CASE STUDY // INDONESIAN BANK

AXONIUS

HOW ONE OF THE TOP **INDONESIAN BANKS** USES AXONIUS TO BUILD A SECURITY HYGIENE DASHBOARD

The **Top Indonesian Bank** provides a comprehensive range of products and services for individual and corporate customers through Community Financial Services (Retail Banking and Non-Retail Banking) and Global Banking, automotive financing through its subsidiaries and digital banking. They have a significant presence in the country through more than 300 branches.

ENSURING ASSET HYGIENE IN A HETEROGENEOUS I.T. ENVIRONMENT

For a leading Indonesian bank, gaining accurate asset visibility and context was its biggest challenge, especially within a heterogeneous IT asset environment. As a decades-old banking organization with hundreds of branches, the asset environment consisted of disparate legacy devices manually managed by its asset management team – meaning asset data could be error-prone and outdated.

According to the Head of IT Security, limited asset visibility and understanding created unknowns about device security coverage and hygiene across the organization. Often, the team uncovered device coverage gaps or assets that weren't recorded because they weren't installed with an agent.

Moreover, audits exposed endpoints that lacked of Endpoint Protection solution, due to branches installing servers independently.

That's why the team chose Axonius.

Employees

- More than 7,000 employees
- More than 300 branches

Key Challenges

- Limited asset visibility and context (what assets were protected or not)
- Poor asset hygiene and compliance
- Manually managing assets

Solution

- Axonius Cybersecurity Asset Management

Results

The Top Indonesian Bank **gained comprehensive asset visibility** to close security gaps, ensure compliance, and strengthen security hygiene.

> "My team, the operation team, the security monitoring team, the governance team all use Axonius. Even teams outside IT security like the IT asset management team, the infra team…they all use Axonius. I consider this a successful implementation because it's being used by so many people."

HEAD OF IT SECURITY FOR A LEADING INDONESIAN BANK

> “Before using Axonius, we did not know where [all of our] assets were located or if they were protected. We couldn’t understand the hygiene of our asset inventory or if an asset was properly installed…it became a critical problem for a leading Indonesian bank”
>
> HEAD OF IT SECURITY FOR A LEADING INDONESIAN BANK

GAINING COMPLETE SECURITY COVERAGE

While the large banking group used SOAR and SIEM tools to correlate and manage asset security, a ransomware incident stemming from a compromised asset endpoint created compliance concerns and triggered the search for a new solution.

“The concept of Axonius itself, being an agentless solution, was my primary criteria [for a new solution],” explained the Head of IT, who was referred to Axonius by a banking vendor. ***“Axonius fit that.”***

When proposing Axonius to IT management, the Head of IT Security understood Axonius was the tool that offered accurate asset feasibility the bank needed to gain visibility into all of its assets and ensure they were protected. ***“[Axonius] is what I need to secure the bank. If not, how can I move on with my job?”***

“Axonius is one of my key strategies to ensure the banks resiliency from a security threat, including ransomware attack.”

STRENGTHENING SECURITY POSTURE AND SECURITY MATURITY

Since implementing Axonius, the IT security team has been able to gain greater visibility and context into their asset environment and coverage. Complete analysis from the Axonius dashboard has facilitated an understanding of all assets secured by anti-malware, EDR, IPS, DLP, and more.

“I refer to the dashboard as the ‘security hygiene dashboard’ and show it to my top management team once a month,” notes the bank’s Head of IT security. ***“Now, IT leaders understand how important Axonius is.”***

Axonius has also been instrumental in the bank’s asset management program to ensure compliance with security frameworks and controls. After deploying Axonius, the banking organization has been able to adhere to its country’s security framework, which requires strong security maturity and hygiene.

With Axonius, the IT security team is on track for 99% of system hygiene, thanks to the ability to identify dormant assets and close coverage gaps.

EXPLORING STRATEGY WITH AXONIUS

Axonius has become an indispensable solution for teams spanning beyond the IT security team. Today, the operations team, security monitoring team, governance team, and the infra team all use Axonius to better understand the asset landscape and develop strategies to improve the bank's cybersecurity approach.

"[My Account Executive] will bring me some interesting concepts around the risk-based dashboard. We are not moving there yet, but this is something I did not previously think [I needed]," shared the Head of IT.

Moreover, the IT security team also works closely with the Axonius team to help enhance the bank's asset security program, paving the way for an improved asset management journey.

> "[The Axonius team] is helpful because they bring me ideas and suggestions beyond my initial needs. We have monthly calls where we explore what improvement looks like, how the journey should look like after this step. For me, the customer, that's very good."
>
> HEAD OF IT SECURITY FOR A LEADING INDONESIAN BANK

Axonius gives customers the confidence to control complexity by mitigating threats, navigating risk, automating response actions, and informing business-level strategy. With solutions for both cyber asset attack surface management (CAASM) and SaaS management, Axonius is deployed in minutes and integrates with hundreds of data sources to provide a comprehensive asset inventory, uncover gaps, and automatically validate and enforce policies.

AXONIUS

Interested in what Axonius can do for you?

LET'S TALK