Attack Surface Management: a Critical Pillar of Cybersecurity Asset Management

Pablo Quiroga, Director of Product Management, Qualys
July 28, 2022 - 5 min read

12

In their recent Innovation Insight for Attack Surface Management report, Gartner calls Attack Surface Management (or "ASM", for short) the first pillar in a broader Exposure Management strategy. According to Gartner, ASM addresses the questions:

- What does my organization look like from an attacker's point of view?
- How should cybersecurity find and prioritize the issues attackers will see first?

An organization's attack surface is made up of all IT assets with points of entry that can lead to unauthorized access to its systems, making those assets susceptible to hacking and exploitation for the purpose of conducting a cyberattack. The average enterprise has a wide array of assets comprising its attack surface.

Types of Attack Surfaces

Digital

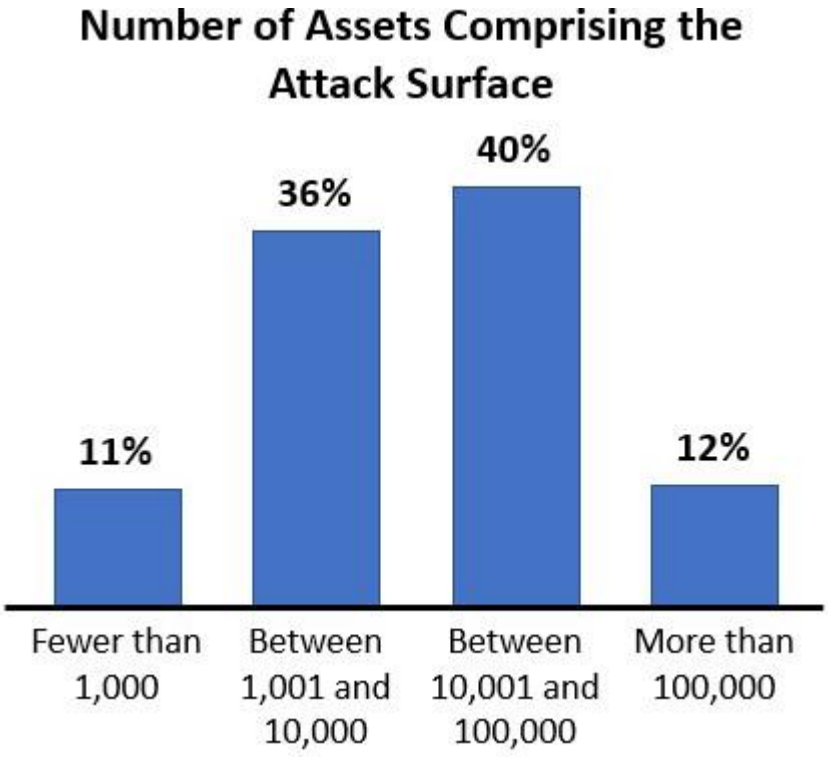
- Applications
- Code
- Ports

- Servers
- Websites
- Clouds & containers
- Digital certificates
- Un/authorized system access points

Physical

- Desktop computers
- Laptops
- Mobile devices
- USB ports
- IoT devices
- Improperly discarded hardware

With digital transformation over the last decade, and the growth of remote/hybrid work models over the last two years, the number of attack surface assets that most organizations must manage has exploded exponentially. Currently, **52% of IT organizations** manage 10,000+ assets.



Source: Qualys

Industry experts cite any number of reasons why the average enterprise's attack surface continues to expand. These include:

- Complex IT supply chain ecosystem
- Device diversity among end-users
- Use of public cloud infrastructure
- Use of SaaS apps and services
- Growth in numbers of remote workers

Enterprise IT departments, and cybersecurity teams in particular, are responsible for inventorying, managing, protecting, and defending the attack surface. What happens if an organization isn't even aware of all its assets?

What Isn't Seen Can't Be Protected

Research from industry analyst firm ESG shows that **69% of organizations** have experienced an attack targeting an "unknown, unmanaged, or poorly managed internet-facing asset." This often involves ones that the organization may have lost

track of or isn't aware even exists (also known as "shadow IT"). It's no wonder malicious actors have a great deal of success exploiting them.

The number and diversity of assets under IT management has exploded, making it challenging to discover them all. However, it's of utmost importance to surface these unknown assets. What isn't seen can't be protected.

ESG's research further finds that **only 9% of organizations** are monitoring 100% of their attack surface. As if keeping track of every possible pathway into enterprise systems wasn't difficult enough, it's also very time-consuming. The study shows that **43% of organizations** spend more than 80 hours on attack surface discovery, only tackling it weekly, semi-monthly or monthly, according to ESG.

It's clear that the volume, diversity, and complexity of IT asset management is increasing—often beyond the capability of Cybersecurity teams to track, manage, and protect effectively.

Enter Attack Surface Management (ASM).

Defining Attack Surface Management

It's no wonder Attack Surface Management has become a hot topic among Cybersecurity professionals.

However, industry analyst firm Forrester Research points out that cybersecurity and risk management vendors are using a dizzying variety of monikers to describe the same thing. These include:

- Asset discovery
- Attack surface assessment
- Attack surface monitoring
- Digital asset discovery
- Digital footprint
- Digital risk monitoring
- Digital risk protection

- External attack surface management

Whatever the synonym used for ASM, Forrester rightly recommends that enterprises think holistically about their entire IT asset estate.

Gartner's definition of ASM as part of Exposure Management, on the other hand, lists three elements as core ASM capabilities: cyber asset attack surface management (for internal assets), external attack surface management, and digital risk protection services.

Whatever the definition, the experts agree that all enterprises need to improve asset visibility, risk prioritization, and security control over their entire attack surface.

Attack Surface Management is Now a Top Priority

We've established that ASM can be defined as the continuous process of discovering, classifying, and assessing the security of all an organization's assets. Accurate mapping of the attack surface, and its effective protection, mitigates the risk of a successful attack. A comprehensive ASM Program should include an accurate, up-to-date inventory of all IT assets with risk assessments as well as an accounting of all security controls or other risk mitigation measures applied.

When most organizations first complete attack surface discovery, they often uncover an eye-opening array of vulnerabilities infecting previously unknown assets. These include everything from bad code, misconfigurations, expired certificates, exposed APIs, EOS/EOL software, to unprotected data and more.

According to our research here at Qualys, our customers are tracking **3X more Severity 4 vulnerabilities** than Severity 1 —and **external assets account for almost 20%** of them. Attackers most often exploit public-facing web assets that are poorly defended and use automated tools to discover them.

But what are the key solution requirements when selecting an ASM solution?

That's a rich topic for another blog post. We can start by saying that comprehensive ASM must include continuous discovery, analysis, and protection. Fortunately,

automated solutions exist to tackle these three key functions of ASM. Analysts agree that an automated approach to ASM is absolutely vital to a successful program. Better still, ASM should be part of a comprehensive platform approach that tightly integrates vulnerability management, endpoint protection, cloud security, web app security, and threat intelligence.

Conclusion

Today's post-COVID world is a challenging place. Cyber warfare, a looming economic recession, and the continuing IT skills gap demand a unified approach to Cybersecurity. It's clear that enterprises large and small need to double-down on ASM as another imperative. Without a dynamic, holistic view of the organization's attack surface in an ever-changing IT environment, exposures and unmanaged assets will continue to accumulate.

In Part Two of this blog series, we'll examine the ways malicious actors exploit an unmanaged or poorly managed attack surface. Plus, we'll examine some typical ASM use cases. Finally, we'll take a deeper dive into what solution requirements organizations should consider when evaluating ASM vendors.

Related

August 3, 2022

Introducing CyberSecurity Asset Management 2.0 with Natively Integrated External Attack Surface Management

July 27, 2022

Join Qualys at Black Hat USA 2022!

July 11, 2022

How to Quickly Prioritize Risks with VMDR 2.0 and Orchestrate Response with CMDB & ITSM Integration

---