Network Security Monitoring delivered through a "Software as a Service" Model by MetaFlows CEO Livio Ricciulli, Part I

Enterprise organizations face the daily challenge of ever-growing threats to their network and IT infrastructure. Not only are these threats growing, but they are constantly changing as well, forcing companies to adapt by changing not only their tools but also their training. Today, I'm talking with MetaFlows CEO Livio Ricciulli about how MetaFlows is addressing these problems by delivering network security monitoring using the "Software as a Service" model.

Joshua: *Livio, thanks for taking the time to talk with me today. The* network security monitoring *space is filled with players today, but nobody is delivering a security product quite the way MetaFlows does. Can you talk to me a little bit about what makes your company and product unique in such a crowded space like* network security monitoring*?*

Livio: We're the only system in the world that can do network security monitoring using the software as a service model. What that means is that the user does not host any of the system, except a very small portion of it – the agent that detects the threats – on their own network. The database where the events are stored, and all the software that analyzes the events, creates reports, and does the analysis, reside on a web server. You're probably familiar with this model used by other "software as s service" applications.

Joshua: *Salesforce is a good example.*

Livio: Another example would be accounting with Quickbooks online – you don't host the data and the application. Everything goes through a browser. We're the first to provide a complete enterprise-ready, very sophisticated dashboard for monitoring the security of an enterprise entirely through a browser. Users simply install an agent that runs in the network and feeds events to a system that resides in the cloud. Then, the user can basically forget about the agent. It just runs there all the time. Everything that you need can then be found in the browser-based dashboard.

This promotes online collaboration between multiple analysts because you can access the data from a secure browser from anywhere in an environment in a way that's as secure as online banking.

Joshua: *How does this affect budget and existing analyst workload?*

Livio: This solution does two things. On the one hand it makes network security monitoring cheaper because most of the processing and the software updates are all taken care of centrally. When we do an update, it is immediately available to all our users. This is common to other software as a service services. But in the realm of security, it's an added value.

Another value-add is correlation. Our customers aggregate all their event data to a single location – our cloud. With that volume of data, MetaFlows can do a more effective job of correlating events across enterprises.

Joshua: *So are can you cleanse the data for analysts, such that they focus on critical threats across all data centers?*

Livio: We've also developed our own algorithm to rank security threats. This will help us to improve security as

well because it will alert people with a similar security posture to pay more attention to certain events than others. This type of targeting is not possible using a traditional model where everybody stores their own events in their own database and they don't share any information. This is very new. Nobody else is doing this as far as I know.

Joshua: *Can you reduce the amount of time security teams spend implementing, configuring and maintaining on-premise software?*

Livio: MetaFlows supports off-the-shelf hardware, meaning you can download our agents for practically any hardware you can buy. We also sell inexpensive appliances for those wanting a more traditional hardware-based solution. In either case, you download an agent from our website that then does traffic monitoring in the enterprise. It includes a suite of applications that are designed to give very broad detection capabilities ranging from looking for bots – computers that are subverted to become Trojan horses- to more of a generic intrusion detection system, where we look for events, like somebody using peer to peer file sharing, that is not a permitted use of the network.

The agent does the monitoring, and when an event is detected, the event data, not the payload just the event, gets fed to our MetaFlows cloud in real time. These events then get stored, correlated, and archived in the cloud. Then, users can interact with Metaflows to look at events, correlate them, and get a picture of what is going on in their network, all through a browser.

Joshua: *Since this is security log data, can you include other log data from devices on a network?*

Livio: We also support log management. We can store all the events logged by third-party devices on the network. So, essentially, we can unify the IDS function and the log

management function all in one place. And this solution is turn-key, you don’t have to install, configure and setup anything, just download it and run it.

In the next blog entry in this interview series with Ricciulli he will explain how MetaFlows is optimizing network security monitoring and performance.