Scrut Automation

A Beginner's Guide To Cyber Asset Attack Surface Management (CAASM)

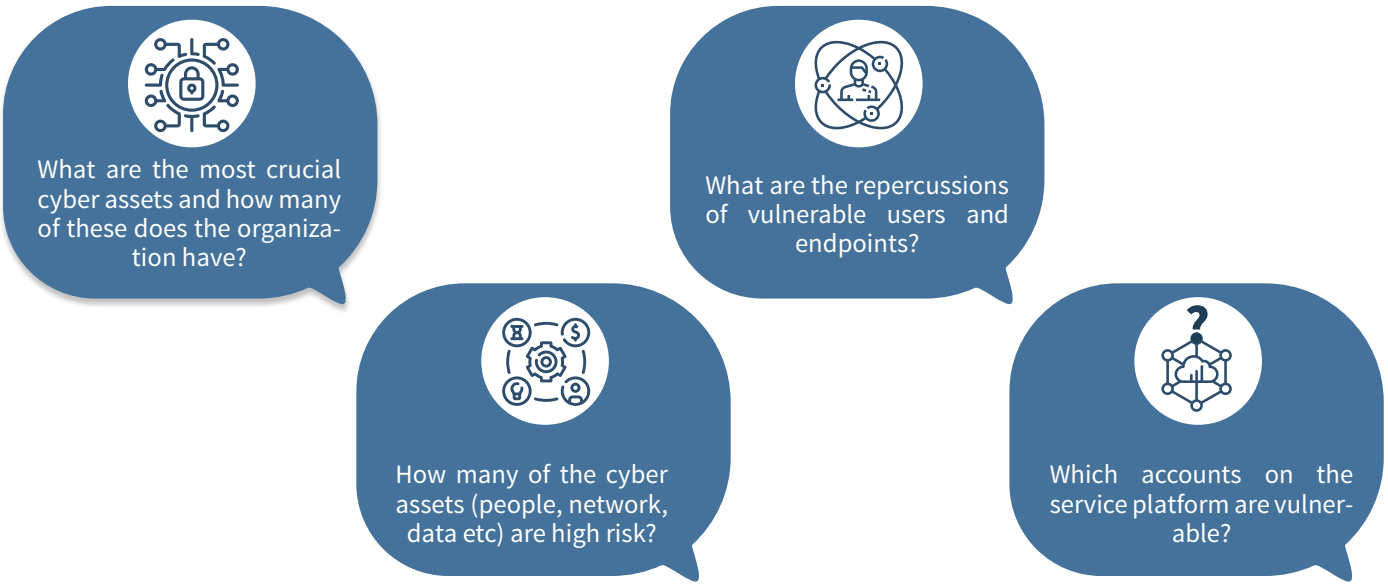
Scrut Automation

Contents

Abstract

The modernization of legacy platforms and the proliferation of **cloud-native** digital transformation initiatives enhance business continuity. It also boosts productivity by leveraging data to drive better business outcomes. But these benefits come at a cost. The swift digital transformation also means an expansion of the cyber asset universe. The more cyber assets, the more the attack surfaces through which cybercriminals can breach networks and systems.

IT, security and cloud teams are struggling to answer even the most common questions about their cloud environment, cyber assets and attack surface. Furthermore, increased attack surfaces make it harder for security teams to detect, investigate, and understand the full scope of a data breach.



This ebook introduces the concept of attack surface management. It also explains how security teams can profit from using **Cyber Asset Attack Surface Management (CAASM) solutions.**

Scrut Automation

CHAPTER 1

Understanding attack surface management

A Gartner report shows that attack surface expansion is today's number one trend in security and risk management.

Modern organizations have several evolving potential entry points (vulnerabilities, pathways, or methods). Through these points, attackers can gain unauthorized access. Thereby exploiting user identities, endpoints, devices, code repositories, networks, cloud workloads, software, etc.

This is due to an ever-evolving and expanding cyber assets universe, which translates into a growing number of attack surfaces. Countering this dangerous trend requires organizations to evolve security strategies and practices. They should check their digital inventory and ensure visibility into the many attack surfaces. Organizations should also proactively mitigate cyber risks before they are exploited.

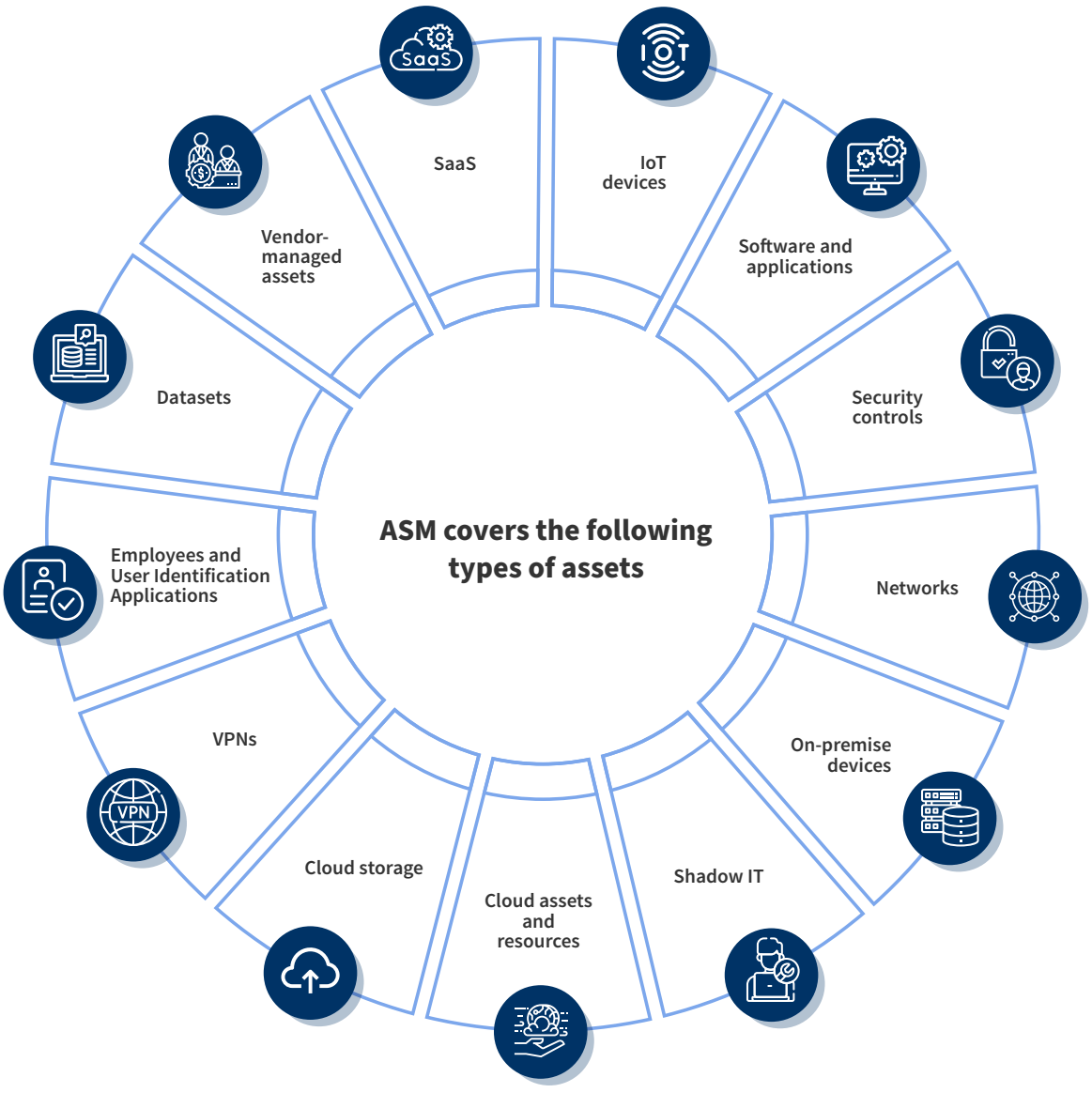
As such, enterprises need to achieve effective risk prioritization and asset visibility. They also need to ensure security control over their entire attack surface. This is where attack surface management comes in.

What is attack surface management?

Attack surface management (ASM) describes the continuous monitoring, discovery, inventory, and classification of attack surfaces within an organization's IT infrastructure.

Did you know?

This approach enables security teams to cover all IT assets vulnerable to malicious attackers. Either from the enterprise networks, through the internet, or third-party providers. It changes security thinking from a defense-oriented point of view to that of an attacker. This reorientation places security teams in a better position to expect and focus on vulnerable attack surface areas.

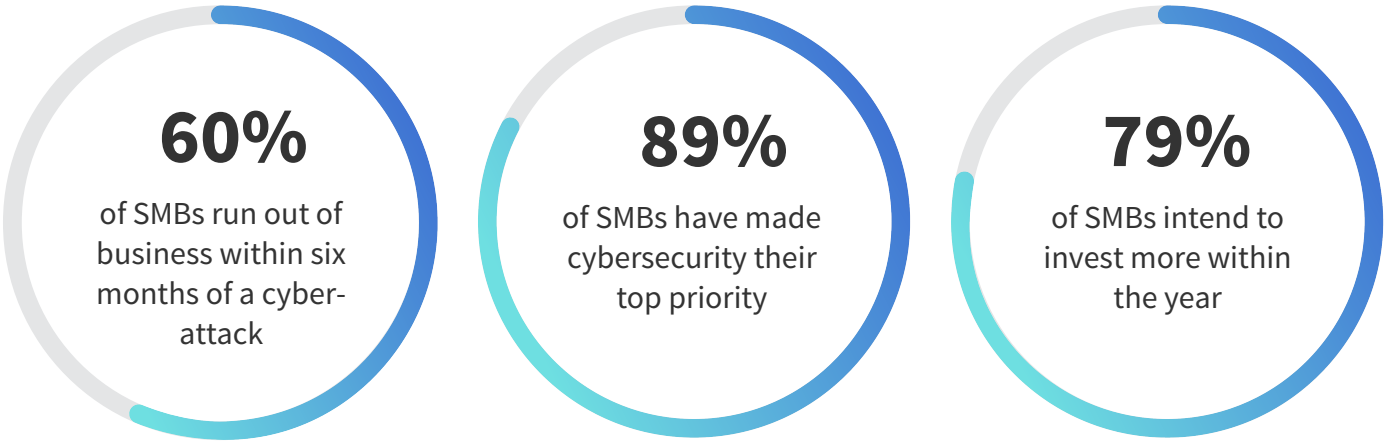


The sheer volume, complexity, and diversity of corporate IT assets make it challenging for cybersecurity teams to manage, track and protect attack surfaces. The prevalence of shadow IT is even more worrisome to security teams. Research shows that 69% of organizations have suffered an attack that targeted an unmanaged or unknown internet asset.

The average company has 975 unknown cloud services, and estimates show that shadow IT cloud usage is 10x the size of known cloud usage.

Did you know?

Even startups and SMBs aren't immune to the large explosion of attack surfaces. SMBs, more than ever, now rely on information technology, mobility, IoT, and the internet to power their businesses. With this evolution and hypergrowth comes an explosion in attack surfaces. Unfortunately, the costs of a security breach are high, especially for SMBS. The average data breach cost in an SMB is ~$120,000 per incident.



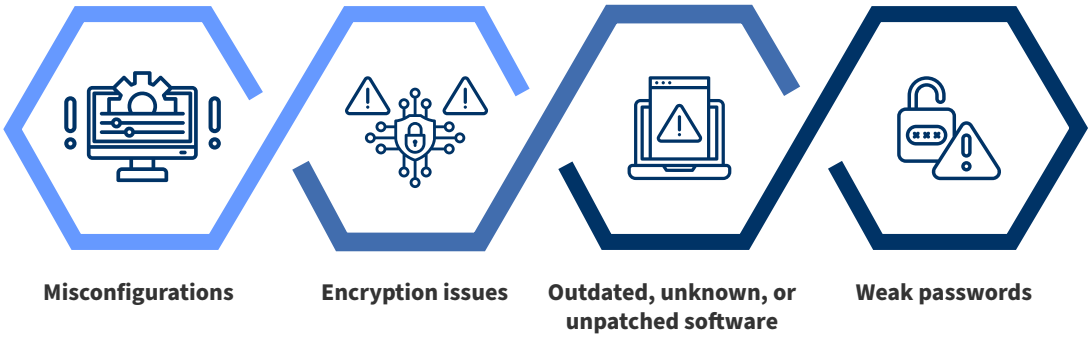
Sources: unbrokerage, cyberhub.allot

SMBs are primary targets for cyberattacks. A 2019 Verizon report showed that 43% of all cyberattacks target SMBs, with 63% of the attempts being successful. According to a Ponemon Institute report, 67% of SMBs experienced a cyberattack, and 58% experienced a data breach in 2018 globally.

CHAPTER 2

The benefits of attack surface management

Most cybersecurity strategies focus on identifying, classifying, and protecting digital assets. Attack surface management automates these activities and extends coverage to IT assets. Including those outside the safety net provided by traditional firewall and endpoint protection controls. It reduces the possibility of cyber breaches and prevents security control failures. It achieves this by providing real-time vulnerability management and attack surface analysis. ASM checks for potential attack vectors, such as



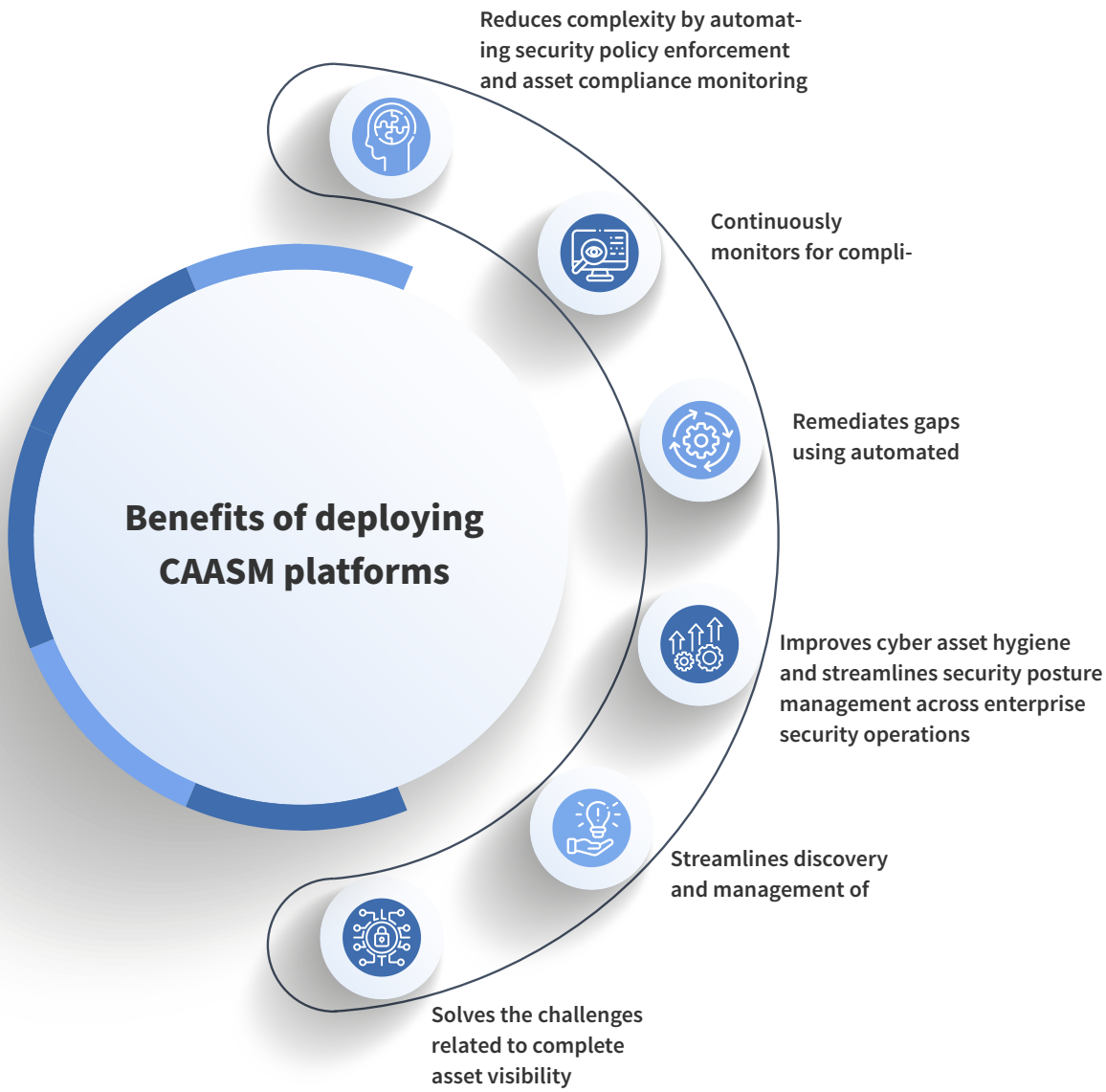
Vulnerability checks and penetration tests show how cybercriminals could launch an attack. These tests are done in controlled environments or on specific sections of IT infrastructure. As such, these tests have limited benefits since modern IT environments continue to evolve and expand. As a result, most assets and attack surfaces could go unnoticed and stay under the radar of even the most rigorous cybersecurity scrutiny.

ASM helps security teams to identify high-risk vulnerabilities, non-compliant controls, security coverage gaps, and shadow IT. It also helps to deploy the best countermeasures to safeguard their assets. Thereby quickly shutting down exposed databases and APIs, unknown and orphaned apps, shadow IT assets, and other exploitable entry points. These actions mitigate the threat of a breach.

Users gain a deeper understanding of the location of all exploitable assets in their IT ecosystem. They also identify the interconnection that exists between them. Such automated asset intelligence teams enable incident response teams to focus remediation efforts on exactly where it's needed.

Making ASM a top priority helps you improve asset visibility. It also helps uncover an array of unprotected data, EOS/EOL software, exposed APIs, expired certificates, misconfigurations, bad code, etc.

Comprehensive attack surface management includes an accurate, real-time inventory of all IT assets. This includes risk assessment, security controls, and other risk mitigation measures. Core ASM capabilities such as digital risk protection, external attack surface management, and cyber asset attack surface management can help security teams achieve this.


Benefits of deploying CAASM platforms
Reduces complexity by automating security policy enforcement and asset compliance monitoring
Continuously monitors for compli-
Remediates gaps using automated
Improves cyber asset hygiene and streamlines security posture management across enterprise security operations
Streamlines discovery and management of
Solves the challenges related to complete asset visibility

Scrut Automation

CHAPTER 3

What are the use cases for CAASM?

Gartner projects that by 2026, 20% of companies will have ≥95% asset visibility due to the continuous adoption of CAASM.

Did you know?

Cyber asset attack surface management (CAASM) continuously monitors IT ecosystems to generate real-time data on an organization's risk profile. They can automatically detect the external IT assets that malicious actors can see. CAASM can also check them against threat intelligence feeds from proprietary, open-source, and commercial security solutions. These tools continuously detect vulnerability and security control gaps. This is done using API integrations to gather all internal and external cyber assets data.

CAASM solutions are powerful tools that can help organizations design and speed up the implementation of very effective security programs. They also enable teams to track changes in attack surfaces and observe the improvements to the organization's risk posture when a risk or set of risks are remediated.

CAASM solutions work by aggregating data from existing data feeds and security tools. They then provide stakeholders with a multidimensional view of their organization's attack surface. CAASM is an emerging technology that enables the resolution of asset visibility and vulnerability challenges by eliminating blind spots and providing security teams with the means to achieve near real-time cyber security and risk management proactively.

Audit and compliance assessmen

Provides outputs and documentation that accelerates audit and compliance assessments by offering near real-time visibility into assets and their business context. This streaamlines evidence collection for compliance frameworks and eliminates the need for "point-in-time" audits with continuous testing.

Identity & Access Management

Detects and addresses privilege boundaries by comparing attack surfaces against popular IAM systems.

Automatic discovery

Monitors IT ecosystems to discover and categorize assets and attack surfaces. It also provides a unified view of all assets including devices, services, apps, users, IoT, on-prem, cloud, managed, and unmanaged assets.

Cyber risk quantification

Aggregates vulnerability, asset inventory, and cybersecurity data into a comprehensive risk quantification model. This provides a unified view of cyber risk and threats in business terms.

Vulnerability management

Assesses security posture and prioritizes detected vulnerabilities based on risk appetite.

How does CAASM compare to other cloud security tools, such as CSPM?

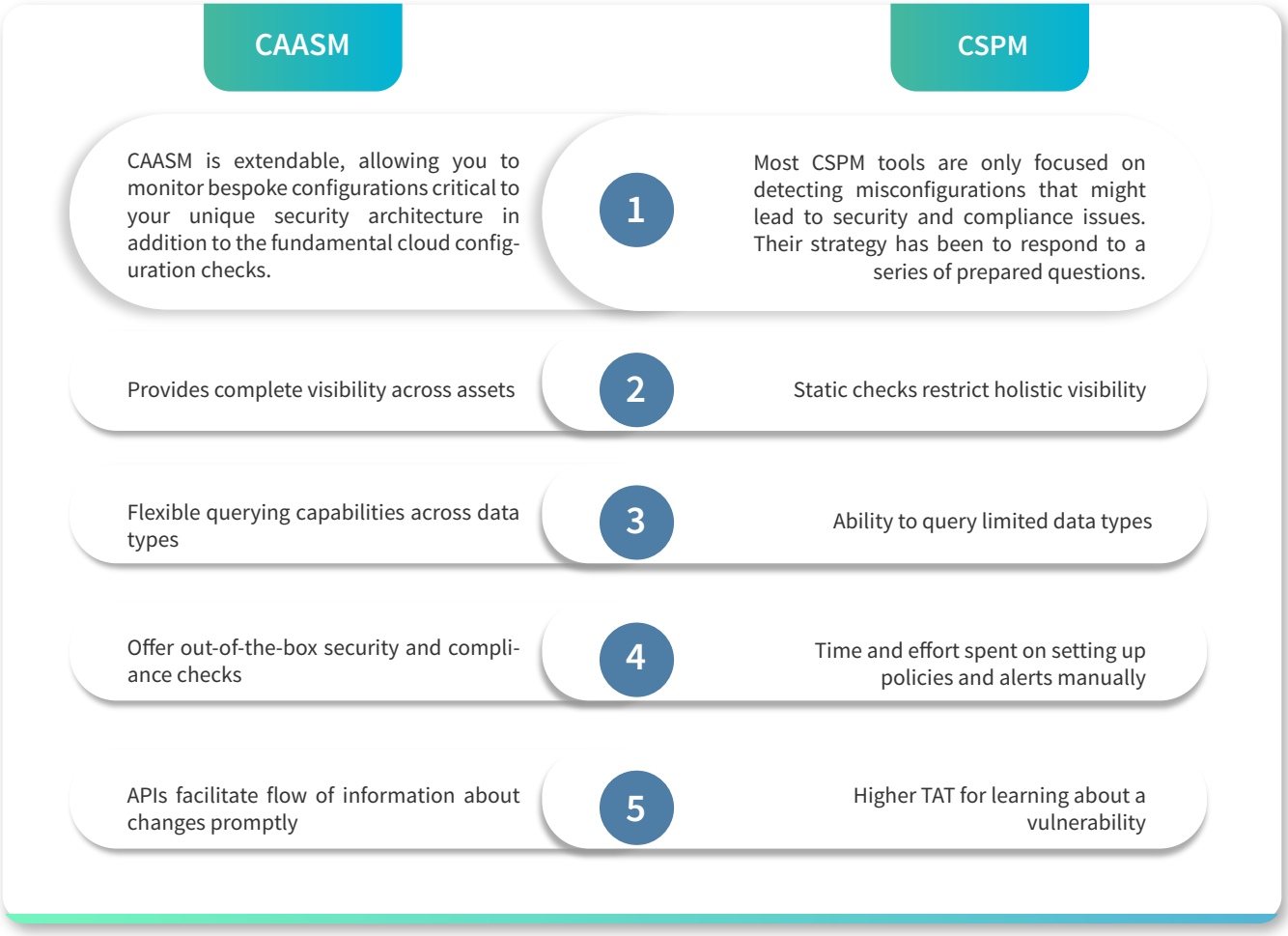
Enterprise assets and attack surfaces continuously evolve as new systems and devices are commissioned and retired and new software is installed or updated. Is a single solution enough to assess and mitigate the risk inherent in such rapidly changing ecosystems?

Although CAASM tools can solve persistent asset visibility and vulnerability challenges, other solutions can mitigate risks and protect critical business assets on the cloud.

For instance, Cloud Security Posture Management (CSPM) consists of several security-focused products and services (including dynamic cloud integration, DevOps, and compliance monitoring) that are laser-focused on detecting misconfigurations that could lead to security, audit, and compliance issues.

CSPM enables cloud security teams to protect the cloud ecosystem. It identifies unknown or excessive risks, assesses security gaps in cloud deployments, reduces misconfigurations, and suggests robust security measures to keep vital business data safe. It provides investigation, risk assessment, rapid incident response, and reporting for cloud security.

CAASM provides modern tech stack asset observability and security offerings that extend beyond the cloud.



Sources: Resmo

Scrut Automation

CHAPTER 4

How CAASM addresses the main issues that security teams face

API-first architecture, cloud adoption, and digital transformation transformed the way enterprise IT infrastructure is built, managed, and secured.

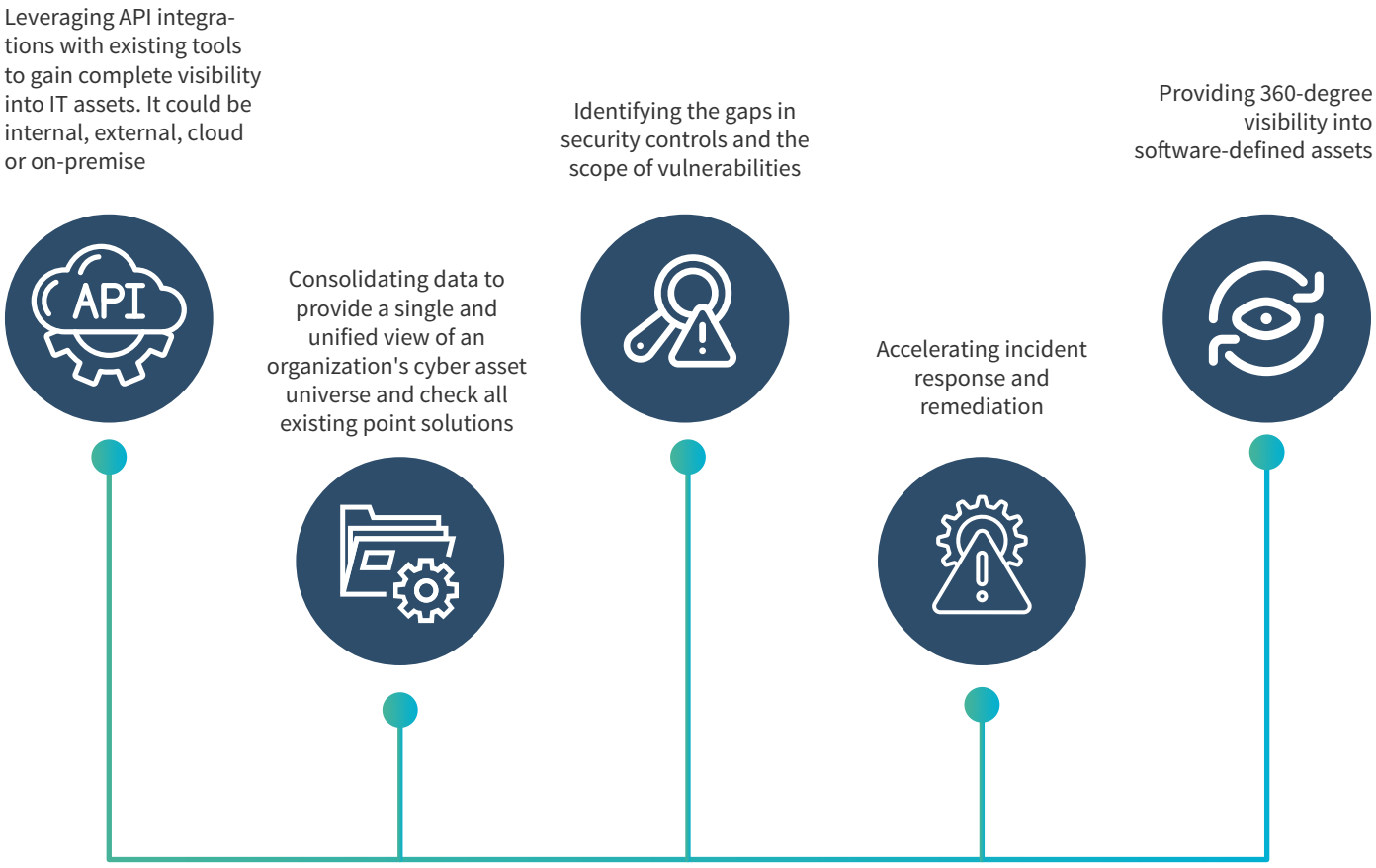
It has become difficult for IT, cloud, and security teams to fully grasp the size of their complex environments. Without the correct data, it's challenging to identify the most vulnerable cyber assets: applications, infrastructure, networks, devices, data, people, etc.

It is vital that security teams deeply understand their organizations' cyber asset landscape and the several implications on risk appetite and security posture.

Understanding your cyber assets and their interrelationships is the first step towards building a robust cyber security program.

IT assets are not just limited to devices with an IP address. They also include operational entities such as vulnerability findings, people, security controls, IAM roles and policies, data stores, code repositories, and others. CAASM tools ingest asset data across existing tools and the entire IT infrastructure. This helps discover and join all assets data while delivering total visibility into every cyber asset on one platform. This visibility also includes a mapping of all intra-asset relationships.

This enables security teams to launch sophisticated queries and get answers to questions about the organization's cyber asset universe. CAASM solutions can help determine the 'blast radius' of all attack surfaces within your IT infrastructure. It can speed up detection and remediation across security operations. This is due to its ability to query for actionable context instantly and visually explore security architecture. CAASM tools can deliver immediate ROI and mitigate the risk inherent in evolving attack surfaces by



For best results, startups in the Fintech, HealthTech, AI/ML niche can go a step further by integrating attack surface management with other capabilities. This involves combining threat intelligence, web app security, cloud security, endpoint protection, and vulnerability management. This is particularly important as startup companies progress along their startup journey, and acquire more attack surfaces as they bring onboard more employees, deploy more endpoints devices and scale their cloud infrastructure from a single to a multi-account, multi-cloud environment.

Scrut Automation: seamless management and visibility into your cyber asset universe and attack surfaces

The rapid pace of digital transformation over the past decade and the rise of remote/hybrid work models resulted in the exponential increase in the number and complexity of corporate IT assets. Currently, 52% of IT organizations manage 10,000+ assets. This also means an explosion in the number of attacks surfaces that enterprise cybersecurity teams have to manage.

These teams are responsible for inventory, management, and protection. They are also responsible for proactively defending the vast array of assets that comprise its attack surfaces. But what happens if your security team isn't even aware that certain assets and attack surfaces exist?

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. Using customized, easy-to-build auto-populated security pages, they can showcase a solid security posture.

Scrut scans your startup's IT ecosystem to identify risks and vulnerable attack surfaces across the code base. It includes infrastructure, applications, vendors, employees, access management, and more. Scrut can track complex, multi-cloud environments and remove audit fatigue by sharing and reusing controls across frameworks and collaborating with auditors on the platform.

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