NZS Capital, LLC

Zero Trust: An Antidote for Cybersecurity Theater

Zero Trust: An Antidote for Cybersecurity Theater

Narrator: "Good morning, good afternoon, good evening and welcome to the NZS Capital podcast.

"In 2020, the average human created about 1.7 MB of data every single second, which works out to a daily total of about 2.5 quintillion bytes of data, an astonishing number that's only set to grow exponentially because the digitization of the global economy is still in its infancy.

"But all that data is vulnerable to theft as illustrated by these recent reports from NPR.

> NPR: "Authorities say the Russians targeted some of America's most sensitive and important computer systems.
>
> "Hackers breached SolarWinds to infect at least seven U.S. government agencies.
>
> "Government agencies were caught off guard by an unprecedented attack."

Narrator: "According to McAfee, global losses from cyber attacks hit an estimated $945 billion in 2020, a 34% increase in two years.

"That figure is also about seven times more than organizations are estimated to have spent on IT security globally in 2020, suggesting there's something of a disconnect between the systems being put in place and their effectiveness.

Joe Furmanski: "The shift online is changing every aspect of our lives – we're rapidly digitizing things like education, recreation, work, finances. To protect ourselves we have to evolve our behaviors from the way we were doing things before, because the number of threats and their severity are only going to go up. This isn't a maybe. It's an absolute certainty."

Narrator: "That's NZS investor Joe Furmanski, who sees an urgent need for all organizations, public and private, to fundamentally re-think their approach to data, device and network security.

"Recent high-profile attacks illustrate what Joe is getting at. Examples include the SolarWinds breach that compromised 100 companies including Microsoft and Intel, along with about a dozen US government agencies including the Treasury and the departments of Defense, Justice and Energy."

Joe: "Embarrassingly, hackers also got into systems at the Department of Homeland Security. This is the branch that's charged with protecting federal computer networks from just these attacks.

"The same Russian group that actually may have conducted that attack also went against other US agencies and even Microsoft, while we also saw a ransomware attack shut down a major US pipeline.

"When you have pipelines getting shut down, we're just steps away from things getting really, really bad. If the wrong people got their hands on key infrastructure, then we could really see a situation where we are on the brink of disaster.

"So it's not our imagination that cyber attacks are becoming more common. We're reading and hearing about them more frequently because they're actually happening more frequently. This is a function of more nation states being involved and participating more in cyber espionage. Cyber crime can do lasting damage to fundamental pillars of our country – finance, power generation, communication, defense, democracy itself.

"So this isn't a story about a kid sitting around trying to hack into your laptop for a bitcoin or something like that. These are well-funded, sophisticated organizations and they are focusing on government and key infrastructure assets using extremely powerful tools that give them the potential to wreak havoc on a global scale."

> "CyberSecurity Ventures predicts by 2025 cyber crime globally could amount to $10.5 trillion.
>
> "Cyber attacks have the potential to take down the power grid, take down the Internet and all the systems that rely on it."

Narrator: "While forecasts like the one from Cybersecurity Ventures cited in that clip from CNBC's "The News With Shepard Smith" should be treated with caution, if the publisher of Cybercrime Magazine is right, then cyber crime will soon be worth more than the illicit drug trade."

Joe: "It's this potential for someone to be motivated to take control of key public and private networks – financial markets, defense, supply chains, power grids, air traffic control, so on and so forth -- that is making lawmakers sit up and take notice and work on putting together a coordinated effort to tackle this.

> Joe Biden: "We've seen time and again how the technologies we rely on, from our cell phones, to pipelines, to the electric grid, can become targets of hackers and criminals.
>
> "In May I issued an executive order to modernize our defenses and improve our federal government cybersecurity. Because of that order, the government will only buy tech products that meet certain cyber security standards, which will have a ripple effect across the software industry in our view."

Narrator: "President Biden's executive order called on the Federal Government to improve its efforts to identify, deter, protect against, detect, and respond to what it described as "persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy".

Joe: "Yeah, so recently President Biden further underlined how urgent and serious this problem is when he actually brought in a number of tech CEOs to the White House for a summit to discuss how the public and private sectors have to work together on the issue.

"President Biden's executive order said the government must "accelerate the movement to secure cloud services". That phrase gets to the heart of the issue because perhaps the most common defense currently against cyber attacks is a firewall. But something like three quarters of hackers say a firewall is no deterrence at all, so in actuality, all you're doing by deploying one is creating a false sense of protection – something known as security theater.

"Moving away from this perimeter style of thinking is something that organizations are struggling to get their heads around, as it requires a cultural shift. It's tough to accept for a lot of IT people who grew up putting the perimeter model in place and staking their careers on it because it's basically saying everything you did over the past 20 years is pointless. It didn't do anything.

"Network architecture has to change urgently and fundamentally to keep pace with these threats."

Narrator: "For Joe, organizations must move away from the firewall framework and design systems to protect networks, data and devices through what's known as zero-trust architecture."

Joe: "So when we started doing business on the Internet, we were doing it all from the four walls of an office building and what we've seen is actually we've been slowly shifting away that permitter, if you will, that was in the office building was slowly expanding as we adopted things like the Cloud and SaaS software and people began to work more and more frequently remotely.

"And that was happening over a slow period. And then COVID hit. And when COVID hit we pulled forward this demand and it really actually showcased how we've been slow to reach to what the future is actually bringing to us, which is a fully disaggregated, decentralized, remote type of environment.

"But even if people are now going back to the office they're doing it in a hybrid way going forward. That means the castle and moat model no longer works appropriately.

"Increasingly organizations are trying to put square pegs into round holes by basically bootstrapping new features into what was an existing model for cybersecurity, but that can't provide the necessary protection with the employees working remotely and using their own devices to connect through public networks, and so on.

"Relying on hardware in your home building and requiring every user and device to back haul through one location is actually becoming more of a threat than a benefit. You think I have this firewall in place, everybody is VPN-ing in, I've checked all the boxes, we're secure. But in actuality, you're not and you've let your guard down.

"As we move toward the Internet of Things and everything being connected, we're discovering that the perimeter model of firewalls between you and the Internet is increasingly inefficient.

"Companies have to move quickly to gain better appreciation of the tools needed for zero trust authentication and access."

Narrator: "The fundamental difference between a firewall model and a zero-trust framework is that the former seeks to prevent a breach while the latter works on the basis that bad actors are already inside your system.

Joe: "Zero trust is not a product. It is a behavioral framework, it is a behavioral model that has to be completely shifted, and that means it is incredibly difficult, because it taxes the cultural setup and the team organization that you have in your IT networks.

"Behavioral models are really, really hard to do. So it's really important to understand that zero trust isn't a single product or a single company or anything like that. It is a mental model for addressing cybersecurity that we haven't really thought of before.

"So zero trust assumes that you're constantly being hacked so therefore it seeks to limit movement around your network to put a brake on the potential of a hacker to cause havoc.

"Another way to look at it is, we previously always said: "hey, I'm going to stop the bad guys at the gate and let the good guys in, and once they're in they can do whatever they want".

"We're now saying everyone is a bad guy that's coming in, and so we're going to limit the access that the bad guys have to everything.

"With zero trust, you're no longer saying hey one you come in through the door you can go anywhere in the building. With zero trust, you have to authenticate yourself when you come in the door, when you want to move from Room A to Room B, when you want to access a device or sign into any new system."

"So as an organization you treat every person or device that is attempting to have some kind of interaction with your network as a compromised entity.

"That's a very different mindset about cybersecurity. It's going from I will keep the attackers at bay to I assume I am already being hacked, I just don't know where it is."

Narrator: "There are three key elements to the zero-trust model. First, every person, device, location, data depository and workload has to have its own identity."

Joe: "But creating and managing identities is more complex than simply assigning an identity to each party that you interact with. You also have to manage what they can access, which is where companies like Okta come in. For instance, if you see a sales rep is somehow into the payroll system, that's probably not right. That person and that device should not have access to that particular system."

> "The Okta Identity Cloud lets you connect the right people, with the right technology at the right time, seamlessly and securely. So whether you're a security leader protecting

> the identities of your workforce and customers, a product team trying to get a new app to market faster, or an IT professional empowering your employees with the technologies that they need to do their best work, you can rely on Okta to help."

Joe: "Another leg of the stool is identity governance, which keeps a watch on each device and manages access in a way that is understandable and broadly sets up some kind of automation, which is an incredibly important thing.

"For example, you hire an in-house lawyer, and in-house lawyers have this kind of identity profile and access, so you get that all set up ahead of time. Then if you let them go, it's not like a month later they still have access to your network. It's automatically shut off. Companies like Sailpoint handle this part of the process."

> "SailPoint is all about identity security for the cloud enterprise. Drive your business forward with the unmatched visibility, automation and acceleration of access it needs for all identities, entitlements, systems, data and cloud services."

Joe: "And the third leg is privileged access management, where you see companies like CyberArk, which say certain people need access to very specific network privileges, for example to set up the cybersecurity.

> "Traditional network defenses are no longer enough. From now on, you have to assume your perimeter has already been breached. That's where having an identity security strategy becomes so important. By taking a zero-trust approach you can grant the least amount of privilege necessary, giving access the second it's needed, and taking it away the second it's not."

Joe: "So creating and managing identities for individuals, devices, files is the first major part of establishing a zero-trust framework."

Narrator: "With a number of vendors each handling different parts of the identity creation and management process, it isn't yet clear which, if any, will dominate in the space."

Joe: "Because the market for zero-trust architecture is still in the early stages and it's still in the high growth stage, it's too early to judge whether one company can organically develop and do all of this itself, or if it's going to need to be best of breed policy.

"Companies would love to have a single vendor do everything for them, but that's not been the case for cybersecurity. Cybersecurity, while we would love to have a single vendor, we always tend to see best of breed. Security professionals want the best product because otherwise they don't feel like they're getting the best defense. And it is likely to be the same, even in this industry going forward in a zero trust."

Narrator: "The second part of the zero-trust framework is endpoint security, which is nothing new – who hasn't heard of Norton Anti-Virus or McAfee."

Joe: "But next gen endpoint protection is cloud based, so it's not a batch process that runs at the end of the night, it's constantly updating, maintaining protection against ever-evolving threats. So that also drives policy understanding and best practices, detection, and response.

"You need to ensure that every endpoint, whether it be a phone, a laptop, whatever it is, is running the most recent security patches. You want to enforce dual-factor authentication so that after you set up an identity for all your endpoints you need a client that's not only doing antivirus but making sure that your endpoints are actually doing what you say they're doing.

"So when one of your endpoints is compromised, you know about it immediately, you can shut that entire identity down. CrowdStrike is a leader here, but Microsoft also has quite a bit of expertise in the space as well as some of the other new guys like SentintelOne."

> "What you might not have heard is that we can keep it safe, because at CrowdStrike, we stop breaches, so wherever you go, go with confidence. Anywhere. Welcome to anywhere. CrowdStrike. We stop breaches."

Narrator: "The last element is something called SASE – or Secure Access Service Edge – which you might think of as like a cloud-based access broker, a provider of secure gateways, kind of a firewall, but in the cloud. "

Joe: "There's not much point doing all that work to create secure identities and endpoints if you don't have a secure network.

"If I'm on my phone or laptop at Starbucks, it's not that secure because I'm on public Wi-Fi channel, so you want to route me through some kind of network that replicates your network security."

> "ZScaler has a massive opportunity to replace that network security model and in the process we offer our customers the opportunity to substantially reduce spending on expensive networking infrastructure as they embrace a mobile first and a cloud first strategy."

Joe: "So the thinking with SASE networks is it's network security very much like we've done for many years but moving it from an on-premise to the cloud. Because of that, it's a part of the zero-trust architecture where you see legacy hardware-based providers and cloud-based companies meeting in the middle.

"So on one side you have ZScaler and CloudFlare up against legacy players such as Palo Alto Networks.

"So this area of zero trust could certainly be a winner-takes-most-market, unlike what we said earlier where everyone's looking for best of breed. It could be a situation where you don't adopt ZScaler as a security broker, then CloudFlare for something else. You go with one or the other.

"So there certainly seems to be a platforming effect in the SASE area that hasn't been present before."

> "With remote work now a clear part of our future, businesses need unified, scalable and easy-to-manage security controls. That's CloudFlare. CloudFlare delivers zero trust security by uniting network security services on a single platform, built on a global network sitting within milliseconds of the world's internet-connected population."

Joe: "Because you're now running a network at the edge, you have a lot of points of presence, or POPs, which can expand what you can provide, so you can have content delivery networks, serverless workloads, which means the TAM isn't just cybersecurity. It can be much, much more and that definitely gets us excited about some of these guys out there.

"SASE networks are not only highly secure, they are also highly reliable and efficient. They let you avoid VPNs, which as anyone knows, is one of the most frustrating experiences ever, with lag, and glitches and so on and so forth. SASE networks utilize hundreds of different points of presence and co-location centers all over the world, which significantly mitigates this."

Narrator: "Growth in the zero-trust space has been strong as the coronavirus pandemic brought forward a lot of demand from organizations that had to hurriedly change their operational procedures to cope with the sudden onset of remote working."

Joe: "Yeah, IT departments were all-hands-on-deck trying to get their systems set up so they could have fully remote workforces.

"So while growth has been accelerating, it could potentially take a breather as we digest some of this pull forward that the COVID brought.

"But organizations have to now be ready for another emergency and the ability to be fully remote again one day if they need to be.

"They have to go back to the drawing board and say how do I set up my organization to be fully remote, even if we do plan on coming back to the office in some way or form? There's no limiting factor to companies setting up for fully remote and having a hybrid situation afterwards.

"So we're going to see growth. The government is getting behind it, Microsoft, Google, all these other companies, they all have committed to investing heavily behind cybersecurity and zero trust and they're going to do so over many years, so we're definitely not in the final innings by any stretch.

"Each segment is growing at different rates.

"Identity growth rates are in the 20s, 30s while the endpoint overall TAM isn't necessarily growing a lot, there are huge markets share shifts occurring, so you're seeing companies like CrowdStrike growing, like, 40% a year.

"Because of that, you have to be selective in where you are going to invest and know which companies are likely to be the long-term beneficiaries from shifting trends.

"Then in the SASE sector, you have companies like ZScaler and CloudFlare that are growing anywhere from 20-50%.

"Legacy cybersecurity companies like Palo Alto are going to see growth as well, maybe in the high single digits, because areas like hardware firewalls are going to grow much [more] slowly than their SASE network offerings or next generation cloud-based services.

"It's logical to imagine that network firewall guys like Cisco, Palo Alto, Check Point, and so on will benefit because they're rolling out zero trust models and they have very large customer bases already."

> "Turned to Palo Alto Networks to help. 'We usually don't have many employees working remotely but suddenly we had to secure 20,000 of them. Palo Alto Networks helped us to make it happen in days.' Flex was able to use Prisma Access, our cloud-based, software-deployed cyber security to protect their remote workforce quickly."

Joe: "But these legacy operators transitioning from hardware to software-based solutions can't just go to their sales force and say we're completely moving to zero trust and this huge revenue stream that we've had for so long, we're shutting it down, we're not going to sell it anymore.

"So they face a dilemma, kinda like the brick-and-mortar retailers embracing e-commerce, around how quickly they shift to zero trust, because doing both concurrently could be disingenuous as they're saying 'we're going to set you up with a zero-trust model that we believe is so great but then we're also going to sell you this high-end firewall'.

"A lot of firms in the space would say firewalls still represent an important piece of the pie and there's no reason not to have them, but it's also a bit like putting a third dead bolt on your front door. If the first two didn't work, then what's the third gonna do? It might slow it down, but it's not going to stop anything."

Narrator: "Because investor optimism about the outlook for the sector has driven up valuations, zero-trust cybersecurity providers are under pressure to deliver the growth required to justify those elevated multiples."

Joe: "It's still early days in zero trust, and so one could really say that the cement is still wet here, and so there's a really wide range of outcomes.

"At NZS, what we do is we actually kind of model two portfolios in one, one of those being the resident head of the portfolio. This represents something like, you know, 60% of our holdings but only 15 to 20 names, if you will, and those

names are focused on stocks that have a narrower range of outcomes, and still represent growth but may not have that asymmetry that you have in other stocks.

"One the other side we have our optionality tail. This is something like, you know, 40% of the portfolio but it represents upwards of 40 different stocks. And here what you have is stocks that have a wide range of outcomes but have significant upside because their TAM is growing, and clearly where a lot of these cybersecurity zero trust names that we've talked about today really fall into that optionality bucket.

"As this evolves, for example as TAM expands, as more companies exert dominance and, more importantly, if we begin to see the platforming effects in things like SASE, that's when we can actually take these positions up, because the range of outcomes begins to narrow.

"And that's what we kind of look at when we want to take something from optionality to resilience. So today these are optional stocks, high asymmetry, but there's a lot of moving pieces and a lot competition that is all looking for the same place but they represent huge, huge upside if things go the way that we anticipate them to go.

Narrator: "That just about does it for this episode so I'd like to wrap up by thanking Joe for sharing his time and insights into this critical corner of the tech universe. If you want to know more, you can find contact details for the NZS team at nzscapital.com.

"I'm Dex McLuskey, thanks for listening and I look forward to you joining us again next time."