Qualys.

WHITEPAPER

External Attack Surface Management

Protecting your Organization from External Threats

Table of Contents

2 Table of Contents

3 Introduction

4 What is External Attack Surface Management?

4 Four Steps to EASM

4 Why Your Organization Needs EASM

5 Three Benefits of EASM

5 How to Implement EASM in Your Organization

5 Best Practices for EASM

7 Conclusion

Introduction

The relentless threat of cybercrime is forcing organizations to step up their game in protecting critical assets from malicious actors. One of the most effective ways of doing so is using External Attack Surface Management (EASM).

The security strategy of EASM is to find and protect internet-facing assets such as devices, web applications, ports and services. Such resources are secured from attack by automatically identifying and fixing vulnerabilities, or simply by closing ports or retiring legacy systems if no longer needed.

The benefits of an effective EASM strategy include better outside-in visibility, more safety and security, better compliance with industry regulations, better customer service, and more efficient operations.

Organizations that implement an EASM strategy are better prepared to identify and respond quickly to potentially crippling cyber threats or attacks.

What is External Attack Surface Management?

External Attack Surface Management (EASM) secures an organization's external-facing assets by proactively discovering, monitoring, assessing, and mitigating risks. Organizations can use EASM to identify and reduce risk associated with their external, internet-facing attack surface including endpoints, servers, web applications, cloud resources, and IoT.

By putting assets online, organizations are exposed to a wide range of risks. These risks can include data theft, ransomware, denial-of-service attacks, and unauthorized changes.

It is possible for an organization to reduce the risks associated with the external attack surface if stakeholders understand the risks and associated measures that can reduce those risks.

Four Steps to EASM

EASM uses a continuous, automated process of four steps: Discover, Assess, Prioritize, and Eliminate.

Discover

Discovery is the first step of EASM: Identifying all external, internet-facing assets that are exposed to the outside world. The adage, "You can't secure what you don't know exists," is a vital concept for EASM. Most vulnerability management programs fail due to blind spots in a modern hybrid environment.

Continuous Assessment

To ensure that your assets are protected, it is imperative to identify cyber risks such as vulnerabilities, unsanctioned exposed ports, expired certificates, and End-of-Life (EoL) or End-of-Service (EoS) applications. Such externally facing risks may be exploited by hackers to gain access to sensitive data or disrupt the functionality of enterprise IT systems.

Risk Prioritization

Analyze and prioritize the likelihood of a vulnerability exploit, risk of outdated software and exposed ports to the internet, or to minimize the impact of a successful exploit.

Risk Elimination

There are several risk elimination strategies stakeholders can use to eliminate the risk associated with a high-level or exploitable vulnerability. Common such strategies include automatically patching software vulnerabilities, closing the risky opened ports, installing virus scanners, automatically shutting down unprotected or unauthorized services, or removing the affected device or software.

Why Your Organization Needs EASM

According to a recent study conducted by Enterprise Strategy Group - **22% of respondents said the attack surface of their organizations has increased significantly in the past two years.**

By identifying and mitigating threats to your systems and data with an external attack surface management program, organizations get an outside-in perspective on what an attacker sees. Such focused intelligence and automated response playbooks will help your organization stay protected from cyber threats.

From a strategic perspective, reducing your organization's cyber risk helps prevent costly downtime, data loss, and reputational damage.

Three Benefits of EASM

There are several benefits your organization can obtain from an external attack surface management (EASM) solution, including:

1. **Better Security Posture**
   An EASM solution can automatically identify and fix vulnerabilities in your externally facing systems and applications, which in turn can help improve the overall security posture of your organization.

2. **Less Exposure to Cyber Threats**
   An EASM solution can help minimize your organization's exposure to cyber threats by identifying and reducing vulnerabilities in externally facing systems, applications, misconfigured ports, unintended databases/buckets or storage devices exposed to the internet. EASM also helps identify applications and systems no longer needed by the organization, which are assets that may be used as attack vectors.

3. **Cost Savings & Improved Efficiency**
   Deploying an EASM solution natively integrated with an application security and vulnerability management platform can orchestrate remediation workflows, reduce the time and effort required to resolve a security breach, and increase efficiency and productivity among IT, security, and compliance teams. The overall result is more efficiency and lower total cost of ownership.

How to Implement EASM in Your Organization

External Attack Surface Management can be implemented in various ways depending on the size and complexity of an organization and its IT infrastructure. The most common approach to identifying and assessing risks across the organization's externally facing digital assets is with a purpose-built EASM software solution. For example, Qualys CyberSecurity Asset Management, with natively integrated EASM is an industry-leading solution to automate the discovery, assessment, and analysis of those risks.

Best Practices for EASM

As your business grows, so does your online presence. Unprotected externally facing exposure increases the likelihood of cyber criminals targeting your digital assets with potentially huge fallout. Fortunately, the use of an EASM strategy and solution will help you reduce exposure to these threats and protect your organization's digital assets.

Here are four best practices for managing your digital assets with EASM:

Build an Inventory

There are several important steps before you begin the process of discovering and protecting assets that are exposed externally, including: getting a full inventory of all devices, online properties, subsidiaries, acquired companies, and their associated assets across all your relevant geographical locations. There are various types of assets in most organizations today -- cloud resources, dynamic changes, and containers, to name a few -- so inventory processes must keep pace with these constantly changing environments.

Identify Potential Risks

Establish a scoring and prioritization system for ranking risk and addressing the most critical issue once you have an inventory. IT/security teams should spend their time efficiently, as most organizations are not able to simply take care of all vulnerabilities and misconfigurations at once.

Also determine who owns and maintains these assets, so when issues arise, you can alert the appropriate team. It is more effective if you communicate quickly and accurately with the right individuals on the right teams in order to reduce the mean-time-to-remediate (MTTR).

Use Proactive Security Measures

To ensure that your organization's assets are protected against potential threats, you need to use proactive security measures. Regularly update and test proactive security measures to ensure they are effective against the latest threats. Examples of these measures include asset hygiene, patching cadences, employee training, firewalls, endpoint monitoring, intrusion detection and prevention systems, and encryption technologies.

Implement Security Policies and Procedures

The importance of digital asset security cannot be overstated. Establish a set of clear security policies and procedures that ensure everyone in your organization is aware of the importance of digital asset security. A major part of EASM is prioritizing vulnerabilities and assets based on their risk and business criticality. The implementation should deploy solutions that natively integrate EASM with a platform like Qualys VMDR, which provides an all-encompassing risk-based vulnerability management solution.

EASM provides the means to help teams effectively manage digital assets. Employing its best practices allows stakeholders to significantly reduce an organization's chances of being exploited by cyber criminals. The best practices also ease the process of controlling your organization's external attack surface.

Conclusion

The goal of an external attack surface management program is to safeguard your company's future by reducing the chances of an attack via vulnerabilities in its external attack surface.

An organization's ability to manage its external attack surface is crucial in today's competitive environment. Controlling and reducing those risks requires having the right knowledge and tools at your disposal to identify potential security threats, correct vulnerabilities in vital assets, and respond to threats in a timely manner.

As a leader in the integrated security industry, Qualys is a great choice to consider for your organization. Qualys natively integrates vulnerability management, patching, compliance, and EASM into a single platform, resulting in comprehensive security protection and comprehensive cyber risk reduction. The integrated platform allows you to automatically orchestrate remediation workflows, reduce the time and effort required to resolve a security breach, and increases efficiency and productivity of IT, security, and compliance teams, and lower the total cost of ownership.