CYCOGNITO

CASE STUDY: GAMING INDUSTRY

CyCognito Platform delivers strong ROI to Scientific Games with increased attack surface visibility and reduced risk and complexity

Business Challenge

Global CISO Kevin Kealy sought a solution that would give him visibility to previously unknown attackerexposed risks and help him report the organization's security status to the Board of Directors, including granular security details for each business unit.

Why CyCognito?

Scientific Games first had access to the CyCognito platform when their previous corporate parent, MacAndrews and Forbes, deployed the CyCognito platform. When Scientific Games became an independent company, Kealy wanted his own subscription to the platform for attack surface visibility and to streamline and automate processes that would otherwise have been manual and piecemeal

Results

By adopting the CyCognito platform, Scientific Games achieves improved attack surface visibility, more efficient management of the business units' security, and ongoing improvements to overall attack surface management workflows. "The CyCognito platform helps us operate smoothly and provides reduced risk, reduced complexity and increased visibility," says Kevin Kealy, Global CISO, Scientific Games.

"The biggest win for me is visibility," says Kealy. The CyCognito platform provided immediate visibility to previously unknown assets in his organization's attack surface and continues to do so. "We have significantly reduced the footprint of obsolete devices; identified them and cleaned them up," he says. One notable example was an unmanaged asset that was an artifact of a joint venture in China, dating from 2015 (well before he had joined the company).

SCIENTIFIC GAMES

CUSTOMER PROFILE

Scientific Games is a global leader in the gaming and lottery industries, offering an integrated portfolio of technology platforms, robust systems, game content, and professional services and marketing solutions. The gaming spaces it operates in include lottery, slot machines, card shufflers, online gaming, and sportsbook. Scientific Games owns well-known brands, such as Bally, Williams and SciPlay, and operates slot machine franchises like Monopoly, James Bond, and Fortune 88.

Headquartered in Las Vegas, Nevada, Scientific Games has approximately 9,500 employees worldwide, with offices and employees on six continents.

ORGANIZATION'S SECURITY GOALS:

- Finding externally exposed risks
- Visibility into shadow IT
- Identifying orphaned assets and retiring or upgrading as appropriate
- Automating manual processes for better security at a lower cost

The CyCognito platform identified the asset and the path that connected it to Scientific Games, but that asset was unknown to the security and IT teams, and they had to track down the people involved in the original joint venture deal to validate the asset's business origin and remove it.

The CyCognito platform also helped him identify a shadow IT effort for a marketing incentive that could have inadvertently exposed customer data. Kealy and his team were able to step in and provide governance for the effort to eliminate the risk. This kind of visibility has ongoing benefits; he notes his business counterparts' amazement that he is able to detect new environments that haven't been publicly released yet.

Another notable example of the CyCognito platform providing visibility that helped him reduce reputation risk was the platform's discovery of web cameras identified as being owned by Scientific Games. In reality, the IP addresses had previously been used by Scientific Games, but had since been released back to the telecommunications company, who neglected to update the IP address registrations. Since Scientific Games was inaccurately associated with those assets, any improprieties with those IPs could have reflected poorly on the organization.

> **With the CyCognito platform we have greatly improved our attack surface visibility and enhanced our attack surface management workflows. The platform helps us operate smoothly and provides reduced risk, reduced complexity and increased visibility."**
>
> **Kevin Kealy**
> Global CISO, Scientific Games

Efficient measurement and reporting to executive leadership and the Board of Directors about the security status of the many business units whose security he manages is another key benefit. "The metrics I share with senior leadership focus on how much I have spent on incident response for the year," says Kealy. "I provide a breakdown by business unit with their A-F security grades as assigned by the CyCognito platform, so leadership can see the business units' security in context with each other. Based on this reporting method, one of my business units was motivated to move from worst to second best and hasn't had an incident since then. And the board is able to see the business value of each business unit's security efforts."

Looking ahead, Kealy anticipates improving workflows based on the rapid and continuing advancements of the CyCognito platform. The introduction of the Remediation Planner, for example, allows him to quickly assess the scope and impact of security posture improvement plans — for his organization as a whole and by business unit.

Ongoing innovations like this that automate processes are highly appreciated. "Automation is king in security. Every time you do something manually, you introduce human error into the process. With the automated CyCognito platform," Kealy says, "We have greater visibility, greater fidelity and greater security."

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