WHITE DIAMOND RESEARCH

WHY A CYBERSECURITY EXPERT CALLS INTRUSION AND ITS NEW SHIELD PRODUCT “GARBAGE” AS INSIDERS LIQUIDATE HOLDINGS

April 14, 2021

RESEARCH SUMMARY

Intrusion (INTZ) hired a promotional CEO last year, launched a new product called Shield, and its stock has risen 800%+.

Shield has no patents, certifications, or insurance, which are all essential for selling cybersecurity products.

Shield is based on open-source data already available to the public.

The datasheets and white papers on INTZ's website don't show details on what their products do, they just have empty buzzwords.

The companies that took part in Shield's beta test case study are associated parties.

INTZ's chairman of the board, Tony LeVecchio, was also the chairman of the board for UniPixel (UNXLQ), which was a touch screen technology pump and dump scam that went bankrupt and faced SEC charges.

INTZ's investor relations rep said the former CFO, Michael Paxton, who was with the company for 34 years, resigned because he's "scared to death".

The Paxton family sold hundreds of thousands of INTZ shares at $8 apiece in October of last year, and are continually selling shares today, with millions more shares to go.

We have a $4 price target on INTZ, for an 85%+ downside.

- Intrusion (INTZ) hired a promotional CEO last year, launched a new product called Shield, and its stock has risen 800%+.
- Shield has no patents, certifications, or insurance, which are all essential for selling cybersecurity products.
- Shield is based on open-source data already available to the public.
- The datasheets and white papers on INTZ's website don't show details on what their products do, they just have empty buzzwords.
- The companies that took part in Shield's beta test case study are associated parties.
- INTZ's chairman of the board, Tony LeVecchio, was also the chairman of the board for UniPixel (UNXLQ), which was a touch screen pump and dump scam that faced SEC charges.
- INTZ's investor relations rep said the former CFO, Michael Paxton, who was with the company for 34 years, resigned because he's "scared to death".
- The Paxton family sold hundreds of thousands of INTZ shares at $8 apiece in October of last year, and are continually selling shares today, with millions more to go.
- We have a $4 price target on INTZ, for an 85%+ downside.

Intrusion (INTZ) is a tiny, struggling data software company that historically has sold to government agencies. The founder unexpectedly passed away a year and a half ago, and a new turnaround specialist CEO, Jack Blount, took his place last year. The moment that Blount joined, the company conjured up and started to aggressively promote a new cybersecurity product it calls "Shield" – INTZ's product that the market is now betting on. Sometimes a new flavor can be sweet at first, but sour in the end. We believe this will hold true for INTZ.

Over the past year, the stock has risen from around $3 to over $25 today, a gain of over 800%. We congratulate them on a great run so far. However, we provide a substantive case on why we don't believe this euphoric rise will last.

We attribute the entirety of this gain to expectations around Shield. The company and its investment banker, B. Riley, have recently made what we believe are unrealistic and far-fetched claims about Shield to entice retail investors into buying INTZ stock. INTZ also recently reported the results of a beta test with numbers and words

that are so extreme, they sound like they come from a bad science fiction movie.

We have a $4 price target on INTZ, implying around 80% downside to its current $26 price.

Shield: A Repackaging Marketed as a Rebirth

In October 2020, following a period of hyped beta testing, INTZ announced the launch of Shield. Shield is the company's latest attempt to bolster its arsenal of products and is peddled as "the only cybersecurity tool that stops threats immediately." Excitement about the product is largely responsible for the stock's >50% rise since the start of 2021.

Despite heavy promotion and a supposedly successful beta test, we do not believe Shield represents a novel offering from INTZ. In fact, we believe the company itself has said this. During INTZ's Q420 Earnings Call, and in a buzz-word flurry (AI, cyber-, supercomputer, etc.), Blount revealed that Shield is simply a mashup of INTZ's existing products. In Blount's words:

Shield is really all 3 of Intrusion's technologies married together in a single product solution.

While this may initially sound exciting, it hardly represents any ground-breaking innovation.

Here are a few other statements that Blount made in the Q420 Earnings Call suggesting Shield is a repackaging of pre-existing technology rather than an innovative offering:

- "**The TraceCop database** that we have created, managed, grown, used for 25 years, is the core of what makes Shield work today."
- "**The Savant technology** that we've had and improved for 12 years, again, is a core piece of the technology of Shield. How we open, inspect every packet of data is with the Savant technology. The only new thing that there is in Shield is the artificial intelligence that learns from the database, that can interpret what it finds when it opens a packet of data, and how it can decide if it's good or bad, when humans could look at that packet of data and have not a clue whether it was normal traffic or not normal traffic."
- "You have to think about Shield as the combination of 25 years of R&D, 25 years of product and development, 25 years of expertise around cybercrime, combined into a single product."

The term artificial intelligence or "AI" is simply an empty buzzword.

Here is what Chris McGarrigle, a cybersecurity expert that we'll go into more detail later, says about the term "artificial intelligence":

People often term change as: artificial intelligence, neural networks, machine learning, natural language processing, all these phrases are 99% of the time bullshit. The algorithm is already there. So artificial intelligence in its most traditional meaning is you give the computer a set of parameters and you teach it on previous data sets, and you allow the computer to basically automatically match each data set based on the information that you essentially made it learn. So that's not anything new, we just used to call it algorithms. And in this case, it can be as simple as this, if the software detects traffic over here, then we have a pattern that we can match it against, which then the algorithm matches the data to that pattern and qualifies it back to the user as bad. So that's artificial intelligence, job done, you can now claim that you have AI.

We believe the timeline of the announcement coupled with the lack of direct R&D investment into Shield preceding Blount's appointment as CEO casts doubt on Shield as the culmination of a quarter-century master plan.

- Though INTZ's R&D accounts for ~39% of the company's expenses (aside from a small peak in 2015/2016), R&D has remained reasonably proportional to its total operating expenses.
- According to its accounting policies, INTZ expenses R&D as it is incurred, thus the recent uptick in R&D expense in 2020 would not be related to Shield (if it truly is a product launching on the back of years worth of R&D).
- Recent financial statements provide no indication that INTZ has been ramping up to commercialize a cutting-edge cybersecurity product.

The following shows INTZ's R&D expense and other operating expenses over the past 10 years:

Source: INTZ SEC Filings

INTZ's R&D spend is disproportionally low compared to peers, despite the stock being valued at a significantly higher sales multiple. We believe that R&D is a significant leading indicator of both sales and valuation in the cybersecurity space. As INTZ's R&D has remained low, we believe its revenues will also remain low.

Source: Y Charts

There are numerous established companies that provide intrusion detection and prevention systems called "IDS" (Intrusion Detection System). As stated on Wikipedia:

"An IDS is a device or software application that monitors a network or systems for malicious activity or policy violations."

The list of vendors include Palo Alto Networks, Cisco, McAfee, FireEye, Snort, Ossec and many others. In short, while new INTZ investors could believe that the company invented the IDS/IPS concepts, this is a well-established and crowded space dominated by well-established players.

We Interviewed A Cybersecurity Expert Who Said Intrusion and Its Shield Product Are "Garbage"

Chris McGarrigle is the CEO of Blackwatch Digital, an established and reputable cybersecurity company. He shared an enormous amount of knowledge about the industry. He has a negative view on INTZ and Shield, which we will reveal throughout this report. On the other hand, he made positive statements on other

cybersecurity companies that we include in this report.

Of note, McGarrigle isn't a stock trader, and hadn't heard of INTZ before we asked him his view. Furthermore, we provide the opinions of two other cybersecurity experts. All three agree that Shield is "vaporware".

The interview started with:

McGarrigle: *There is little to no public information on the products, let alone any in-depth technical part of it. They have a partner portal on the website and things like this. But there's no support portal on the website. There's no knowledge base, there's no support articles.* ***There's nothing where you can actually see the problems that customers have (that can then be addressed)****. Like if you go to Cisco's or Microsoft's websites, you will see an enormous support section where people will come across problems and there's a solution for them. If there's a flaw in the software, there's a solution for it.*

The info is thin on the data sheets for TraceCop or Shield. The Shield is horses___. That's just garbage.

White Diamond Research ("WDR"): *What part of it is garbage?*

McGarrigle: *All of it. It's telling me nothing. There is no data on the data sheet.*

Just like McGarrigle said, you can see on Cisco's home page there's a community page for people using their products. There's nothing like that on intrusion.com.

We'll quote more of McGarrigle's opinions throughout this report on the topics we discussed.

Intrusion's Product Datasheets Have No Substance, Are Just Filled with Vague Buzzwords

McGarrigle was shocked at the lack of substance in INTZ's datasheets for their three main products: TraceCop, Savant, and Shield. "These are the smoking gun", he said.

You can see INTZ's three so-called "Datasheets" on its resources tab on its home page, as shown below:

Source: Intrusion Resources Page

McGarrigle stated:

There's a section on the datasheet for Shield that says "protect the company by" and there's 10 data points. But ***there's no mention of any actual technology that's been implemented here****. It says "blocking, fuzzing, contract hacking, poisoning." I'd expect a 21-year-old to say this when looking for a job.*

WDR: *It's just a bunch of buzz words?*

McGarrigle: *It really is.*

The following are the data points on the Intrusion Shield datasheet:

Source: Intrusion Shield Datasheet

We agree with McGarrigle, this isn't really product data. We believe it looks more like an advertisement to impress uninformed retail investors than a prospective customer would look at to evaluate the product's specs. INTZ's datasheets are extremely short and don't show any details of the product.

For example, take a look at a datasheet from an established cybersecurity company, like Cisco (CSCO). Its datasheet for its Cisco SecureX platform shows details like diagrams, screen shots of it in action, response workflow descriptions, product and third-party integrations, and regional cloud availability.

Another example is the datasheet for Palo Alto Networks (PANW) PA-220 Firewall appliance that can be found on its website. It has much more detailed information than INTZ's datasheets. It shows performance and capacities, hardware specifications, operating temperature, input voltage, max current consumption, etc.

Stunningly, McGarrigle revealed that INTZ's "extensive database" referenced in its TraceCop datasheets is no different than open-source alternatives widely available to the public.

Said McGarrigle:

Even if you look at their popular product, Tracecop, the main feature on the data sheet says:

"Intrusion TraceCop is the most extensive database in the world, because it holds The Domain Whois, the IP Netblock Whois, DNS Records, and Usage and Metadata."

First of all, the Domain Whois is an open source, open database, available to anyone. *So you don't need TraceCop for that. IP Netblock Whois is an open database, easily searchable on the internet via websites. You don't need that. DNS records are, again, completely independent. Anyone who has access to the internet doesn't need a piece of software to read it.* ***And then the final piece the Usage and Metadata, "250 open source threat intelligence feeds". So you're actually claiming there that it's "open source". So you don't own it. There's no owned IP there. So you can say that they are the consolidator of free information, but that's all they are.***

The following is the list that McGarrigle refers to on the datasheet for TraceCop:

Source: TraceCop Data Sheet

For Savant's datasheet, McGarrigle said:

If you look at the Intrusion Savant datasheet, it comes close to it where on the first subject it says it "has 20 Gbps of bidirectional protocol decoding and packet capture." First of all, that's just bad grammar the way that's even been written. It makes me think it's not written by a technical person.

The following is the section from Savant's datasheet that McGarrigle refers to:

Source: Savant datasheet

The Companies Featured From the Shield Beta Test Are Small And Have Existing Relationships with Intrusion

In INTZ's Needham Virtual Growth Conference presentation on 1/13/21, a slide shows the testimonials of three companies that were part of the Shield beta test. This slide is shown below:

Source: Needham Presentation

All three customers have existing relationships with INTZ.

- B. Riley Financial is INTZ's investment banker who organized the equity raise in October 2020 and then issued a glowing initiation report on the stock.
- Bard Associates is a shareholder of INTZ.
- We interviewed the IT Manager for NovaTech, and he said the only reason why they got involved in the beta testing is because an IT securities guy works for both NovaTech and INTZ. We provide more details on this interview later in this section.

On 1/13/21, INTZ released two press releases when it finished its beta testing on Shield. They are shown below:

The original PR is linked here, the "corrected" one is linked here.

In the PR, INTZ made a lot of bold claims for a product with no real traction in the market. It states:

"Beta testing of **INTRUSION *Shield*** confirmed the solution's efficacy by stopping a total of 77,539,801 cyberthreats from 805,110 uniquely malicious entities attempting to breach 13 companies that participated in the 90-day beta program. ***Shield*** was able to continuously protect these companies from ransomware, denial of service attacks, malware, data theft, phishing and more."

These numbers don't seem real, but something out of a science fiction movie. This means that on average, over the 13 companies, each company was attacked 6M times over the 90-day trial period / 66k times per day / 2.7k per hour / 46 times per minute.

Total threats	77,539,801
Threats /	
per company	5,964,600

per company per day	66,273
per company per hour	2,761
per company per minute	46

Source: Author Calculation

How have these companies been able to function so far, as they've been attacked many times per minute by ransomware, malware, data theft, phishing and DDoS attacks?

The company also claims that Shield is so good, it could have prevented the recent Sunburst malware attack. The PR states:

"In fact, analysis by **INTRUSION** also concluded that ***Shield*** would have defended against the Sunburst malware that was at the heart of the recent cyberattacks involving SolarWinds and FireEye, which impacted many government agencies and 18,000 SolarWinds customers."

SolarWinds (SWI) is a $5B+ IT infrastructure management software company. It sells security and data protection products. It spent $32M in Research & Development (R&D) and $82M in Sales and Marketing (S&M) in Q420, and a whopping $126M for the entire year 2020. We don't believe that INTZ has developed a more sophisticated malware defending software than SWI, given what each company has accomplished and that INTZ has invested so little in R&D.

Regarding this outlandish claim by INTZ, McGarrigle said:

Yeah, that's just garbage. My problem with that is, that's a huge overreach. If they said something like "our platform would've helped in early detection of it and sped up recovery post compromise", then yeah, ok that's fine, see what you're doing there is adding value to a situation that was pretty bad. But to say that you would've prevented it – no chance in hell, my friend. Solarwinds and all the companies that use it are not Mickey Mouse places. And first of all, the compromise started by someone inside the company, so right now we don't really have much software that prevents that type of compromise, so that's (expletive) straight out the door. And any companies that Microsoft uses for its software, millions of dollars of the world's best intrusion protection, malware prevention, packet inspection, software and hardware on the planet that Microsoft employs, and it circumvents all of those, a mix of social engineering and traditional cyber-attack. To say that their software would've stopped it without any evidence, is garbage. Because in the cybersecurity world, and the penetration testing world, there's a really easy way to back that up. You do what we call a proof of concept. You have the parameters of the compromise, so we do a proof of concept to show how the hardware or software would've prevented it. And if they didn't publish that proof of concept, it's like me telling you I'm the world's greatest soccer player.

INTZ has not revealed any proof of concept that shows that its software would've helped stop the Suburst malware attack. It simply says:

"analysis by **INTRUSION** also concluded that *Shield* would have defended against the Sunburst malware."

But this analysis that INTZ claims they did is not published anywhere that we have seen. Therefore, it's about as credible as us saying that we're the greatest MMA fighters in the world, without showing any proof.

A Look At the Case Studies

INTZ shows on its website three companies featured in the beta test case studies. These companies are AM-Liner East, NovaTech and Willow Street Agency. Willow Street Agency has 40 estimated employees, AM-Liner East has 123 estimated employees. We spoke with the IT manager at Novatech in Lynchburg, VA, and he said it has less than 50 employees. These are small companies to pay $2K per month for Shield.

According to INTZ's Investor Relations rep, 12 out of the 13 companies that took part in the beta test are now customers. The details of their arrangements aren't disclosed. What's interesting is many of the companies in the beta test are small, which would likely make the $2k/month minimum cost (100 employee equivalent) too prohibitive for several of these customers.

I didn't realize we were part of any published case study with them, I knew we were participating in a beta program but I wasn't aware they were publishing anything from that.

Said the IT manager from NovaTech in our interview. He also said:

I'll give you the background of how we got in. One of the major players over there used to be a full time IT security guy over here. He still is part time, on an as-needed basis for IT support. He offered us this opportunity to participate in this beta program. So we took him up on it and we've been evaluating it for about 8 months now. We are happy enough with the service to the extent that we signed up for three days.

Dr. Tyson B. is the IT security guy who works for both NovaTech and INTZ. On his LinkedIn page it shows he started working with INTZ right after Novatech:

Source: LinkedIn

This above images from LinkedIn show a clear relationship between INTZ and Novatech through Tyson B. Investors should view these deals cautiously as we believe they are more indicative of the company trading favors with an associated party than the potential for converting a customer.

A Look At Intrusion's Executives And Directors

Jack Blount, CEO

Ward Paxton and Joe Head founded INTZ way back in 1983. Paxton led the company as Chairman, Co-Founder, President, and CEO while Head served as a Director and Executive Vice President. The company has historically always had miniscule revenues and a tiny market cap. Ward Paxton unexpectedly died on 10/24/19 and the company hired a new CEO.

INTZ announced on 5/27/20 that it hired Jack Blount as its new President and CEO. Blount's history is of a

turnaround CEO. As the PR says regarding his background:

He has served as the CTO, COO, and CEO of eight technology, turnaround companies and has served on twelve technology company Board of Directors, five of which were public companies, and he held the role of Chairman of five of those companies.

On Blount's website, jackblount.com, it advertises Blount and his turnaround successes.

Source: jackblount.com

Blount's resume doesn't suggest that he is a genius programmer or masterful inventor that is going to suddenly create a groundbreaking billion-dollar cyber security product that the world lacks and needs. It suggests he's a good salesman, organizer, and wheeler and dealer businessman.

We don't believe the company's outlandish claims about how good the Shield product is and we have skepticism on how much value-add Blount actually contributed to the inception of the product.

Tony LeVecchio, Chairman of the Board

Not long after Blount was hired, on 8/6/20, INTZ appointed Anthony (TONY) LeVecchio to its Board of Directors.

Blount is quoted in the PR:

"I've worked with Tony on several boards over the past twenty-five years and he has always been a strategic resource to me on acquisitions, strategic partnerships and distributor agreements."

As stated in the PR, LeVecchio was the co-chairman of UniPixel (UNXLQ), a company we know well. UNXLQ was another hyped-up technology company selling a new kind of touch screen film that turned out to have worthless tech and is now bankrupt. UNXLQ faced SEC charges for misrepresenting the company's technology to investors. Adam Gefvert, CFA, the head analyst at White Diamond Research, published three bearish reports on UNXLQ in 2013 and 2014.

Now, LeVecchio is Chairman of the Board for INTZ, like he was for UNXLQ. We believe this should be a big red flag for investors and a premonition of things to come.

Michael Paxton, former CFO and the son of the former CEO

On 12/24/20, INTZ announced that Michael Paxton was stepping down from the Company's Board of Directors effective 12/31/20.

Paxton had been with the company for 34 years as the CFO. He is also the son of the former CEO, Ward Paxton. We believe the resignation was telling: if INTZ was on the cusp of finally making a breakthrough, we believe Michael Paxton would have stuck around to reap the rewards We think Paxton's departure on the back of shares rising 800%+ in the last year further validates our views of an overvalued promotional story.

The recent share sales by Paxton further reiterate his vote of non-confidence. On 3/12/21, he filed to sell 50K

shares, and filed on 3/16/21 that he has already sold 12,500 of those shares. On 10/21/20, Paxton filed that he holds a whopping 2.08M shares, which is 12.3% of total INTZ outstanding shares.

We reached out to INTZ's investor relations ("IR") rep, Joel Achramowicz to get more information on the company and its future. We asked him:

Why would Michael Paxton resign after working with the company this long and helping with the technology? Wouldn't he want to stick around and see the company forward?

Achramowicz replied:

Actually no...he's scared to death and he wanted to cash out. He has no interest in being an entrepreneur. He had no value to the company. Some people say he should be sitting on the board – no! He didn't even know what he was sitting on. The best thing he could is leave and sell his stock and that's what he's doing.

McGarrigle believes these "fears" may be related to the lack of indemnity insurance the company has against the product claims it has made.

McGarrigle stated:

Why would he be scared to death in the first place? That to me sounds like he's scared to death of getting sued. And that should be a simple thing to see the amount of liability and indemnity insurance the company actually has for its executives in the first place. If he's scared to death because there's no protection against if someone uses the product and it turns out not to stop an attack, or a compromise or whatever else, are they then liable for it? And where does the liability end in the US, does it come all the way down to the directors of the company?

We can talk a lot of that, because at Blackwatch we had a huge Lloyds of London policy of like $80M of coverage, which cost us $1.2M a year to get that underwritten. And that was just to protect us from everything from professional misconduct from one of our consultants all the way through the actual products and services we offer. So that goes back to my point, if your product is good enough then you should be able to get things like insurance. Lloyds of London looked at our software, they used their consultants to review it and see what the risk was. Before they provided us with $80M of cybercrime insurance and things like that, they took a fairly exhaustive look at it. So you can show that to your customers and say "look here is the proof, it's not just us saying it". And these guys (Intrusion Inc.) have nothing, they have absolutely nothing.

It doesn't seem like INTZ has adequate insurance for its Shield product. Looking at the **latest** 10-K, it says they have business liability insurance, but doesn't go into detail and states that the company is at risk of product liability. We expect Michael Paxton to continually dump his shares of the company in the near future.

Intrusion Was Recently Uplisted To The Nasdaq At The Same Time Insiders Sold

On 10/9/20, INTZ announced its uplisting to the Nasdaq from the OTC exchange, and the sale of 3.1M shares at $8 per share. 1.1M of those shares were sales by insiders, mainly the Paxton family.

Michael Paxton, Mark Paxton and Julie Paxton all sold shares in this offering at $8.

As shown in recent filings below, Mark Paxton sold 219,469 shares at $8, and has 1.4M shares remaining.

Julie Paxton sold 265,448 shares at $8, and has 1.7M shares remaining.

The Paxton's have become very wealthy in less than a year's time from the huge rise in INTZ stock, each now worth tens of millions of dollars. In their wildest dream they likely never thought the stock would get this high. We share that view and believe investors would be best off to head for the exits like the Paxtons.

Other Cybersecurity Experts Posted Their Skepticism Of Intrusion On Social Media

Aside from McGarrigle, there have been two other noteworthy skeptics that have posted negative views of INTZ's products on social media. Although they are anonymous, it seems quite clear to us that they are also have expertise in cybersecurity.

The following thread is noteworthy:

Source: Twitter

Source: Twitter

Source: Twitter

On INTZ's Yahoo Finance Conversations page, here is what an apparent cybersecurity expert that goes by "CyberDad" has to say about INTZ. He is sure that it's a scam:

The above post echoes our views. We don't believe Shield was the result of a 25-year master plan by the company.

One of CyberDad's criticisms is INTZ doesn't say exactly what its Shield product does. CyberDad said above that he would "love to see a whitepaper that shows exactly what their product does". On INTZ's website, they do have a whitepapers section. While the whitepapers of most tech companies feature their products, none of INTZ's directly mention Shield or its two legacy products! They are just industry reports on cybersecurity from other parties:

Source: Intrusion Whitepaper Webpage

Lastly, CyberDad posted:

CyberDad compares INTZ to legitimate cybersecurity companies, Secureworks (SCWX) and Essentire, that offer a similar product to Shield. He points out problems with the Shield product, and how it won't be able to attract an enterprise customer. McGarrigle had the same opinion.

Intrusion Has Not Completed Any Certifications

INTZ doesn't mention having any certifications on its website or in its 2020 annual report which was recently filed on 3/9/21. McGarrigle told us:

*I wouldn't touch these guys (Intrusion). I certainly wouldn't put them in any type of environment**. Like my opinion, I wouldn't even deploy software from these guys in an enterprise environment. Not because of their functional risk, but there is absolutely no authority or certification process** that tells me that their software would not actually present or implement more problems than it could ever resolve**. Like there's no 3rd party certification, there's nothing.** And when you deploy the software, it goes into the most sensitive parts of your network. So you don't open your network up, open to software that's not certified. It needs to have a rubber stamp of approval before I would even touch it and actually deploy this.*

If you look at OWL cyber defense. You look at their website. Now I've worked with these guys for years, and they know their stuff, and they are a huge defense contractor. You look at their certifications they've got from their defense departments, I'll deploy the software and hardware from these guys any day of the week. They represent the company properly, everything they say is actually backed up with external verification.

The following are the certifications and awards that Owl Cyber Defense shows on their website. We've circled the ISO certification, as that's an important one. There aren't any certifications shown on INTZ's website.

Continuing McGarrigle's statement on certifications:

EAL certified, certifications and awards. Intrusion is not even ISO certified, they aren't ISO 27001. They aren't Soc Type 1, Soc Type 2. This even means that they haven't certified that the company and the way they make their products adheres to any external verification or certification, that's just dumb that they aren't doing that, it costs $5K to get ISO certification. But what it does is it confirms that you have the processes internally that can actually deliver these products and support them.
ISO 27001 would be your IT processes. A company like that should absolutely have their certification. It's the basic one they should have. The company (Intrusion) is bullshit.

The following is what it says about EAL (Evaluation Assurance Level) testing on Wikipedia:

Source: Wikipedia

This page explains ISO 27001 certification:

This page explains the difference between a SOC Type 1 and SOC Type 2 report.

Source: linfordco.com

INTZ doesn't have any of these basic, and necessary, certifications for an IT security company. That's a huge, and dangerous, red flag which suggests that its Shield product doesn't perform well enough to pass these assessments.

Intrusion Has No Patents For Its Shield Program

The fact that Shield doesn't have patents or patents pending seems to confirm our expert's view that all of INTZ's IP is open-source. INTZ's 10-K doesn't state the company has any patents for TraceCop, but it has some for Savant. It says: "In addition, we have received two patents, and we are in the process of applying for patents for our ***Shield*** family of solutions. "

However, we couldn't find any patents pending for INTZ's Shield on uspto.gov.

McGarrigle stated regarding INTZ's patents:

I looked last night to see if there's any patents or patents pending. I couldn't find anything. And going back to the previous point, if the industry average is 30%, and your false positive rate is 0.001%, at the very least, pay $600 for a patent pending application. If your product is as good as that. And if you don't know that you should be doing that, then that's just a wider level of incompetence in general. If I was a shareholder, I'd be pissed.

We go too far the other way (at Blackwatch Digital), we put a patent on everything. Like if you turn on the light a different way, we put in a patent for the office lol. But that's part of the game, it's to try to protect as much of the IP as they have. If you're not doing stuff like that, then it's highly suspicious. ***So I'd like to see a patent pending on the capability of the false positives. There needs to be a process, the technology, or something that can be depicted that they have a patent.***

If you don't have a patent and don't have a certification by an external vendor, then there's serious questions as to what you actually have.

Intrusion Has Failed to Create Successful Products Since TraceCop

Since its launch, the TraceCop product line has been the lynchpin of INTZ's business. The company has gradually sought to form a team of products around it. We found the company has sold TraceCop as far back as a quarterly filing in 2008 where it's mentioned. In the company's earnings calls, they mostly discuss current and prospective customers of TraceCop.

As of INTZ's Q4 2009 Earnings Call, Ward Paxton disclosed, "most of our revenue is generated from sales of TraceCop."

92% of cumulative net product revenue from the first 9 months of each fiscal year from 2013 to 2020 has been generated by the TraceCop product line.

As it wound down earlier offerings, INTZ brought its 24/7/365 network monitoring product line, 'Savant' to market in 2010. Upon release, the product was touted as "an exciting new product family" with "many potential applications". Savant remains a part of INTZ's product suite today. However, the Savant product has been a flop and has recently seen quarterly revenues below $50K.

Below are a few examples from INTZ's filings which illustrate Savant hasn't provided a significant contribution to INTZ's product mix:

Q2 2012 Earnings Call: "Practically all of our revenue at this time is from TraceCop products and services. As you remember, our TraceCop family of products and services is used to discover and identify bad guys. We expect this requirement to continue to grow for a long time."

- Q3 2014 Financial Statements: "Decreased product revenues were primarily due to an unexpected lack of growth in sales of our Savant product line. TraceCop sales for the quarters ended September 30, 2014 and 2013 were $1.5 million and $1.6 million, respectively. Savant sales were $0.5 million for the quarter ended September 30, 2014 and were $0.4 million for the quarter ended September 30, 2013.
- Q3 2019 Financial Statements: "Increased product revenues were primarily due to an increase in sales of our TraceCop product line. TraceCop sales for the quarters ended September 30, 2019 and 2018 were $3.9 million and $2.7 million, respectively. Savant sales remained the same at $29 thousand for the quarters ended September 30, 2019 and 2018."

INTZ has identified this dependence on one product line as a risk in the notes to its filings (also shown below).

Source: INTZ 2020 10-K

With 2020 revenues declining to pre-2013 levels, and the Savant product teetering near obsolescence, we believe INTZ created Shield as a lifeline. However, we think it's fate will be no different than Savant's.

We Are Doubtful That Intrusion's Recent Sales "Agreements" Will Lead to Significant Revenue

On 3/31/21, INTZ announced that it signed a "new agreement" with leading global consumer products company Kimberly-Clark (KMB). One of the reasons why investors should be skeptical of this "agreement" is that the announcement doesn't include any financial details or terms on duration. We are not convinced that the contract is revenue generating and believe the "generalizations" in the announcements could imply a pilot program.

We don't believe a company the size of KMB would agree to migrate its network to a cybersecurity software that doesn't have any 3rd party certifications, without first testing it on a trial basis.

On 4/6/21, INTZ announced a new Shield customer, Lippert Components from LCI Industries (LCII). We don't think this sale is a big deal because Lippert was a former customer using INTZ's Savant service. This is also another associated party sale. James Gero is on the Board of Directors of both Lippert and INTZ. As shown in the screen shots below:

Source: Lippert's Board of Director's page

Source: INTZ Board of Director's page

Notice the Lippert executive, Jamie A. Schnur, president of the aftermarket, used the buzzword "AI" when describing why it is a Shield customer. However, Schnur isn't the IT guy in charge of cybersecurity.

We spoke with the investor relations rep of LCII. He said that the CFO told him that there's a wide range of programs they use for cybersecurity. From emails, to cell phones, to any of their machinery that's hooked up to the internet. And they report to their audit committee about their cybersecurity measures.

Risks To The Short Thesis

Shorting INTZ isn't without risks. There's the risk that the stock could go higher from more of the company's promotional presentations and PRs. It reached an all-time high of $29.90 on 3/16/21, rising over 20% from the previous day's close. INTZ presented at the ROTH Investor Conference that day, so it probably rallied from being presented to investors at the conference.

There are no options on the stock, so traders can't buy puts, they have to short the stock to profit off the decline. The borrow rate isn't much, only about a 2% annual rate on the retail brokers we've seen. It trades on the thin side, about 150K shares or $4M per day on average. If insiders keep selling shares, the float will increase which should increase the stock's volume and decrease the share price volatility.

Why We Believe Intrusion's Share Price Will Fall Relatively Quickly

INTZ is making the claim right now that it has an amazing new cybersecurity product that had a successful beta test with glowing customer reviews, the world needs it and it will be wildly successful. There's no need for tweaking, the finished product is ready now.

We claim that it's all smoke and mirrors, and the product won't sell very much. Either the company will prove to be correct, or we will. It won't take a long time to find out who's right, especially if Blount takes off for his next turnaround opportunity before the stock collapses.

How We Estimated A $4 Price Target on Intrusion

From the extensive due diligence that we've done and presented in this report, we found that Shield isn't a good product. Therefore, we don't expect that INTZ will keep many customers after the initial sample period. Cybersecurity is a very competitive industry, and we don't believe INTZ will be able to compete in it. As INTZ fails to hold onto customers, it will also fail to make a significant amount of revenues. Even if some customers do stick around, it will be as an add-on to an existing, main security system.

Right now, INTZ has 17.5M shares outstanding. So a $4 share price would put the market cap at $4 x 17.5 = $70M. This market cap is assuming that Shield fails to gain traction in the commercial market, and that becomes apparent within a year. A $70M market cap is still considerably higher than INTZ's historical market cap. It traded between $3-$4 per share for much of early 2020, and it had a much lower share count at that time.

WHITE DIAMOND RESEARCH

Independent institutional-grade research focused on identifying asymmetric risks in small and micro-cap equities.

LEGAL DISCLAIMER

As of the publication date of our reports, White Diamond Research, along with its clients, affiliates, and related entities, may have a short position in the securities discussed and stand to realize significant gains in the event that the price of the stock declines. Use White Diamond Research at your own risk. You should do your own research and due diligence before making any investment decision. No information contained in our reports should be interpreted as financial advice.