all required use cases. And a proven track record of experience? That's a must, too.

As you set out on your search for an EASM solution, consider this evaluation checklist. Use it to guide your conversations with vendors, compare solutions to each other, and narrow down your selection.

General Qualifications

Does the vendor meet table stakes expectations for functionality and service? A miss here is your sign to keep searching.

My external-facing assets, both known and unknown, including hosts, services, websites, and certificates, are discovered in near real-time	
I don't have to pay additional fees for more frequent scanning	
The vendor is an established solutions provider that serves enterprise customers across industries	
A named Customer Success Manager and dedicated support with SLAs are provided	

Data Depth and Accuracy

What kind of data will inform your understanding of assets on your attack surface? An EASM solution is only as good as the internet intelligence behind it. Look for a solution powered with accurate, comprehensive, and up-to-date data to ensure that your team can base decisions around a reliable source of truth.

A multi-perspective scanning engine from 7 Tier-1 ISPs across 3 continents is used	
Daily comprehensive scans of the top 100+ ports are conducted	
Extensive scanning is conducted on IPv4, IPv6, and name-based hosts	
Research-backed Predictive Scanning provides intelligent targeting of all running services	
Superior coverage of 65K ports (standard and non-standard) is provided	
Automatic protocol detection provides intelligent protocol awareness regardless of port assignment	
Vulnerable cloud storage buckets are detected	

Asset Details

How much are you able to learn about assets and exposures on your attack surface? The right context is key to not only remediating existing exposures, but preventing similar security gaps in the future. Look for a solution that can provide details about asset relationships, ownership, and history.

Attribution trails show how an asset was discovered (ex: specific DNS lookups are available)	
SSH, RDP, and end-of-life software can be investigated with intuitive queries	
Protocols on non-standard ports can be identified	
I can easily understand where my assets are hosted and see ownership information	
Device type labels clearly identify host type (i.e. IoT, Database, VPN, etc.)	
I can search thousands of indexed fields and see detailed information about service configuration and vulnerability	
I can easily add and exclude assets from the solution’s attack surface monitoring without contacting the vendor	

Dashboards and Reports

Robust data is great, but only if you can make sense of it. How will a solution organize information about your attack surface for you? You should be able to acquire concise, actionable insights from user-friendly dashboards and reports.

Raw attack surface telemetry is aggregated in an easy-to-understand dashboard that includes trends and a view of my attack surface at-a-glance	
Assets with geolocation data can be mapped by country	
Hosts with critical risks and CVE priority can be identified by category or severity	
I can identify the discovery source of my assets	
I can view dashboards that identify trends of risks and hosts count	
I can view reports on hosts and ports to determine total attack surface	
It's easy to identify expired certificates, including those that are currently expired or those that will expire in the coming week or month	
Queries can be used to segment the attack surface	
Reports on attack surface activity can be generated quickly for executive review and compliance needs	

Operationalization and Integrations

Will the solution play nice with other security tools in your tech stack? You should be able to leverage attack surface data throughout your entire security ecosystem with native integrations and API endpoints.

No deployment or configuration is required to onboard the solution	
My authentication provider is supported by the solution	
A full-featured API allows programmatic access and integration	
I can integrate with my existing SIEM tools, with all necessary workflows supported	
I can manage my attack surface in the cloud with cloud connectors for the Big 3 Cloud Providers (Google, AWS, MSFT Azure)	
I can create distinct workspaces to support subsidiaries, mergers and acquisitions	
I can integrate with ticketing tools and easily assign out tickets to my IT team	
RBAC for different workspaces and users is supported	

Risk Triage and Prioritization

Will your team be able to quickly understand and remediate risks that are truly critical? What kind of support is offered during a zero-day? The last thing you want is time wasted on false positives or cloudy insights.

I'm notified about the most relevant and critical risks on my attack surface	
The severity of discovered weaknesses and exposures can be determined with 300+ different risk fingerprints	
Precise context about discovered risks is provided, along with recommendations for remediation	
99%+ CVE visibility can be gained using scans	
I can prioritize different risks in the solution based on my organization's policies	
Removing assets can be done on a single asset or recursively	
During a zero-day, the vendor's rapid response team communicates within 24 hours with recommendations for remediation	
Zero-day risks are quickly built into the solution and re-scans can provide immediate validation that remediation efforts are working	

Next Steps

Investing in any new cybersecurity solution can be a big decision, but when you know what to look for, it's one you make with confidence. To learn more about the specifics of a best-in-class External Attack Surface Management solution, reach out to our team at www.censys.com/contact/.

ABOUT CENSYS

Censys is the leading Internet Intelligence Platform for Threat Hunting and Exposure Management. We provide governments, enterprises, and researchers with the most comprehensive, accurate, and up-to-date map of the internet to defend attack surfaces and hunt for threats. Censys scans 63% more services than the nearest competitor across the world's largest certificate database (>10B), reducing the likelihood of a breach by 50%.

Founded by the creators of ZMap, trusted by the U.S. Government and over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the Internet.

censys

WEBSITE
www.censys.com

E-MAIL
hello@censys.com