ceocfointerviews.com

Issue: January 18, 2016
The Most Powerful Name in Corporate News

Revolutionary New Unified Cloud Security with One Security Stack offering the Entire Back-Up Fundamentals as an In the Cloud Utilities

Babak Pasdar
Founder & CEO
Bat Blue Networks

CEOCFO: ***Mr. Pasdar, the tagline on your site indicates that Bat Blue Networks is the cloud security company. How do you earn that tagline?***
Mr. Pasdar: We are the first and only company to offer the entire stack of security fundamentals as an in the cloud utility. Today organizations have to select a number of physical products that are logistics dependent. Then there are a number of in the cloud security proxies they have to choose. These proxies have a number of limitations, such as being limited to the web, limited to proxy aware applications and they are directional. Some of them can only protect a browser going out to the Internet, while others can protect Internet coming into a web server. However, nothing out there can deliver the entire security stack as an in the cloud utility like Bat Blue Networks.

CEOCFO: ***How are you able to have such a comprehensive offering, when others do not?***
Mr. Pasdar: It goes back to a failure of imagination and what drives the business side of the security industry. For example, everyone tries to force you into certain categories, but the Bat Blue Networks approach is completely different. Our team has had a great deal of experience in delivering fully operationalized security for some of the largest companies in the world. We realized that security today requires building a whole bunch of one-off security silos. All of which are made of individual products that have to be strung together. Customers end up with many different combinations of products -- billions of possible permutations. This approach is very complicated and does not deliver uniform and consistent security across all of an organization's distributed assets.

We looked at the problem and noticed that organizations are more distributed than ever before. They are distributed in branch offices, data centers, cloud instances, SaaS applications and mobile devices. And now more and more organizations are getting IOTs introduced into their environment. Therefore, to try to build one-off security silos, one for the data center, one for the branch office and another for each and every cloud instance or SaaS application, is really exacerbating the security problem.

It is taking an already complicated scenario and making it exponentially more complicated. Therefore, we decided to have one security stack, and rather than piling that stack on each and every asset or at each and every site, we decided to offer a security stack that operates completely in the cloud, and distributed assets connect into our stack. That is why we can simplify security, because we offer a single stack that supports all of the various distributed assets, rather than having to support dozens and dozens of individual stacks for each and every company.

CEOCFO: ***What has been the response? Are people aware that it can be done, and do you run into any skepticism?***
Mr. Pasdar: More and more organizations are becoming aware as we introduce them to it and the response has been amazing. The industry is suffering and in pain. You can see the body language of the CIOs and CTOs that we talk to. We ask them if they have a strategy to find their data. Once found, how do they plan on securing it. Distributed assets are a real challenge and the security tools today do not do distributed very well. Bat Blue's platform was designed from the ground up to secure distributed!

Bat Blue Networks' approach is a logical and reasonable approach that solves a great many problems for them. When we do ROIs for customers that we have, they recognize 40% plus cost savings. They recognize the significant simplification of their security. We reduce them from 16 security policies down to one, and from 20 something vendors down to just a hand full. We take them from 30 different products, down to just a couple. Therefore, the cost savings are there, the simplicity is there, and the fact that Bat Blue Networks can deliver uniform and consistent security across all of those distributed assets means enhanced and improved security over the traditional model.

Let me highlight another factor. If you consider that security engineering time and expertise are among the most expensive technology resources an organization buys, we asked customers how much of those resources are spent on installing and managing products, versus operating security. The answers are eye opening. In fact, the average mid-sized organization spends better than 80% of their security resources on managing boxes, not operating security. It's even more for smaller companies. We free them to be able to focus more on security.

CEOCFO: ***As physical threats that are front and center in the news, is cyber security falling by the wayside or it helping to increase interest in that area as well?***
Mr. Pasdar: You just touched on a very key point for Bat Blue Networks. The two are very interrelated. In fact, Bat Blue Networks tracks what happens from geopolitical events, socio-economic conditions, social mood and Darknet activity and we cross-reference that to cyber activity. Cyber activity is driven by much of those four types of events, so when a geopolitical event occurs, like the Paris attack or Charlie Hebdo attack, or San Bernardino shooting, the cyber byproduct of these is what we call a Cyber Tail. The Cyber Tail is the cyber driven element of geopolitical events, socioeconomic conditions and such.

"Distributed assets are a real challenge and the security tools today do not do distributed very well. Bat Blue's platform was designed from the ground up to secure distributed!"- Babak Pasdar

Look at Russia and Eastern Europe where many of the hackers are from. They can be correlated to socioeconomic conditions after the fall of the Soviet Union, when the economy was poor. Many well trained computer programmers and PhDs who could not find jobs resorted to some alternative approaches, and ended up being hackers.

The Cyber Tail is a very critical component of what is happening in the news from a geopolitical and socioeconomic or social mood standpoint. Much also has underlying roots in the Darknet.

CEOCFO: ***How are you reaching out to potential customers and how will people find you if they are looking for a better solution? What keywords or phrases would someone use to find you on an internet search?***
Mr. Pasdar: Bat Blue has spent a great deal of time building validations. We actually have a book coming out as a CXO's guide to building a more effective, agile and sustainable security model, with Unified Cloud Security. That is what we are calling the category that we are in, Unified Cloud Security.

We have already built a great deal of validation. The model makes a great deal of sense, but is different and customers want to have details and data points. They want to be able to go through all of the beneficial points and they want customer references. We have built all of that. Our reference customers share their pain and how they found relief after the transition to our platform.

These are medium and large organizations who are using our platform, because it ended up being the only thing viable for them, given budgets, time lines and security standards to achieve. So now we are focusing on outreach. We are using print media, social media, industry events, podcasts and webinars to get the message out. We want to let the world know that there is an alternative and better approach to security out there. It is something that will allow you to be agile and secure, as well as being affordable. Bat Blue is the sustainable security option.

CEOCFO: ***What is involved in an implementation?***
Mr. Pasdar: Our Unified Cloud Security, called Cloud/SEC, is security that you turn on, not build out. So you just have to connect into our platform. It surprises many how easily we are introduced into their environment.

We have had customers that were not meeting PCI compliance standards, that within the same day turned us on and became PCI compliant. We recently had a customer that had to deal with the byproduct of two acquisitions three months apart, and the acquired companies had web properties, cloud instances, SaaS applications, branch offices and retail

stores. They did not have a viable way of getting security implemented using traditional security models, and they knew that once they signed the risk was theirs.

They scheduled to turn-up the first office at 5:00pm to our platform. The director of security, who was personally involved, called me up and 5:45pm. He told his wife that he would not be home until after midnight. By 5:45pm he was out the door with complete security and visibility. He did not expect that. It was much easier than he thought. We are very excited that customers recognize the value and the benefits. We are setting the bar higher in simplicity, cost and sustainability. We want customers to expect more and better from their security solutions than headaches like logistics, big price tags and anemic results. Bat Blue eliminates the headaches.

CEOCFO: ***How do you send information to a company when there might be a breach or you see something going on? How do you evaluate the level of the threats?***
Mr. Pasdar: Bat Blue is a security platform that they turn on and immediately get the Bat Blue Events Story, a live feed to the customer's security information management platform. They can also use our portal and get live information as things are occurring as to what the threats are, how critical they are, and what the security priorities should be. Our approach is to block bad activity in real time. To expect customers to do incident response is not always viable. In general, we just block the bad stuff. We are aware of the applications, how they are being used and when things are breaking or being used in unusual ways. Based on all of those data sets, we can identify when something is misbehaving. We block it and the customer gets notified, rather than telling the customer that something bad is happening and expecting them to respond. That is not an effective approach for operating security.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

Bat Blue Networks

For more information visit:
www.batblue.com

Contact:
Gillian Ibach
212-461-3322
gibach@batblue.com