Seeking Alpha

Long Ideas | Tech

Intrusion's New Product Could Be A Very Big Deal

Jun. 5, 2020 6:34 PM ET12 comments | 7 Likes
by: Shareholders Unite

Summary

- The company has introduced a new product called Shield, which is complementary to their existing products and mostly meant for the commercial market where Intrusion hardly has any presence.
- They hired an experienced new CEO with numerous contacts in his rolodex, which will come in handy.
- The new product is in addition to the existing business, which reduces the risk, and even the existing business will likely benefit from the new CEO's contacts.
- The new product Shield is a simple add-on to a company network and functions as a SaaS business, that alone should make the stock much more attractive.

We have been following Intrusion (OTCQB:INTZ) for years as the trail of articles we left behind here on SA will testify. We sort of lost sight of the company a bit as we feared their business had reached a plateau, mainly selling into the DoD in what is a fairly laborious sales process, and they might simply not have the scale large enough to grow beyond that.

Well, we worry much less. First of all, we want to thank fellow SA contributor Aaron Warwick's article from waking us up from our self-induced slumber and attending us to the strategic reorientation that the company is in the process of making. We suddenly got interested again.

Until Wednesday, May 27, that reorientation seemed to consist of:

- Hiring a new salesperson with ample connections in the DoD that could increase sales there. This is already working, with that new salesperson harvesting 6 or 7 new contracts, three of which are in procurement already.
- The possibility of putting the company up for sale.

- The possibility of partnering with a large company that could launch them into the (much larger) commercial space as they simply lack the manpower to do that on their own.

This sounded already interesting enough for us to buy shares for the SHU portfolio, but in their previous (May 14) regularly Q1CC, they also mentioned a yet to be introduced new product, one that would be complementary to their existing ones.

They couldn't say too much about that at the time, as they were still in the process of writing and filing the (no less than 13) patents for this new product, but it sounded interesting because it was filling a hole in their line-up: real-time prevention.

You see, TraceCop enables you to see figure out who the bad guys are who breached your network, Savant analyses data traffic packets in real-time, assuming your network has already been breached and tries to find which traffic goes to dodgy destinations from what part of your network, so you can find the source of the breach.

But real-time protection, that was not something the company was offering, until now that is. The company also introduced a new CEO, Jack Blount (his CV can be seen here). Blount was already on the May 27 CC, and he was rather enthusiastic, to put it mildly.

TraceCop and Savant

To be able to understand Shield, their new product, you have to know a little about their existing products, TraceCop and Savant.

TraceCop (company website):

> is a suite of Internet monitoring and tracking products that provides unprecedented capabilities for the identification of malicious and illegal activities based on historical and current Internet usage data. At the core of the TraceCop™ offering lays an unparalleled data collection process which continuously collects, processes and stores vast amounts of historical Internet usage and traffic data into the TraceCop™ Databases.

There is a GUI that enables users to peel out relevant data through patented algorithms that make:

> complex associations based current and historical public information including IP addresses, domain names, host names and personal information extracted from Whois information including email addresses, names, phone numbers, fax numbers and physical addresses. These associations provide the potential to uncover identities of unlawful companies and individuals who have attempted to deceive others.

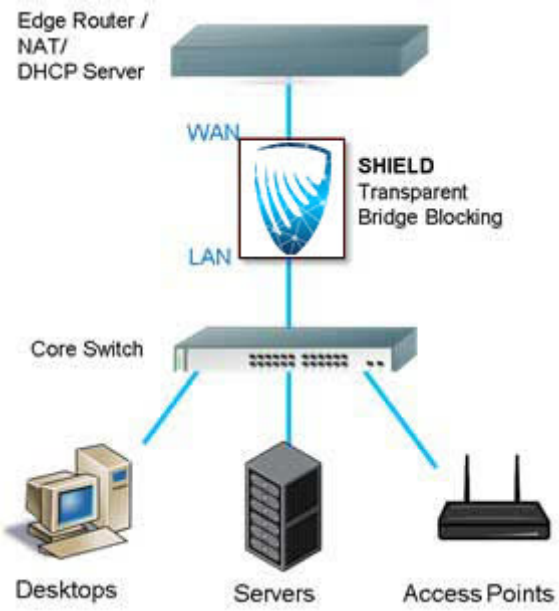
Basically, it is a **forensic tool**; it helps you when you have a security breach to identify the perpetrators. These databases are pretty unique, there is nothing like it out there.

Savant is basically a real-time network traffic monitoring. It helps you identify security breaches that have already happened. For instance, by identifying curious outgoing network traffic that isn't related to known company processes or, with the help of TraceCop, goes to known compromised actors or sites.

While very useful in identifying security breaches that have already happened, neither TraceCop nor Savant can actually prevent them from happening. Enter Intrusion Shield, the new product.

Intrusion Shield

Intrusion Shield is a device that sits between the edge router and the rest of the company network:



It combines process flow, that is monitoring and analyzing incoming traffic in real-time looking for suspicious behavior with TraceCop's databases of bad actors. All this is automatic, AI-based.

That in itself is a huge improvement over using TraceCop alone, because that was a manual product working on queries, and given the size of TraceCop databases, one can only do so much that way. As Jack Blount, the new CEO said on the May 27 CC:

> The company's revenues have been coming from consulting to agencies on a one-on-one basis. That is about the hardest way in technology to make money.

Basically what Shield does is take TraceCop's databases and Savant's real-time network traffic monitoring and automate the process with the help of AI. This has a number of immediate advantages:

- What used to be diagnostic tools helping you to locate security breaches and figure out where they happened and by whom, it now becomes a real-time protection tool, a shield.
- Rather than the labor-intensive, consultancy-type business the company had with TraceCop and Savant, greatly limiting their market reach, suddenly, the market opens up for them as Shield hardly requires any hands-on labor in installation or running. It's turnkey and runs automatically.
- Their consultancy business feeds into the algorithms of Shield as here is where they discover new suspect behavior and learn of new ways of network security breaches.

On the latter, from the May 27 CC:

> So I will continue to grow our federal business, our large corporation business and consulting because when we're asked to come in and consult with these people, we'll come -- they bring us in on the hardest problems they can't find or deal with. And they really want our help to be able to focus on that problem. So by doing that, that's where we get the expertise that we build into the AI that makes this product work. So we will continue to grow, focus and make our consulting business critically important for this company, just as been in the past.

We have talked to a few people who are not familiar with the company's products, and when we try to explain Shield, they are incredulous, and we can't blame them. It indeed sounds too good to be true.

But realizing what the company already has, labor-intensive forensic diagnostic tools like TraceCop and Savant, simply automating their execution on a rule basis (algorithms) and it starts to make sense. From the company website:

> Using AI Shield real-time identifies anomalies in your network traffic using novel patented and patent-pending methods of process flow technology to reduce that time to day one. Most breaches today are what is called malware free compromises - no alarms trigger in a firewall or endpoint solution. But the common denominator is that nothing happens without communications. Shield uses AI to uncover surreptitious communications and attempts to steal your data. Shield uses cutting edge and patented techniques to identify malicious activities without signatures using process flow technology.

Shield isn't signature-based as most cybersecurity products today. Cyber-attacks today are mostly written and operated by AI. That is, every time they come at you, they are slightly different, which is difficult for a signature-based security approach to deal with. This is why you see so many security breaches despite the billions spend on cybersecurity products.

There are, of course, other advantages, 10-30% of company employee worktime is wasted on visiting social networks, YouTube, and porn sites even (which also happens to be a great source of malware), and this too can be prevented with Shield, recovering at least part of the 10%-30% of lost labor productivity of companies which install it.

Shield SaaS business model

The product is intended for the commercial market, which is exactly where Intrusion hardly has a presence. But, given the new CEO's history in the Ministry of Agriculture where he set up a cybersecurity program, it can just as easily be used for extending the reach in government beyond just the DoD (and that holds for their existing products as well).

In order to get into the commercial market, the company isn't going to hire a huge sales force in order to sell the new product. Instead:

- They will start to activate the potential 18K channel partners which the new CEO (in previous capacities) helped to build.
- They will use big distributors like Ingram Micro, where the new CEO isn't exactly an unknown quantity and he already has an appointment.

Contrary to TraceCop, which requires extensive hands on company help selling and operating it, Shield requires very little instruction and is simple to install. In the words of the new CEO, "the product sells itself."

He also said on the May 27 CC (we really recommend listening to that in full) that the market for Shield is "the most unlimited market I have ever serviced by far." Normally, we would be inclined to qualify this as hyperbole, but this is a guy who (PR):

> Blount began his career as an engineer at IBM and was then recruited from IBM for the role of SVP of Business Development at Novell in the 1980s, where he helped expand its business from $50M to $2B in just six years. He has served as the CTO, COO, and CEO of eight technology, turnaround companies and has served on twelve technology company Boards of Directors, five of which were public companies, and he held the role of Chairman of five of those companies.

This is only a part of his CV, so expressions like "most unlimited market" coming from a guy with his background makes us sit up and take notice. And he put his money where his mouth is, becoming CEO of tiny Intrusion, and he has "never been more energized and excited about joining a company than I am now about Intrusion," according to the PR. He sure managed to convey that enthusiasm during that CC.

What we also particularly like is not just the fact that Shield is much less labor intensive to install and operate compared to TraceCop, it also runs on a SaaS business model.

They will charge something in the order of $20 per seat per month, which is very affordable even for small companies. And they can quit when they want, but they will be unlikely to do that as Shield generates

reports specifying from which threats they were protected over a time period, according to Jack Blount, the new CEO.

The upshot

We have some useful pointers here:

- The new Shield comes entirely on top of, and in addition to its existing business, which is almost exclusively just with the DoD.
- But even here the new CEO, with all his contacts in government, can be helpful in opening up other doors (for instance like in the Ministry of Agriculture where he for years set up a cybersecurity program).
- Let's not forget that the company already hired a new salesperson with extensive contacts in the DoD and he has already managed to get 6 or 7 new contracts, three of which are in the procurement phase.
- But the new product, Shield, is opening the vast commercial market, where Intrusion has basically no presence, multiplying its TAM by an order of magnitude, if not more.
- And it does so requiring very little manpower, no complex installations or operations and hand-holding by company people necessary. It's a turnkey solution that is a simple add-on for organization's networks. You switch it on and it works.
- It has introduced an attractive SaaS business model for the new business based on Shield, producing predictable revenue streams. That alone should have given the stock price a jolt. No more endless handwringing about this or that government agency renewing its contract or having budgetary problems.

Risk

It is difficult for us to see any risk since Shield, the new product comes in addition to its existing business, and even the latter are likely to benefit from Jack Blount's experience and numerous contacts.

What we don't know is how good Shield is, but we really urge you to listen to the May 27 CC where Jack Blount keeps on raving about it. If it can get experienced people like him enthused and coming to work for the company, then who are we to nag?

There was a price drop after the May 27 CC, but that is probably caused by:

- People in for a quick buck expecting that the company would put itself up for sale, which isn't happening.
- People disappointed they haven't joined with a big partner, but Jack Blount addressed this in the CC saying they wanted to keep more of the spoils for the company.

We have been buying quite a few for the SHU portfolio, as we see a potentially open ended upside here.

Conclusion

Intrusion has done so much with so little. They have carved out a niche, almost exclusively in the DoD where they have established a profitable business with their TraceCop and Savant products. This is a laborious, labor intensive sales and operational process, but the company has nevertheless been good at it.

The new salesperson the company hired a couple of months ago already is giving the existing business a bit of a lift as he has an ample rolodex containing people in DoD and the government.

The new CEO, given his background, can also take things beyond the DoD to other government agencies, like the Ministry of Agriculture where for years he led a cybersecurity project.

But the real upside is in the commercial market where Intrusion was basically absent. Now, they have a simple product, an add-on which every company can use and switch on, operating on an asset light, highly attractive SaaS model, and this comes all on top of their existing business.

We have no idea how good Intrusion Shield is, or how widely it can penetrate the market (it's pretty cheap so even small companies can afford it), but it is all in addition to their existing business so we're not seeing much risk to that.

Any sales of Shield will be additional and start generating a recurring revenue stream on top of existing revenues. It seems to us that the risk-reward situation of this stock has improved pretty substantially with that.

Disclosure: I am/we are long INTZ. I wrote this article myself, and it expresses my own opinions. I am not receiving compensation for it (other than from Seeking Alpha). I have no business relationship with any company whose stock is mentioned in this article.
