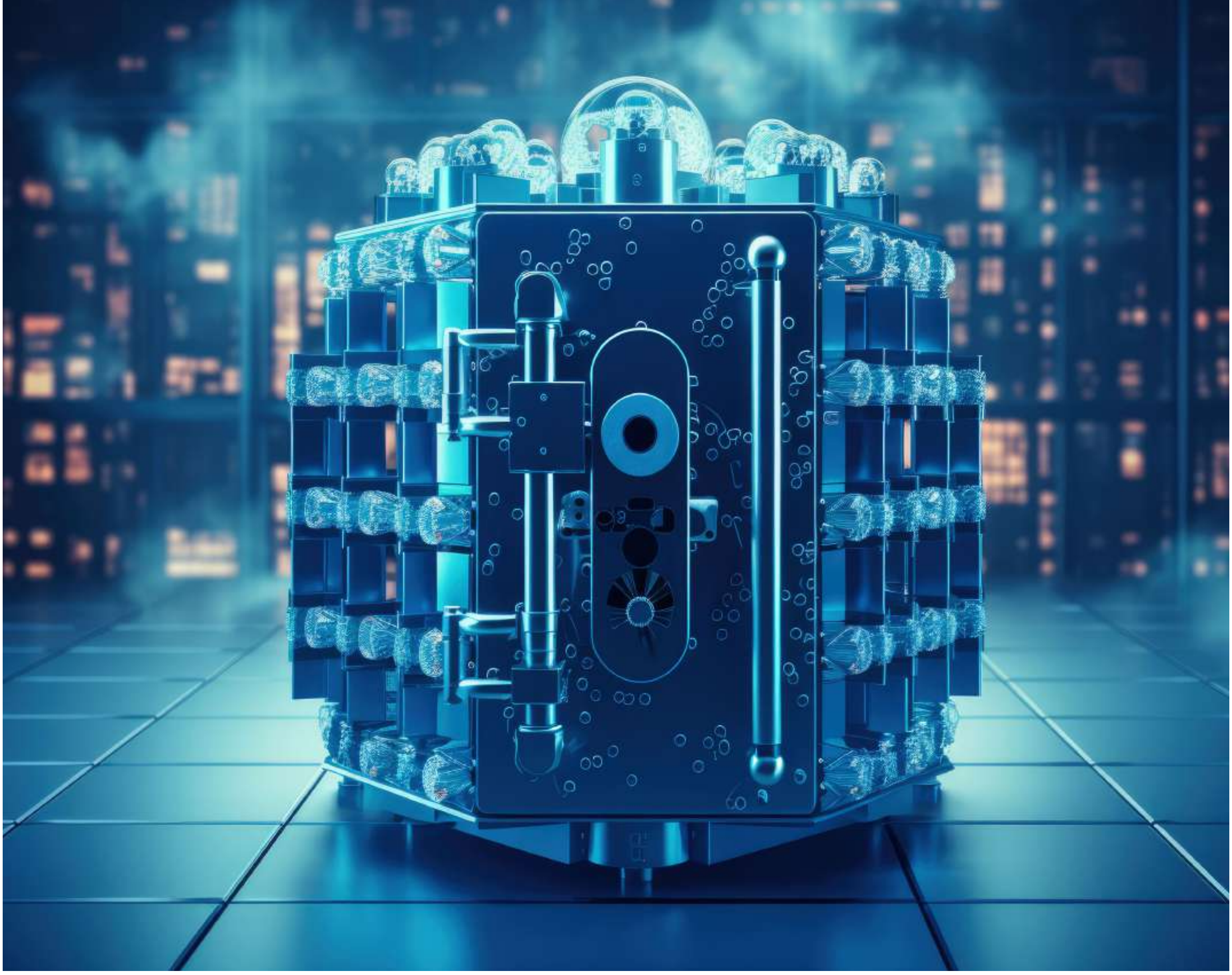
AUJAS
CYBERSECURITY
An NSEIT Company

aujas.com

Shielding your digital assets: The power of External Attack Surface Management

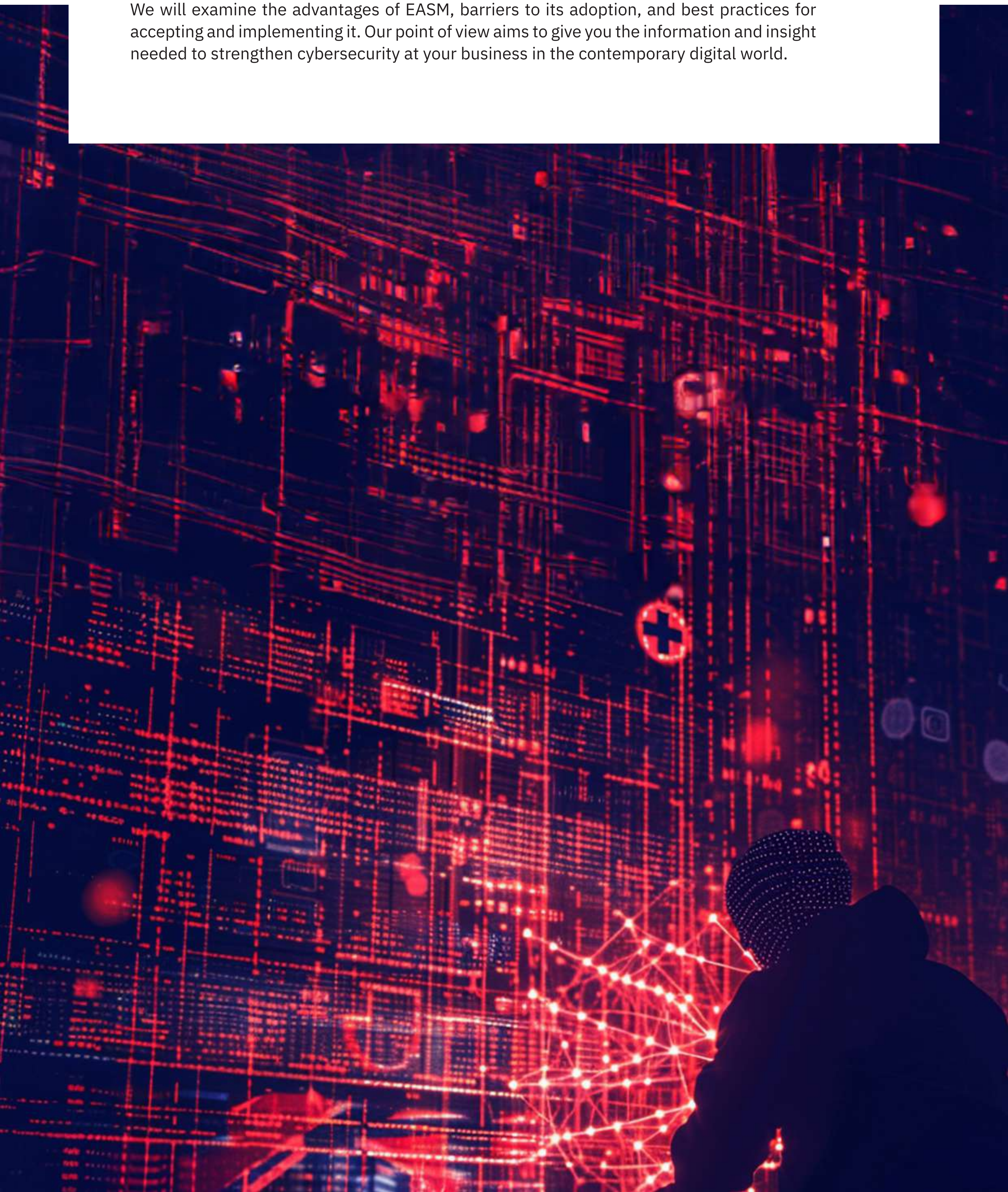
WHITEPAPER | SECURITY VERIFICATION SERVICES



Abstract

External Attack Surface Management (EASM) is a vital tool for organizations to protect their online vulnerabilities. This whitepaper looks at how important EASM is to modern cybersecurity strategies and how it helps businesses fight off cyber-attacks.

We will examine the advantages of EASM, barriers to its adoption, and best practices for accepting and implementing it. Our point of view aims to give you the information and insight needed to strengthen cybersecurity at your business in the contemporary digital world.



Introduction to the threat landscape

Digital transformation and emerging threats

Organizations that adopt digital technologies and move their processes and operations to the cloud for efficiency and scalability invariably expose themselves to cyber-attacks. Today, all digital assets, from cloud storage to cell phones and Internet of Things (IoT) devices, can be hacked if they are not secured adequately.

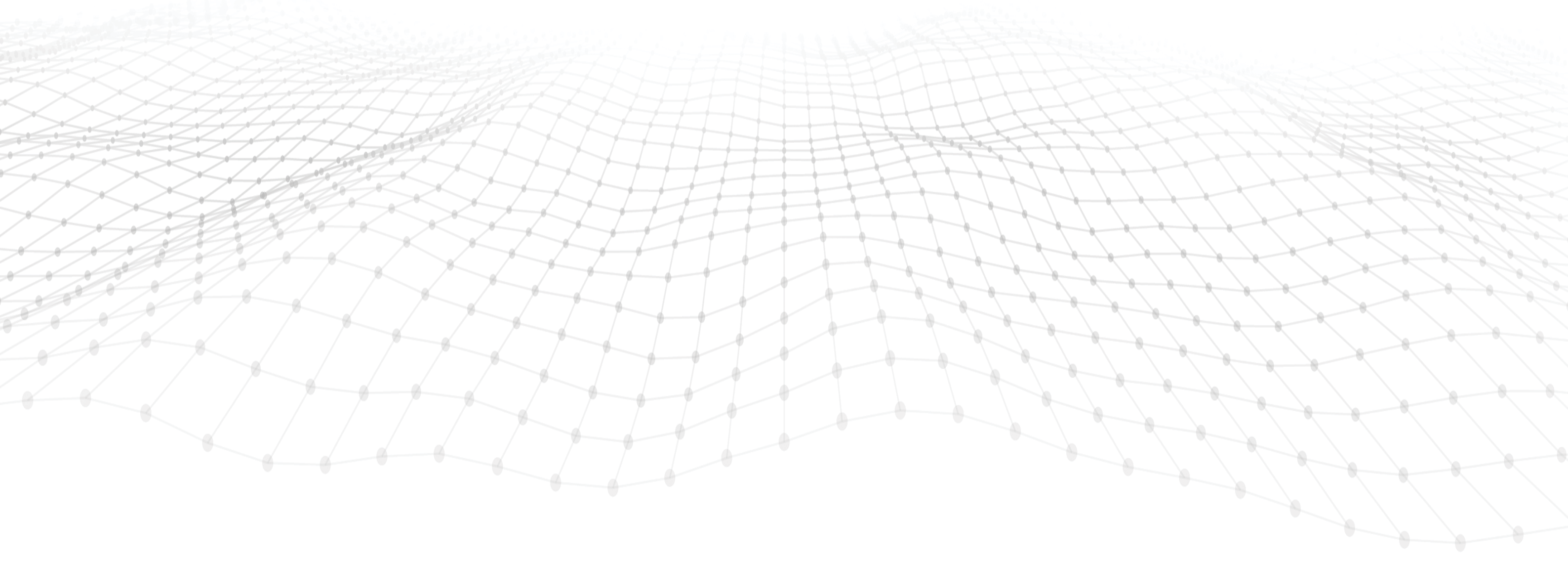
The hybrid work paradigm has made things more complicated. Besides securing their physical office technology, organizations must now deal with risks related to employees logging in from different locations. The increased digital footprint of the organizations and the corresponding threat surface make it easier for cybercriminals to exploit the weaknesses in the security system. Mergers and acquisitions (M&A) are another major activity that can lead to security vulnerabilities. The external assets from the acquired organization need a thorough and quick assessment and integration in such scenarios. The combination of different systems and data from various entities can create security gaps, providing cybercriminals with new chances to breach the network. It is important for organizations undergoing M&A to implement non-compromising security measures during their transition phases to protect the organization's digital infrastructure.

The logic is simple: as technology advances, so do the methods employed by those who seek to exploit it. Modern hackers, too, leverage technological advancements to their benefit. It is not uncommon to find hackers using Artificial Intelligence(AI) algorithms, among other things, to architect more sophisticated attacks. Malicious programs like ransomware and phishing schemes too have become smarter than ever before.

The importance of attack surface management

An 'Attack Surface' is a possible entry point, or attack vector, where an unauthorized user can access a system and extract data. As a business grows its online activities, its attack surface increases proportionately. Managing this attack surface well is essential to finding and fixing security weak spots before hackers can take advantage of them.

This involves keeping a constant check on all the ways data flows in and out of the organization and making sure these points remain secure. To achieve this, security teams must use tools that help them monitor attack surfaces in real-time. Regular checks for weak spots, strong protection for all devices, and solid overall network security are the main ways businesses can keep their digital doors locked to threats.



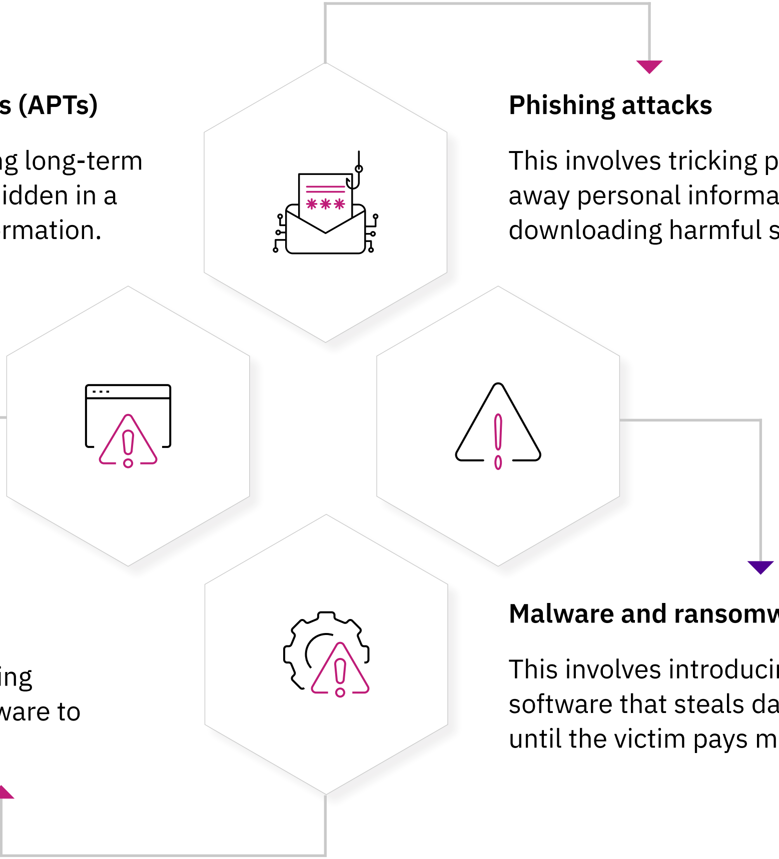
Analysing historical trends in cybersecurity vulnerabilities

- **Reporting vulnerabilities**

  In the past few years, the number of reported security problems, known as Common Vulnerabilities and Exposures (CVEs), has significantly increased. This improved reporting of CVEs shows that organizations are getting better at finding and reporting security issues. This knowledge and understanding of the known security issues is precious in preparing the defence for future threats. Organizations can study old data to see patterns in cybersecurity issues and predict new and emerging threats.

- **Cyber threats of today**

  With increasing awareness about cyber-attacks, hackers have changed their approaches and methodologies. They now use smarter methods like:



Advanced Persistent Threats (APTs)

This method involves planning long-term attacks where hackers stay hidden in a network to keep stealing information.

Phishing attacks

This involves tricking people into giving away personal information or downloading harmful software.

Exploiting software flaws

This method involves exploiting weaknesses in installed software to access systems.

Malware and ransomware

This involves introducing/installing bad software that steals data or blocks access until the victim pays money.

Understanding EASM

What is EASM?

EASM manages the digitally exposed threat/attack surface and safeguards the vulnerabilities creeping in through this exposure. It involves identifying, analysing, prioritizing, and mitigating vulnerabilities using various tools, solutions, approaches, techniques, and methodologies. The scope of the digital landscape or threat/attack surface includes websites, APIs, cloud services, employees of organizations, and network infrastructure.

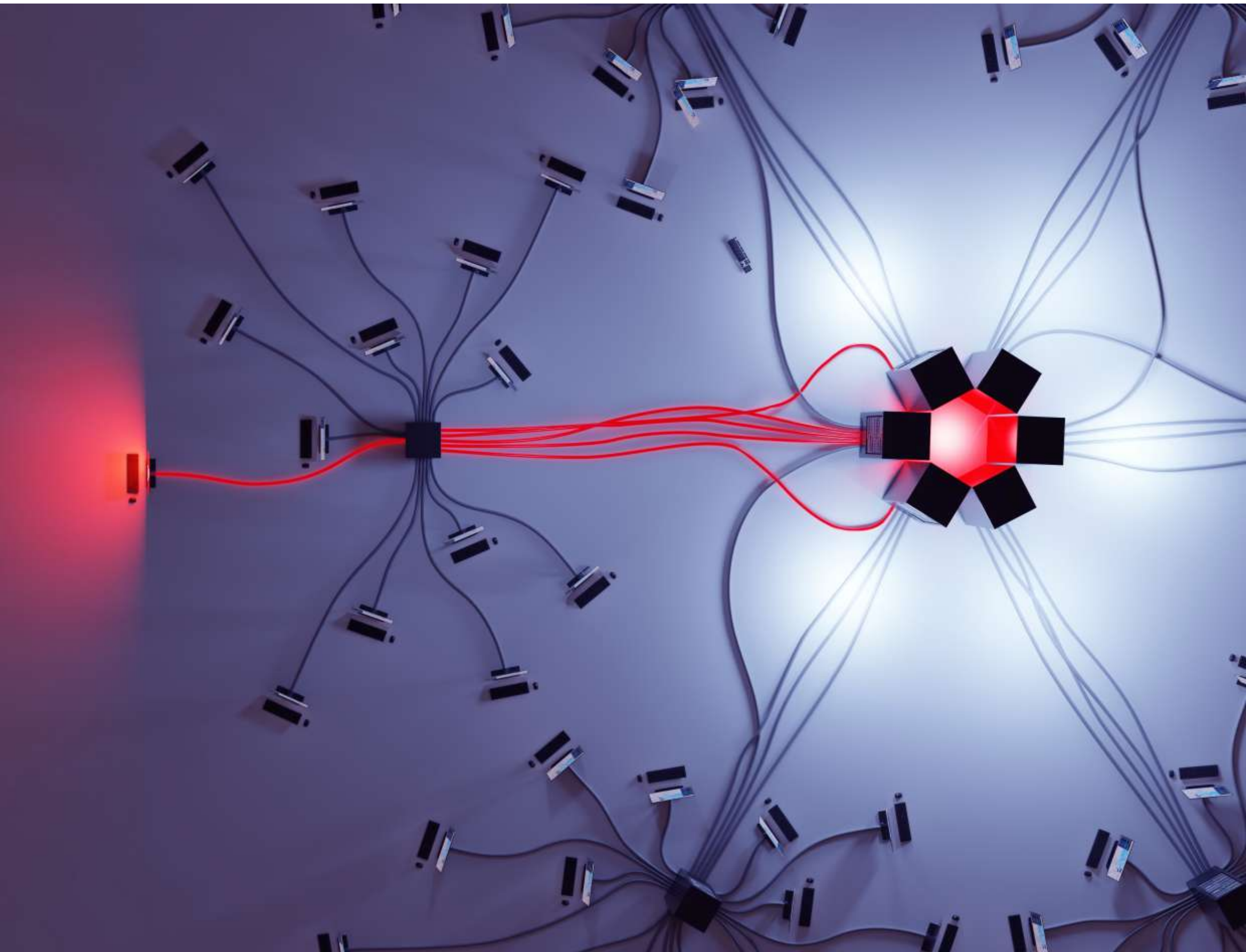
The reach of EASM

EASM covers every digital asset an organization has exposed to the outside world, whether on purpose or by accident. This scope includes all assets managed by the IT department, including known systems and software, as well as shadow IT assets—those systems and software that are used within the enterprise without the IT department’s approval or awareness. These systems and software pose significant risks and are potentially vulnerable (or exposed) to multiple vulnerabilities that can be exploited by hackers.

How EASM works?

EASM tools use scanning technology, threat intelligence, and predictive analytics to give a real-time picture of an organization’s external attack surface and foresee possible attack methods.

This disciplined, vigilant approach helps organizations defend against cyber threats effectively by maintaining a clear view of their vulnerabilities and taking swift, informed action to address them.



Key components and capabilities of EASM

EASM comes equipped with a suite of tools designed to give a clear view of your security landscape and provide proactive measures to strengthen your defences. Here’s how they work:

- **Reconnaissance and discovery**

  These solutions kick off their process with a thorough scan to identify all the digital assets of an organization, both those in plain sight and those hidden away, like unused applications or unauthorized IT projects. This discovery ensures that every part of your digital environment is known and monitored.

- **Asset definition and vulnerability identification**

  Once all assets are defined based on their types and criticality, the system scans for any vulnerabilities—these could be anything from outdated software to exposed data points. This step is crucial as it spots potential weak spots where attackers could break in.

- **Risk validation**

  After pinpointing the vulnerabilities, the next step is assessing how dangerous each one is. The system analyses each vulnerability and prioritizes them based on multiple factors, which include the type and criticality of the asset, the probable impact of identified vulnerabilities, and the ease of executing exploits.

- **Mitigation recommendations**

  With a clear understanding of the risks, the EASM system suggests specific actions to fix these vulnerabilities. Recommendations might include decommissioning a service/component, fixing misconfigurations, patching or updating components/systems, creating custom solutions, and implementing compensatory controls.

- **Real-time alerts on emerging risks**

  In a world where new risks can emerge from various sources, EASM solutions help you stay ahead with real-time alerts, providing immediate notifications about new threats. This allows an organization’s security team to act quickly and decisively to mitigate the following risks:

Shadow IT

Unauthorized systems and software can be introduced into the enterprise, bypassing IT department controls.

Cloud migration

Shifting to cloud infrastructure introduces new security challenges and risks that must be addressed.

Mergers and acquisitions

These bring in new assets and vulnerabilities that need to be quickly assessed and manage

Expanding remote workforce

An increasing number of remote workers can create additional entry points for potential threats.

By combining these capabilities, EASM solutions not only help organizations map out their security landscape but also enable them to act swiftly and efficiently, prioritizing security efforts and using resources wisely. This proactive approach minimizes vulnerabilities and keeps the digital infrastructure secure from potential threats.

Common mitigation techniques for managing external attack surfaces

Effectively managing an organization’s external attack surface involves a variety of strategies designed to reduce vulnerabilities and shield against threats. Here are some common approaches and best practices:

Prioritizing and categorizing attack vectors

A key aspect of EASM is a methodical approach to understanding and managing risks:

Risk scoring

Each vulnerability gets a score based on how severe it is, how complex it would be to exploit, and the potential impact on the organization. This scoring helps determine which issues need immediate action.

Contextual analysis

It is crucial to understand the setting of each vulnerability. For example, a small bug on a crucial server could be more threatening than a more severe issue on a less critical system.

Threat intelligence

Using detailed threat data from around the world that is specific to certain industries helps predict which vulnerabilities might be targeted next.

These steps help organizations focus their efforts where they’re needed most, ensuring that the most serious vulnerabilities are addressed first.

Mitigation techniques and best practices

To protect their external attack surfaces, organizations can use several effective techniques:

Risk scoring	Keeping software and systems updated is crucial to protect against known vulnerabilities.
Configuration management	Systems should be set up following security best practices to avoid configurations that could open vulnerabilities.
Access controls	By applying strict access controls and adhering to the principle of least privilege, organizations can ensure that individuals only have the access needed for their roles, reducing potential entry points for attackers.
Encryption	Encrypting data, both when it is being transmitted and when it is stored, ensures that sensitive information remains secure, even if other defences fail.
Network classification	By dividing the network into secured zones, it can be made harder for an attacker to move around the network if they do gain access.

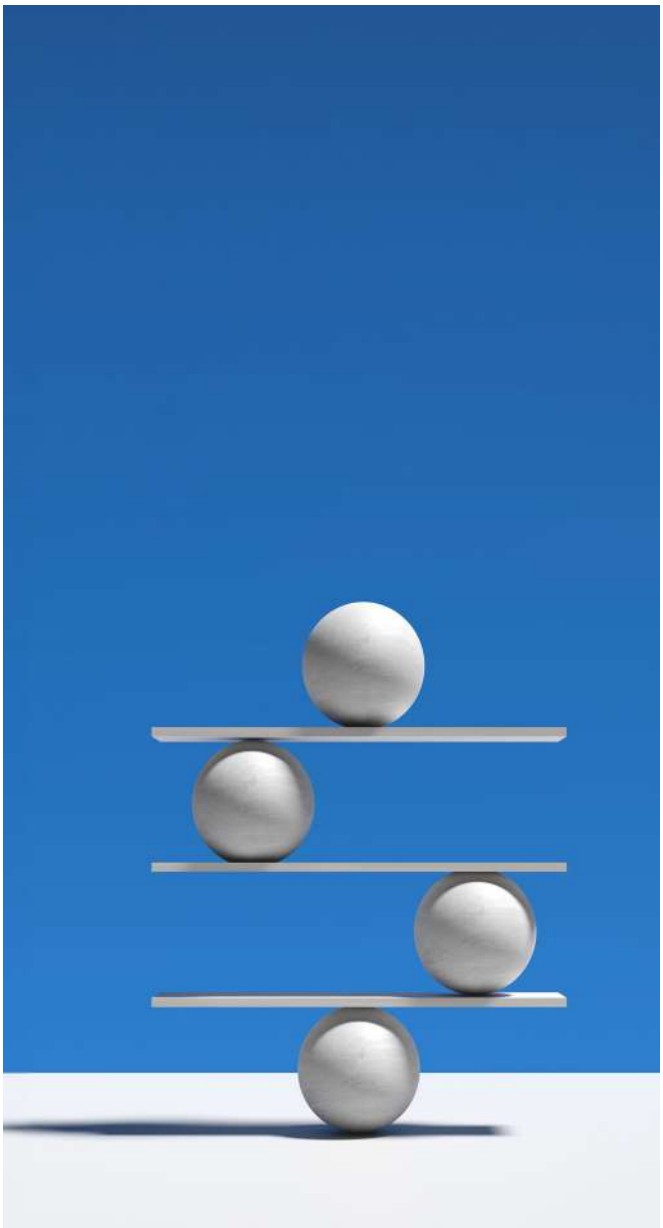
Alongside these techniques, continuous monitoring and regular security reviews are vital. They help ensure that an organization’s security keeps up with the changing tactics of attackers and that security measures remain robust and effective.

Challenges in the adoption of EASM

The adoption of External Attack Surface Management (EASM) brings substantial advantages to organizations yet implementing it can also pose a series of hurdles that need careful consideration. Here's a closer look at these challenges and how they can be effectively addressed:

Integration and compatibility issues

A key obstacle is integrating EASM solutions with the existing mix of old and new technologies within an organization's IT ecosystem. This blend can make it difficult to incorporate new tools seamlessly, potentially creating coverage gaps that diminish the overall security posture.



Scalability challenges

As organizations expand, so do their digital landscapes and the complexity of their IT infrastructures. An EASM system must be flexible enough to scale and adapt to incorporate new assets and meet changing security demands, a task that can be particularly demanding for multinational corporations with varied operations.

Regulatory compliance

Regulatory compliance is a crucial element of data management. EASM systems need to align with various data protection and privacy laws globally. This demands a thorough understanding of laws and frequently requires adjustments to the EASM system to follow compliance. This process often requires ongoing training for personnel, updates to security policies, and continuous compliance monitoring, adding complexity to the cybersecurity framework.

Budgetary limitations

Deploying a comprehensive EASM program requires significant resources, which can be a stumbling block, especially for smaller organizations. Balancing the costs of EASM solutions with other cybersecurity needs is a critical decision, requiring strategic resource allocation to optimize impact.

Continuous education and skill development

The field of cybersecurity is always changing, which means that practitioners must continually update their skills to handle new threats. To keep up, organizations need a solid plan for training these professionals. This involves getting buy-in from important stakeholders and consistently reviewing the threat landscape to make sure the organization is well-equipped to meet its security challenges.

Considerations before implementing EASM

It is vital for organizations to consider several factors to ensure a successful EASM implementation. These considerations are crucial in crafting a strong EASM framework that matches the organization's aims and enhances its security posture.

Thorough asset discovery

Creating a detailed inventory of all external digital assets is the cornerstone of effective EASM. It's essential for organizations to set up ongoing mechanisms to uncover and keep track of these assets. This process should encompass everything from widely recognized assets to less visible elements like shadow IT and forgotten resources, ensuring that every part of the digital footprint is accounted for.

Developing a risk assessment framework

Creating a risk assessment framework is crucial. It involves setting up a system to evaluate and categorize assets based on their criticality and vulnerability. This framework should feature detailed criteria to assess the potential impacts of a security breach and estimate the likelihood of different threats.

Continuous monitoring and quick incident response

A dynamic approach to monitoring the external attack surface is necessary to detect threats as they occur. Alongside this, an efficient incident response plan is crucial. This plan should enable the organization to quickly address vulnerabilities and security incidents, reducing potential damage and disruption.

Harmonious integration with existing security measures

EASM needs to integrate smoothly into the broader cybersecurity strategy rather than exist as an isolated system. It's crucial that any EASM tools implemented are compatible with current security protocols and practices to form a cohesive and robust defence system.

Stakeholder involvement

Getting key stakeholders involved is vital for EASM to be successfully adopted and effective. This involves gaining the support of top executives and making sure that IT, security, and operations teams are aligned and committed to the EASM objectives.

Addressing these areas thoughtfully will help establish a solid foundation for EASM, aligning it closely with the organization's objectives and security requirements.

How Aujas Cybersecurity can help?

Aujas Cybersecurity offers an EASM implementation approach and framework designed to support your organization's EASM efforts. Leveraging our domain and industry expertise, we help you address key challenges associated with EASM adoption, streamline security processes, and enhance your overall cybersecurity posture.

Comprehensive EASM services

We provide a range of services that cover the entire lifecycle of external attack surface management, including:

Risk management and compliance

We assist you in developing risk management frameworks that comply with relevant regulations and standards such as Sama, Tiber, CCPA, NYDFS, CERT-IN, etc., helping mitigate risks while ensuring compliance.

Threat intelligence and analysis

We integrate cutting-edge threat intelligence into EASM practices, providing you with insights into emerging threats and enabling proactive defence strategies.

Empowering clients with tailored tool selection

By thoroughly understanding the client's unique demands and requirements, we expertly guide organizations in selecting the most suitable tool from our extensive partner network. Our tailored approach ensures that the chosen solution aligns perfectly with the client's specific needs.

Risk-based vulnerability prioritization

We combine the attacker's perspective with business value, business impact, existing security controls, and remediation status to build a stack-ranked list of your most risky targets.

Integration and interoperability

Understanding the importance of seamless integration, we ensure that our EASM solutions are compatible with existing IT environments and security tools. This integration enhances the effectiveness of security measures without disrupting your current operations or requiring significant system overhauls. Our comprehensive services include asset discovery, vulnerability identification, and ticket creation to ensure the timely resolution of security issues.

Gap assessment

To maximize the return on investment for our clients, we conduct a thorough gap assessment of their Attack Surface Management processes. A comprehensive manual assessment complemented with the automated EASM platform assures identification of the misconfigurations and vulnerabilities in your external assets. By identifying areas for improvement, we work closely with organizations to optimize the tool's usage and unlock its full potential, ultimately enhancing its overall security posture.

Conclusion and recommendations

EASM has become a crucial element of contemporary cybersecurity strategies, especially as digital environments grow more complex and expansive. Implementing EASM equips organizations with the detailed visibility needed to proactively manage vulnerabilities and strengthen their defences against emerging cyber threats.

However, adopting EASM involves thoughtful consideration of several key areas: meticulous asset management, thorough risk assessment, and seamless integration of new solutions with existing systems. Additionally, organizations must navigate potential hurdles such as scalability, compliance with regulations, and ensuring compatibility across various technologies.

We strongly recommend that organizations consider collaborating with cybersecurity experts to address these intricacies. Expert guidance can greatly enhance the effectiveness of EASM implementations and ensure these systems adapt alongside organizational growth and shifts in the cybersecurity landscape. This strategic approach can bolster an organization's overall security stance, safeguard digital assets, and support its broader business goals.

By adhering to these recommendations and utilizing expert services, organizations can improve their capabilities to detect, analyse, and respond to external threats, thereby securing their operations against the diverse risks of the digital age.

About **Aujas Cybersecurity**

Aujas Cybersecurity -An NSEIT Company empowers clients with enhanced security resilience by minimizing the potential for attacks, threats, and risks. We specialize in architecture risk analysis, comprehensive threat modeling, rigorous penetration testing, and secure coding guidelines. By partnering with us, you can strengthen your security defenses and maintain a robust security posture.

For more information, visit us at www.aujas.com or write to us at contact@aujas.com.

Cupertino | Dallas | Jersey City | Ottawa | Riyadh | Dubai | Mumbai | New Delhi | Bangalore

Follow us at: