CYCOGNITO

CASE STUDY: SPECIALTY INDUSTRIAL MACHINERY

Mirion Streamlines Vulnerability Prioritization with CyCognito

Gains attack surface visibility across its digital supply chain, accelerates remediation, lowers cyber insurance costs

Key Results

- Reduced cybersecurity insurance premium and deductible while increasing its cyber-risk coverage
- More than 5,000 assets tested and monitored
- Gained comprehensive visibility into its attack surface and digital supply chain
- Accelerated remediation of critical risks
- Scaled security team's efficiency without increasing headcount

Story

Safety and compliance are at the core of everything Mirion does. When Craig Meyer, the Acting CISO, first joined Mirion in 2022, he faced a complex digital landscape. There wasn't a good perimeter map or a way to prioritize remediation. Meyer's first priority was to gain a clear understanding of the company's diverse attack surface and to address any security gaps.

"We had a history of federation, which means that we had many different business units running internet-facing services as well as third parties supporting us," he says. Getting a good understanding of our true perimeter was a major challenge."

Meyer emphasized, "If you do not address your external attack surface, you're putting yourself at significant risk. Any security professional will tell you that the first thing that you need to do to be successful in cybersecurity is understand your assets and software; you have to know what your exposures are because if you don't know that, you don't know what you're trying to secure or how to secure it."

MIRION

CUSTOMER PROFILE

Mirion is a global leader in radiation detection, measurement, analysis, and monitoring solutions for nuclear energy, defense, and medical markets.

Headquartered in Atlanta, Georgia, Mirion operates over 40 different sites worldwide. The company has expanded rapidly through acquisitions, integrating diverse business units and subsidiaries to offer comprehensive solutions.

With a presence in over 12 countries, Mirion's global IT team plays a crucial role in safeguarding the company, its customers, its employees, and its shareholders from cybersecurity threats.

Mirion's cybersecurity strategy at the time relied heavily on manual processes, including annual penetration tests and manual scans. The company manually reviewed over 300 IP addresses, more than 60 websites, and its Microsoft Azure tenant, which left gaps and provided limited visibility into its rapidly evolving attack surface.

"It was an effort to do a manual review of what our IP addresses were. We were trying to use vulnerability scanning to search the Internet and see what was exposed," he noted. "We were going to specific sites and looking at what was on the firewalls to find what was internet facing."

"The problem with the pen test is when you have as many properties as we have, you just can't get the breadth of scope across your entire enterprise," he says. "It shows you an important sliver of what your exposures are, but it doesn't show you the breadth of your exposures."

With a history of acquisitions, Mirion faced additional challenges in identifying the company's true perimeter as its attack surface continuously expanded, increasing cyber threats without proper visibility. As Meyer put it, "Discovering your perimeter isn't merely just asking your business units what their perimeter is because they may not know for the same reasons that you are struggling."

Manually finding new and acquired assets was not enough. Meyer knew he needed an automated solution that would provide comprehensive visibility and dynamically discover and assess Mirion's attack surface and digital supply chain for critical risks.

> "I would recommend any company get an external attack surface vendor like CyCognito, which has methodologies to search for your company's exposures that don't require you to provide the breadcrumbs necessary to find them."
>
> **Craig Meyer**
> Acting CISO

"We were looking for a product that gave us the most complete visibility that we could get," he says. "A product that could detect our perimeter with the most limited input from us to inform the solution."

Immediate Impact

During the initial proof of concept, Meyer was impressed with the depth and quality of the mapping and vulnerability assessment that CyCognito captured.

"In just a couple of weeks of turning on the proof of concept, we found things that we previously hadn't found, in fact, quite a number of them," he shares. "Importantly, when it found them, it also categorized them into the business units and the subsidiaries that were operating."

> We found things that we previously hadn't found; in fact, quite a number of them."
>
> **Craig Meyer**
> Acting CISO

Effortless Set-up

For Mirion, getting started with CyCognito was a breeze, requiring no complicated setup or changes to their existing IT environment. In no time, Meyer's team gained valuable insights into their attack surface and began addressing vulnerabilities immediately.

"Implementation was a cinch," he says. "There are very few products in the security space that you don't have to do a lot of work to integrate or implement; they just work. This is one of the few; simply by turning on CyCognito and getting access to the console, we were already using it to remediate vulnerabilities. It's something that you can hit the ground running with."

"CyCognito was very easy to use and very user-friendly. Of the products we evaluated, it did the best job of mapping our true perimeter. It gave us great insights into our environment without needing to feed it data and teach it about ourselves."

Dynamic Discovery and Mapping

Immediately after the first dynamic discovery, Meyer gained a complete inventory of Mirion's internet-facing assets and had a clear picture of how its systems were structured into various business units. This extended coverage was essential to understanding real-world risk exposure.

Expedited Remediation Through Critical Risk Prioritization

The platform's security grading, along with threat intelligence, provides clear, actionable steps on how to swiftly fix vulnerabilities before they can be exploited.

> CyCognito is not just reducing vulnerabilities. It's also reducing the exposure that can either turn into a vulnerability or maybe become a zero-day, so we've reduced the potential for vulnerabilities as well."
>
> **Craig Meyer**
> Acting CISO

This enables Meyer's team to prioritize and focus on remediating the most critical risks first. "We're able to make much more effective use of our resources and headcount," Meyer says. Now, his team spends more time on remediation rather than searching for vulnerabilities.

Once the remediation process kicks off, CyCognito continuously rescans and assesses the issue to ensure it has been properly remediated.

A key moment that underscored the value of CyCognito's automatic scanning and continuous testing was when CyCognito uncovered a vulnerability that Meyer's team patched, which was later targeted by an IP address associated with a nation-state threat actor.

"While we can't be sure, there is a fair chance that the proactive remediation that was enabled by CyCognito actually helped us avoid a security incident," Meyer says.

Strengthens Software Supply Chain Defenses

Because Mirion serves critical infrastructure companies, each involving a highly sensitive and complex software supply chain, one of the biggest concerns is the security of its supply chain partners. With the help of CyCognito, Mirion has significantly improved visibility into its software supply chain, allowing Meyer's team to identify potential exposures early and take preemptive actions to secure them, gaining better control over its supply chain security.

By leveraging CyCognito's platform, Meyer's team has been able to quickly identify instances where IoT devices deployed from customer sites were connected to the internet by current or former customers. These devices, designed for internal use, were never intended to be publicly accessible, yet several were exposed on the internet.

Meyer explains, "We've been able to reach out and let them know that these devices aren't intended for public exposure and should not have been on the Internet," he says. "That's not to say that they weren't secured, but they're just not things we want to have on the Internet."

This situation highlighted the potential risks of having IoT devices exposed. "One of our worries is selling a device into a customer environment and then that device somehow, maybe through a zero-day or something, becoming patient zero of a breach of that environment," Meyer notes. "Even if we weren't directly responsible, we don't want to see our customers at risk or experience brand damage from an event like that."

Meyer reflects on this 'aha' moment as pivotal, recognizing the critical need for continuous monitoring to secure Mirion's software supply chain ecosystem, stay ahead of emerging threats, and reduce the likelihood of a cyber incident that could disrupt operations or compromise sensitive data.

Improved Risk Ratings and Reduced Cyber Insurance Costs

Within six months of implementing CyCognito, Mirion's cybersecurity scores with supply chain security companies like BitSight and Security Score Card improved dramatically and are now considered to be leading the manufacturing industry with advanced scores.

One of Meyer's proudest achievements was "being able to tell senior leadership that we had reached the advanced level of scoring and that we made significant progress and a massive amount of improvement in just the first six months."

> "We were able to reduce our cyber insurance premium, increase our coverage, and reduce our deductible—all at the same time; I attribute a significant part of that to CyCognito."
>
> **Craig Meyer**
> Acting CISO

CyCognito helped Mirion reduce its attack surface by uncovering websites from older acquisitions that had never been integrated or decommissioned. Some of these were still hosted by Mirion, incurring unnecessary ongoing costs, while others were hosted by third-party providers that weren't billing the company, leaving these unknown and unmanaged assets vulnerable.

"While the third-party hosted sites weren't super dangerous to us directly, it definitely is dangerous from a brand management standpoint," Meyer says. "If those sites were attacked by a third party and then used as a watering hole attack against our customers, that would impact us negatively."

"With CyCognito, we were able to significantly improve our security scores by addressing and mitigating the vulnerabilities identified in the CyCognito scans," he adds.

"CyCognito has put us in a position where we can talk with confidence to our customers, 'We work hard to secure our perimeter.' And you can see those results in third-party scores that have gone up a lot since we have deployed CyCognito."

Not only did these improvements bolster their reputation with customers, but they also played a critical role in reducing cyber insurance premiums, increasing coverage, and lowering deductibles. Mirion's enhanced security posture also allowed the company to renegotiate terms with its cyber insurance provider, all during a year of higher-than-average inflation.

Looking Ahead

Meyer's success in transforming Mirion's exposure management strategy has not only elevated Mirion's cybersecurity posture but has also positioned the company as a resilient leader in its industry.

Today, Meyer's security team has full visibility of its entire attack surface and digital supply chain and is focused, efficient, and confident in its ability to protect the business from emerging threats.

"We're better protecting our proprietary data, the data of our customers, and better protecting our shareholders," he explains.

Looking ahead, Meyer remains committed to advancing Mirion's security strategy, noting, "To improve our security posture, we're going to keep doing what we're doing. It's a constant challenge because we continue to have a strategy to grow through acquisitions."

As Mirion continues to grow and navigate the complex landscape of interconnected business units, CyCognito will remain a critical ally in its exposure management strategy.

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit **cycognito.com**.

CYCOGNITO