INTRODUCTION

Any physical or digital interface that a hacker could use to try to input their own data or use as an attack vector to gain unauthorised access to a system and extract data or other sensitive information is referred to as an attack surface.

Application-level external attack surface management (EASM) is the ongoing process of identifying and analysing Internet-facing assets in order to hunt for flaws and irregularities. Your Internet-facing assets are exposed in different locations and to different degrees, which you may learn about by mapping out your attack surface with external attack surface management.

Organizations are becoming more exposed to attacks as a result of increased use of the public cloud and tightly knit supply networks. To decide what steps to take to safeguard the attack surface, individuals on the front lines of cybersecurity must be able to recognise and monitor changes in their external attack surface.

Risks associated with the use of cyber-physical systems and IoT, open-source code, cloud applications, complex digital supply chains, social media and more have brought organizations' exposed surfaces outside of a set of controllable assets.
– Gartner

Depending on how complicated the organisation is, it may be challenging to even identify the assets or access points that make up the attack surface, let alone take remedial action. Assets can be classified as Known & Unknown with each having their own challenges and requirements.

KNOWN ASSETS

The assets you are familiar with and keep a close eye on are known assets. They consist of the numerous subdomains that make up the domain, the security-checking Apache installations, the primary web application, and the login screens.

UNKNOWN ASSETS

There will always be assets that are not known, which makes the attack surface vulnerable. They are frequently the consequence of coding errors, the installation of rogue or shadow IT software, or the outcome of an unsecured supply chain, and they can be more difficult to detect for a developing firm without the proper processes and tools. In other cases, new flaws in existing code are discovered via pure inventiveness on the part of pentesters or ethical hackers who explore in places that others don't.

ATTACK SURFACE TYPES

CLOUD STORAGE

Your instances' server hardware is well-secured by cloud storage providers like Amazon Web Services (AWS) or Azure. Yet, the company is in charge of managing access to the cloud and configuring it securely. Cloud providers are responding to concerns with more security safeguards, yet data in the cloud is still being compromised as a result of incorrect settings.

Nowadays, monitoring for errors and appropriate access management policies may be automated.

WEB VPN

VPNs are used to safely and anonymously transmit data over public networks. They work by masking user IP addresses and encrypting data so it's unreadable by anyone not authorized to receive it. But the Web portals of these VPN are mostly outdated or infested with SSL/TLS vulnerabilities resulting in user info leak or unnecessary exposure.

DNS DOMAINS

User requests are sent to DNS servers for resolution which point traffic to the intended URL. These DNS servers can be hijacked to learn, read and redirect user traffic to malicious destinations. Fredrik N. Almroth shared details of how he ethically hijacked the top-level domain of a sovereign state and temporarily took over 50% of all DNS traffic for the TLD, something that could have easily been exploited by malicious hackers

OUR APPROACH

With our External Attack Surface Management technology, Ignitec provides total coverage of your attack surface, which includes both the breadth and depth of your attack surface.

We have taken the DAST technique and transformed it into the External Attack Surface Management methodology. We've built our EASM platform using the DAST approach as the foundation, making it extremely scalable and offering greater value to clients.

APPLICATION MISCONFIGURATIONS

Permissions set by developers might be too liberal and they might even lose track of Crown Jewels leading to misconfigurations. Misconfigurations can happen easily, and often by accident. Misconfigurations are often caused by the mismanagement of multiple connected resources like Kubernetes, serverless functions and containers.

"95 percent of all security breaches are due to misconfigurations, and those mistakes cost companies nearly $5 trillion in between 2018 and 2019 alone" – Gartner

SURFACE INSPECTION

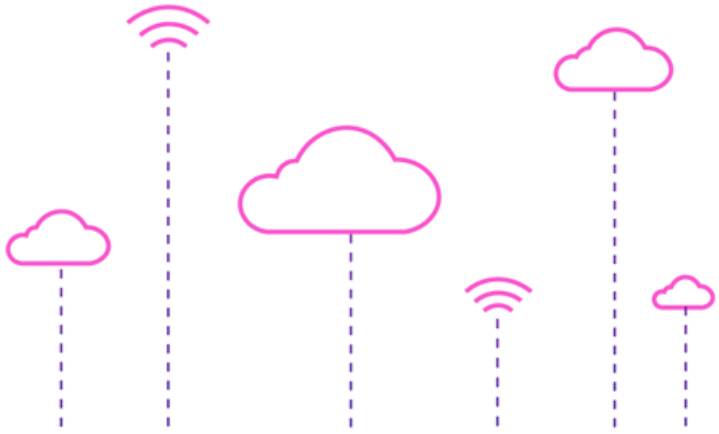
Surface Monitoring provides additional value by uncovering assets you might not even be aware of and by scanning those assets for vulnerabilities three times per day. Surface Monitoring executes continuous checks on the domain level.

APPLICATION SCANNING

Application Scanning, often known as a DAST scanner, goes beyond what a "conventional" DAST scanner can do by using crawling, fuzzing, and authentication to uncover vulnerabilities in assets that are typically inaccessible by stateless testing.

CYBER RANGE

A Hyper-realistic simulation platform comprising of real networks, servers, and storage that mimics every major digital infrastructure and attack scenario. They resemble a specific corporate network nearly exactly, with the exception that they do not receive real-time production traffic. Everything our Red Team tests is done on the duplicate of actual infrastructure that is existing in their business, they are completely free to launch several assault scenarios without being concerned about the potential for damage. They may use this to run rigorous attack scenarios to see how well it defends against actual cyberattacks.



THE FOLLOWING ARE SOME ADVANTAGES OF IGNITEC'S EASM STRATEGY:

- Constant and automated discovery, inventory, and monitoring of all Internet-facing assets.
- Added vital details to assets, such technologies housed on each asset and open ports, DNS record kinds, and so on.
- Payload-based testing has a 99.7% accuracy rate for assessing vulnerabilities.
- Personalized Attack Surface Policies on your attack surface and notifications of changes.
- A special crawler designed for evaluating the security of contemporary online apps.
- A fuzzing engine that discovers new places to look for flaws that affect security or other odd behavior.