Scrut Automation

Key Attack Surface Challenges Cloud-Native Companies Are Facing Today

Scrut Automation

Contents

Scrut Automation

Introduction

In recent years, companies have been adopting cloud-native technologies in their business models due to their ability to enable businesses to achieve agility, maximize flexibility, minimize operational costs, and automation of services. Cloud-native technologies can be defined as a standard for building cloud-based applications through a set of technologies and design patterns.

This enables the technology to support thousands of concurrent users without system and hardware failures, as well as prevention of malicious attacks. The most popular technology is on-demand computing resources such as mobile applications, data management tools, the internet of things (IoT), and the telecom market landscape.

Cloud-native technologies are bringing convenience to companies, but there are several risks, such as attack surface, that are threatening their adoption. The main concerns with these attacks include data stealing, malware injections, wrapping attacks, authentication attacks, denial of service attacks, and data privacy.

Even though it is the duty of the provider to improve their security measures in order to win their customers' complete trust, the users must be informed of the dangers associated with utilizing these technologies.

58%
say the growing volume of APIs in modern cloud-native apps is **causing them problems**

67%
say DevOps is responsible for choosing networking and security solutions

70%
of companies with high levels of deployment automation test security at least daily

86%
say their organization is actively using or has **started using cloud-native apps today**

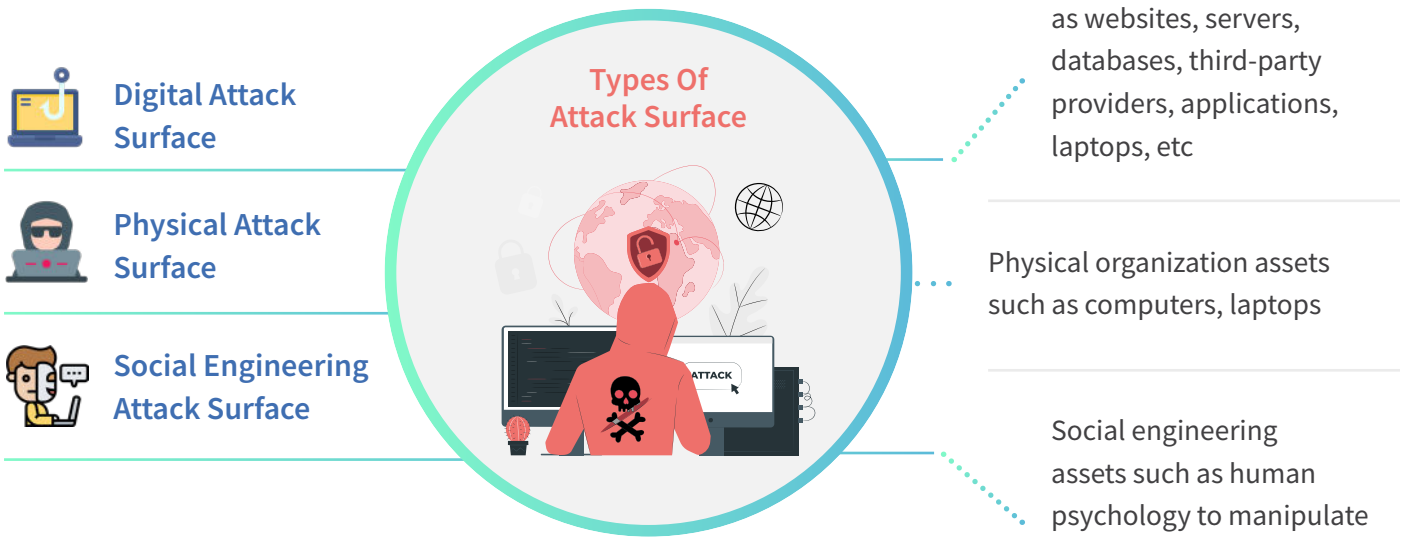
Sources:
https://businessinsights.bitdefender.com/organizations-adopting-cloud-native-apps-struggle-with-security-issues-stemming-from-api-sprawl-survey-shows
https://www.nutanix.com/theforecastbynutanix/news/cloud-native-application-security-concerns-and-tools

How Expanding Attack Surface Puts Organizations At Risk

Organizations are continuously benefitting from the rapid change in the technological ecosystem that is making production easier. However, the challenges of protecting organizations from expanding attack surface are increasing.

Attack surface are the external vulnerabilities that an unauthorized person can use to access organizations' systems. In simple terms, it is the number of known and unknown potential security risks across all organization systems, from software and hardware to networks. The attack surface affect different areas of organizations, which can easily cripple their operations. This may include email inboxes, mobile applications, websites, cloud services, or even logistics management tools. Protecting the cloud services should be the priority of organizations to ensure they keep the number of attack surface to a minimum.

There are different ways that expanding attack surface puts organizations at risk today, and this can be clearer if the attack surface are broken into the following types: Digital Attack Surface, Physical Attack Surface, and Social Engineering Attack Surface.



Digital Attack Surface

Most organizations today depend on internet connections to carry on with their business. These, however, puts organizations at risk since any hacker with an internet connection can access organization systems by capitalizing on poor cybersecurity measures. The main components used to implement these include websites, servers, databases, third-party providers, applications, and laptops, to name a few. The more devices an organization is connected to, the larger the digital attack surface.

Moreover, these attacks can be enhanced by weak passwords, misconfiguration, internet-facing assets, shared databases and directories, outdated devices, and Shadow IT. Organizations at times use weak passwords or easy-to-guess passwords, thus giving hackers an easy time accessing their systems. Misconfigurations occur when ports, network channels, and firewall protocols are misconfigured, allowing hackers to intercept organization communication systems. Internet-facing assets involve web applications and servers which, when not well-manned, can be manipulated to divulge or destroy sensitive data.

Physical Attack Surface

These are attack surface that can only be implemented using physical organization assets such as computers, laptops, and any physical component. When an attacker accesses an organization's physical assets, it is easy for them to implement their attack without needing internet access. This can occur through device theft, insiders, and baiting. Device theft is where an attacker may break into an organization and steal some of the physical components that he/she may need to infiltrate an attack.

Baiting is an instance where an attacker may leave a certain device, such as a USB flash drive, in a public place to bait an employee in an organization into plugging it into an organization's computers and thus downloading malware unintentionally. An insider can as well be used to plant some malicious software into an organization's system to enable an attack.

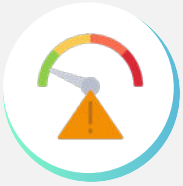
Social Engineering Attack Surface

These are attacks that are implemented by using psychology to manipulate victims into doing what should not be done. This may include sharing information that should not be shared, downloading applications that should not be downloaded, or even visiting some dangerous websites. In general, social engineering attack surfaces use human ignorance or lack of knowledge of how attack surface are implemented.

These attack surface generally affect authorized persons in an organization who are susceptible to social engineering attack surface. The most popular method used in these attacks is **phishing**. This is where victims receive messages, emails, or calls from scammers who impersonate trusted organizations or government officials and have the victims download or disclose sensitive information to them.

The Importance Of Attack Surface Management (ASM)

Attack surface management is the continuous measures put in place to manage all the blind spots that hackers utilize to gain access to organizations' systems. Most organizations at one point in time have experienced attacks that started by the exploitation of unknown or known unmanaged internet-facing assets. Attack surface management (ASM) is important to organizations in the following ways:

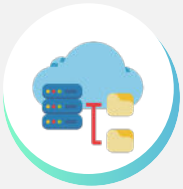


Risk Reduction

Employs hackers' approach

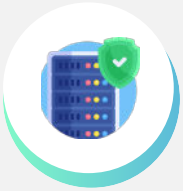
Data Protection

Strong authentication procedures



Cloud Governance

Robust cloud management infrastructure



Subsidiary Risk Assessment

Subsidiary level surface attack segmentation

Reduction Of Risks

Through ASM, organizations can map their digital footprints and enable them to identify the potential vulnerabilities that can be used maliciously and seal them. This can be achieved by actively monitoring organization systems to identify all new and make sure that the old threats are managed. Most of the time, it begins by continuously updating the inventory of the organization's internet-facing IT assets. This method is known as the **Hackers' Approach**, where one can discover all the known and hidden threats.

When the risk is discovered, the assets are continuously monitored to manage the risk of being a potential attack vector. The security team can further take short-term actions to mitigate these threats among the actions including strengthening passwords, deactivating applications that are no longer in use in the organizations, OS patches, user training on phishing, and installing user biometric access to systems, and finally, revising security controls around the company system usage and maintenance.

Hackers' Approach:

Data Protection

Through ASM, organizations can identify potential threats in the storage and data transfer systems in time. An example is the financial or data information of the organization that does not have enough security measures in place to protect it. Through ASM, upon discovery, they can create more secure data management tools with enough authentication procedures for those who have access to this data. Organizations can consider implementing two-factor authentication procedures, which are more secure and reliable.

Cloud Governance

There are hundreds of unknown cloud services that organizations cannot be familiar with but through ASM ecosystem shadow, IT manifested can easily be managed. Through ASM, this problem is managed by systematically putting in place measures that better manage the cloud infrastructure within an organization.

Subsidiary Risk Assessment

It has been difficult for security teams in organizations to keep up with the required security standards in organizations. However, through ASM, teams can easily segment attacks surface per subsidiary and easily solve the problem. Additionally, the ASM comes with a self-service model that allows security teams to have full control of the system and add new assets in accordance with the attack surface identified.

It is worth noting that the attack surface threat is a wide topic that even security operations team have their limitations in resources and skillsets. This, therefore, cannot be exhausted or managed at once, but with consistent monitoring of vulnerabilities, these challenges can be kept to the minimum.

DID YOU KNOW?

Several tools have been put in place to help solve this problem, including Vulnerability Management (VM), Cyber Asset Attack Surface management (CAASM), Cloud Access Security Broker (CASB), Cloud Security Poster Management (CSPM), and Security Rating Services (SRS).

It should be noted that these are not complete solutions to every threat that an organization may face. According to research, ASM tools can only detect 30% more than the IT teams in organizations. To enhance efficiency, the ASM tools usually combine their efforts with other threat identification software to supplement their accuracy and thus manage otherwise unknown blind spots.

Attack Surface Management Tools And The Rise Of CAASM Solutions

Attack surface management tools work hand in hand with ASM to mitigate attacks. ASM seamlessly integrates with the management tools and the existing security stack to supplement and complement each tool's tasks in threat detection.

ASM Tools

Vulnerability Management (VM)

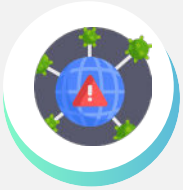
Finds threats within the software and code-based systems

Cloud Security Poster Management (CSPM)

Identifying misconfiguration issues and compliance risks in the cloud

Security Rating Services (SRS)

Provides continuous, independent quantitative security analysis and scoring for organizational entities



Cyber Asset Attack Surface Management (CAASM)

Focused on enabling security teams to solve persistent asset visibility and vulnerability challenges

The main attack surface management tools are as follows:

1. Vulnerability Management (VM)

This tool tries to enumerate the tactics, techniques, and procedures used by real-world attackers. This helps to understand the types of risks the systems are facing and thus offers light into the effectiveness of the existing security measures and pitfalls within them. The main purpose of this tool is to find threats within the software and code-based systems and thus address the company's cyber health. This tool works together with ASM to examine the internal and external security of a company in all corners of its internet environment.

2. Cloud Security Poster Management (CSPM)

The main purpose of this tool is to identify any form of misconfiguration issues and compliance risks in the cloud. CSPM is a security product aiming to automate security and provide compliance assurance in the cloud. It works in a way that it examines the system and then compares its performance with a given compliance cloud standards. This tool mainly applies to institutions that have already adopted a cloud-first approach

and have interests in extending their security to hybrid and multi-cloud environments. In a typical enterprise cloud, the environment is complex and fluid since there are thousands of instances and accounts, and thus, managing it is only possible through tools such as CSPM. Without this automation, the misconfigurations arising as a result of this complexity may remain undetected for a long putting organizations at risk.

3. Security Rating Services (SRS)

According to this Gartner report, "Security Rating Services (SRS) is a tool that provides continuous, independent quantitative security analysis and scoring for organizational entities. The services gather data from a variety of public and private sources via passive and active (but non-intrusive) means, analyze the data using proprietary analysis and rate the entities using their standard scoring methodologies." The main purpose of this tool is to tell how likely a system will be infiltrated.

4. Cyber Asset Attack Surface Management (CAASM)

According to Gartner report, CAASM "(CAASM) is an emerging technology focused on enabling security teams to solve persistent asset visibility and vulnerability challenges.

CAASM enables organizations to see all assets (both internal and external) through API integrations with existing tools, a query against the consolidated data, identify the scope of vulnerabilities and gaps in security controls, and remediate issues." The threat landscape is continuously changing and thus putting organizations at a major risk. This, however, has been made easier due to the availability of CAASM. The sole aim of this tool is to make sure that the challenges faced by organizations, such as data loss, among other challenges, are dealt with in one single instance.

Scrut Automation

The Benefits, Value, And Example Use Cases Of A CAASM Solution

Organizations are continuously evolving in terms of security and dynamism, especially in cloud applications, digital supply chains, social media, and open-source codes. However, this has led to expanding attack surface, making them vulnerable to threats and making it difficult to manage their assets. This means that organizations must look beyond the traditional methods of threat protection and use the most robust and new methods to protect their customers as well as their assets. This is where the CAASM solution comes in since it bridges this gap by providing an accurate, near real-time view of all organizational assets to ensure robust cyber resilience. The following are among the benefits and values that organizations can enjoy by taking advantage of this tool:

Explicit visibility of organization cloud resources

One of the main challenges in managing an organization is securing cloud resources, which is among the main challenges with a public cloud. CASM solutions createa solution that diversifies assets to consolidate both cloud and SaaS assets in one location where the IT team can easily access and gain visibility.

Fast risk detection and response

The sole purpose of a CAASM is to detect security threats across cyber assets and respond within the shortest time possible. A CAASM platform can achieve this and additionally allows one to investigate resources visually, and once a query is sent, an instant response is received.

Eases the IT department's hassle in managing compliance and improving cyber resilience

At times, automation makes things harder than they were expected by the IT teams. However, CAASM platforms have automated the compliance checks allowing the usage of conformance packs upon which it allows the use of rules to automate security and compliance to the best practices.

Improving productivity

The main aim of CAASM is to simplify the challenge of gaining and maintaining full control and visibility of company digital assets in a unified area. Since CAASM can easily detect and respond to security threats, a benchmark is set to allow the IT team to focus on other tasks to improve the security of the cyber assets. This saves time, which would otherwise be used on the tasks that CAASM easily undertakes.

Using Scrut Automation To Secure Attack Surface And Monitor Risks

Cloud is the new trend that companies are taking to store their assets, but they need to be aware of the challenges that come with it, such as attack surfaces. More than 60% of the companies that have already shifted to this trend have increased their security risks unknowingly. Shifting to this trend creates vulnerabilities that malicious users can exploit to harm the company. It is for this reason, companies must understand the threats and solutions to the threats of adopting the cloud company system. They must, therefore, be willing to secure their assets in the best way possible by the utilization of the new technologies discussed above.

In particular, Scrut offers complete visibility into cyber assets and helps manage infosec risks on a single platform. Organizations can use Scrut to automate their risk assessment and gain the confidence of potential customers by showcasing a strong security posture using customized, easy-to-build auto-populated security pages.

Click here to learn more about how you can use Scrut Automation security platform to gain complete visibility into your cyber asset universe, automate risk assessment of attack surfaces, and develop/ implement a risk treatment plan that accepts, mitigates, transfers, or avoids each detected risk.