censys

Swiss Life Gains Full Clarity with Censys Attack Surface Management

Company Profile

For more than 165 years, Swiss Life has provided financial security for individuals and corporations. From their start as a life insurance company, to their growth into comprehensive life, pensions and financial services, they serve as an important function from their headquarters in Zurich, Switzerland. With locations and teams dispersed throughout Europe, Swiss Life's primary divisions fall within Switzerland, France and Germany, with additional competency centers in Luxembourg, Liechtenstein, and Singapore. Swiss Life Asset Managers offers institutional and private investors access to investment and asset management solutions with locations in Switzerland, France, Germany, Luxembourg, the UK, and Norway. With an eye towards enterprise governance and compliance, as well as a need for consistent security across dispersed divisions, they reached out to Censys.

Swiss Life wanted to understand the risks contained within their external attack surface

As a financial company that deals in a critical aspect of their clients' lives, Swiss Life attaches "great importance" to their corporate governance policies. In following with their procedures around international accounting, auditing, and a code of conduct to safeguard the interests of their shareholders, policyholders, and staff, Swiss Life wanted to better understand the risks contained within their external attack surface.

Because their corporation is divided into several divisions (Swiss Life Switzerland, Swiss Life France, Swiss Life Germany, Swiss Life International, and Swiss Life Asset Managers), Swiss Life had faced challenges with not only having a bird's eye view of governance and compliance issues security teams were finding, but that each team was working on their own, with their own processes when it came to discovering vulnerabilities.

> **[How we] found what was unknown was by accident; there was no real standardized process to find the unknown.**

Wolfgang Bauer, IT Security Manager
Swiss Life Deutschland Operations GmbH

Already in place for the teams were their Vulnerability Management (VM) tools, which scanned for internal assets, as well as assets they already knew about. But the real quandary they turned to Censys for was regarding external assets, or assets that were not located in data centers. How is an organization supposed to find and protect those external assets which are not known to security teams? How can they be expected to know the unknown?

And, once those assets were located using Censys, how would they know which of their divisions the asset belonged to, and should therefore work to remediate it?

What did Swiss Life expect to find?

- Unknown or “leftover” pieces of IT on the internet
- Hosts and ports they were unaware of
- Old, or forgotten assets
- Vulnerable legacy applications
- Assets resulting from Shadow IT or malicious intent

Revealing internet exposure through Censys’ Attack Surface Management (ASM) platform

Even with Swiss Life’s highly dispersed teams creating a complex attack surface, Censys was able to onboard them quickly onto the Attack Surface Management (ASM) solution. Immediately after Censys’ initial internet-wide scan, Swiss Life’s security leaders were able to see their internet assets and prioritized risks all in one place within our dashboard.

Although Swiss Life follows very stringent security policies, they were surprised to see how many “leftovers” there were; even with processes in place for discontinuing and decommissioning services.

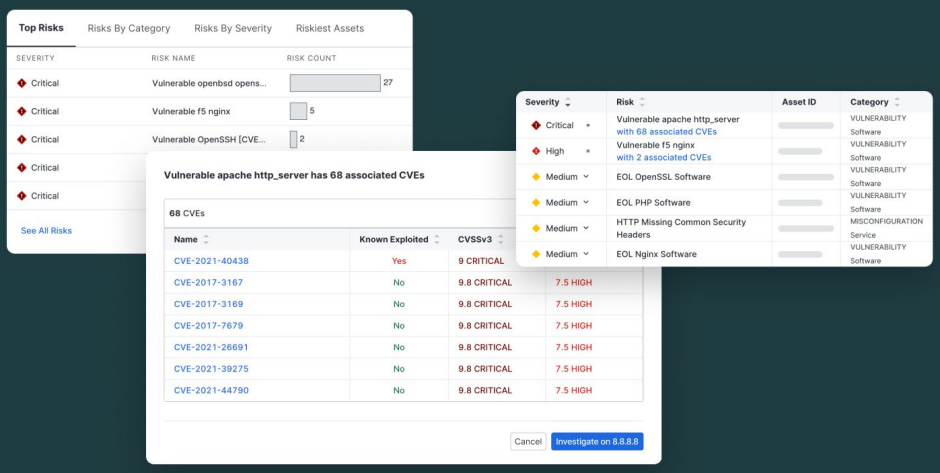
> **“Censys helps us see links between assets and DNS entries or outdated software, but in one screen so we don’t have to search for them.”**

Wolfgang Bauer, IT Security Manager
Swiss Life Deutschland Operations GmbH

Swiss Life found Censys’ Workspaces capability to be incredibly useful for segmenting and managing assets within their dispersed teams. Security leaders could see vulnerable external assets as well as which division they belonged to. Armed with this information, it was easy for Swiss Life to alert the division’s security team to triage and then fix the issue. The separation of workspaces also reduced the overall noise each division was exposed to, allowing them to focus on only the assets that belonged to them. Additionally, segmentation of divisions allowed visibility for leaders, but did not reveal attack surfaces to or between divisions, an essential need for compliance.

With Censys’ ASM tool in place, the Swiss Life divisions are more efficient at locating unknown external assets, can better understand their internet exposure, and ensure that the Swiss Life brand continues to be aligned with their purpose to enable people to lead a self-determined life.

> **“When managing any attack surface, finding a new risk means you must also find the person responsible for remediating. With Censys ASM Workspaces, it is simple and easy to segment our attack surface so that it is clear who within the division needs to take action.”**



Censys research has shown that attackers begin full Internet scans for vulnerable systems within hours of public vulnerability disclosures

How Censys compares to competitors

Swiss Life tested Censys' ASM as well as our competitors' and found that Censys:

- Provided easier-to-understand classifications in our dashboard
- A clear link between how an asset was found and its origin
- Better visibility into software, risks, and certificates

77.9%

more Internet-facing assets were found by Censys ASM than a Global 500 company believed they owned

66%

of the services Censys uncovers are on non-standard ports

2 million

database exposures have been identified by Censys' own research along with more than 1.9 million RDP exposures across a dozen cloud providers that we investigated

Why Censys?

Censys ASM is powered by our industry-leading Internet scanning platform that discovers 85% more services than our nearest competitor.

Censys continuously scans more than 100 protocols across the top 3,500 ports on the full IPv4 address space every 10 days and the top 100 ports daily.

More than 100 protocols	**Across the top 3,500 ports**	**Every 10 days on the full IPv4 address space + top 100 ports daily**

Censys is the only Attack Surface Management provider that uncovers unknown storage buckets on AWS, GCP, and Azure that contain sensitive data.

At Censys, we work relentlessly to make the internet a secure place for everyone. As the leading Attack Surface Management provider, we take the guesswork out of understanding and protecting the organization's digital footprint. From the world's most comprehensive real-time view of global networks and devices, Censys provides a comprehensive profile of the exposed assets on the internet, delivering the tools and insights to manage potential risks. We are on the forefront of helping organizations stay one step ahead of risk, and seeing threats before they become complications. From the corporate network to the cloud and beyond, a secure internet starts with Censys.

Start your Censys today at www.censys.com.

censys

VISIT
censys.com

CONTACT
hello@censys.com

Censys' mission is to be the one place to understand everything on the internet. Frustrated by the lack of trustworthy Internet intelligence, we set out to create the industry's most comprehensive, accurate, and up-to-date map of the Internet. Today, Censys delivers real-time Internet intelligence and actionable threat insights to global governments, over 50% of the Fortune 500, and leading threat intelligence providers worldwide.