EXTERNAL ATTACK SURFACE MANAGEMENT:

How to gain visibility and take control of your organisation's digital presence

SC MEDIA
THE CYBER-SECURITY SOURCE

CTM360®
CYBER THREAT MANAGEMENT

Contents

Summary

Digital transformation has fuelled an accelerated migration to the cloud. As organisations find new ways to do business online, they face continuous challenges securing their digital presence on the internet. With reports of cyber attacks and data breaches increasing every day, unaddressed security gaps still exist globally; it is critical to recognise and address these in a practical and measurable way.

Organisations often do not realise or accept that they are potentially and continuously exposed on the internet. There is often hesitation or an inability to realise the opportunities threat actors have. As a result, the external attack surface is left vulnerable to relentless and mostly unseen adversaries. Security teams have to work to make their organisation an overall harder target by understanding, consolidating and controlling their external attack surface that lies in cyberspace and within the reach of threat actors.

"To make your organisation a harder target, it is important to gain complete visibility and control over your digital assets. Typically, the larger the organisation, the bigger the external attack surface. Understanding of this space is emerging quickly but practical adoption still lags worldwide. Rather than avoiding this reality, it is vital to get an external attack surface management solution that provides tangible visibility and actionability."

External Attack Surface Management (EASM) is a critical component of the modern-day security program. Greatly augmenting Defense-in-Depth and as part of a holistic Digital Risk Protection strategy, EASM helps security teams keep full visibility of their organisation's security posture across the internet. It also allows organisations to centrally control their digital presence.

As a whole, EASM includes:
1 digital asset discovery;
2 cataloguing of all existing digital assets;
3 timely prioritisation for mitigation of (i) issues, (ii) misconfigurations and (iii) exposed vulnerabilities. It also enables **4** benchmarking (across peers, competitors). Once an organisation's posture is consolidated and managed centrally, it is recommended to extend this same approach across **5** all third party vendors, partners, suppliers, etc.

In this white paper, we explore what makes up an organisation's external attack surface, why it is important, the challenges in securing this surface, and strategies for managing risks early.

Part one: What is an organisation's external attack surface and why is it important?

The external attack surface, or digital footprint, is made up of different pieces of information that are visible and accessible publicly. When correlated together, these data-points provide an accurate picture of the organisation's security posture in cyberspace. Threat actors are already cataloguing all such available data as part of reconnaissance activities to profile their intended targets. This is the homework that turns a potential target into an eventual victim. A weak security posture invites unnecessary attention and encourages threat actors to perform reconnaissance.

Furthermore, while migrating to the cloud, the boundaries between an organisation's network and the cloud are increasingly being blurred. Outside the firewall, threat actors continuously research all aspects of an organisation to (1) gain insight on digital assets, (2) identify opportunities to construct an attack (3) understand dynamics of staff, teams and departments, and (4) map the extended network of vendors, suppliers, partners or customers.

"EASM is important because it provides you with a hacker's perspective of your organisation, as a target."

External attack surface management includes profiles of data-points that may include but are not limited to domains belonging to an organisation, the underlying DNS information, certificates, servers, Internet of Things (IoT) devices, social-media profiles, mobile applications, list of key individuals and more. Each of these are potential targets for threats actors performing reconnaissance on an organisation.

To curate the above data-points, external attack surface management platforms use passive and non-intrusive methods of scanning. These do not actively scan for data, but rather listen to the internet to get as much information by relying on the right data sources. There are many data-feeds and sources of information readily available on the internet; these are then collated to get a comprehensive view of the security health of an organisation.

EASM is important because it provides you with a hacker's perspective of your organisation, as a target. Often organisations are unaware of their digital presence and thereby it becomes essential for them to manage it centrally. Most commonly, such initiatives are derailed due to common challenges.

Part two: Key benefits of External Attack Surface Management

1 Providing visibility

The external attack surface expands as organisations increase their overall internet presence. This also increases the level of complexity and confusion for teams, including IT and security. Different teams, different objectives and often, diverging job responsibilities mean new gaps in security arise unexpectedly and are left visible on the internet. A lack of full visibility also introduces inefficiencies that cost organisations both in terms of money as well as resources.

"Threat actors are increasingly leveraging data from the public domain to profile organisations. Understanding your external attack surface is a vital first step towards consolidating your overall security posture and preventing the opportunity for those with malicious intent."

Arsalan Iqbal, director, CTM360®

To solve for this, EASM ensures an organisation has a complete and continuous view of their digital assets. These data-points and any changes should be tracked quickly and accurately. When engaged with an EASM vendor, highly evolved ones will also provide updates on a daily basis as digital assets change on the internet.

"Threat actors are increasingly leveraging data from the public domain to profile organisations. Understanding your external attack surface is a vital first step towards consolidating your overall security posture and preventing the opportunity for those with malicious intent " says Arsalan Iqbal, director at CTM360®. "You will be surprised how much data is already there for public consumption."

2 Providing control

The second issue is about control over digital assets – or the lack of it. When working in silos, IT security or information security departments may be unaware of new digital assets or of changes in current ones. At times, these assets fall completely in a blindspot. In each situation, lack of control greatly increases risk and allows opportunities for adversaries.

Part two: Key benefits of External Attack Surface Management / *cont'd*

3 Taking ownership
Great confusion arises when proper ownership is not defined. This is seen in many organisations where employees, contractors, third-parties do not take responsibility; this grey area then causes security gaps. EASM enables the right stakeholders to take ownership within their respective domains.

4 Full alignment in prioritisation of issues
Prioritisation of external security issues are typically driven by domain expertise of security practitioners or by specified mandates. There may also be a lack of importance assigned to certain issues or a misalignment in prioritisation. EASM provides an on-going view of issues as they are detected and enables timely prioritisation for remediation.

"If you can control your own digital assets, you immediately minimise the risk of an external party attempting to take advantage of your external attack surface."
Arsalan Iqbal, director, CTM360®

5 Continuous monitoring, notifies on changes, modifications
IT and security teams may not be aware as data-points emerge or change; these are seldom tracked continuously. This is one of the biggest benefits of practical external attack surface management solutions, as it enables continuous monitoring and alerting.

6 Identifying new vulnerabilities
Cyberspace is not linear and as new exploitable vulnerabilities are identified, EASM seamlessly factors those in to ensure new vulnerabilities / misconfigurations are accounted for. EASM also allows for new vulnerabilities to be immediately mapped to specific digital assets as they appear.

"If you can control your own digital assets, you immediately minimise the risk of an external party attempting to take advantage of your external attack surface. EASM facilitates a black and white world, where whitelisted digital assets must be protected and reinforced, whereas blacklisted data-points need to be contained or mitigated." says Iqbal.

Part three: How threat actors view organisations' attack surface

How do cyber criminals choose their victims? In the physical world, criminals look for an easy target: a house with weak security, the one that leaves its doors unlocked. In the digital world, the same applies and if an organisation is not fully aware of its presence across the internet, security teams will not know which doors need locking, and they are left vulnerable.

Alarmingly, there are other data-points that are less technical and target human weaknesses:

1 Employees oversharing on social media or on their CVs on job sites;

2 Employees registering digital assets in a personal capacity for their company;

3 Different departments launching digital assets without proper coordination;

4 Employees using their corporate identities to register on platforms for personal use.

At the first stage of the Cyber Kill Chain, adversaries regularly perform reconnaissance; they try to understand weaknesses and identify ways to pinpoint vulnerabilities, misconfigurations, information exposure and gaps in overall IT hygiene. Often these adversaries leverage a known vulnerability or exploit in specific products.

"If an organisation is not fully aware of its presence across the internet, security teams will not know which doors need locking, and they are left vulnerable."

Contrary to perception, adversaries may regularly bypass the traditional security stack by delivering a fraud, scam or attack completely outside an organisation's network and security controls. Financial and cryptocurrency frauds are some cases that regularly cause significant financial losses, yet there is no often strategy to stop these. EASM remains the first step towards countering such incidents by empowering security teams to know what they have to protect in the external space.

Part four: What are the challenges to gaining visibility?

The old confines of an organisation's network are long gone. There are a range of dispersed assets, on-premise and in the cloud, across core networks and third-party partners and suppliers. The importance of external attack surface management has never been greater.

A Gartner report, *Emerging Technologies: Critical Insights for External Attack Surface Management,* a category Gartner calls EASM for short, has paved the way for this category to be mainstream.
"It is essential to have complete visibility and control over your presence in cyberspace," says Iqbal. "This will ensure that your organisation can safeguard its external attack surface, thereby making the organisation a harder target"

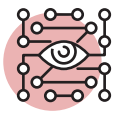
There are many reasons why an organisation's visibility into its digital presence may be lacking. These include, but are not limited to:

1 Dispersed landscape
In cyberspace, adversaries are continually looking for data-points that they may leverage from the public domain. There is no requirement to be on premise or with access from the inside. Every day, plenty of opportunities to exploit the external attack surface exist.

2 Rise in cloud activities
More work in cyberspace means more data-points relevant to an organisation get exposed frequently. These serve as starting data-points for attackers in their reconnaissance activities.

3 Shadow IT
In the context of the external domain, on-premise or digital assets may become exposed on the internet, without the knowledge or approval of security / IT teams.

4 Department siloes
Many organisations have digital assets managed by siloed teams, such as IT, Security Marketing, Legal, HR, Corporate Communications, etc. Often, people in one team may know nothing about the assets that are another team's responsibility.



5 Beyond your own organisation
Third-party vendors and suppliers also may increase the exposure of an organisation. In current times, supply chain risks are continually exploited as organisations may not have visibility or oversight. When compromised, an organisation's supply chain can have a big downstream impact.

Part four: What are the challenges to gaining visibility? / *cont'd*

Why traditional tools often may not be enough
There are many security tools available and in use that help give greater visibility into the external attack surface, but these may only go so far...

Vulnerability scanners
These give insight into vulnerabilities but are generally used periodically as per scheduling or preference.

IT asset management
Very few organisations maintain a Digital Asset Register, i.e. an inventory of digital asset data-points from cyberspace. It is more common to see information security or IT asset registers.

Penetration testing
Penetration testing does not give complete visibility of your organisation's presence across all digital assets and is typically performed at a point in time. EASM greatly augments Penetration Testing, as it approaches security from another dimension.

Part five: How organisations may consolidate their external attack surface

In simple terms, external attack surface management means the different teams in your organisation work to recognise and secure all digital assets in cyberspace.

But to do that, they require visibility. Teams cannot reduce the attack surface without knowing the full picture. This is done through discovery and inventory of all knowable assets, followed by prioritisation and remediation of issues (misconfigurations, vulnerabilities, etc.)

"Teams cannot reduce the attack surface without knowing the full picture. This is done through discovery and inventory of all knowable assets, followed by prioritisation and remediation of issues."

CTM360®, a Digital Risk Protection (DRP) platform, encourages organisations to align with the benefits provided by EASM. When used in conjunction with surface, deep and dark web detections, cyber threat intelligence, brand protection, anti-phishing, data leakage monitoring, etc. External Attack Surface Management remains the crucial piece that ties all aspects together.

CTM360® currently cites the following four steps to ensure that organisations can secure their digital presence, thereby becoming a harder target.

1 Understand your external attack surface
2 Quantify and assess your organisation's digital risk
3 Prioritise and remediate issues
4 Manage third party risk across your supply chain

"A solution such as CTM360®'s HackerView gives organisations a full view of an organisation's external attack surface."

Part five: How organisations may consolidate their external attack surface / *cont'd*

1 Understand your external attack surface
Organisations need to holistically identify their presence through curation of data-points from various platforms, networks, social media, digital certificate, registrars, etc.

2 Quantify and assess your organisation's digital risk
Organisations should identify, assess, and address risks in a tangible and measurable way. This may be quantitative or also summarised as a digital risk scorecard.

3 Prioritise and remediate issues
By carrying out an audit of an organisation's digital footprint, organisation's should also prioritise by criticality and severity. This enables them to pinpoint issues that exist in their digital presence from a hacker's point of view.

4 Manage third party risk across your supply chain
Organisations need to continue monitoring their digital footprint, as well as extend that mentality across the supply chain and partners. EASM facilitates enhanced visibility on digital risks across vendors, suppliers, partners and peers.

A solution such as CTM360®'s HackerView gives organisations a full view of an organisation's external attack surface. It provides a complete digital inventory with any associated weaknesses with guidance on how to become a harder target.

A comprehensive External Attack Surface Management platform also gives visibility across third parties, such as vendors, partners, and customers. Such a platform can give your organisation a digital risk score of these third parties so you can inform them of responsibility to an organisation's security in a timely manner.

Part six: The five key takeaways

Adversaries never give up and the expansion of the external attack surface has increased opportunities for threat actors. It is important to:

1
Realise the importance of your external attack surface and take initiatives to holistically control your digital footprint.

2
Understand the importance of a harder security posture to safeguard your organisation in cyberspace.

3
Align all stakeholders so that everyone within the organisation has an understanding of digital risks in their respective domains and where their ownership lies. Increasing coordination between all teams ensures better results.

4
Visibility & Control of your digital presence are essential – and that means consistent monitoring of you and your third-party external attack surfaces.

5
Find a partner, such as CTM360®'s HackerView, that specialises in External Attack Surface Management. Set-up ongoing monitoring and establish constant visibility. This is a crucial step in having a harder security posture in cyberspace.

About us

CTM360® is a subscription service powered by EDX Labs, offering 24 x 7 x 365 Digital Risk Protection to detect and respond to threats. CTM360® specializes in offensive defense to identify and manage cyber blind spots outside your network. Offered as a service and with an ecosystem built in the cloud, CTM360® remains a leading detection & response provider in cyberspace and the digital domain.

Contact:
Vinod Johnson, Technical Accounts Manager – CTM360® Digital Risk Protection – +973-77-360-360
vinod@CTM360.com
www.ctm360.com

CTM360®