ALIGNING IT SECURITY AND COMPLIANCE TO IMPROVE TRACKING OF ACTIVITIES AND THREATS ACROSS CONTINENTS

A global energy producer deploys Spyglass, Catapult's centralized security and compliance solution, and sees results from day one

A major international energy producer was looking for a way to centralize its cybersecurity operations, making it easier for IT to track user activities and threats across continents. As a global industry leader with locations in over 20 countries, this company holds itself to a high standard for innovation and its leaders see evolution—especially regarding cybersecurity—as a non-negotiable. Thus, they partnered with Catapult to adopt a cutting-edge IT security and compliance solution: Spyglass.

Built on Microsoft technologies including Enterprise Mobility + Security, Power BI, and Operations Management Suite, Spyglass helps this company more efficiently and effectively detect threats, allowing administrators to view, locate, and track global network activity via a single dashboard. Most importantly, Spyglass offers ongoing service, on-demand technical expertise, and a dedicated coach to foster perpetual improvement, aligning practices with evolving industry regulations and an ever-shifting security landscape.

THE CHALLENGE

Catapult knew that they would have to meet the complex set of needs, regulations, and compliance standards that this global company required. The company had competent security staff in place, but an excess of competing projects and disparate information made it challenging for administrators to track and act on critical security alerts. Additionally, multiple security tools operated as siloed solutions, which did not share signals or correlate information. The lack of integration was very difficult to manage and made poor use of existing data, which—with the help of predictive analytics—could help power a more proactive security practice.

Through combined efforts, Catapult experts and the company's security staff implemented Spyglass in just six weeks, automating signals from over 15 solutions, streamlining user adoption with the help of video content, and harmonizing formerly siloed data to provide visual insights. By consolidating signals from all the different tools, it became much easier for the security team to identify real threats and to tactically remediate them without interrupting users. Spyglass also provided the company with an all-encompassing view of their security needs to ensure compliance and protection at a glance.

Spyglass helped connect disparate cybersecurity tools and funnel information from the company's entire security ecosystem into a single dashboard. Additionally, Spyglass created a customized solution framework based on the company's specific security and compliance needs and aligned tools and policies for future success with ongoing coaching and guidance.

RESULTS: ROI FROM DAY ONE

On day one, the Spyglass Security Coach could detect suspicious signals and anomalous user behavior, uncovering the perpetrators in the initial stages of updating direct-deposit information for over 50 compromised accounts. Catapult worked closely with the company's security team to intercept this massive attack, and within hours of the discovery, provided policies and settings changes to remediate and prevent similar attacks in the future.

They successfully halted an attack that would have defrauded the company over $300K. This discovery helped the company dodge a time and cost-intensive investigation. They saved a potential of $900K in downstream investigative costs and captured all actions and locations of the bad actors. Additionally, since no information was stolen, the company avoided the costs and reputation damage associated with having to publicly disclose a breach.

> "For years, the trend in cybersecurity has been for companies to resolve each new challenge on an ad-hoc basis by accumulating more and more products, but we knew that this approach would eventually bring endless rounds of trial and error, the need for IT staff with an impossibly unique set of specializations, and disconnected data points. This is why we opted for a more modern approach."
>
> *Director of IT*

ANOTHER CASE IN POINT: THE EQUIFAX BREACH

Known to be the largest hack ever recorded, the 2017 Equifax breach exposed personal information of at least 147 million people, including their names, birthdays, addresses, social security numbers, and driver's license numbers—putting customers and employees at serious risk of identity theft, and damaging the credit bureau's reputation. The breach, which Equifax blamed on a web server vulnerability in its open source software, could have been easily prevented by a modern security and compliance solution like Spyglass.