From: <[redacted]>
To: jeffrey E. <jeevacation@gmail.com>
Subject: Fw: [New post] Tanium Magic
Date: Sun, 22 Jun 2014 23:15:41 +0000
Importance: Normal

What I mentioned… this is the blog post on http://www.a16z.com

Sent from Surface

From: Learning by Shipping
Sent: Sunday, June 22, 2014 3:36 PM
To: Steven Sinofsky

New post on **Learning by Shipping**

Tanium Magic

by Steven Sinofsky

ss

Lightening doesn't often strike twice, but in the case of the father and son team of David and Orion Hindawi, founders of Tanium, Inc., that's exactly what has happened. Tanium is a prime example of a modern enterprise software company—solving the new generation of today's problems using skills and experience gained from being successful founders in the previous generation.

Forming the company

David Hindawi, a PhD in Operations Research from UC Berkeley is an entrepreneur who led the creation of several successful companies through the earliest days of the PC era. His early efforts focused on getting PCs connected to the "net" and keeping them running smoothly.

In 1997, David teamed up with his son Orion, then an undergraduate at UC Berkeley, to form BigFix. BigFix solved the problem of communicating with all the end-points (PCs, servers, virtual machines, and more) on enterprise networks to gather configuration data and deploy product updates. BigFix was a remarkable product for the time routinely scaling to 100,000 end-points. In 2010, IBM acquired BigFix and integrated it into the Tivoli Software portfolio marking a successful exit.

Some might have been content to rest on their collective laurels having invented the technology, built a company, and scaled a business to the most elite of enterprise success stories. Instead, David, Orion and the key architects of BigFix had an even bigger idea.

Forming Tanium came about as the team reflected on these product shortcomings. "We recognized that enterprises needed endpoint control that was much faster than they could get with existing tools, and challenged ourselves to leapfrog the state of the art, including

BigFix, where basic management queries could take days." Orion recounted, "We knew that nothing short of a 10,000 times speed improvement over the state of the art at the time would solve the problem, and we needed to fundamentally change the paradigm of systems management and end-point security to accomplish that. We are lucky to have one of the few engineering teams in enterprise management who are smart and ambitious enough to do that".

The team, mostly members of the original BigFix engineering group and all experts with years of experience in large enterprise management, worked in their Berkeley, CA offices for almost two years before the first customers saw the early results of their new product. When seeing the product in action, it was clear to early customers that the team had in fact *built a better mousetrap*. Tanium was born.

Meeting Tanium @ a16z

When Orion first came to Andreessen Horowitz to meet us and introduce Tanium we had no idea what a surprise we were going to see. Collectively we are many old hands at systems management and security. Many folks at a16z share the experience of having built Opsware and my own experience at Microsoft make for an informed, and perhaps tough, audience.

Orion popped open his laptop, clicked a bookmark and navigated to Tanium's web-based "console". At the top of the screen, we saw a single edit control like [redacted] see for a search engine. He started typing in natural language questions such as "show computers where CPU > 75%" and "show computers with a process named WINWORD.EXE". Within seconds, just like using search, a list of computers scrolled by as though it was just an existing spreadsheet or report. At this point we reached the only reasonable conclusion—-Orion was showing us a simulation of the product they hoped to build.

After all, we were all quite familiar with the state of the art for this type of telemetry (BigFix in particular represented the state of the art) and we knew that what we were seeing was just not possible.

But, the demonstration was not a simulation or edited screen capture. In fact, Tanium was running on a full scale deployment of thousands of end-points. This wasn't even a demo scenario, but a live, production deployment—*the magic of Tanium*. As we learned more about Tanium and how it easily scales to 500,000 end-points (not theoretically, but in practice) and the breadth of capabilities, we were more than intrigued. We were determined to do what we could to invest in David, Orion, and team.

Redefining *State of the Art*

In enterprises, one team is generally responsible for securing end-points, while another is responsible for managing them (systems management). Typically, each team uses its own tools, and each is independently struggling to keep pace with modern network security threats and the scale of modern networks.

Today's IT Pros on both security and management teams know the types of information they need from their network. With current tools these questions require careful planning, significant infrastructure, and a fine balance between what IT needs to know and the cost to the end user who is working on the computers that are being queried – if you get it wrong, you can cause slow logons and sluggish performance at inconvenient times. However, to effectively manage and secure networks and provide assurance of compliance with government and industry regulations IT Pros absolutely require information such as hardware configuration, software inventory, network usage, patch and update status, and more. In addition, today's socially engineered security risks are often combinations of seemingly simple combinations of running programs, files or attachments on the system, and a few other clues. An IT Pro walking up to a PC or Mac could easily obtain all of this information, but for all practical purposes it is impossible for them to gather that data from the thousands of end-points they are responsible for with any level of ease or timeliness.

Getting that data at scale is typically hard and slow because almost every *Systems Management* tool uses a classic hub (servers) and spoke (end-points) architecture. IT Pros deploy multiple servers running on network segments with high-end databases and significant networking hardware combined with fairly elaborate end-point runtimes. Even when this state of the art deployment is carefully tuned, the best case at very large scales can be *3 days* to "compute" the answer to critical operational questions, assuming you knew ahead of time you were going to ask those questions. By this time the information would be out of date and by then the whole problem you were thinking about has probably changed. As a result most IT Pros know that best case the data is approximate, and worst case just worthless. For mission critical problems, such as compliance with HIPAA (healthcare) or PCI (electronic payment) regulations, this is more than just inconvenient for IT, it can cause a painful failure with board-level visibility.

The state of the art for Security is all about building stronger and taller walls between the enterprise network and the internet. We're familiar with these approaches across the basics of firewalls, more sophisticated security appliances and adaptive architectures, and of course the typical security suites that run on end-points. Unfortunately, the *bad guys* are wise to that game, and modern threats are created anticipating that these protections are in place—in many cases, the bad guys actually "QA" their attacks against the systems enterprises use before they release them. In addition, today's malware is targeted to particular organizations, and is often put in place by a series of seemingly benign or undetectable actions. Malware, a bot, or a backdoor make their way onto the network leaving behind a series of benign clues—a running process, a changed file, a memory signature, or a specific network packet. It is only taken together that a pattern emerges. It is only after the fact or with an IOC (*indicator of compromise*) in hand that IT Pros can potentially track down end-points that have been compromised. Unfortunately, IT is literally swamped by IOCs to investigate and there are no effective tools that support this wide range of questions and even if you could, the state of the art would give answers in days, long after the damage was done.

Even with these challenges, both of these state of the art approaches have their place in a modern network. It would be irresponsible to run a network without basic asset management or network firewalls and end-point protection such as anti-virus. Unfortunately, for the vast majority of both threats and systems management, the needs of IT Pros are far more dynamic and complex than existing systems can provide. This is the opportunity where Tanium adds unique value to the tools of the modern IT and Security professional.

At 16z, we love the opportunity to partner with enterprise companies that are either working to radically improve the way a given IT need is met with software or transforming the IT landscape by re-creating or re-defining the traditional categories with unique software. Tanium is magical because it is transformative across both of those measures.

Innovating Tanium

In practice, the Tanium team accomplished nothing short of a complete rethinking of how IT Pros manage, secure, and maintain the end-points in their network—every node on the network can now be interrogated, managed, updated, and secured, *instantly* from a browser. Literally, you can ask almost anything of an end-point from basics such as configuration, patch status, software inventory compliance, performance, reliability measures, telemetry, network activity, files, and more (basically anything you can ask of a running system) and get answers back in seconds. Not only can you ask questions, but you can take actions as well—distribute and install updates, shut down processes or executables, remove or quarantine files, and so on. All of this happens in seconds, across your entire network of end-points, across LAN segments and the WAN, from branch offices to headquarters to the data center.

Orion walked us through the magic of Tanium. It became clear very quickly that David, Orion and team have invented a completely new way to think about managing and securing a network of computers. The magic of Tanium is built out of four innovative technology pillars:

1. **Runtime**. The Tanium runtime builds on the end-point management lessons of BigFix. The runtime serves as the platform for asking the end-point questions in the scripting language of your choice (VBscript, Powershell, WMI, Python, Unix Shell, and most any other language), packaging up the answers and getting them to *single* server/VM that coordinates the activities. The runtime also provides actions allowing you to make changes across your entire network, instantly. The end-point runtime is a couple megabytes, takes almost no CPU or RAM, and incurs nearly imperceptible network usage.
2. **LP2P Networking:** End-points secured by Tanium do not drive up costly WAN traffic but instead communicate between end-points on the local area network. Expensive WAN load is vastly reduced because rather than all end-points trying to reach a single data center across the WAN, answers and actions are coordinated across an incredibly efficient *linear peer-to-peer* (LP2P) architecture—an innovative hybrid of mesh and peer-to-peer concepts designed and validated for the enterprise. LP2P is self-healing and architected for fault tolerance, transient end-points, and global WAN segments connected in a typical manner.
3. **Natural Language**. The interface to Tanium is through a simple text box where you can use natural language to ask questions of the entire set of end-points. Just like using web search, each question gives you suggestions for follow up questions, refinements, and ways to improve your queries. You use natural language questions to generate tables, charts, time series, and other representations of your near real-time network status—instantly.
4. **Security**. The entire Tanium platform was of course architected from the ground up to be secure enough for the largest enterprise and federal networks - Tanium affords IT Pros incredible power and flexibility in managing and securing end-points, and they recognize the need to ensure that power stays in the right hands. As a result, all traffic is FIPS level secured, actions are controlled and validated by signed

certificates, and administrators have fine-grained control over the types of queries and actions permitted by different users within IT.

If you're running existing state of the art tools for managing and securing your end-points, you have a fixed set of diagnostic questions that you routinely ask and then store the answers in a database for later analysis. Even if it's a simple question like what version of OS software your computers are running, it will take a few days or more to get answers. If you have a crisis requiring new information, you likely push out an emergency logon script or dreaded background process to add a new question to the list of slowly collected answers, and days later you know the approximate answer.

As a result of the innovations above, Tanium completely upends the thinking about how this should work. By analogy, if you think about the current state of the art as a printed set of classic encyclopedias then Tanium is like having the entire internet at your disposal through a search engine. Rather than a set of fixed questions and answers, you use Tanium to explore your end-points. When new security threats arise you can immediately explore your risk by using any telemetry to diagnose your risk and then using any mechanism to take corrective actions—instantly.

A top of mind example for all of us is the outbreak of Heartbleed. As soon as your operations center received notice of this vulnerability, there was one simple question "what variants and versions of OpenSSL are we running across all servers and VMs". Almost no management and inventory system would have this readily available. Many would have first relied on what was believed to the "standard" images, but later would find out that isn't enough. With Tanium, you just ask a question in natural language and within seconds you can have any level of details required on the servers and VMs running OpenSSL. You can then shut those servers down, deploy updates, or monitor actions—instantly.

Identifying and securing end-points for compliance with regulations, software licensing, or corporate policy is equally simple. When talking to Orion about Tanium, I searched my own experience for what I thought was a trick question. I wanted to know "how many end-points had attached USB memory stick and written to it recently" (a potential information leak, compliance issue, or malware vector all in one simple and common operation). Once again Tanium's magic delivered an answer from a natural language query in just a few seconds for thousands of computers.

In addition to all of this, Tanium is also a true platform. IT Pros can utilize mature REST, SOAP, and syslog APIs to connect the results of Tanium queries to their favorite big data destination and develop time series models of their end-points, and mine the data for patterns. Because the Tanium runtime has such a minimal impact it is possible to collect thousands of independent data points continuously from hundreds of thousands of end-points, feeding the predictive analytics and big data systems that enterprises are building today with extremely valuable data. This type of analysis allows for finding points in time when the network changed, identifying malware, bots, and other exploits that we all know escape traditional firewalls and anti-virus. Using the platform, IT can also create tailored dashboards and custom actions that enable monitoring and guarantee compliance of end-points with standards.

Tanium and a16z

I could go on and on about the magic of Tanium that David, Orion, and the amazing team created. In fact when we talk about Tanium we describe it as an entrepreneur *trifecta*. First, David and Orion are experienced and successful entrepreneurs. Second, Tanium is a product that builds on innovative and inventive technology that could only come about from a team with years of experience and a depth of understanding of the enterprise. And third, Tanium is already a successful and profitable company with dozens of customers in massive, mission-critical and global deployments.

With this incredible story, Andreessen Horowitz could not be more excited to be leading an investment in Tanium. I'm personally super excited to be joining the Tanium Board where I will work closely with David, Orion, and the team.

--Steven Sinofsky (@stevesi, [redacted])

This post is also on a16z.

Steven Sinofsky | June 22, 2014 at 3:30 pm | Tags: a16z, enterprise | Categories: a16z, posts | URL: http://wp.me/p31nkB-hg

Unsubscribe to no longer receive posts from Learning by Shipping.
Change your email settings at Manage Subscriptions.

Trouble clicking? Copy and paste this URL into your browser:
http://blog.learningbyshipping.com/2014/06/22/tanium-magic/

Thanks for flying with WordPress.com