An Overview of Attack Surface Management

Businesses are finding themselves in the unviable position of having to deal with rampant cyberthreats while they push their Digital transformation strategies forward and continue to navigate the remote workforce environment.

Improving cyber-resilience can be a daunting task especially for organizations that have resource constraints due to the pandemic. And so having visibility of technology ecosystems, from the perspective of attackers, is essential and organizations of all sizes and cybersecurity maturity need to address this.

> **External Attack Surface Management will become part of a broader vulnerability & threat management push aimed at discovering and managing external-facing assets and potential vulnerabilities.**
> **– Gartner**

Challenges and threats for SMEs

More businesses are digital today than ever before. As a result of that, digital footprints keep increasing, which means that there are significantly more entry points and vulnerabilities for cyber criminals to exploit. It is no surprise then that we hear of new breaches with every news cycle.

In fact, we've seen a fivefold rise in the number of security incidents and breaches in 2020, and $1 trillion was lost to cybercrime during that same year. There are other trends that have exacerbated this issue. Cyber-attacks used to be sophisticated and in the realm of nation states and cybercrime syndicates. But not anymore. They've been democratized so pretty much anyone with a couple of hundred dollars' worth of tools can cause damage.

And these breaches aren't just occurring due to persistency of intent by malicious actors but, interestingly, many of these data leakages are a result of a simple human error. More than half the data leakages that happened last year were the result of simple misconfigurations or human negligence. With regulatory frameworks and data privacy laws coming into play, data breaches have also become more costly than ever, with the average breach in the region costing $6 million (according to IBM).

ASM as a Technology

Historically, organizations used to be in a particular line of business, and they would use IT to support that. With the increase in digitization and online presence, we're seeing that IT is now at the core of many businesses.

And this has created new opportunities for organizations but also a host of challenges and risks that they need to mitigate.

42% of security leaders acknowledge they experienced a breach as a result of shadow IT and a lack of clarity around their attack surface. – SANS

Having to work with rapid development environments, with 3rd parties (vendors, agencies, partners etc) means that your technology ecosystems are expanding in size and frequently changing in nature. So, it has being able to continuously keep track of where these assets might be hosted and the vulnerabilities and threats that they are exposed to has become a very complex proposition.

It's very difficult for organizations to keep track of what and where their assets are. Firstly, because there's been an increased dependence on 3rd parties so much so that you're not even the one operating that asset or service – someone else is operating it on your behalf – but also due to the nature of the frequent changes and the rapid development cycles completed to accommodate customer demands.

How ASM helps tackle these challenges

The more attack surface management becomes mainstream, the harder it is for cyber criminals to find assets to exploit.

Security teams worldwide are stretched thin, and in need of a platform that could provide them with aircover and support. They need to achieve comprehensive visibility with 0 effort or input from their end. This full visibility is very important because it's almost impossible to protect the unknown in the first place.

So, to help uncover the 'unknown unknowns' – assets lacking awareness or ownership, sitting out there on the open Internet and publicly exposed. But also, visibility of where all their assets reside, geographically, as well as by cloud provider, or datacenter.

Once that visibility has been achieved and maintained around the clock, threat assessment can be performed as part of the platform, which runs a host of standardized and non-standardized threat assessments against all the assets that belong to that organization.

With a team of dedicated security researchers that are constantly researching the latest hacking methodologies that malicious actors are using, it's possible to analyze these, reverse engineer them and include them into a Threat Assessment Engine which then allows for the detection of some of these threats that are specific to certain technology stacks. This is where the magic happens, and how blue-chip company data of over 120 million people were protected from exposure.

Again, this problem is no longer centric to large companies but affect any entity that is digital enabled or internet facing. So, the focus is on making Attack Surface Management completely autonomous so even companies with resource constraints can rely on having an external, 24/7 partner to rely on for cybersecurity so they can focus on other areas of their business and security.

> **Of the 4.1B records lost so far this year, 75% involved the misconfiguration or unintended exposure of databases or services.**
> **– Gartner**

Attack Surface Management use cases

The most important one is the comprehensive visibility and there are many examples of where we've alerted global organizations to the existence of certain assets that they weren't even aware existed.

The second use case around 3rd risk. A lot of solutions that manage or report on 3rd risk depend on user and customer inputs to be able to monitor these assets and relationships. By continuously scanning the entire Internet and only using the name of the organization for attribution, we're not only able to pick-up all your assets but also ones that are by 3rd parties or contractors and through which you may be exposed.

The third use case is misconfiguration, which has been in the news a lot lately. These simple misconfigurations, like a server sitting with a standard password or without a password protection or any form of other misconfiguration has led to more than half of data leaks last year. The Capital One hack where 100 million credit card applications were illegally accessed, was caused by an AWS server misconfiguration. Capital One was fined $80 million. So, the ability to detect these kinds of misconfigurations is another major area for us.

And then the fourth use case is what we call the non-coded threads. These are typically either business logic flaws or integration flaws that might leave data exposed if undetected, and these non-coded threat are not covered by existing solutions.

Finally, is the ability to also detect source code leakage, which can include either exposed credentials or other sensitive information that might be damaging to the organization.

What makes spiderSilk Resonance different

From the very beginning spiderSilk wanted to build a solution with ZERO inputs required from the customer, because many solutions require extensive seeding and input information and effectively become just as good as the input that is provided.

With Resonance, the spiderSilk Attack Surface Management platform, the only thing that is required from a customer is the name of the organization. Once that is entered into the system, the Resonance platform can scan the entire Internet, more than 4.2 billion IP addresses on a continuous basis.

> **68 %of organizations have experienced an attack originating from an unknown, unmanaged, or poorly managed company asset. Even more (75%) expect they will experience this type of attack in the future.**
> **– ESG**

Through that scan Resonance can attribute which assets out there belong to your organization and that starts to build your asset directory. And that's fundamentally different from a lot of approaches being taken that are dependent on the customer telling the solution what their assets are.

Also, by being external and independent, it doesn’t require any integrations deployments which is a relief for the majority of security guardians who may already have a host of intertwined solutions. So, the platform was built in such a way that it is a pull experience; not push. It is fundamentally meant to support security guardians and organizations by being autonomous, and that’s where spiderSilk’s customers, partners and MSPs have seen the most value from Resonance.