{ƨf/ȅōŜℕ È ¦ ōƛlj

Thank you for downloading this SolCyber case study. Carahsoft is the Public Sector distributor for SolCyber solutions available via NASPO ValuePoint, TIPS, and other contract vehicles.

To learn how to take the next step toward acquiring SolCyber's solutions, please check out the following resources and information:

For additional resources:
carah.io/SolCyberResources

For upcoming events:
carah.io/SolCyberEvents

For additional SolCyber solutions:
carah.io/SolCyberSolutions

For additional cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
SolCyber@carahsoft.com
844-445-5688

To purchase, check out the contract vehicles available for procurement:
carah.io/SolCyberContracts

For more information, contact Carahsoft or our reseller partners:
SolCyber@carahsoft.com | 844-445-5688

SolCyber | Ubiq

SolCyber x Ubiq

INTRODUCTION

SolCyber helps growth-stage cybersecurity startup Ubiq strengthen their security posture and efficiently report on security to their board.

THE CLIENT:

Ubiq is a growth-stage cybersecurity startup that enables engineering and security teams to integrate client-side encryption directly into their applications via APIs in minutes, mitigating their breach and data theft risk.

THE SITUATION:

Cyberattacks are becoming increasingly prevalent, with small and midsize businesses being targeted on a regular basis. The attacks are increasing in frequency and severity, and the

reputational damage and financial repercussions of ransomware attacks are causing businesses to collapse.

This is especially true of early-stage and growth-stage companies that are still building name recognition and trust with customers.

Boards today are keenly aware of these cyber risks and are having more conversations around cybersecurity than ever before — especially across sensitive and high-risk industries. Reporting on cybersecurity is becoming a regular agenda item in board meetings and business leaders are expected to take a more aggressive approach to protecting their data from malicious players.

THE CHALLENGE:

As a growth-stage startup, Ubiq operates a very lean, cross-functional security team across product development, DevOps, and infrastructure. One of the challenges a small team presents is that resources need to specialize in several security domains, which can be difficult given how rapidly threats and priorities can shift. As much as the team wanted to do more and go deeper in certain areas, they were limited by time and resources.

"As a security company, security is ingrained in everything we do. But at the end of the day, we have finite resources, which forces us to prioritize key areas," says Ubiq CEO Wias Issa. *"But even after prioritization, we knew that to fundamentally improve our security program, we would need to nearly* ***double the size of our security team****."*

During a recent board meeting, one member asked when the company would start providing expanded reporting on its cybersecurity program and posture. Issa was pleasantly surprised to hear the question, given how young the company was. As someone who has worked in cybersecurity for the last 21 years, he understood the board's concern. Unfortunately, to further strengthen the company's security posture and reporting capabilities, Issa knew he would need to double his team or hire an MSSP to focus on critical, high priorities areas.

WHY SOLCYBER?

Ubiq decided to partner with SolCyber and purchased the Foundational Coverage package, along with a few additional add-ons based on the company's specific needs. What drew Issa to SolCyber was the fact that Ubiq would not have to separately acquire any security technologies.

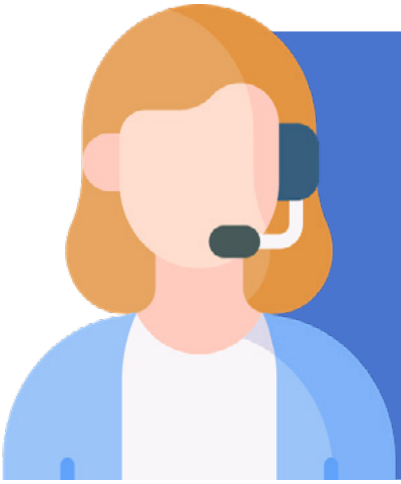
"Most MSSPs require clients to determine what products they need, what areas of their environment they want to focus on, ***comb through the 3,500 security vendors****, interview top vendors, and then establish contracts before even engaging the MSSP,"* notes Issa.

"SolCyber, on the other hand, knows that every company needs certain "table stakes" cybersecurity tools to protect their organization, so they established relationships with the top vendors in each category and hand clients like us a curated tech stack that's ready to go from day one."

Because Ubiq is a growth-stage startup with a lean team, they were grateful to skip the upfront work of finding security vendors, which can sometimes take six to nine months. With vendor contracts already in place, thanks to SolCyber, the Ubiq executive team could focus on what they do best — building and running a company.

"Thanks to SolCyber, we have someone watching our back on an ongoing basis," says Issa. *"They helped us increase our security posture tactically. If something happens, I know they'll find and respond to the issue quickly. But they also help us strategically, meaning our cyber resiliency will improve over time."*

Issa and his team now feel their security program has materially improved with the addition of leading technology, effective security tools, and a reliable detection and response team. Despite being a young company, the team can report on active cybersecurity efforts to the board with minimal effort and rest assured that their security posture is as strong as it can be.



"The SolCyber business model lends itself very well to small and midsize businesses," claims Issa. *"They are always available to listen and give smaller companies like Ubiq the same time and attention as a larger corporation. I know that when I call,* ***SolCyber will pick up****."*

SolCyber

About SolCyber

SolCyber, a ForgePoint company, is the first modern MSSP to deliver a curated stack of enterprise strength security tools and services that are streamlined, accessible and affordable for any organization. SolCyber is disrupting the status quo, by providing a new standard of managed security services that work to reduce cyber risk, wastage, and complexity. We believe in a secure environment for all. For more information about SolCyber, visit **solcyber.com** or follow us at **@SolCyberMss** or on **LinkedIn**.