Cyber Insights 2023: Attack Surface Management

About SecurityWeek Cyber Insights | *At the end of 2022, SecurityWeek liaised with more than 300 cybersecurity experts from over 100 different organizations to gain insight into the security issues of today – and how these issues might evolve during 2023 and beyond. The result is more than a dozen features on subjects ranging from AI, quantum encryption, and attack surface management to venture capital, regulations, and criminal gangs.*

SecurityWeek Cyber Insights 2023 | Attack Surface Management – Attack surface management (ASM) is an approach for delivering

cybersecurity. IBM describes the attack surface as “the sum of vulnerabilities, pathways or methods – sometimes called attack vectors – that hackers can use to gain unauthorized access to the network or sensitive data, or to carry out a cyberattack.”

ASM requires “the continuous discovery, analysis, remediation and monitoring of the cybersecurity vulnerabilities and potential attack vectors that make up an organization’s attack surface. Unlike other cybersecurity disciplines, ASM is conducted entirely from a hacker’s perspective, rather than the perspective of the defender. It identifies targets and assesses risks based on the opportunities they present to a malicious attacker.”

ASM is consequently predicated on total visibility of assets, vulnerabilities, and exploits.

Demise of the perimeter and growth of complexity

Attack surface management is not a new concept, notes Mark Stamford, founder and CEO at OccamSec. “As long as there has been a thing to attack, there has been an attack surface to manage (for example, the walls of a castle and the people in it).” The castle is a good analogy. If you can see the wall, you can attack it. You can batter it down, you can employ the original Trojan Horse to gain access through the front door, you can find a forgotten and unprotected entrance, or you can persuade an insider to leave a side gate unlocked.

For the defender, relying on the wall and being aware of any weak areas is not enough. People are also part of the attack surface, and the defender needs to have total visibility of the entirety of the attack surface and how it could be exploited. But the wall is a perimeter, and we no longer have perimeters to defend – or at least every single asset held anywhere in the world has its own perimeter.

“The attack surface,” continued Stamford, “is anything tied to an organization that could be a vector to get to a target. What this means in practice is all your applications that face the Internet, all the services (beyond applications) that are reachable, cloud-based systems, SaaS solutions you use (depending on what the bad guys’ target is), third parties/supply chain, mobile devices, IOT, and your employees. All of that and more is your attack surface and all of it needs to somehow be monitored for exposures and dealt with.”

The need for ASM, like other current approaches to cybersecurity (such as zero trust, which itself can be viewed as part of ASM), comes from the demise of a major defensible perimeter. Migration to the cloud, expanding business transformation, and remote working all add complexity to the modern infrastructure. If anything touches the internet, it can be attacked. Even the addition of new security controls that send data to and from the cloud add to the attack surface.

“The adoption of multi-cloud and hybrid cloud will continue to rise in 2023,” comments Aditi Mukherjee, director of product marketing management at Lacework. “As enterprises continue their cloud migration and digital transformation, they will realize that traditional approaches with siloed tools, rules-based policies, and disparate security data actually introduce more security risks, creating an expanded attack surface for bad actors.”

But ASM goes beyond the cloud alone. “The traditional attack surfaces are physical, digital and social,” explains Sam Curry, CSO Cybereason; “but digital really needs to be broken down into subdomains for classical environments and networks, legacy data centers, cloud infrastructure and the aggregate software-as-a-service topography.”

He doesn’t believe ASM will provide a complete answer, but is a solid doctrine for minimizing the exposure in each domain,

giving least options and succor to attackers. “There are also key existing and emerging control planes around identity, application governance and data-centrism that need to be strongly protected and managed in a similar manner, even before thinking of the advanced techniques around obfuscation and deception.”

All security strategies, he says, should think about both reducing complexity in each attack surface and control plane, about gaining leverage in each, about reducing vulnerabilities and exposure in each and about how to bring the full security game to bear in each.

Attack surfaces will get more complex and more distributed throughout 2023; and effective ASM will be more complicated.

Management is the key word in ASM

The complexity of the modern infrastructure makes the complete elimination of threats an impossible task. ASM is not about the elimination of all threats, but the reduction of threat to an acceptable level. It’s a question of risk management.

“The idea behind attack surface management is to ‘reduce’ the ‘area’ available to attackers to exploit. The more you ‘reduce the attack surface’ the more you limit and minimize attackers’ opportunities to cause harm,” says Christopher Budd, senior manager of threat research at Sophos.

He believes that ASM will be more challenging in 2023 because of the attackers’ increasingly aggressive and successful misuse of legitimate files and utilities in their attacks – living off the land – making the detection of a malicious presence challenging. “We can expect this trend to continue to evolve in 2023, making it more important that defenders update their detection and prevention tactics to counter this particularly challenging tactic,” he says.

Part of reducing risk comes from understanding what vulnerabilities exist within the infrastructure, and which of them are exploitable. Omer Gafni, VP surface at Pentera, reminds us that ASM looks at threats from the attacker's perspective. To effectively reduce risk, you need to understand not only what vulnerabilities exist, but also which are exploitable and serve the hackers' end goals.

"With the number of annual reported vulnerabilities now exceeding 20,000 per year, companies cannot remediate every alert, and need to become more surgical with their remediation strategies," he says. "To achieve this, we will start to see a shift from a focus on vulnerability to exploitability. Companies will start to put a major emphasis on understanding which targets are most impactful from the hacker's perspective, and therefore the most exploitable targets."

CISA's Known Exploited Vulnerabilities Catalog (the KEV list) can help here. Focusing remediation on exploited vulnerabilities is a key part of ASM, and the catalog is described by many as 'CISA's must patch list'. This list will continue to grow through 2023.

Pentesting and red teaming are also effective ways of locating exploitable vulnerabilities, but in the past, they have not been used effectively. "One of the most frustrating things as a pentester is when you return to organizations a year later and see the same issues as before," says Ed Williams, director of Trustwave SpiderLabs EMEA. "There is no value to this for the clients. They are not maturing. In fact, they are regressing."

But he expects an improvement – perhaps encouraged by the growing acceptance of ASM – in 2023. "I expect an unprecedented appreciation for how pentesting effectively exposes gaps in security, and this in turn will help to reinforce the importance of those all-important security basics. In 2023 I implore organizations to work with

pentesters for the best, year on year result."

Chad Peterson, MD at NetSPI, believes the nature and effectiveness of pentesting will evolve over 2023, "The attack surface has become more fluid, so you have to be able to scan for new assets and entry points continuously," he says. "In 2023, organizations will combine traditional pentesting, which in many cases will still be required for regulatory needs, with the proactive approach of more continuous assessment of their attack surface. The result will be better awareness of the attack surface and more comprehensive traditional pentesting as there is more information about the true attack surface."

Sample problem areas

SaaS

Ben Johnson, CTO and co-founder of Obsidian, chooses SaaS. "2023 will be the year of SSPM [SaaS security posture management] and securing SaaS," he says. "But for that to happen, we must continue educating organizations on the risks of SaaS. In doing so, organizations must ensure their left-of-boom teams (vulnerability management and GRC) are able to reduce SaaS risk while ensuring their right-of-boom teams (security operations, incident response, threat hunting) have continuous threat management capabilities."

SaaS security has given organizations the ability to scale applied security, not just awareness. "Now is the time to distribute security hardening and operations to go with the distributed technology and distributed responsibility. As we know, the pandemic sped up the hybrid work model, and organizations that prioritized endpoint or public cloud security over the past couple years are now ready to secure SaaS and the modern workflow."

The browser

Jonathan Lee, senior product manager at Menlo Security, focuses on the browser, which is possibly the biggest single threat surface. This is where users spend most of their time. “Vendors are now looking at ways to add security controls directly inside the browser,” he said. “Traditionally, this was done either as a separate endpoint agent or at the network edge, using a firewall or secure web gateway.”

The big players, Google and Microsoft, are also in on the act, providing built-in controls inside Chrome and Edge to secure at a browser level rather than the network edge, he added. “But browser attacks are increasing, with attackers exploiting new and old vulnerabilities, and developing new attack methods like HTTP smuggling. Remote browser isolation is becoming one of the key principles of zero trust security where no device or user – not even the browser – can be trusted.”

Noticeably, 2022 has already seen investor interest in startups developing secure browsers – such as Red Access and LayerX.

The user

Ed Williams highlights a failure in using and accounting for the user – and uses ransomware as an example. “Cyber threats, including ransomware, will never be prevented by implementing shiny new products and solutions unless the underlying security issues are addressed. Therefore, in 2023,” he added, “I hope organizations shift their mindset away from feeling as though they need the latest tempting tech, and instead focus on consistently achieving the human-centric security basics. These basics include patching, strong passwords, and a detailed security policy.”

Visibility

If ‘management’ is the key word in ASM, ‘visibility’ is the key enabler. You can only manage what you can see. “In 2023, organizations should embrace the mindset of empowering their teams with visibility into assets and relationships and overcoming data silos between AppSec, infrastructure, and data security teams,” suggests Erkang Zheng, founder and CEO at JupiterOne.

He recalls the words of John Lambert: “Defenders think in lists. Attackers think in graphs. As long as this is true, attackers will win.” Attackers will win, especially if cybersecurity defenders cannot quickly understand graph-based relationships between data, networks, and user accounts in their own networks to limit the blast radius when they are under attack.

“Contextual intelligence is likely necessary to win in a threat vector where organizations face more complex, destructive, and irreversible threats than ever before,” he says. “This visibility and understanding are the primary benefits of attack surface management technologies and practices, along with secondary benefits such as compliance and evidence automation.”

Marcus Fowler, CEO of Darktrace Federal, has no doubt that ASM will be a top priority for organizations in 2023. The problem is the attack surface is never static; it’s constantly evolving with the level of risk changing daily. “Tracking down the full extent of the attack surface is not something that can be left to human resources. It requires real-time data from an AI engine taking a hacker’s approach,” he says. He believes that most organizations currently miss as much as 50% of their true attack surface.

“That’s where seeing AI take on the key ASM functions of discovery, assessment and prioritization, risk prevention and

integration can expose the true level of exposed risk," he added. "Only the automation and scalability of AI can provide the up-to-date, continuous copy of the internet that CISOs need to get a grip on the attack surface. Paired with AI's unique understanding of an organization's digital estate, you get an outside-in, inside-out risk management program that will be vital for the CISOs of tomorrow."

Part of ASM is external attack surface management (EASM). Microsoft defines the external attack surface as "the entire area of an organization or system that is susceptible to an attack from an external source." We should note that this excludes malicious or naive insiders, who should also be considered as part of a full ASM approach to cybersecurity. Nevertheless, there will be a growing number of EASM support systems released by security vendors during 2023. CrowdStrike, for example, announced in September 2022 that it would be buying EASM company Reposify, with an expectation to close during CrowdStrike's fiscal third quarter.

"In response to evolving attack tactics and an expanded attack surface," comments Karin Shopen, VP of cybersecurity solutions and services at Fortinet, "we expect a shift in the tools CISOs consider in 2023. When it comes to attack surface management, CISOs will shift from one-time assessments to constant and continuous early evaluation of their organization's external attack surface. EASM solutions, which help provide organizations with an adversary's view of their attack surface, will be at the top of their lists, as will machine learning and the use of seasoned threat hunters that offer takedown services."

Furthermore, she added, "CISOs and security teams will more closely evaluate EASM solutions based on their ability to not only detect but prioritize and remediate threats using machine learning to help resource-depleted SOC teams."

Chris Morales, CISO at Netenrich, describes his own approach.

“I have one priority for 2023 – to be data driven for risk making decisions,” he says. “My commitment starting fiscal year 2023 is to be data driven with quantitative risk management practices. That means providing the business units with a dashboard and trending metrics to the state of assets, vulnerabilities and threats that comprise their attack surface. From this we can continually score threat likelihood and business impact to make informed decisions on where to best focus resources.”

It isn’t simple, but worth the effort. “Making this happen requires a tightly integrated security stack that shares data into a single aggregated data lake to threat model and answer questions.”

The concept is supported by Shira Shamban, CEO at Solvo. “In 2023, we are going to see a data-centric approach to cybersecurity emerge and grow,” she says. “At its core, cybersecurity is a problem of managing all the data, assets, and sensitive resources an organization has, and determining how to protect it. This sensitive data can often include PII, PHI or IP. This is the top concern for CISOs and security practitioners, so security approaches and products will begin to put data at the center, rather than focusing solely on the environments the data is in.”

The way forward in 2023

Attack surface management is nothing short of a complete methodology for providing effective cybersecurity. It doesn’t seek to protect everything, but concentrates on those areas of the IT infrastructure that can be attacked. There is no product that can provide ASM, but a growing number of products that can help. It requires complete visibility of all assets, and detailed knowledge of exploits so that assets can be protected. It is, like zero trust, a journey – one that is gaining traction and will gain more traction in 2023.

Mark Stamford describes the problem and offers his own route for the journey. “ASM tools produce a lot of noise that can send a security group down an endless number of rabbit holes. In the rush to simplify the problem everything gets reported on and all kinds of vulnerability data gets included. There’s usually some shoddy logic applied which seems to state if you have a lot of stuff facing the Internet you are more at risk, which piles further pressure on the security group. I’ve seen ASM tools which report on old SSL certs, low level vulnerabilities, all kinds of stuff that really, poses little to no risk.”

The route he proposes is to start by discovering all the assets, organizations, devices, and people that could create a problem. Then assess which could have a harmful impact. “A web server hosting some static pages in AWS, that connect to nothing, may cause a headache, but is probably not going to lead to a breach,” he says. “On the flip side, your Internet accessible financial system is a key component.”

Next assess how everything is connected – could an attacker get from A to B and cause an impact. “Draw a circle around that and start looking at how you protect it.” But importantly, “Accept that you don’t need to protect everything and move from there.”

The real problem, he concludes, is that data is everywhere. “This really does expand the attack surface, so you have to use a logical, risk-based approach which considers the context of your business – how you achieve what you are trying to achieve – and then protect it.”

About SecurityWeek Cyber Insights | *At the end of 2022, SecurityWeek liaised with more than 300 cybersecurity experts from over 100 different organizations to gain insight into the security issues of today – and how these issues might evolve during 2023 and beyond. The result is more than a dozen features on subjects ranging from AI, quantum encryption, and*

attack surface management to venture capital, regulations, and criminal gangs.

Related: The Rise of Continuous Attack Surface Management

Related: Investors Bet on Cyberpion in Attack Surface Management Space

Related: IBM to Acquire Randori for Attack Surface Management Tech

Related: Attack Surface Management Play Censys Scores $35M Investment

Cyber Insights 2023: Attack Surface Management