AXONIUS

CUSTOMER CASE STUDY

Cimpress Uses Axonius to Double EDR Coverage and Reduce Incident Response Time

cimpress™

Cimpress plc invests in and operates a wide variety of businesses that use mass customization to configure and produce small quantities of individually customized goods for a broad spectrum of print, signage, apparel and similar products.

EMPLOYEES
12,000

KEY CHALLENGES
- Gaining asset visibility across 11 distinct businesses
- Identifying and remediating coverage gaps in security policy

SOLUTION
Axonius Cybersecurity Asset Management Platform

RESULTS
By connecting to the Axonius Adapters across their multi-business environment, Cimpress has been able to automate asset discovery to create one clean inventory – allowing them to double EDR coverage and dramatically reduce incident response time

Managing Assets Across a Highly Decentralized Organization

When Daniel Fabbo took over as the Manager of Security Engineering at Cimpress plc in 2018, he realized his job responsibilities had just grown 10-fold. Cimpress, a multinational organization with over 12,000 employees, is structured as a strategically-focused group with 11 distinct businesses operating underneath its umbrella.

Fabbo, who had spent his last four years as the Senior Lead Information Security Engineer at Vistaprint, a company that operates under Cimpress, found himself with a unique challenge. He was now responsible for managing and securing assets at not just one, but all 11 businesses.

To make things more challenging, Cimpress was highly decentralized. The organization had no interconnected network, but instead chose to leave ownership of the disparate infrastructures to the individual businesses.

Connecting Disparate Infrastructures

In his first two years, Fabbo and his team depended on each individual business having its own up-to-date, accurate asset inventory. It was a process Fabbo described as a "rudimentary asset management system," where his team had to "jump through hoops to identify if a system is critical or not." When his team was able to get their hands on the data they needed, it was often error-prone – a direct result of the manual data collection process.

Plagued by data accuracy and collection issues, Fabbo struggled to identify gaps in his Antivirus and EDR coverage. When the security team identified an incident or vulnerability, they found it difficult to locate and then understand the particular asset or assets in question – causing delays to their incident response program.

"It's extremely hard to find an asset management solution that can cover 11 distinct businesses… especially without having an agent installed," Fabbo explained.

The "Aha" Moment

Fabbo was challenged to not only support multiple businesses under the Cimpress umbrella, but also by the separate set of systems and tools used by each of those businesses. This made keeping a clean, up-to-date asset inventory impossible.

Once introduced to the Axonius Cybersecurity Asset Management Platform, Fabbo immediately saw the value in its ability to pull data from a wide range of existing systems. With over 260 Axonius adapters, Fabbo saw the opportunity to connect those disparate systems operated by each business and provide "clear sight across the whole business."

"Axonius has such a varied number of adapters that they are easily integrated into the various environments that we have," he explained.

"Axonius has helped us automate a lot of the asset discovery in collection and inventorying, simply by being able to automatically go out and have a touch point with all of the different critical infrastructure pieces that we have within our environment, collecting data from disparate sources, and correlating it into one clean inventory," continued Fabbo.

AXONIUS

> “If you don’t know the assets that you have in your environment and how up to date they are, then **you’re going to want to take a look at Axonius.**

DANIEL FABBO
MANAGER OF SECURITY ENGINEERING
CIMPRESS

The Outcome: Identifying and Enforcing Gaps in Security Coverage

With the ability to automate asset discovery for the first time, Fabbo and his team were now able to turn their focus to more pressing matters within their SOC and incident response programs. Soon, Cimpress was utilizing Axonius to quickly identify vulnerabilities, discover coverage gaps in their existing EDR solutions, and ensure their environments were secure.

“Axonius has been able to give us insight where we didn’t have it in the past. For instance, Axonius can tell us what our coverage for EDR is across our enterprise, ...identify where those gaps are, and target those gaps with our security team to go in and work with the individual businesses to make sure that they’re being protected,” Fabbo described.

“Prior to using Axonius, we had about 40 percent coverage of our EDR deployment. And after Axonius, we were able to identify those areas where we were missing coverage and were able to increase that to 80 percent,” he continued, noting that the remaining gap in coverage is an expected result of ephemeral devices.

Along with identifying coverage gaps, Axonius has now become a critical aspect in the incident response workflow at Cimpress. In the past, when a vulnerability was discovered, the security team had a gap in their ability to swiftly and accurately identify the system and owner of the particular IP in question.

Axonius also reduced the person-hours it had once taken Cimpress to investigate an incident, instead allowing the team to work on “more profitable ventures.”

“With Axonius, now we can do a quick query, identify which business owns that IP or that asset, and reach out to that business to say, “Listen, there is a vulnerability within this asset and we need to remediate it,’” Fabbo explained.

Beyond the security team, Fabbo found that his ability to build a quick query within Axonius was particularly useful for his counterparts working in IT who often struggled with their own visibility issues.

“In the old days, the IT team would have had to launch a script within the environment to collect the information. But using Axonius, I was able to do it in a matter of seconds, saving them hours of work,” he explained.

See for Yourself.

Axonius is the cybersecurity asset management platform that lets IT and Security teams see devices for what they are in order to manage and secure all. **Interested in seeing what Axonius can do for your organization?**

LET’S TALK →