3 Ways Financial Institutions Leverage Cyber Asset Attack Surface Management (CAASM) to Improve Security Posture

By: Dave Twichell, Axonius

Financial institutions know complexity. FIs were among the most impacted by the shift to remote work (going from 22% to 64%), and saw a massive uptick in weekly cyber attacks from under 5,000 attacks per week in February 2020 to more than 200,000 in April 2021. It's no wonder that understanding, managing, and securing the attack surface is an urgent priority for the finance industry.

At the same time, a new category emerged: Cyber Asset Attack Surface Management (CAASM). Coined by Gartner in its 2021 Network Security Hype Cycle, this class of solution lets customers see all assets (on-premise and in the cloud) through API integrations with existing data sources and use queries to identify gaps in security controls, and automate response actions.
The increase in remote work and attack volume at FIs coupled with an emerging solution to manage the cyber attack surface is leading financial institutions to embrace CAASM. Here are 3 examples of how FIs are leveraging cyber asset attack surface management today:

1. Understanding the Internal and External Attack Surface

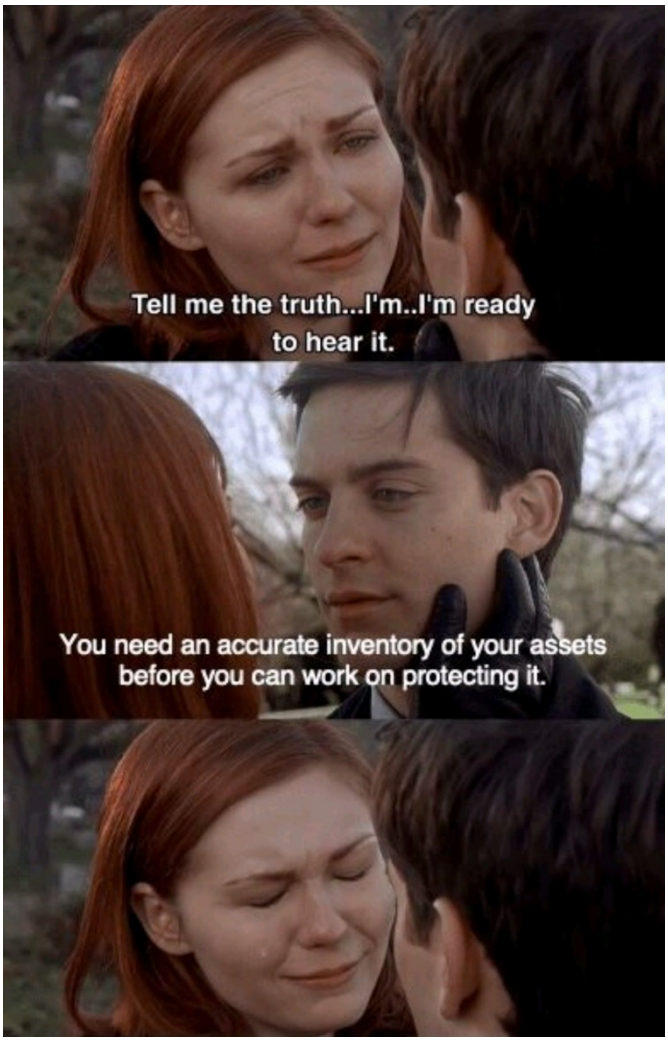
Attack surfaces can be external and internal. External attack surfaces include public and customer facing applications, such as cloud and mobile banking applications, websites, and more. The internal attack surface represents everything inside an organization's network that employees use on a regular basis.

The good news is that there are a number of excellent security tools that help FI security teams manage and secure their internal and external attack surfaces. Yet, even with these tools, many teams still struggle with asset visibility.

CAASM solutions are aiming to fix that. Digital Federal Credit Union (DCU) recently detailed how Axonius helped them correlate data from their existing security tools to gain comprehensive, always up to date visibility into their assets.

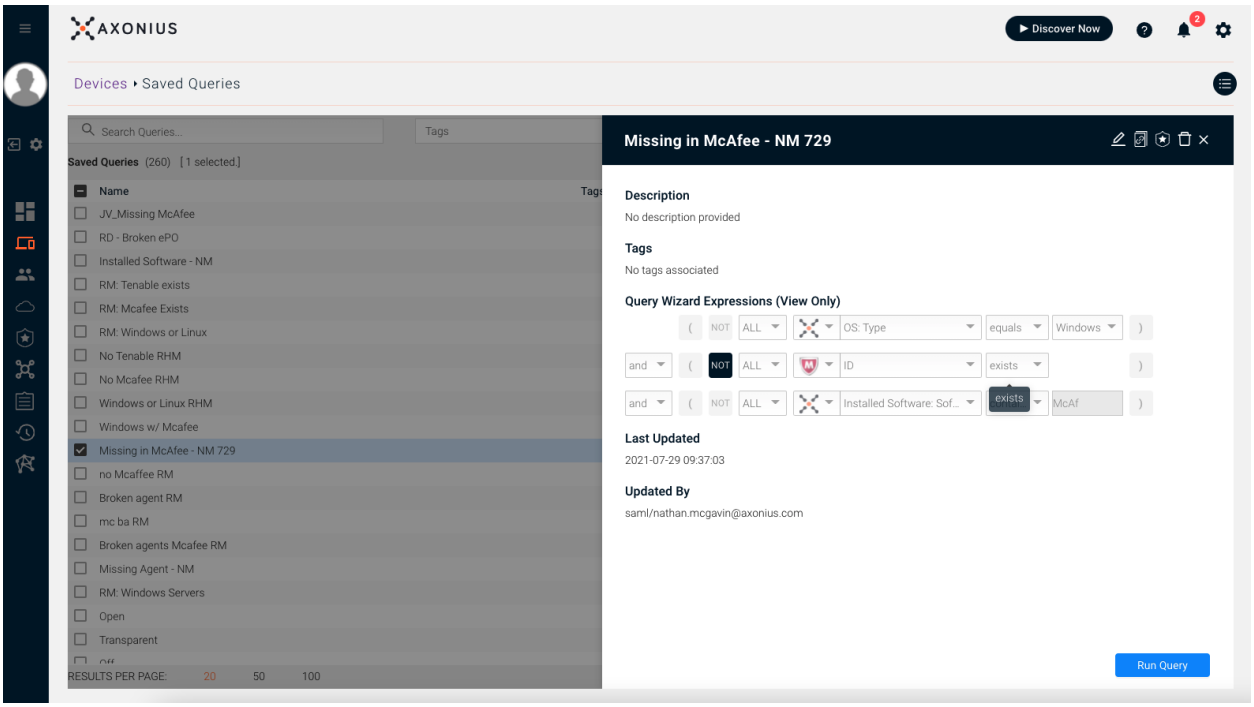
> "Axonius took what we thought we knew about our assets and gave us something a lot closer to the truth. It was able to take separate pieces of data, combine them together to reconcile that data, and really show us where our gaps were."
>
> - Mike Conroy, Assistant Manager of Information Security Risk Management, DCU

Or if memes are your style:



2. Conducting Security Control Validation

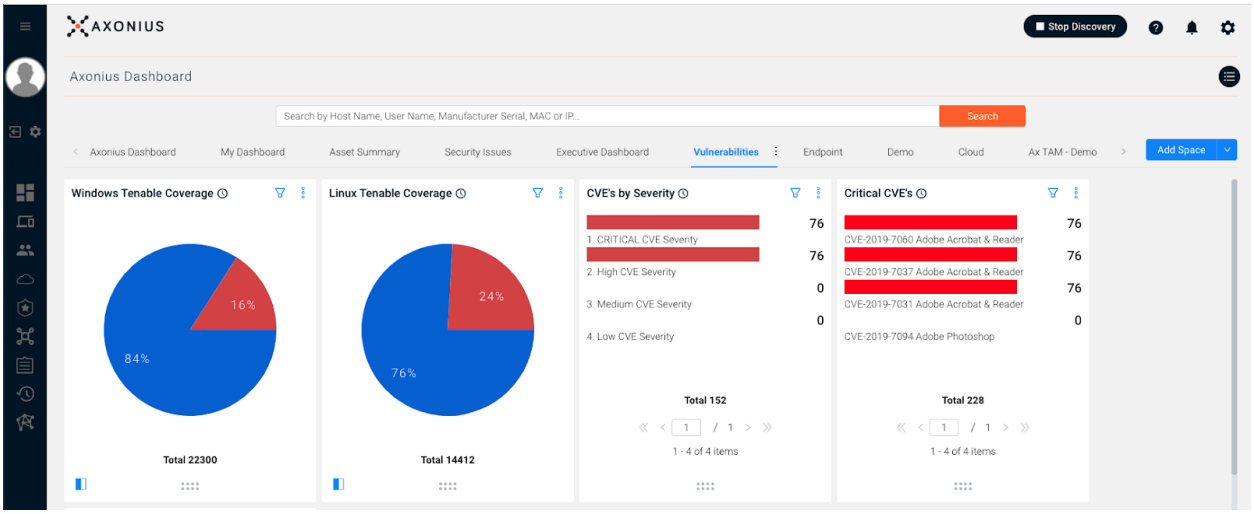
Financial organizations have already invested in security tools that, when deployed and working correctly, can protect their assets. Security control validation is the process of testing individual controls or a set of controls to ensure they are effectively protecting against a variety of cyber risks. Performing security control validation exercises helps find missing security controls, misconfigured security controls, and security control effectiveness.



Security control validation exercises are greatly aided by a cyber asset attack surface management platform like Axonius. Because Axonius correlates data from existing management and security tools, organizations can easily see how their security controls match their IT assets in one central view. This helps security teams discover coverage gaps and validate that security tools are working properly.

3. Enhancing Red Team Exercises

With the increase in the sophistication and volume of attacks financial organizations are seeing, red team exercises have become more useful. Red team exercises simulate attacks and test an organization's security efficacy, help uncover vulnerabilities, and evaluate the risks they pose to the business.



CAASM can help inform red team exercises. They can point teams to the places where vulnerabilities occur, where security controls are missing or inadequate, and can give red teams a punch list of assets to test, then address any weaknesses they find.

By leveraging API integrations with existing tools to provide a consolidated view of all assets, CAASM allows IT and security teams to gain confidence in what assets they have in order to secure them.
Download the 2021 Gartner Hype Cycle for Network Security to learn more.