Tachyon Review (2018)

By David Strom

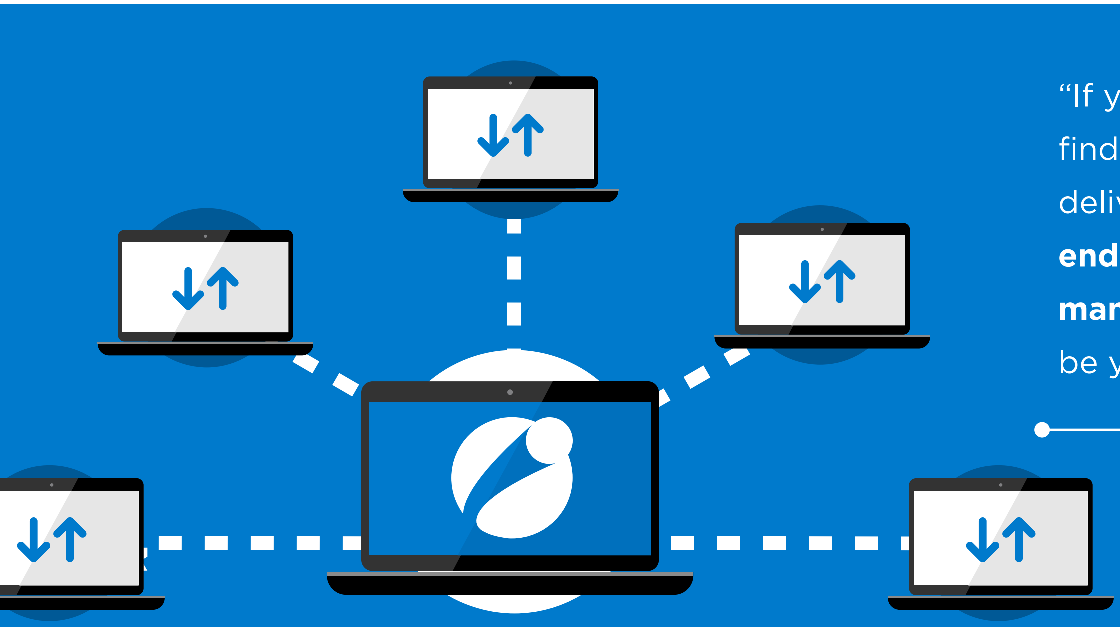
Since writing my review of a dozen endpoint detection and response (EDR) tools for Network World two years ago, this market segment has gotten more competitive. New vendors have entered the scene, some with tools that originally came from the traditional anti-virus space or from other protective products. Malware has gotten more inscrutable and more difficult to detect, as hackers get better at hiding their wares and blending different attacks together. And enterprises have migrated to more mobile and cloud-based computing, introducing new threat vectors. As a result, enterprises have a harder time defending their networks and have to get better at evaluating threats in a larger context.

> “Oftentimes, my queries were answered with literally a blink of the eye, even on **large test networks with thousands of endpoints.”**

Added to this is the increasing frustration from IT managers, who have gotten "box fatigue," meaning that they have become tired of purchasing separate products for detecting intrusions, running firewalls, and screening endpoints. And they are more paranoid too, as the number of data breaches continues unabated, despite all these disparate tools to try to keep attackers at bay.

1E's Tachyon comes to the EDR space in a completely different direction, and it is almost easier to describe what it isn't than what it is. Yes, Tachyon does do endpoint detection, although that isn't really its exclusive benefit. And yes, it does have a variety of responses to security events, although that really isn't the entire picture of how the product works either. Unlike more narrowly-focused security products, Tachyon operates in a wider arena that responds to a lot of different events. It does have endpoint configuration management functions, although again that somewhat misses the point of the product, where it places that management in an overall framework to keeping your computing collection healthy and malware-free. Finally, Tachyon isn't really a fully-featured mobile device manager in terms of examining device posture and health.

If you are in the market to buy an EDR product, like one of the ones that I reviewed for Network World, you probably would initially reject Tachyon because of this perceived lack of focus. This paper is to get you to rethink that initial rush to judgment. If you are thinking of finding a solution that can deliver **real-time automated endpoint remediation and management,** then this should be your first choice, especially if you need a tool that emphasizes improved automated and almost real-time operations. Tachyon isn't searching for a needle in a haystack filled with log files and other data, but figuring out that first you need to look for something that doesn't appear to be a piece of hay. This means you can discover all sorts of ad hoc and serendipitous things that you may not even have known required fixing.



"If you are thinking of finding a solution that can deliver **real-time automated endpoint remediation and management,** then this should be your first choice."

Think about Tachyon as what Google was trying to do back in the late 1990s. Back then, no one knew anything about search engines. But we quickly figured out that its simple query interface was more than an affectation when we got some real utility out of those queries. That is where we are today with Tachyon: think of it as **the search tool for finding out the health of your network.**

I should note that Tachyon is just one of several enterprise management tools sold by 1E, a vendor who has been around for decades.

Use cases

Here are some use cases where the Tachyon platform excels:

- **Deploying patches across a mixed OS environment.** Many patch management tools don't offer the ability to set workflow waypoints to determine if certain tasks are successful before moving on the next task. Tachyon does this quite readily, using an advanced API and scripting language that I'll get to in a moment. One IT manager I spoke to was able to patch thousands of Windows computers in a matter of minutes that were scattered across the globe, with some of them not even sitting on corporate networks.
- **Which PCs have been compromised by a particular malware strain?** There are many EDR tools that can answer this question, but usually the answer requires a security specialist to navigate numerous screens and be skilled enough to interpret a cyber kill chain diagram and understand the various reports. Tachyon uses a natural search box query function that can have an answer to the question without becoming a CISSP first.

> "Tachyon is **extremely easy to use.** Many EDR products require lots of skills and copious classroom training. Tachyon is as simple to use as a search query. "

- **Figure out why a particular office can't install some software.** One of 1E's customers was having trouble running Skype for Business in a branch office. The company created a product pack using Tachyon's API to check for network conditions, and found the branch had its network misconfigured. Now any customer can download this code and use it to check for these circumstances.
- **Why is my web browsing slower today than normal?** Tachyon can be setup to show you the normal range of browser latencies and when conditions depart from these norms, and do it without a lot of scripting or CPU load.
- **Managing the frequent changes brought about by running an always-online business.** Today's enterprise has an increasingly more complex infrastructure. As companies move to more virtual and cloud-based servers and more agile development, there are more moving parts that can be very brittle. The same situation can be found when an organization is growing rapidly, and adding hundreds of PCs a day to its network. In these situations with such large networks, even if just a small fraction of a percent of that gear has a bug or isn't setup properly, it becomes almost impossible to ferret out and fix. This post on LinkedIn's engineering blog is a good case in point. "Any service that is live 24/7 is in a state of change 24/7, and with change comes failures, escalations, and maybe even sleepless nights spent firefighting."

Tachyon's main focus

Tachyon has focused on the following four principles:

- First, it wants to help IT managers **react precisely and quickly to a wide variety of circumstances, including when there is a breach** to their systems. Malware can live inside a network for months or years. IT has to do better at rooting it out and eliminating it more quickly.
- Second, it provides for **better and more accurate automation tools.** There are many products that claim to be able to automate routine IT functions. But Tachyon automates the non-routine as well, to make it easier for IT staffs to do more with fewer resources. Given the reduced headcounts in IT, this couldn't come at a better time.
- Third, as part of its automation features, it also ensures that these routines are being done per expectations and **takes note of when these routines fail to complete.** This is a critical piece and necessary if IT is going to trust its use. One IT manager told me that he thinks Tachyon is unique in this area and one of the reasons his company continues to use it.
- Finally, it is **extremely easy to use.** Many EDR products require lots of skills and copious classroom training. Tachyon is as simple to use as a search query.

Tachyon’s extensibility

At the heart of Tachyon’s automated abilities is a scripting language called SCALE that looks very much like SQL commands. It brings its various component modules and functions into a coherent whole, making the product very extensible. You assemble SCALE commands in its Instruction Management Studio, or can download pre-built code Tachyon community website, called Tachyon Exchange. (The Skype for Business tool mentioned above is one of those items on the Exchange directory, for example.)

Most products nowadays come with their own APIs and extensions, but 1E takes this seriously and makes them useful and usable. **This makes Tachyon very flexible at responding to all kinds of events, not just security-related ones.** In effect, you can use these extensions to automate responses to events that you don’t even know you have experienced, or don’t know that you have a problem or how to formulate a solution. That is actually backwards from most security products that start out by assuming you are looking for the source of a breach and want to remediate those parts of your infrastructure that have been exploited. This is also goes to the heart of why Tachyon is so potent.

A good example of **how Tachyon is extended is with its ServiceNow integration.** Since both products make use of REST, it was relatively easy for the 1E engineers to build an application that adds Tachyon query functions into the ServiceNow help desk and ticketing operations. Work is underway to integrate the two tools even deeper.

Another project was built to check the latency to load Google.com and have that as a report from a query. It took just a few milliseconds to run and happens in the background to produce a report that shows you the different latency expectations across different geographies. How often do users complain that the Internet is too slow?

Is Tachyon a mobile device manager (MDM)?

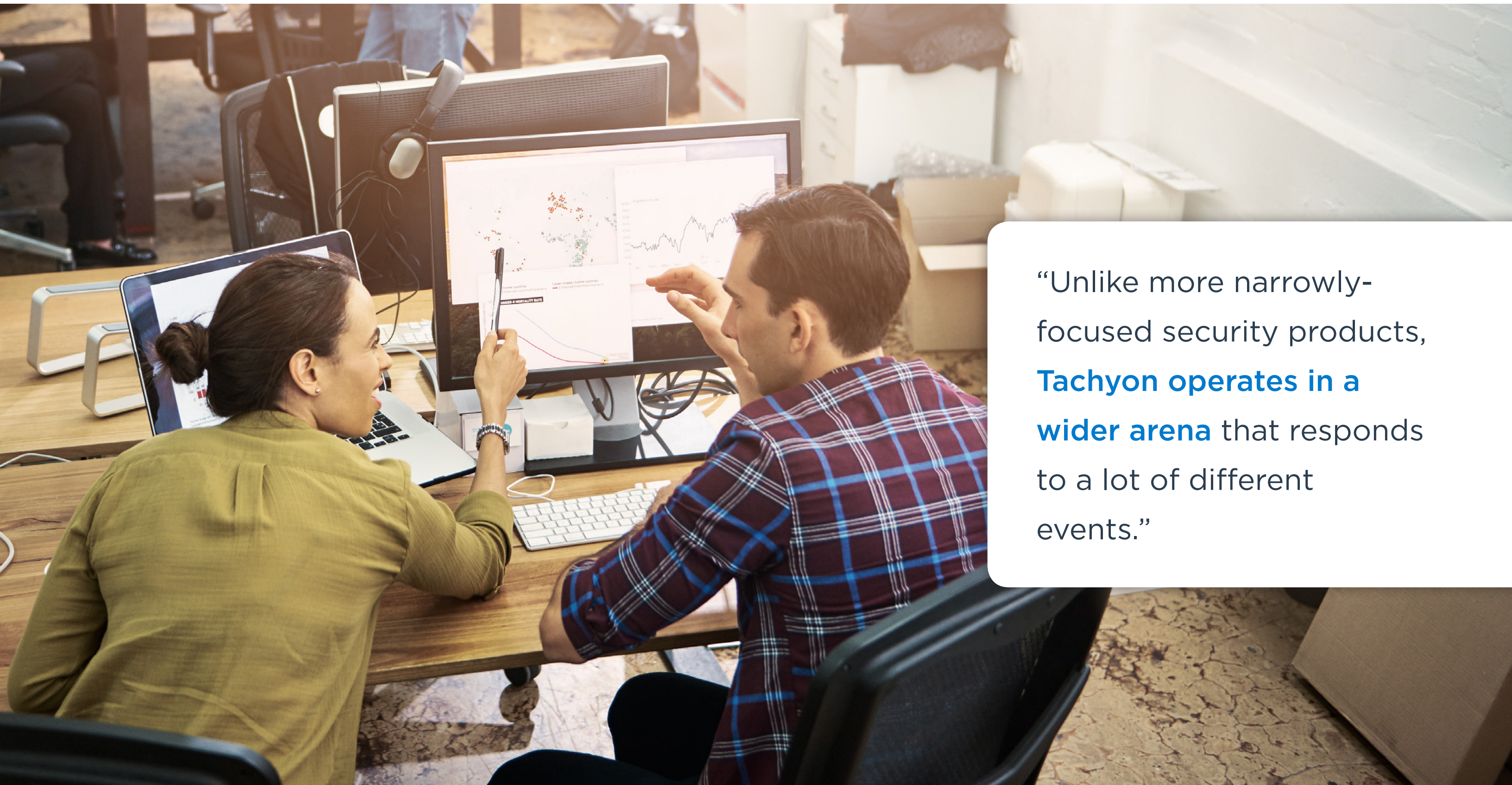
In a word, no. While some security products (Centrify and Duo come to mind) have significant MDM features, Tachyon isn’t one of them. While it could perform a remote wipe of Android devices, this feature hasn’t yet been implemented. And other MDM features (such as determining device posture, app protection and rootkit detection) aren’t easily implemented in Tachyon. Also, it doesn’t yet offer support for iOS devices (although this is underway), which is a significant drawback in organizations that want to manage this collection.

One typical MDM (or perhaps intrusion prevention) feature it does have is the ability to white and blacklist specific apps. Tachyon supports this.

Comparison with EDR typical functions

As I mentioned earlier, much of Tachyon's functionality differs from what is done in a typical EDR context. In some cases, it works better than the typical EDR, and in some cases not as well. Let's review.

- **Remediate endpoints.** Many EDR products spend a lot of effort on how they quarantine endpoints. Tachyon has this ability by limiting an endpoint to just communicating with its own servers and refusing any general Internet access. This has the benefit of being able to quarantine a PC that is sitting in a coffee shop and connected to the Internet, and not being able to do anything other than first be remediated before the administrator can open up its connection to the general online world. With many EDR products, you would have to first bring this PC to an internal network before it could be remediated. Any endpoint running the Tachyon agent can be isolated within milliseconds, provided it is recognized either by an automated query or by a network administrator.
- **Protect a wide range of legacy OS's.** Here is one place that Tachyon has an obvious advantage, in a very deep support for older OS's. Many EDR tools only support Windows 7 and 10 devices and not much more of anything else. Tachyon goes all the way back to XP (and even includes embedded XP devices too.)



"Unlike more narrowly-focused security products, **Tachyon operates in a wider arena** that responds to a lot of different events."

- **Discover malware.** Tachyon also operates differently in terms of malware discovery. Many EDR products excel at matching patterns, processes, or file paths to particular malware behaviors. Tachyon doesn't do this, but has a way to accomplish the same goal. For example, let's say you rerun a query every morning (or more often, perhaps) which checks to see if critical services are still running, or if the endpoint has downloaded some new software since the previous day. This report could be used as actionable information to see if malware has changed the state of the machine, which ultimately is more useful than checking for a particular malware signature.
- **Integrate security feeds.** Many EDR products can tap into malware discovery feeds (such as from VirusTotal and others). While 1E did include this feature in Tachyon (to support the TAXII threat feed), it is used by its automated routines rather than by any manual customer-initiated effort. You can accomplish most of the same result by re-running daily queries, such as searching for particular botnet command and control IP addresses for example.
- **Search for ransomware.** Tachyon can't directly search for specific ransomware, although as I have said previously it can look for specific file hashes, command server IP addresses or unusual processes that appeared only recently. (More on this below.)
- **Operate across AD or network domains.** Tachyon agents are tied to a particular installation through the distribution of certificates. These have to be added to each endpoint prior to the agent installation, which can be accomplished through other mechanisms such as Windows AD trusts. Some EDR products simplify this process through the use of self-signed certificates, which makes them easier to install but less secure. But this also makes Tachyon able to operate across AD domains.
- **Programmable scripts.** As I mentioned earlier, Tachyon is very extensible with its API, and you can write some impressive automation routines as a result. Many other EDR products have scripting (like Tanium) but are not as flexible or are more cumbersome to implement. Also, Tachyon is designed for high performance: rather than using script languages such as VB or PowerShell, its APIs talk directly to core endpoint OS functions. This is actually quite clever: why reinvent what is already being done by the OS itself? This is how Tachyon saves time and packets in its queries, and why its results are delivered almost instantly.

You could make an argument that a daily discovery of malware isn't soon enough, particularly with some persistent viruses that remain hidden inside a network for months. But then, many EDR products would have a hard time finding these persistent threats too. Witness the average time that malware has persisted has remained the same from year to year, according to numerous studies. Sadly, this time is usually reported in terms of months. Finding malware within a few days would certainly be an improvement.

All agent-based products suffer from the same fate: if a laptop is offline for a significant time period, it could take time to "catch up" with applying patches and synchronizing with various updates when it returns to connectivity. In Tachyon's case, its agent looks for the queries that have occurred since the last time it was connected. This could take a lot of elapsed time, or it could be rather quick. One thing in Tachyon's advantage is that it has been designed not to be a Chatty Cathy when it comes to network bandwidth usage, and be very parsimonious with its packets.

Tanium Core comparison

Tanium has been around longer and has a more mature product used by a larger customer base. But it has inferior core technology that is slower to respond to queries and uses more network resources than Tachyon. One user said, "Tanium is very network intensive and this is because it is sending scripts to run on each endpoint. With Tachyon, it is sending the native OS system calls which are much less network and processor intensive." This could be caused by the peer-to-peer design of Tanium, although I didn't directly test this.

Tanium also has a tired UX that is getting a bit long in the tooth and an unused API that is rarely implemented. While both products will give you the same answers to the same questions about your security posture, with Tanium the answers require a more skilled operator to configure and obtain the information. As one user said, "If I want to automate my workflows, Tachyon has the better and more usable processes." Also, Tanium has a lot slower query response time, whereas Tachyon's responses take just a few milliseconds, and seem almost instantaneous.

Bit9 Carbon Black comparison

Carbon Black focuses on fixing what is wrong with your endpoints, assuming your network will eventually be penetrated. Unlike some other EDR products, it offers a more network-centric view of your endpoints. Like Tachyon, their agents act both for collecting data and for remotely controlling the endpoint. Its quarantine mode is similar to Tachyon, where a PC can only communicate with its servers. Its main dashboard is inadequate and will be quickly overwhelmed with a large network or with lots of activity.

Cylance Protect comparison

Cylance tries to block the bad stuff from executing in the first place. Its focus is on how much it can actually stop binary files from executing on your PCs. It does this by treating every binary file as if it could be a zero-day infection, which seems extreme but could be effective.

You have to investigate an infection with its malware chain tools to find the PC which originated the infection.It comes with a preset list of dozens of"watchlists," which are similar to Tachyon's instructions and are cut and pasted into its management console. The difference is that these watchlists are closely tied to security feeds.

One nice feature for IT but frustrating for users: you can lock down the PC, once you are satisfied that it is free of infections, so that you can't make any changes or add any executable programs that aren't already there. Its main dashboard is inadequate and an administrator will be quickly overwhelmed with a large network or with lots of activity.

CrowdStrike Falcon Host comparison

Falcon comes from a deep threat-hunting background and has evolved into an EDR product. It is one of the easiest products to install and covers Windows, Mac and Linux endpoints. It has some very large installations, some of more than 80,000 endpoints. It also has a quarantine feature that they call network containment. It is probably the closest competitor to Tachyon in terms of feature parity, use of automation (most infections are handled without any operator intervention), extensibility and simplicity of operations. It is limited to a single network domain however.

Some words on price, performance and throughput

One of the benefits with Tachyon is the speed at which it produces results. Oftentimes, my queries were answered with literally a blink of the eye, even on large test networks with thousands of endpoints. While I couldn't test across large production networks, I have spoken to customers who run these installations who report it is blazing fast. One 1E representative told me, "As an example during performance testing we have tested consistently sending 4 instructions a second to 10,000 endpoints without impacting the performance, which adds up to be 345,600 instructions per day. Most of our customers are just using a single server to deploy Tachyon." One reason for this is that the Tachyon agent is very lightweight, and unlike many EDR products, there is only a single agent that is installed on each endpoint.

> "Tachyon: think of it as **the search tool for finding out the health of your network.**"

Tachyon is priced at $30 per endpoint per year, which puts it on par with or less expensive than most EDR products. There are volume and multi-year discounts that can bring this unit cost down.

Conclusions

Tachyon is an interesting EDR approach that can do much more than its competitors. It offers a very accessible and flexible product that can remediate problems on both the network and its endpoints, along with a very efficient and ad hoc query rubric that has a lot of appeal for both security experts and newbies.

About the author

David Strom (@dstrom, strom.com) is one of the leading experts on network and Internet technologies and has written and spoken extensively on topics such as VOIP, convergence, email, cloud computing, network security, Internet applications, wireless and Web services for more than 35 years. He has had several editorial management positions for both print and online properties in the enthusiast, gaming, IT, network, channel, and electronics industries, including the editor-in-chief of *Network Computing* print, DigitalLanding.com, and Tom's Hardware.com. He currently writes and curates the Inside Security email newsletter that goes to more than 11,000 subscribers. He has also written two books on computer networking. He began his career working in varying roles in end user computing in the IT industry. He has a Masters of Science, Operations Research degree from Stanford University, and a BS from Union College.

About 1E

1E is redefining endpoint management. Our solutions help keep every endpoint secure and current with the latest software and applications: that's every device in every location, fully automated, and in real-time.

Learn more about Tachyon

David Strom
https://strom.com
@dstrom