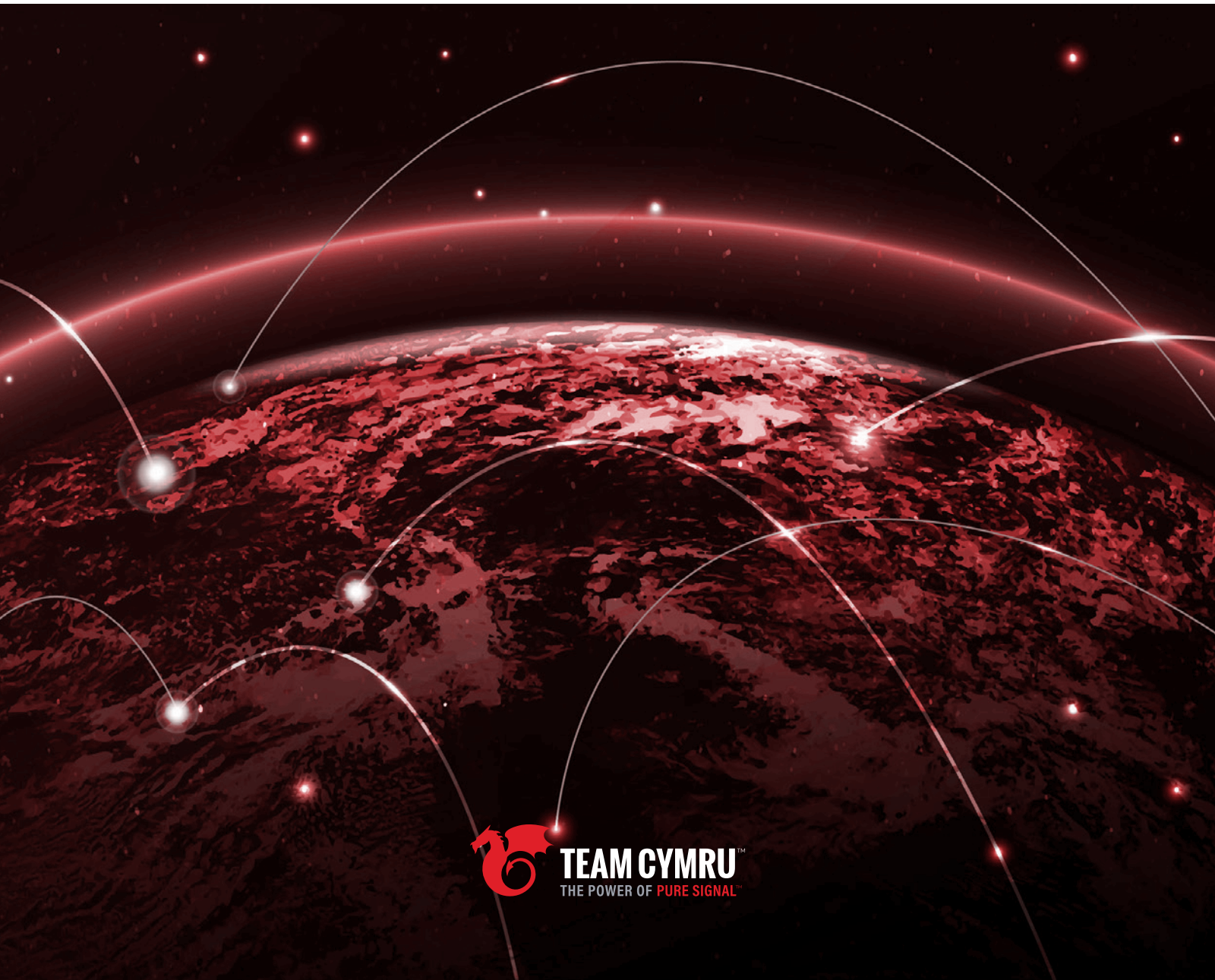
EBOOK

INTRODUCING

Attack Surface Management v.2.0

How missing out could lead to your next breach

By Brad LaPorte, Former Gartner Analyst, Cybersecurity Industry Expert
and creator of the term 'Attack Surface Management in 2019'



Cybersecurity tools have matured over the years and become more and more capable of detecting threats and vulnerabilities, monitoring breaches and taking action. But at times, they have resembled a gangly, uncoordinated adolescent – growing in size and strength but not always able to move quickly and elegantly when required.

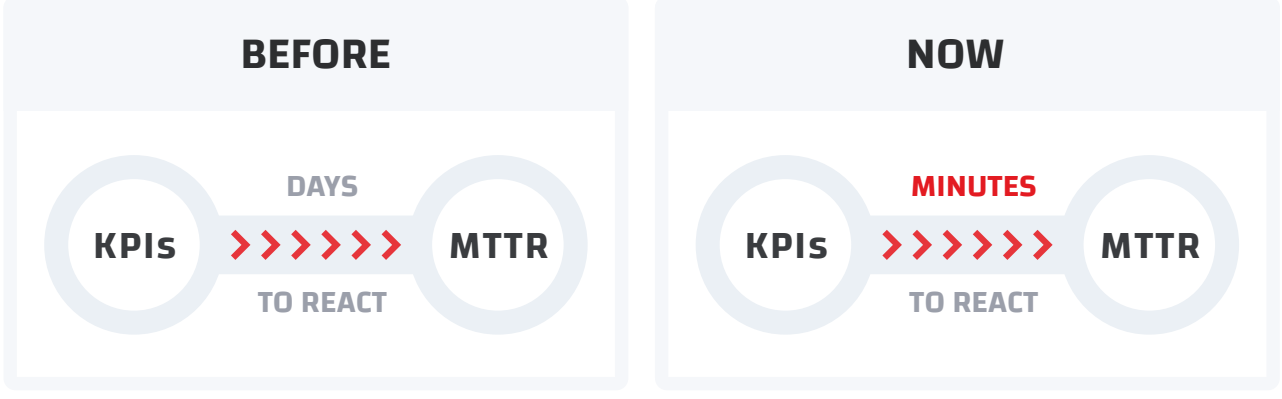
According to *IBM's 2022 Threat Intelligence Index* report, vulnerabilities in internet-facing enterprise software are being exploited and weaponized at an increasing rate:

Over 1/3rd of attacks in 2021 used vulnerability exploitation - *opportunistic "scan-and-exploit" type attacks that are both voluminous and devastating due to the sheer speed and effectiveness that automated programs can now operate*

In addition, vulnerability exploit attacks grew 33% year over year in 2021 - *the number of incidents that were caused by vulnerability exploitation this past year rose 33% from 2020*

The warnings are clear; **this attack vector is a primary and preferred method of attack and will increase and evolve moving forward.** *Decision-makers have to ask themselves, 'Is my budget and spend proportionate to this growing attack vector?'*

What makes the situation even worse, the amount of time between disclosure of a new vulnerability and the start of active exploitation has been reduced to a matter of hours, leaving defenders with less time to react and respond. Key Performance Indicators (KPIs) for the Mean Time To Respond (MTTR) is now measured in minutes as opposed to days.



Amount of time between disclosure of a new vulnerability and the start of active exploitation

The attack surface is no longer stopping at an organization's 'four walls.' ***According to a recent survey by Anchore,*** conducted in December 2021, over half of the companies surveyed were targeted by software supply chain attacks in 2021.

Log4j was revealed on December 9. Before that date, 55% of respondents said they had suffered a software supply chain attack. After that date, that number jumped to 65%, or an increase of 10%.

The number of dependencies that organizations now have to prioritize and take immediate action on goes up significantly with the adoption of new technology and exposed architectures such as containers and cloud-native deployments. Organizations need to create a more mature approach with containers and prioritize risk exposure that these extra attack surfaces are created by this digital transformation.

Security professionals are forced to get creative, implementing a multitude of disparate tools that:

- **Alert them to threats**
- **Inform them of vulnerabilities**
- **Sniff out those vulnerabilities or threats in the infrastructure**
- **Automates responses**

That's a lot of tasks to execute seamlessly. Information isn't disseminated uniformly nor put into context. Actions in response can be too slow or ineffective. Attacks that could have been better anticipated and stopped slip by the security team. Growing teams with many tools and significant budgets have still been largely ineffective due to these complexities; clearly, changes are needed.

For lack of a better term, let's call that level Attack Surface Management (ASM) v1.0 – the first stage of attack surface management.

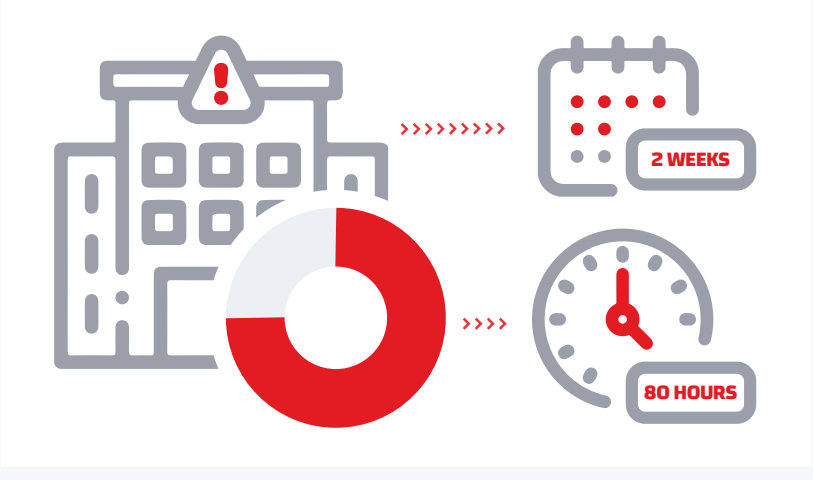
Now comes ASM v2.0. With one well-integrated tool, security teams see the whole cyber field at once, anticipate moves by the other side, view their teammates' defensive lapses, and slap away the attack. But first, let's review why ASM v1.0 isn't able to compete.

The limitations of first-generation attack surface management

Developments happen fast in cybersecurity, and you may have missed the introduction of this new class of products of attack surface management. And if you're like most organizations, you're not using this product. ***Given my experience at Gartner and as an expert in this field for the past 20 years, 75% of organizations still rely on spreadsheets to manually manage their attack surface.*** Furthermore, it's taking the average organization over 2 weeks, or 80 hours, to update its attack surface inventory for every time a point-in-time assessment update is conducted.

75%

Of organizations still rely on spreadsheets to manually manage their attack surface.



Compounding the problem is the overall expansion of the attack surface, both internal and external. One fact that explains why: 60% of knowledge workers are now remote, according to Gartner's ***"Top Trends in Cybersecurity 2022."*** This is a trend that will continue. In addition to combating attack surface expansion, Gartner highlights in their report that organizations are prioritizing consolidated solutions that address critical use cases in a single approach. Across multiple security domains, security technology convergence is accelerating. This is driven by the need to reduce complexity, leverage commonalities, reduce administration overhead and provide more effective security.

Source: *Gartner, Top Trends in Cybersecurity, 2022*

Gartner uses the term "attack surface management" to describe the processes, technology, and professional services deployed ***to discover*** external facing enterprise assets and systems that may present vulnerabilities. Examples include an organization's own servers, domains, certificates, credentials, public cloud service misconfigurations, and extends outwards to include the same list for third-party infrastructure and partner software code vulnerabilities. Anything internet visible that malicious actors could exploit.

When I originally wrote this definition, I intended for it to be straightforward and simple to ensure that it was not confused with traditional risk management or vulnerability management methods. But in doing so, I unintentionally limited ASM's full potential. At the time, over half of the organizations had little idea what their attack surface really was, not to mention what a truly accurate risk posture was. We needed a starting point. A lot has changed since 2019, which has brought on the evolution of ASM v2.0.

Notice the verb Gartner applies in this definition: Attack surface management is merely discovering the vulnerabilities in an organization's infrastructure, not necessarily doing anything about them. Nor does the definition explain how the system initially determined what vulnerabilities to look for. It's a bit like handing an inspector a list of possible hazards you're worried your house contains, then getting back a sheet with checkmarks to the ones you have or don't have. The inspector isn't going to fix them. That's someone else's job.

This segmentation of responsibilities becomes a chain that's only as strong as its weakest link. Before the attack surface management tool can perform any of its functions, it needs good upstream information about the vulnerabilities and threats.

The limitations of first-generation attack surface management

1st

Vulnerability Scanners can gather a certain amount of data, but they can't account for everything. This is further exacerbated by the complexity of hybrid environments across cloud and on-premises infrastructures. In addition, if IT assets are in the cloud, but "unknown" or unmanaged, they will never be scanned for vulnerabilities, creating significant and immeasurable risk.

2nd

Threat intelligence needs to be as robust as possible, anticipating attacks to detect anomalies and give early warnings of dangers. It needs to have an embedded business context at the forefront and be actionable.

3rd

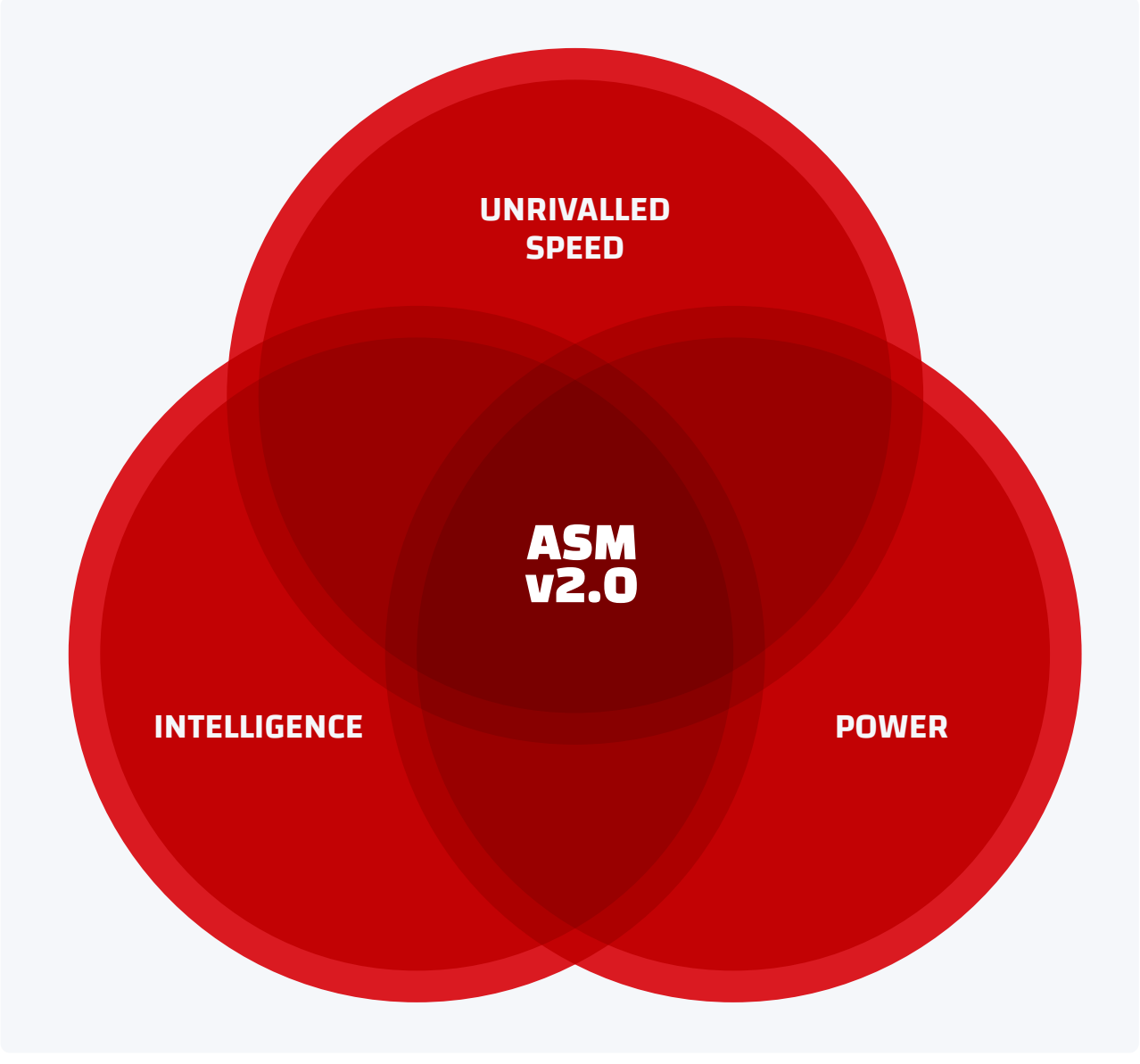
Vulnerabilities are important to know about, but without an automated way to prioritize them by danger to a company's assets, they can overload a security team and send it on useless remediation missions.

4th

And increasingly, security information-gathering efforts must look beyond the internal threats and vulnerabilities to those posed by third parties. Cybercriminals are increasingly using software suppliers as efficient carriers of their malware.

Faced with these dangers, security teams are forced to use complicated toolsets in response. Quoting from that "Top Trends in Cybersecurity 2022" report again: "Gartner clients increasingly express frustration with the operational complexity of the modern security stack. Given the human capital constraints, efficient cybersecurity remains out of reach for the majority of organizations."

Bringing it All Together...
ASM v2.0: Brings *Unrivalled Speed, Intelligence, and Power*



When it comes to cybercrime, delayed responses can cost organizations millions. Each hour that passes after an initial attack allows the threat actors to extract more and more valuable data. But speed alone is not enough.

You need to start with a deep understanding of threats and vulnerabilities. This is what Team Cymru has achieved with its Pure Signal™ Recon solution. Gathering signals from across the globe, this solution gives security teams visibility far beyond their internal infrastructure and traces a threat more than a dozen hops to its source. IPs that are associated with confirmed malicious activity get added to a dynamic IP Reputation feed, traditionally used to create a network-level block list.

That reputation information is now also fed to the insight engine of Team Cymru's Pure Signal™ Orbit – a recently launched solution – to identify both known and unknown customer assets, remote connectivity, and third- and fourth-party vendor assets. Those assets are continually monitored to determine the presence of vulnerabilities or threats. Then this is what I call the "v2.0" version of ASM, and provides risk scoring so both the C-suite and security teams gain the vantage points they need: strategic views to drive business decisions, tactical views to prioritize remediation efforts.

Having awareness of vulnerabilities and threats posed both internally and externally is a critical advantage. With ASM v2.0, security teams can detect supply chain threats as well as dangers posed by business partners. Corporate leaders contemplating a merger or acquisition can check to ensure that the other organization is not inadvertently hiding threats or vulnerabilities.

And of course, it's all integrated into a single platform, which drives speed and accuracy because there's no time wasted trying to take the information provided by one tool and then apply it to a second, third or fourth, all critical data, threats, and risks need to be integrated into a single place.

This leads to a bonus attribute: reduced costs. Not only is there a pricing advantage by buying one tool instead of four, but the administrative costs of managing a single tool also provide ongoing savings.

ASM v2.0 is a truly better together story - bringing best-in-class threat intelligence and never before seen visibility of your expanding attack surface into a combined solution.

About the Author

Brad LaPorte is a former Gartner Analyst and a Partner with High Tide Advisors.

He works closely with Team Cymru as a strategic advisor to help customers ascend to the next level of cybersecurity proficiency.

Want to learn more?

We'll be happy to help you discover your own attack surface, and explain how ASM v2.0 can help your organization.

GET IN TOUCH