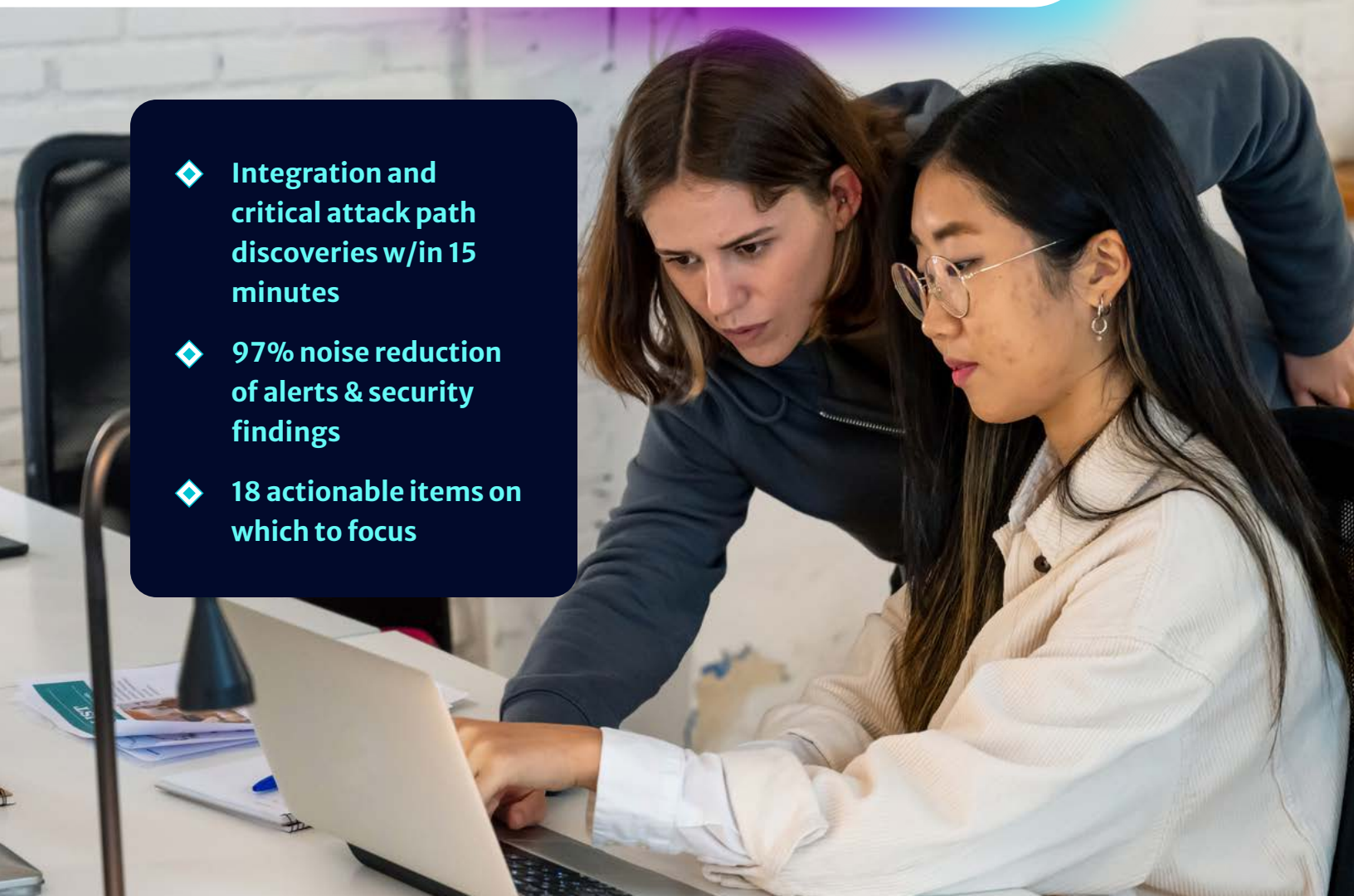
Lightspin | PageUp

Case Study

Context-driven cloud security enables PageUp to focus on their most critical vulnerabilities

How Lightspin's critical attack path offering added business value to PageUp, giving their engineers time back in their day to focus on bigger challenges in the cloud



- Integration and critical attack path discoveries w/in 15 minutes
- 97% noise reduction of alerts & security findings
- 18 actionable items on which to focus

The Challenge

The PageUp Security & Compliance team had been using a cloud security tool that provided them with visibility, but in the form of hundreds if not thousands of error messages and alerts, without any context. Reviewing such an enormous number of alerts without an understanding of actionable exploitable gaps in their nearly 100 AWS cloud account structure cost their team too much valuable time.

PageUp needed a cloud security partner that could provide them with the visibility and coverage they needed, but most importantly, the context to know what was important and what was not.

"From the moment of integration, Lightspin's platform provided our team with 18 critical and actionable attack paths to focus on, rather than the 20K – 30K CIS benchmarks that other tools were sending us. CIS benchmarks are designed to be generic, but with Lightspin, the context and the potential attack paths surfaced gave our team the ability to easily understand what we needed to remediate and why."

Brad Barnett
CTO at PageUp

PageUp

Industry: Software
Customers: 50 million+ users in 190 countries

PageUp is a SaaS talent acquisition and management provider, offering a full suite of modern tools to help businesses attract, engage, and retain high performing teams and deliver measurable results. PageUp provides exceptional hiring and engagement experiences with Recruitment Marketing (sophisticated content management, marketing automation and candidate relationship management), Recruitment Management, Onboarding, Learning, Performance, and Succession tools.

PageUp has a mature AWS presence in terms of operation and security, with over 80 AWS accounts thanks to their "Castle within Castle" design of AWS based on Landing Zone. This was presented at AWS Summit 2019 & On-Demand Elevation in AWS request process.

The Solution

When PageUp's CTO, Brad Barnett saw Lightspin's attack path platform, he knew he had found a special solution. "Everyone operating in the cloud needs context," commented Brad. **"Lightspin offered a context-driven approach to cloud security, which helped us focus on the real problem instead of looking at 20K alerts, which is what most 2nd and 3rd generation CSPMs would give."**

Lightspin delivered the actionable insights that PageUp needed to add great value and reduce the time Brad's team needed to comb through endless lists of non-critical alerts. Lightspin's graph-based technology is what drives the solution's ability to make the right connections between otherwise disparate findings across CVEs, risky permissions, escalated privileges and connected identities, misconfigurations, and beyond. Ultimately these connections map critical attack paths for Security and DevOps teams, giving them the proper context they need to better understand the highest priority and critical risks in their cloud environment. In so doing, Lightspin delivers maximum cloud security value, while minimizing the cloud security resources (engineers and developers) required to do so.

"Lightspin has given PageUp's cloud security engineers valuable time back in their day. Instead of spending multiple weeks discerning critical from non-critical alerts, attack paths reduced the guesswork and provided the ability to prioritize the problems that matter most. Our team now remediates critical issues in a week instead of in a matter of weeks or months"

Brad Barnett
CTO at PageUp

Shifting from PageUp's previous cloud security tool to Lightspin was a no-brainer. The value add was immediate – within the first 15 minutes of connecting to Lightspin's platform, PageUp discovered 18 actionable items to work with, alongside the actionable insights of how to remediate these issues. PageUp's security and compliance team are now better able to focus on more complex business issues and speed up time-to-market.

The Results

- **Integration and critical attack path discoveries w/in 15 minutes**
- **97% noise reduction of alerts & security findings**
- **18 actionable items on which to focus**

Lightspin

Lightspin is home of the attack path. Our graph-based cloud security is built by and for cloud engineers. Lightspin's next-gen cloud security platform protects cloud and Kubernetes environments from build to runtime and simplifies cloud security posture management and cloud native application protection for security and DevOps teams. Using advanced graph-based technology, Lightspin prioritizes risks across the cloud environment focusing security efforts on the critical issues that matter most and provides ready-made IaC to DevOps engineers. Lightspin is proud to focus on small and medium-sized businesses running workloads in the cloud, offering a free version of the robust platform. Lightspin also serves Fortune 500 customers across the globe and is headquartered in Tel Aviv, Israel with offices in New York City, USA.

To learn more, visit **www.lightspin.io**