DATASHEET

NSFOCUS

External Attack Surface Management (EASM)

IDENTIFIES HOW EXPOSED YOU ARE

KEY BENEFITS

IT asset VISIBILITY

Emergency Vulnerability Announcement

Vulnerability Analysis

Prioritization and Remediation

USE CASES

EASM IDENTIFIES HOW EXPOSED YOU ARE

The NSFOCUS External Attack Surface Management (EASM) can be run once or as a subscription service with various levels of monitoring SLAs to meet requirements from organizations with the smallest internet footprint to multi-national businesses that own IP ranges all over the world.

VULNERAVILITY SCANNING AND MANAGEMENT

Customer could perform vulnerability scanning and manage risks by NSFOCUS prioritization and remediation algorithm.

ADVANCED PENETRATION TESTING

NSFOCUS expert are available for conducting penetration testing on customer assets to discovery vulnerabilities in depth.

OVERVIEW

Almost every organization today has some kind of connection to the internet. Whether it is to host multiple ecommerce sites or just have email access, internet connectivity is a necessity for doing business. But being on the internet is not without risk. Worse, most organizations do not know how big their risk is.

What is the level of exposure on the internet? Even with a managed network firewall, it can be difficult to know what IP addresses, ports, or services an organization has available on the internet. Is there a rogue server internally hosting a warez FTP site? What prevents a business unit from installing their own link to the internet, bypassing the corporate firewall. What is the effect of mobile devices and PnP services within the organization? Most organizations don't know because they cannot see themselves from the outside.

External Attack Surface Management (EASM) is an emerging market category that Gartner created in March 2021 to describe a set of products that supports organizations in identifying risks coming from internet-facing assets and systems that they may be unaware of.

IT ASSET VISIBILITY

NSFOCUS EASM continuously discovers your internet-exposed attack surface, find potential risk. Platform shows the change of your internet-exposed attack surface, send alert email when high risk vulnerability detected.

EMERGENCY VULNERABILITY ANNOUNCEMENT

NSFOCUS update critical and emergent vulnerability information in hours, which including vulnerability description, affected software & version and remediation plan will be automatically sent to customer via email. Relevant scanning could arrange accordingly.

VULNERABILITY ANALYSIS

NSFOCUS EASM provides periodical and on-demand vulnerability scanning, finding misconfigured assets; network architecture flaws; data exposures, authentication and encryption weaknesses; or other risks including common vulnerabilities and exposures (CVEs). The advanced penetration testing is also available to perform on customer assets.

PRIORITIZATION AND REMEDIATION

NSFOCUS EASM platform prioritize risks and vulnerabilities and provide alerts based on prioritization analytics. Prioritizing risks in the external attack surface makes it possible to know where to focus first. Based on prioritized risks, customer could create remediation plan and arrange resting on platform.

NSFOCUS SAAS Platform

Powered by NSFOCUS SAAS Platform-ADBOS, NSFOCUS External Attack Surface Management service help you identify how you are exposed to Internet and understand your attack surface better than hacker. You can leverage the unified platform to visualize your assets, get the security status, and understand where to start based on the vulnerability prioritization results.

WHY NSFOCUS

Gartner Recognized Sample Vendor in EASM Category

NSFOCUS External Attack Surface Management service has been recognized by the International Consulting Agency Gartner and we are named as a sample vendor in in Gartner® Research 'Competitive Landscape: External Attack Surface Management.

Strong Attack and Defense Capabilities

- 8 Security Research Labs: **200+** security experts specializing in cloud computing security, IOT, Internet of Vehicles, Industrial Internet, AI-based intelligence defense, big data, offensive and defensive.
- 4 Attack and Defense Teams: specialize in attack and defense practices (Capture the Flag, cyber drills). The experience is accumulated and leveraged in our VAPT testing process.
- Comprehensive Security Qualifications: CCIE, Security+, CISSP, OSCP, CREST, CISM, CISA, Pentest+, PMP, ITIL, COBIT5.
- CERT Team: a dedicated group of experts who handle computer security incidents for customers worldwide 24/7.

Strong Vulnerability Mining Capabilities

- Over the years, NSFOCUS has dug out 230+ high-risk CVE vulnerabilities on popular IT products from Microsoft, Adobe, Google, Sun, Cisco, HP, IBM, etc.
- Awarded by Microsoft Bug Bounty Program for 7 consecutive years.
- Awarded by Mitigation Bypass Bounty program for 6 consecutive years