martinwolf

MW Executive Perspective®

Unique Viewpoints from Industry Leaders

February 2015

Orion Hindawi

Co-Founder and CTO, Tanium

Editor's Note: *In this issue,* ***martin****wolf interviews Orion Hindawi, Co-Founder and CTO, Tanium. Orion Co-founded Tanium in 2007 with the mission of creating security products that provide truly instant data collection and action capabilities, allowing enterprises to manage their assets with 15 second latencies, rather than the hours or days of latency they are used to today, with huge benefits to their security and stability. He has led the development of security management platforms over the past 15 years, first at BigFix and now at Tanium, and also serves on Tanium's Board of Directors.*

IT security has been a concern dominating the recent news cycle. Do you see that trend increasing in 2015 or subsiding?

I think what a lot of people don't really understand—even those whose job it is to fully understand—is that a lot of the attacks that we're seeing are really just good hygiene issues. If you look at things like the most recent attack at Anthem, Target or JP Morgan, people fixate on the idea that these are really advanced attacks, but the fundamental issue that many of these companies have is that they don't know the basics of their IT operations. So if you ask these companies how many computers they have—forget about their exact real time state or security—the answer is "we don't know." What OS are they running? No idea. And where are the vulnerabilities? Can't answer that, either. Companies don't have basic telemetry on the state of their environment.

So the question is not if these attacks are going to increase—absolutely they are going to increase as everything is computerized and there is more data worth stealing—but the real problem is that the gap between where we need to be and where we are today is so vast that many companies have almost given up. They don't actually give up, but they rationalize and accept the risk as a cost of doing business, focusing on mitigation rather than prevention. And it all really stems from the fact that the tools most companies have on their ends—antivirus, firewall—are 25-year old tools that don't work anymore, leaving companies with no idea what to do. Even with an infinite budget, in many cases companies wouldn't know how to actually solve the problem. There's more and more attack capacity, from nation-states to commercial enterprises, but the disparity of information and inability to take action that matters is what we're seeing over and over again in our customers.

If many of these problems are good hygiene attacks, does that mean we have the potential to see the success of these attacks go down even if the incidence of attacks go up?

Definitely. There are some key things you should be doing. Here's a few examples. Microsoft releases security patches every week. You should be installing them, especially if they are critical security updates applicable to your computers. If you have dual factor authentication, you should be using it. If you have data at rest, you should be encrypting it. I just named three things corresponding to three of the biggest attacks in the last year. In each case, if the victim had done one of these things, they could have avoided the attacks. And if you're not doing these things, and not defending yourself at all or relying on old and outdated tools, you’re putting yourself at risk.

The problem is, these companies have hundreds of thousands of computers, so actually enforcing all of these security measures is tough. Is our goal to reduce the number of attacks? Absolutely. Is the goal to reduce the severity and the cost of those attacks? Absolutely. But I think there's a misconception in the market that you have to hire hackers and super analysts with unbelievable data analysis skills to achieve that. It turns out we've known for a while how to reduce the vast majority of attacks. If you put good protection on your data—basic stuff—you can prevent these attacks. But until now we didn’t know *how* to do this on hundreds of thousands of computers. And that's the problem that Tanium solves—being able to actually go into all of the things you're supposed to be doing and verify that you're secure across all of your machines.

“The amount of changes in their environments was increasing so much that data from 5 minutes ago was already too far behind.”

So how does Tanium help solve these problems?

The most effective way to understand how we're going about solving these problems is to understand where we came from. My cofounders and I started a company called BigFix back in 1997. BigFix was (and still is—IBM has bought it and now uses it as its endpoint management system) a really novel way to do systems management. Systems management is this problem of accessing endpoints—whether they're servers, laptops, etc.—and setting them to look how you want them to look, whether through patches, configuration, whatever.

The solution that BigFix offered was a revelation for people: it was able to ask questions of their endpoints and learn the answers within a day, instead of weeks or even months. We soon found that our customers were coming to us over and over again asking for an even faster turnaround. They needed the data in seconds, or minutes at most. And this was important with the rising trends of cloud computing and virtualization. The amount of changes in their environments was increasing so much that data from 5 minutes ago was already too far behind.

What we realized was that we had to literally start from scratch. So we took 12 engineers out of BigFix, sat them around a whiteboard, and basically told them "look guys, start from the basic principles and reinvent from the ground-up knowing what you know now." And that was the founding of Tanium, which is a systems management solution that is literally 10,000x faster than the next best system on an enterprise scale. If you look at the biggest banks on Wall Street, and the biggest retailers, technology, and healthcare companies, they're deploying Tanium. We have many of the Fortune 100 companies, including 5 of the top 10 banks and the #1 physical and online retailers, using Tanium to see exactly what's happening on their endpoints.

A good example of this would be OpenSSL. There was a vulnerability called Heartbleed that everyone freaked out about—and it required companies to know what version of OpenSSL all of their computers were running. It took some companies months to do that. And some companies still don't know the answer. Our customers typed in an English language query that got them the answer back in 15 seconds. And then they can use that information to actually go back there and identify specific problems or fixes to execute. Our customers use Tanium to identify where the problem is, which machines are affected, and how they can address it? And most importantly, they trust that their data is accurate and true, and that their solutions will fix the problem.

Tell me about your role as CTO. How do you ensure Tanium stays ahead of the evolving security threat?

There are two things that make my job easy. First is that our clients are some of the most attacked companies, and as a result they have dedicated security teams that are very forthcoming with us about the new attacks that they are seeing and how they are dealing with them. This helps us devise a roadmap to make sure they have the data they need to do their job and close off the attack vectors as quickly as possible. So the first thing we do is establish this collaboration with our customers to increase our ability to solve these new problems.

The second thing that I do is, for the last 17 years, we've been building scalable enterprise software. We have a team with a lot of experience doing that, and my job is to make sure that whatever I'm hearing from our customers is being reflected in the products that we're building. One of the things that a lot of people don't realize is that if you build a product that works on 10 computers, it's not a simple question of repeating the process 100,000 times to get to a million deployments. Instead, there are needs for things like broad access control, certified cryptography, PCI compliance or other certifications, and several other factors. So we need to make sure that we're architecting our systems in a way our customers can actually use them.

"His literal quote was 'meteors, nuclear weapons and cyber [threats] are the three things that can put my bank in the ground.'"

I was talking to one of the CEOs for one of the largest banks in the country, and he told me that at this point, regulation is annoying. Competition is annoying. But cyberattacks pose an existential threat to his bank. I think his literal quote was "meteors, nuclear weapons and cyber [threats] are the three things that can put my bank in the ground." And until Tanium, many people felt unequipped to handle this existential threat.

Last year we saw Blackstone's acquisition of Accuvant and subsequent merger with FishNet. Are you seeing broad consolidation in the space?

We've been seeing a huge amount of attention being paid to cyber threats in the last 12 months in various fields—including software distribution, asset inventory, vulnerability assessment, and other operations. And Blackstone understands that. Accuvant and Fishnet are huge vehicles to get cyber into organizations, and as a result they'll have a lot of leverage. As far as consolidation, I'll say this: many of the vendors in our industry are losing money so quickly that I can't believe they'll stay in business through the year. If you look at the burn rate—even in the larger companies—their marketing and sales expenses are so high that it's unsustainable.

The reason a lot of these companies are losing money is because systematically their products are designed to sell support. And if you look at the quotas put on salespeople, they're so low—especially with hardware-based sales—it's difficult to see how they'll become profitable. So I expect companies that today are spending hundreds of millions of dollars each year to not be present for much longer.

Is Tanium's business primarily US-focused, or are you global?

Today, we're very US-focused. One of the things about us having done this a couple times is that focus is generally an important word for our company. Even as we grow, it's important for us to saturate the chasm rather than simply crossing it and expanding further. We took a very deliberate approach to the Global 2000 based in the US and making decisions in the US, and started there. We are moving pretty aggressively in specific markets outside of the US—you'll see more on this front from us in the coming months.

Do you have your eyes on any M&A targets or are you going to keep holding off? What's your acquisition strategy?

What concerns me the most is maintaining our culture at Tanium, even as we grow. Tanium has a really strong culture where customers and employees are well aligned on the fact that they wait to build products that customers use with great results. To be honest, I'm not sure we can maintain that excellence through acquisition—I don't think we can find a company with perfect alignment with this culture and a product we can slot in really easily. As a result of that, we could probably acquire new products and or revenue, but not while maintaining that customer experience. Tanium has grown over 400% YoY from a revenue and personnel standpoint in the last year—I don't think we can keep growing at that clip and add fuel to the fire with M&A while keeping everything in balance.

> *"People are addicted to this idea that if they come up with a product and market the hell out of it, they can become a billionaire in six months."*

What's the secret to such tremendous growth?

From my standpoint, the secret is we took five years to build a product with zero marketing and zero sales. Let's take a step back. There's this theory of minimum viable products, especially now. You see smartphone apps put together in two months that somehow sell for $1.5 billion. And people are addicted to this idea that if they come up with a product and market the hell out of it, they can become a billionaire in six months.

I don't want to do that, even if it were guaranteed. I'm not an investment banker, I'm a software engineer. What I want isn't a flash in the pan—I wanted to build a really resilient, strong platform that we trusted immensely before we went to market. So we went into this knowing we would take a long time to work on it, and took 5 years to build this strong, resilient platform before going to market. This meant we worked with five of the largest enterprises in the world in beta, deploying this in the scale of tens of thousands without a single salesperson on staff. The result is a product that's fundamentally different than anything else in the market. And since then, having 500% growth and being profitable has not been that hard. When we walk into a meeting, people understand why they need what we do. I was sitting in a final meeting with the CSO of one of the largest technology companies in the world. He told me that our product cost too much money. He told his staff to find something cheaper that does what Tanium does, but they found there were no other companies that do what Tanium does.

You've been able to secure a significant amount of funding, especially in the past year. What are your investors looking for?

We had no plans to seek VC funding. David (my co-founder) and I were able to self-fund Tanium, and we would have been able to continue doing so, but this was about being able to get top-quality, passionate people to work with us in building this company. I think when Andreessen Horowitz looked at Tanium, they saw that. They saw people passionate about solving a very important problem. That's why I say our culture is so important. I want to be able to open my browser and be confident that when I connect to my bank or I pay my taxes, or when I think about the federal government and our armed forces, I know they are secure.

Do you expect to touch the money anytime soon?

We're profitable enough that I don't expect us to need it. We're growing at the fastest rate we can, money aside, and we're profitable through the process. The money is our protection from meteors or nuclear weapons.

Do you expect to stay independent?

Yes. The only way Tanium is going to be acquired is if somebody is able to convince us that they will be able to serve our customers better than we can as a company. To take a step back, liquidity in this market is not a problem. There are tons and tons of people who want to get a stake in high quality companies whether they are public or private. What is a problem is when you're part of a big company and you want to do something independent and the bureaucracy slows you down. Someone is going to have to explain to me, my cofounder, our employees and our customers, how we would all benefit from being acquired. And I want to make a serious point here. If I think I'm benefitting and my customers are not, that's not OK. I need to understand how everyone will come out ahead—and that's a hard thing to do. I can't say never—but I can definitely tell you I think somebody has a tall hill to climb.

> *"I want to be able to open my browser and be confident that when I connect to my bank or I pay my taxes…I know they are secure."*