Censys

What You Don't Know *Will* Hurt You

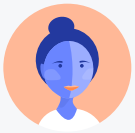
How Attack Surface Management can supercharge your Vulnerability Management Program

Summary

One of the major indictments of Equifax in the analysis of their 2017 compromise was not having a complete inventory of their assets[1], especially those that were Internet facing. In fact, it was an Apache Struts server that the company was unaware of that was the source of this major data breach. Although Equifax was aware of the general vulnerability, and was using a vulnerability management (VM) scanner to detect vulnerable servers, their VM scanner was not aware of the server that ultimately led to the breach.

This example shows how failure to identify and track a company's Internet attack surface can leave organizations at risk of a breach even if they are actively using VM scanners. Attack surface management (ASM) solutions help close this gap by identifying and tracking increasingly cloud-centric businesses. This whitepaper is a primer on attack surface management and how it increases asset visibility to complement a vulnerability management program.

This Information is Beneficial For...



Security Leaders

Vulnerability Managmement Professionals

This document is intended for security leaders or vulnerability management professionals looking to understand Attack Surface Management (ASM) and how it differs from and complements vulnerability management.

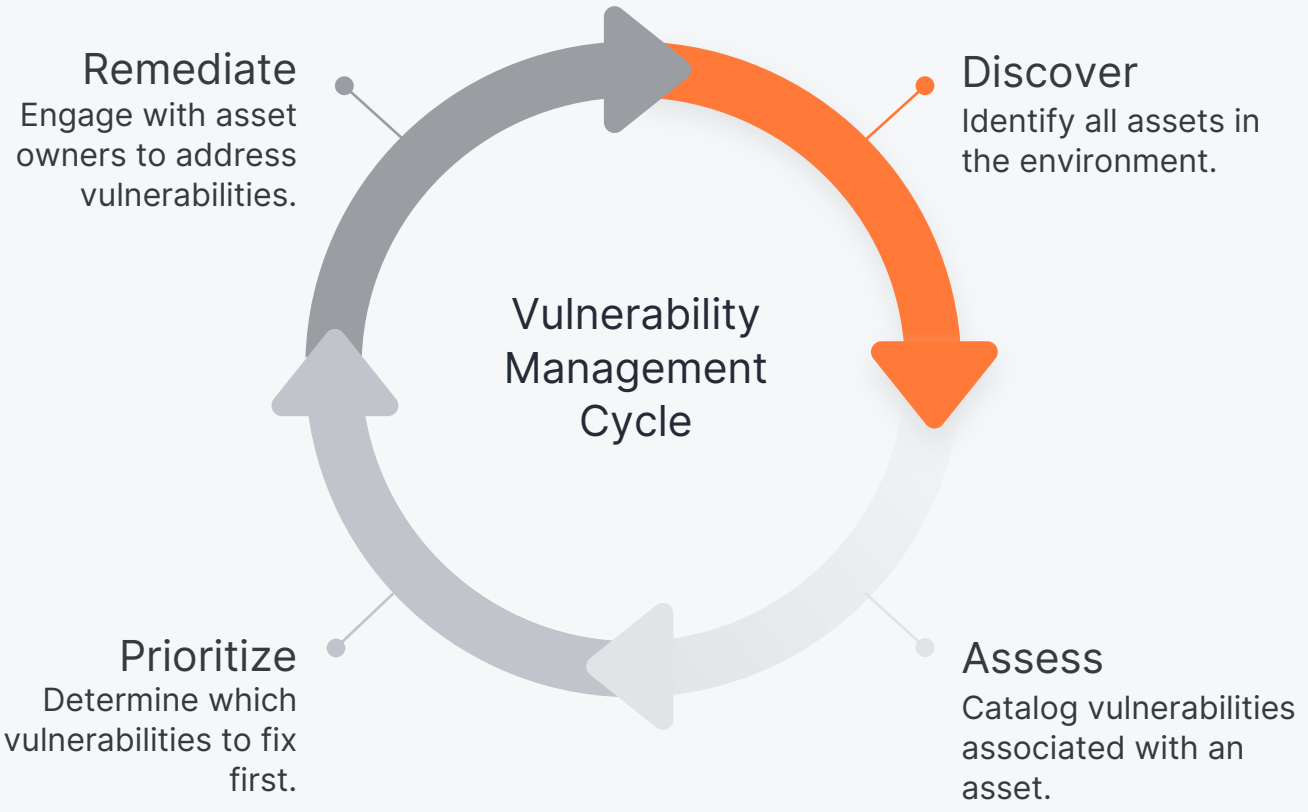
[1] https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf

Background

Every major cybersecurity framework cites asset inventory/ identification as the first step in a successful security program.

Background

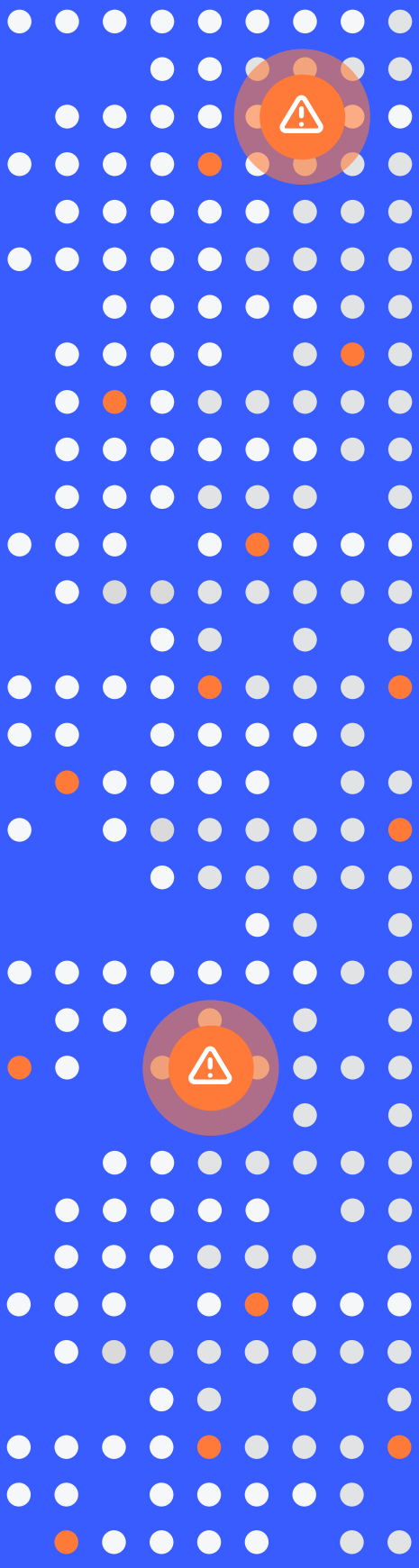
As the diagram below demonstrates, asset discovery has always been at the heart of both successful cyber security programs, and vulnerability management programs more specifically.



This phase of the vulnerability management lifecycle has become more difficult, while at the same time becoming more important, as IT environments have become more distributed and assets have shifted to the cloud.

History

In the late 1990s and early 2000s, there were many fewer asset classes, and almost all resided on either a corporate campus or in a datacenter. Vulnerability scanners were first developed around this time and were extremely effective at identifying new hosts in a known IP range, like a datacenter or corporate campus. As the 2000s progressed, especially the second decade of the century, **two trends emerged that made traditional asset discovery much more difficult.** These two trends would result in the end of the concept of the fixed network border.



History

The First Trend:

- The increased deployment of laptops
- An increasingly mobile workforce

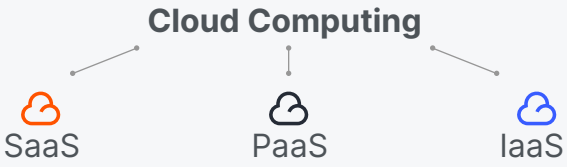
The Second Trend:

- The increased federation of IT

The **first change** was the increased deployment of laptops and an increasingly mobile workforce. Employees began using mobile devices to access email, applications, file servers, and more from anywhere on the planet at any time. Hardware assets became difficult to track and many of the company's assets walked out the door at the end of each workday. The recent events surrounding COVID-19 have highlighted and intensified this trend. Proper security for this change has been effectively addressed by tools like:

- **Network Access Control (NAC)**
- **Endpoint agents**
- **Zero trust architectures**

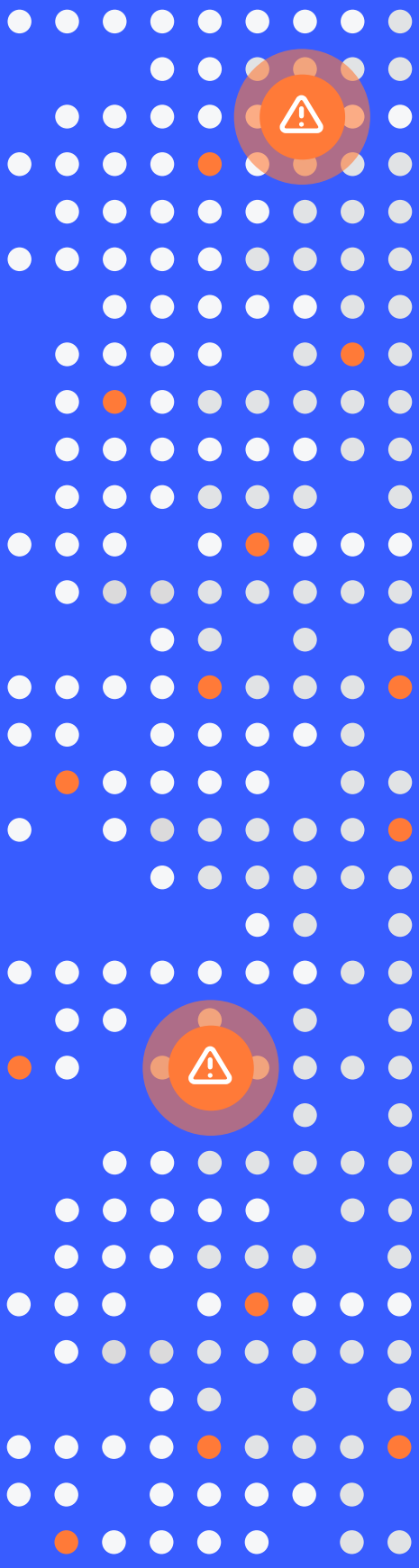
The rest of this paper will focus on the **second major factor** in the disappearance of the fixed network border: the increased federation of IT, propelled by the introduction and explosion of Cloud computing in all its forms.



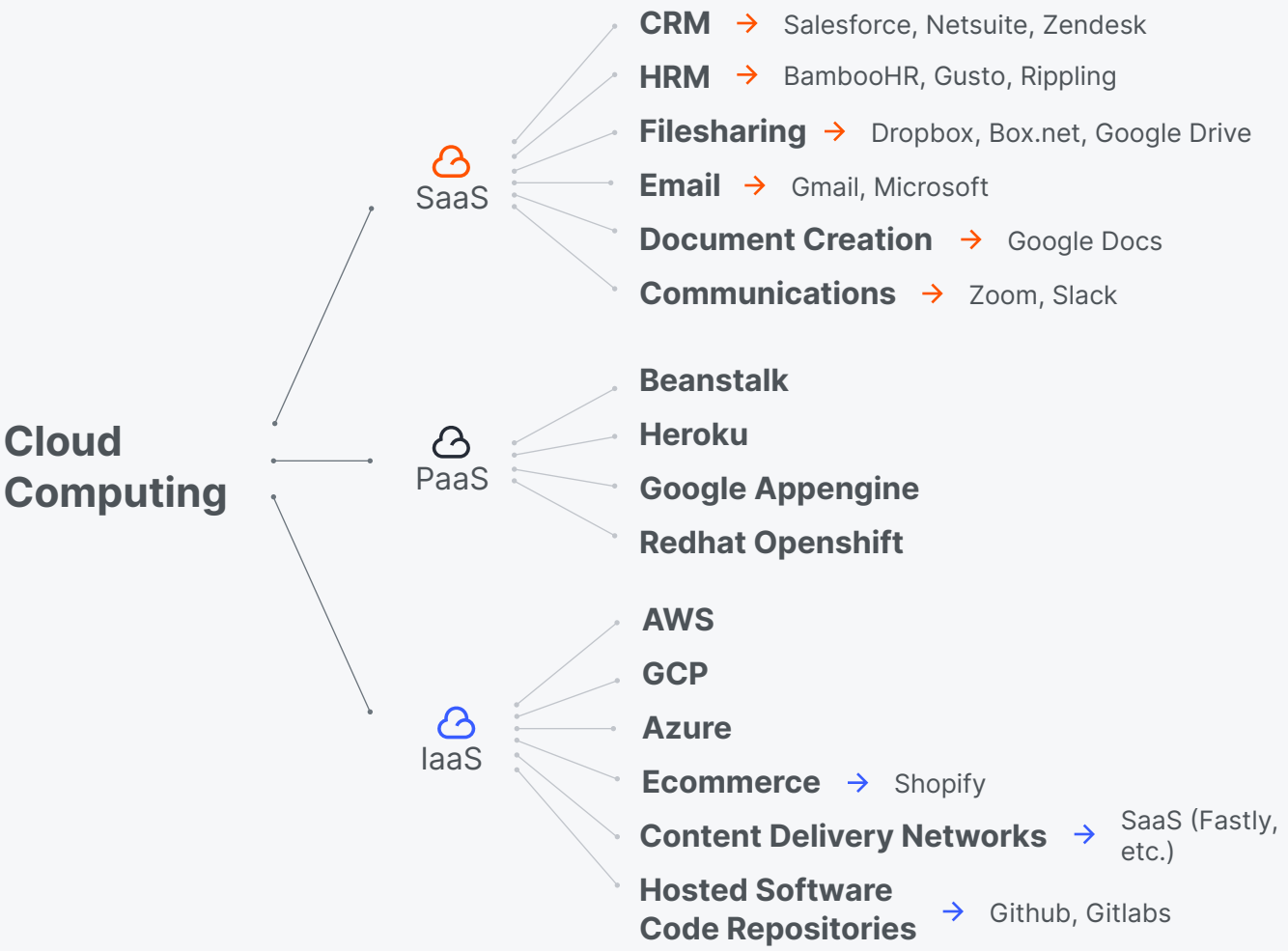
For many organizations who were expanding in the mid 2000s, central IT couldn't or wouldn't support the business needs of their internal customers. While this situation had existed for as long as IT itself, the low cost, wide availability, and ease of deployment of cloud services allowed individual business units to easily procure services outside of the standard IT model. And because it was not centrally managed, this "Shadow IT" circumvented the security and monitoring of centrally managed projects. This increasing de-centralization of IT resources meant that much of a company's attack surface was now outside the organization's network boundary, making asset discovery via traditional vulnerability scanners nearly impossible.

Today

In the modern IT environment, a business is composed of a variety of services, delivered by a multitude of vendors, in many network locations. In the graphic below, we've sketched out an example of how a typical enterprise might be utilizing different tech services across their organization.



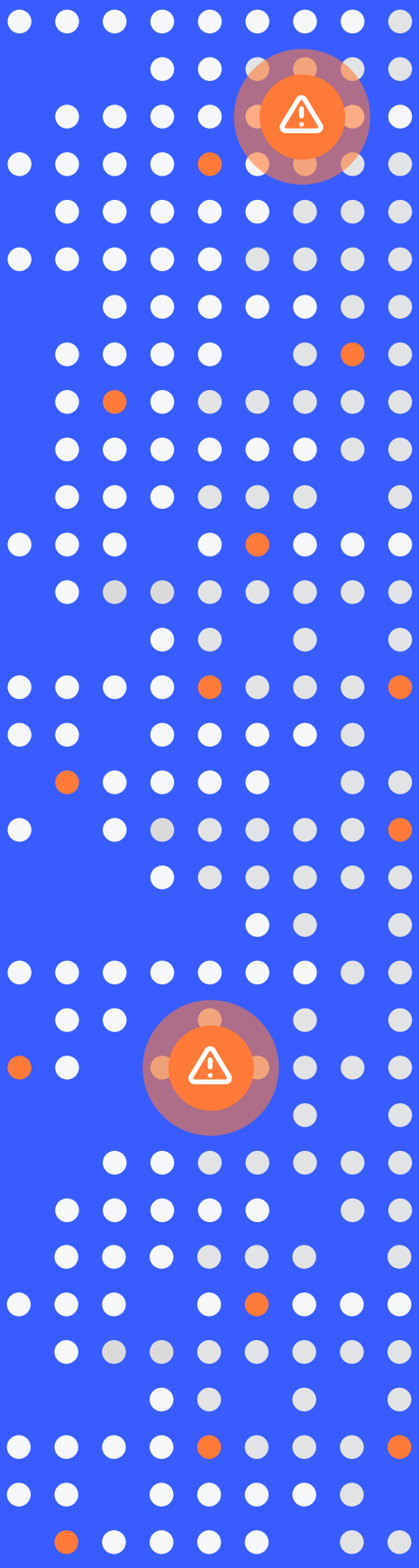
Today



An important note here is that the definition of asset ownership today is also not clear, as a direct result of the move to subscription-based software, where a customer rents access to an application or server.

For example, while a customer does not "own" their salesforce.com instance in a traditional sense, this service is a resevoir of important business data, and certainly contributes to the overall risk profile of the organization.

Attack Surface Management



Diversification of asset types and locations has made comprehensive asset inventories significantly more difficult, which can work to the advantage of adversaries. A partial solution to this problem is the use of tools like cloud connectors and container scanning capabilities to assist with asset detection. These technologies do an excellent job of asset discovery in known networks/accounts/ locations, but they cannot find the “unknown unknowns”: assets that are completely unknown to the core of the business.

Attack Surface Management

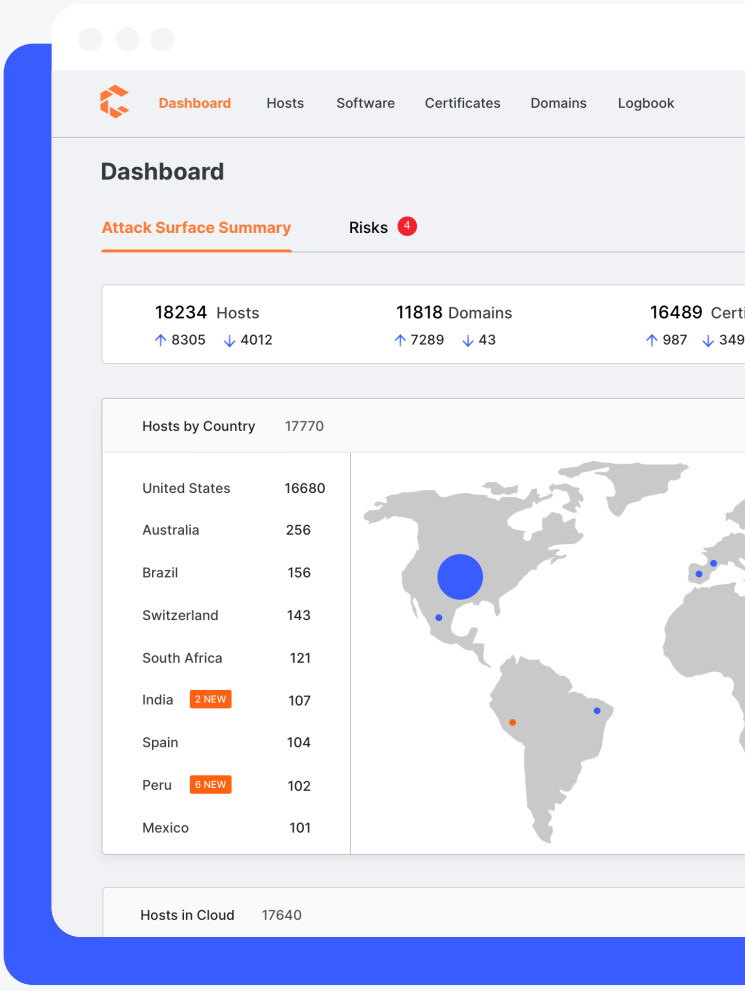
Examples of unknown unknowns include:

- **Marketing websites stood up by 3rd parties**
- **IaaS instances** - Often development, testing, or staging infrastructure paid for with a credit card and stood up by engineering groups, running applications such as:
  - **Cloud orchestration/ development tools**
    - Kubernetes
    - Docker
    - Jenkins
  - **Web/application servers**
    - Apache
    - Nginx
    - Tomcat
    - WebLogic
  - **Content management systems**
    - WordPress
    - Joomla
    - Drupal
  - **File storage sites**
    - Amazon S3
    - Google Cloud Storage
    - Azure blob storage
  - **Database servers**
    - MySQL
    - Elasticsearch
  - **System Backups stored in cloud infrastructure**

Attack Surface Management

New assets can be located anywhere the world, in multiple clouds, with subtle, hard-to-detect connections back to traditional corporate infrastructure. This makes asset discovery using existing internal tools and systems, such as configuration management databases, and patch management tools ineffective for this class of assets.

New tools such as the Censys Attack Surface Management Platform were developed to address the problem of unknown unknowns. These tools are purpose-built to help IT and Security departments detect assets that are difficult or impossible to find using traditional methods. By pairing large Internet-scale datasets with sophisticated discovery techniques, Attack Surface Management tools help network defenders shorten the time to discovery for previously unknown assets, increasing the chances they can be secured before attempts at compromise.



Better Together

Organizations have invested considerable time and resources developing their vulnerability management programs. But the perceived unwieldiness of IT practices and the proliferation of self-service and cloud services has created large gaps in the inventory fed to vulnerability management programs. These gaps increasingly contain business-critical or sensitive data. Pairing an attack surface management tool with existing VM programs allows organizations to understand the full scope of their network, and the cyber risks associated with all significant assets. This process has traditionally been conducted on a periodic basis in the form of penetration tests or manual inventory exercises, but attack surface management (ASM) solutions can automate much of this work and provide continuous discovery and monitoring of the external attack surface.

An effective ASM tool will help surface what are likely some of the riskiest assets for a business, if only because those assets are Internet facing and less likely to be centrally managed and monitored. Pairing tools takes advantage of the strength of each. ASM tools discover new, previously unknown assets, which they then feed to vulnerability management tools, which perform in-depth, detailed assessments of specific vulnerabilities present on hosts. A partnership that shortens the time between asset deployment and discovery and remediation of any vulnerabilities now exposed improves the overall security posture of the modern, online business.