Secure Communications

An Interview with Mike Koclanes, President, Vaporstream

Mike Koclanes

EDITORS' NOTE *Mike Koclanes has more than 30 years of management experience in IT, messaging, network, storage, and data management. He has held executive positions at leading technology companies like VMware and Sun Microsystems. Prior to joining the Vaporstream team, Koclanes was Sr. Director of Global Networking and Messaging services at VMware, Inc. In 2008, he founded Boulder Data Solutions serving as President and CEO. Prior to this, Koclanes was President - North America of Plasmon and Founder, CEO, and CTO of CreekPath Systems Inc. where he was recognized as a "Storage CTO of the Year" in 2003 by the Enterprise Strategy Group. Koclanes raised venture capital to start Creekpath and that firm is now part of Hewlett Packard through its acquisition by Opsware. He has also served as Vice President of Marketing, GM of Storage Automation, and Director of New Products at Sun Microsystems and CIO at Exabyte. Koclanes has a degree in Computer Science from the Missouri Institute of Science and Technology (MS&T), formerly University of Missouri-Rolla/Missouri. He was in the first group of inductees to that University's Academy of Computer Science.*

COMPANY BRIEF *Vaporstream (vaporstream.com) is a business technology company innovating e-communications solutions to improve the productivity, efficiency, and security of business. Vaporstream products are based on its patented Streamed E-Communications Platform that uniquely creates e-information exchanges that cannot be intercepted, stored, downloaded, printed, or distributed. Vaporstream is being rapidly adopted as a new e-communications standard by IT professionals, small and medium businesses, and global enterprises to improve collaboration, access, and responsiveness, and to protect confidential communications.*

What led you to found Vaporstream?

Vaporstream was a unifying concept that tapped into our belief that people should have the right to express themselves freely and clearly with certainty that only the intended recipient will get the communication, and that it won't be taken out of context or be used against them.

In the business world, the time came to declare that we all have a responsibility to protect the privacy and confidentiality of our IP. We have a responsibility to our shareholders, our fellow employees, and our customers to protect them and their confidential information.

We felt that if we could create a solution like this in today's increasingly insecure world, it would have great value. With the pace of today's business activity and with global, highly distributed workforces, a method for talking to one another using modern technologies that ensure that information couldn't be breached, forwarded, or propagated would represent a viable business proposition.

Is there much competition in this space?

This is a disruptive technology; the incumbent is e-mail in the enterprise. It is still a $12-billion per year business and the technology was written where things are stored and forwarded, and it's so pervasive that there is a lot of momentum behind it. Nonetheless, there is a growing number of competitive so-called secure messaging solutions, but there is nothing geared to business and professionals that has our level of privacy, containment, and governance. As recent rulings by the FTC indicate, some of these consumer products, like Snapchat, have falsely advertised their claim of disappearing messages.

All of the Internet messaging businesses are fundamentally based on the model of letting you use their service, pretty much for free, because they want to capture and market your habits and information. We're a bit disruptive to that, because we're creating a system where the information isn't stored. There is no way even for Vaporstream – much less anyone else – to see your messages.

It's bucking the trend so there wasn't a lot of social networking companies developing this because their investment in technology was counter to this. However, the growing interest in privacy issues is causing many new competitors to emerge. Furthermore, messaging applications have been attaining excellent valuations through acquisition, as other platforms try to address the privacy void.

How does this technology work?

Encryption is necessary for this environment – the problem is that encryption alone is not sufficient. If you send an encrypted message across the Internet, it might very well avoid interception. But once it gets to the recipient and is decrypted, it's now clear text that can be copied, pasted, forwarded, or printed. So encryption only solves part of the problem.

The other piece is containment. On that side, we had to revolutionize the approach and develop a technology where nothing is ever written to permanent media. It only exists in volatile RAM. So it's going to be as ephemeral as a voice conversation.

The notion is that we separate the message body and the header. When you send a message with the Vaporstream application, which could be on your computer or on a smartphone, the message header gets encrypted separately from the body. The body is then encrypted with a public key for which the private key needed to decrypt only exists on the specific receiving device. It's encrypted directly on that receiving device – Vaporstream doesn't even have access to it.

The message header and body goes into our cloud. We have to be able to decrypt the headers so we know where to send them. When the recipient clicks on the message, the body is pulled down. It's fully encrypted while in our memory and as it's being delivered. Once it's on the recipient's device, that recipient is the only one who has the ability to decrypt the private key that decrypts the body. The message header and body are never shown at the same time. Once read or replied to, the message no longer exists, anywhere.

It's a very unique approach and was not trivial to implement properly. Vaporstream has patented this approach.

What is the market for this product?

The product is targeted to organizations and enterprises and tends to be those enterprises where there is most concern about protecting your IP for key groups such as corporate executives, development teams, and M&A teams. Another example is dialogues with HR, when communicating information that is only intended for a specific employee to see. It is also used in communicating confidential passwords or account ids, with employees or customers.

Would this be valuable across all industries?

The use cases exist in every industry. It's ideal for companies that have a lot of M&A activity and for those whose IP is at risk, as well as those that have international workforces that travel to countries that are well-known for intercepting communications. It is also perfect for those industries where confidential communications are regulated to protect the consumer, such as medical with HIPAA and financial services with account information. ●