

## Simplifying the Messy World of Encryption and Key Management via APIs.

*An Interview with Wias Issa, CEO, Ubiq*

**Companies of all sizes are developing applications** which allow them to service employees, customers, and partners more efficiently and effectively. It's been said that "every company is now a software company," and whether you believe that or not, it is indisputable that many companies are building and deploying apps daily and that those without internal development resources are relying on outside firms who build apps on their behalf.

Continuous and rapid development is no longer a niche field. And applications hold the sensitive and proprietary data which give companies a competitive advantage. It is therefore imperative that custom-built applications remain secure, from the first line of code through production.

For years, security teams have argued that they should be integrated into the software development lifecycle, ensuring developers only deploy applications that have been checked for security and/or have built-in critical security controls. This, however, slows delivery and the highly sought-after DevSecOps has never come fully to fruition for most companies. That said, developers are not ignorant to the need for secure development, even if they're not trained specifically in security practices. As such, there has been an increase in the number of development platforms which introduce turnkey security controls or capabilities such as authentication, or perform security checks throughout the development process, helping the busiest developers include security along the path to deployment.

For one company, Ubiq Security, out of San Diego, CA, development tools that enable securing coding practices didn't go far enough. Their mission was to introduce a security platform that enables developers to incorporate data encryption directly into their applications in minutes, with as little as 3 lines of code and 2 API calls, and without requiring any past encryption or cryptography experience. Wias Issa, CEO at Ubiq, sat down with TAG Cyber to discuss their unique platform.

**TAG Cyber:** *With all the tools on the market built for developers, why did you want to build another platform for application security?*

**Wias:** Most of the security-focused developer platforms out there today are centered around secure coding practices and identifying vulnerabilities. Very few enable developers to build security controls into their applications.

Over the last 7-10 years, we've seen the emergence of what many are calling the next trillion-dollar software wave—API-based developer platforms—led by companies such as Atlassian, Twilio, and Stripe, to name a few. But when you take a deep look at the vendor security industry, we're way behind the API curve—the majority of vendors are still in the hardware and software game, requiring customers to deploy technology into their infrastructure or onto their systems, which is an expensive and resource-intensive activity for customers.

**TAG Cyber:** *At a technical level, what does the platform do for developers and application development?*

**Wias:** It enables developers to quickly build data encryption directly into any application, across multiple programming languages, without requiring prior encryption knowledge or expertise. And as new cryptography and encryption innovations emerge, we adopt them into our platform, so they don't have to.

**TAG Cyber:** *What are the primary reasons Ubiq sees this as a gap in the market?*

**Wias:** For years we witnessed countless developers, application security engineers, and infosec experts express frustration around the complicated and messy world of encryption, cryptography, and key management. Things that are very difficult to get right and too easy to get wrong. So, we made it our objective to simplify it down to a few lines of code and 2 API calls, eliminating all of the messiness and complexity.

**TAG Cyber:** *What are the major benefits or reasons why developers would look at this solution versus what they are currently using?*

**Wias:** Plain and simple, it saves them the time, hassle, and risk of figuring it out on their own, and allows them to get back to building a great product.

**TAG Cyber:** *How easily can a developer start embedding/integrating encryption at the application layer using the Ubiq platform?*

**Wias:** A developer can go from having no encryption controls in their application to full encryption and integrated key management capabilities in as little as 5 minutes. But don't take my word for it, check out our [demo here](#), where our Chief Architect integrates encryption into two different applications in less than 7 minutes.

**TAG Cyber:** *One topic that always arises when discussing encryption technologies is key management, and how difficult this is for many organizations, how does Ubiq address this?*

**Wias:** "I love and enjoy key management," said no one ever! Key management is an ongoing and expensive pain in the (you know where) for everyone, so we built our platform to handle all of the complexities of key management (secure storage, rotation, etc.), while ensuring that only our customers can access their keys.

**TAG Cyber:** *Onto the world's worst kept secret, developers and security teams don't always seem to get along. Does that change?*

**Wias:** Haha! Very true. I believe it does change. Look, at the end of the day, developers want to build great products and security teams want to make sure those products are built with security in mind. Our platform empowers developers to quickly and elegantly build encryption into their applications, so they can get back to focusing on their product while also satisfying the security team's needs of building strong encryption controls directly into the application, which means one less thing for the security teams to have to worry about—acquiring, deploying, and managing another security tool—after the application is deployed into production.

***TAG Cyber:*** *How does this solution affect the cyber risk to an organization and their threat model?*

**Wias:** I believe it drastically improves it in two ways. Firstly, it eliminates the risks of DIY encryption approaches. Especially for those who are bold enough to roll their own crypto. Secondly, introducing encryption at the application layer, which is really the point of data inception, access, etc., improves an organization's overall threat model, because you're no longer relying on just "unaware" storage-layer encryption tools and controls, which haven't materially involved or improved in 20+ years.

***TAG Cyber:*** *What would you say are the 3 major business benefits to an organization adopting your technology?*

**Wias:** It's really 4 things: save developer time, reduce risk, reduce costs, and an improved threat model. We believe that by enabling developers to build encryption controls directly into their application, we save developer time and allow them to focus on the core business; reduce the risks related to DIY approaches; save the downstream costs related to acquiring, deploying, and managing a plethora of disparate encryption tools; and improve an organization's threat model by introducing encryption directly into the application layer and not simply relying on storage-based encryption controls.