Interview: Rocco Donnino – Executive Vice President of Corporate Development, AppRiver, Switzerland



"The company´s focus is Email and Web security, and in today's environment this must be done in layers, an approach called "defence in depth"."

10.11.2017

Tags: Switzerland, AppRiver, Cybersecurity, Digitalization

Rocco Donnino, executive vice president of corporate development of AppRiver AG, a cybersecurity company with headquarters in Switzerland and Florida, US, discusses the strategic steps in establishing AppRiver across Europe and the services they provide, specifically the layered security approach portrayed throughout the healthcare and life science sector. Furthermore, he highlights the advantages of having a cloud-based system and the importance of cyber protection as our lives become more digital.

Could you please introduce our international readers to AppRiver and your current operations?

AppRiver is a global Cybersecurity company, focused on Email and Web protection that specialises in small- to mid-sized organizations. In 2012, we formed AppRiver AG to service the European market. Positioning the company in Switzerland was a strategic move to work closely with our partner, green.ch, a data network host that uses our cybersecurity technologies, to protect their customers. When green.ch built a state of the art data centre, it was an opportunity for us to plant our feet in Europe, and now we run completely as a Swiss-owned entity that conducts operations under the Swiss government legislation for privacy and data protection.

We realised early on that having our services within Swiss borders was important for expansion throughout the DACH Region (Austria, Switzerland and Germany) and, equally, we have located

ourselves in the UK, Spain, the Nordics, the Netherlands, France and most recently, Italy. All our services are cloud-based; therefore, our customers' mission critical information never leaves Switzerland.

What is the strategic importance of European operations within the global AppRiver group?

[Featured_in]

Thus far, Europe has been a success! The UK, Swiss and German markets are very strong for us, as they are large in terms of scale, and have many small- to mid-sized businesses that value our services. Furthermore, our strong interaction with green.ch allows us to increase distribution of our technology to their customers. With 15 years of experience in the industry, we have worked diligently with their customers on the migration of Green's hosted Microsoft Exchange to our Secure Hosted Exchange platform.

What was the key strategic step when you made the move to Europe?

One misstep that many companies make when relocating to Europe is they believe throwing money into the marketplace automatically gains traction, though this is not always the case. We decided to focus on certain key regions like DACH and offer language support within our applications, while guaranteeing our product was the best in breed for productivity and security.

Furthermore, we can offer local assistance 24/7/365 days per year with white-glove technical support service through our trademarked program: Phenomenal Care®. This has been an enormous success and ensures we can always deliver superior technical support to our customers in their native language.

What are the main challenges you have faced?

[related_story]

Brexit is an obstacle we are currently dealing with, as a large amount of our business is located within the UK. The lack of clear compliance laws is also a challenge since it delays the adoption on much needed security and encryption policies, however, the General Data Protection Regulation (GDPR) is quickly changing that situation.

Nevertheless, the main challenge has always been ensuring that when we enter a market we meet the specific desires of our customers. We are not able to utilize a blanket approach and attack each country in the same way; therefore, we must tailor our service depending on the situation, as each

region has its own specific needs and customs.

How is your layered defence service applicable to the healthcare and life science industry?

The company´s focus is Email and Web security, and in today's environment this must be done in layers, an approach called "defence in depth". Each person uses email in some form, and AppRiver was founded to prevent cyberattacks on cloud customers that did not have a large abundance of resources. This is done upstream; meaning, email protection is conducted by securing and blocking the threat before it hits the customer's inbox. This success led to our clients wanting us to take over their entire mailbox and mail server. As a result, AppRiver launched our Secure Hosted Microsoft Exchange offering in 2006.

Today, an increasing amount of threats are Email and Web-based. In that regard, we believe that Email and Web security go hand in hand; therefore, we monitor the network each time our clients access the internet so they do not have access to any viruses. Throughout all these processes, we provide layers and create depth in the protection system using services such as anti-spam, anti-virus and anti-phishing.

In the healthcare industry, email encryption has been an extremely strong area for us. For example, when a doctor sends an x-ray file to a patient via email, it is like sending a postcard at the post office. The perception is that nobody can view this information, but the reality is that administrators can see this confidential file at any time. Therefore, we have developed an end-to-end encrypted technology, so the file can be sent privately by the doctor and the patient can encrypt the message at no extra cost. This allows physicians to send private files to their patients from their office.

Furthermore, we are the only company that offers a technology allowing an incorrectly sent file to be recalled by the doctors, as the file resides in our own data centre. Also, files can be prevented from being forwarded to ensure only the chosen individual can view the patient-sensitive information. In general, it is about providing a safe, private and easy-to-use service. The fact that our platform is interoperable across all email systems and readily available via an app on mobile devices, means we are always in touch with our clients' needs and how they interact through the course of their business and lifestyle.

What makes the healthcare industry such a soft target for cyberattacks?

They do not fully understand the security applications available to them in the market. All the services are available to a doctor through a single subscription, allowing them to send the information to their patients who subscribe to their network. It is about establishing a social network based upon a circle of trust between doctors and their patients. Also, medical associations are great avenues for us since they pass on to their members the benefits of working with AppRiver's productivity and security services.

The attack on the NHS last year caused widespread concerns and clearly indicates the significant importance of Web and Email protection systems in ensuring information is kept private to build confidence and trust within the patient population. Using our experience in the sector, we can provide best practises across the healthcare industry.

How would you describe your customer base?

We have customers in 49 countries across the globe, and despite our technology being easily upscaled to large enterprises, we decided from an early stage to target small- to mid-sized companies. These generally are sub-100 staff members and equally entail country affiliates of the larger healthcare players. This approach gives us a clear positioning on the needs of the market.

A key factor in the success of our products is that we are a cloud-based organisation; therefore, the administrator, customer or partner servicing the customer can view the information on a single pane of glass, including email, web security and encryption. It requires no software and is all located in the cloud, allowing the user to simply turn on a product and obtain the licence. Furthermore, everything is a month-to-month subscription, rather than an upfront payment and annual contract style scheme.

Where do you see the European network of AppRiver evolving in the future, especially within the healthcare space?

Our technologies have a tremendous amount to offer in this sector, especially as the "bad guys" keep getting worse. Across the industry, it is hard to find a business that specialises in our areas that has not been acquired or consolidated. AppRiver has done this successfully for over 15 years. We have always focused on security, despite branching out over the years into productivity tools that fit together with the services we offer.

We feel that the healthcare industry is an area we are aiming to strengthen in the future and we must better educate this sector, as well as reach out further via partnerships. In turn, we will see the healthcare aspect of our business continue to grow as we achieve success in this specialised area.

See more interviews