What is Attack Surface Management (ASM)?

In this article, you will learn more about Attack Surface Management (ASM) and how it can be used to enhance the security of your network.

The many benefits of leveraging the Internet in business have prompted more organizations to establish an online presence. This creates more digital footprints online, leaving any business owner vulnerable to cyberattacks.

Interestingly, being hacked is not entirely the attacker's fault. As a network owner, if you fail to secure your system, you will suffer consequences in the event of an attack.

In this article, you will learn more about Attack Surface Management (ASM) and how it can be used to enhance the security of your network.

What is Attack Surface Management?

Attack Surface Management is the process of monitoring, evaluating, and securing network components, in order to protect against cyber attacks.

It is the process of performing a security task from an attacker's perspective to prevent any possible attacks in the future. This makes Attack Surface Management a primary concern of any security chief, chief technology officer, or any other cybersecurity officer.

There are two types of ASM: Controlling attacks from outside and inside the organization.

1. Control external attacks

Controlling external attacks is the process of managing assets exposed to the Internet by narrowing down any vulnerable entry points. It is done through systematically detecting, classifying and allocating risk scores to all identifiable assets, and then reducing these scores.

2. Control attacks from within the organization

As the name suggests, this is the management of operations on assets that are only accessible from within an organization. In most cases, this control takes place not online, but inside the company.

ASM tools

Several tools make it easy to implement ASM effectively. These tools expose potential blind spots and processes that allow attackers to evade tough defenses to protect the network.

Some of the popular tools on the market include Sandbox Attack Surface Analysis Tools from Google, Rapid7 InsightVM, UpGuard BreachSigh, OWASP Attack Surface Detector and CoalFire Attack Surface Management, among many others.

Why is Attack Surface Management important?

According to one report, about 27% of malware occurrences are related to ransomware. Ransomware attacks typically target small and large businesses every 11 seconds. Continuous attacks on businesses are the fundamental reason every company should take cybersecurity seriously.

Let's take a look at some of the reasons why Attack Surface Management is important.

1. Misconfiguration detected

Attack Surface Management helps detect misconfigurations in firewall, operating system or website settings. It is also useful in detecting ransomware, viruses, weak passwords, outdated software, and vulnerable hardware.

2. Protect sensitive data and intellectual property rights

With Attack Surface Management, it's easier to secure sensitive data and intellectual property. Instead of breaking into your system freely to access such confidential information, attackers will encounter strong resistance.

When properly implemented, Attack Surface Management also helps to reduce risk, since IT assets are hidden. Just as intrusion detection systems pick up on malicious signals around your network, it alerts and removes unauthorized access.