

Peter Mantas of Logos LP presented his in-depth thesis on Zscaler (US: ZS) at Wide-Moat Investing Summit 2019.

*Thesis summary:*

Zscaler is a SaaS cybersecurity company that protects inbound and outbound gateways for enterprises that have users accessing the corporate cloud networks for applications. The bulk of revenue is divided into two platforms: Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), with the majority of revenue generated by ZIA. The company has a unique secular growth story as enterprises transform their cloud-based architecture for mission critical workflows, meaning more enterprises will start transitioning critical tasks to the cloud over private networks. This transformation will take decades, and the company is partnering with hyperscale cloud vendors such as Microsoft and Amazon. The business has strong economics: recurring revenue, high FCF-to-sales ratio, and strong revenue growth (+61% last quarter), with strong gross margins (80+%). The company has had a strong run in 2019 but Peter believes that high returns on capital, the defensive nature of the service, and low capital requirements are likely to push the stock higher in the ongoing market cycle.

*The following transcript has been edited for space and clarity.*

Zscaler is one of the newer cloud-based cybersecurity vendors. The company protects inbound and outbound gateways for enterprises. The easiest way to think about it is to imagine Zscaler as the offramp when you're about to access cloud applications for large enterprises. The bulk of the revenue is derived from two main sources: Zscaler Internet Access (ZIA), which effectively protects users when accessing applications in the cloud, and Zscaler Private Access (ZPA). The revenue split is around 80/20 or 85/15 ZIA to ZPA.

ZIA protects users connecting to applications and protects the overall network. It monitors and secures users accessing those applications, both inbound and outbound, making sure that nothing gets through or leaves the organization. There's malware and endpoint protection as well. It effectively sits between the user and the internet.

ZPA, on the other hand, is a whole new way for organizations to access corporate networks remotely. It is meant to effectively replace VPN. In traditional VPN, you would have data centers and corporate networks with legacy appliances. Users would have to log in to these appliances to get access to the entire corporate network. ZPA is a software solution in the cloud which taps into a database and does application segmentation, meaning people can only access the applications remotely.

What are some of the product advantages of Zscaler? It's a full cloud deployment unlike legacy competitors that utilize virtual and physical appliances. It has full scalability, meaning you can add users easily and instantly. The company has over 100 data centers around the world, so there's complete redundancy and latency. It's a purpose-built cloud protecting the organization with full security stack, so it has URL filtering, DNS security policies, and data loss protection. There's the ease of deployment, and significant cost savings. A lot of organizations, especially Fortune 500 companies, spend a significant

portion of their budget on updating their infrastructure and corporate networks. A lot of the legacy competitors account for a large chunk of those costs. Zscaler transforms the way an organization would think about how much it should invest into its data centers or private networks because this security is highly sophisticated, but at the same time, it offers much greater cost savings to the organization - the capex comes down, and it's more secure.

One other advantage of Zscaler as a company is its sharp focus on what I like to call access security for the enterprise cloud. Other security vendors may provide a broad range of services and solutions, but Zscaler is focused on access security for cloud applications that will transform the organization in the long run.

What's the current landscape? Cloud computing is not new. It's been around for 20 years. At the beginning, when it started to take off, organizations were quite reluctant to move many applications to cloud. Over time, a significant number of organizations with sensitive operations started to move more and more mission-critical workflows to the cloud. The most recent example is the US National Security Agency (NSA), which moved some mission-critical workflows to AWS. Many large organizations set to deploy Platform-as-a-Service, Infrastructure-as-a-Service, and IoT or sophisticated mobile solutions are starting to shift those deployments to the cloud so that their teams of engineers, consultants, and professional service employees can access those applications to ensure that the company is achieving the digital transformation it aims for.

The first cloud phase involved the adoption of platforms such as Azure, Oracle, and AWS. These are not new things. The second wave is the exponential growth of these applications in the cloud and the transformation of mission-critical workflows from legacy data centers or corporate networks to the cloud. As growth continues over time and the cloud applications and technologies accessing the cloud become more sophisticated, more security will be needed. Internal applications will continue to play a major role in enterprise capabilities, and there will be significant investment in the next 10 to 15 years.

What are the risks and competition around Zscaler? The biggest risks the company faces are from legacy competitors, the three main ones being Cisco, Checkpoint, and Palo Alto. Many of these legacy vendors had a similar birth to Zscaler's, rising amid the tremendous growth in the late 1990s or early 2000s. These are large organizations with highly visible cash flow and revenue, which creates visible resources. Many organizations with legacy data centers or networks that require endpoint security or spend tens or hundreds of millions on appliances each year see on their invoice Cisco or Checkpoint or Palo Alto. When you have such a trust with your provider, it becomes difficult to trust the new kid on the block. Luckily for Zscaler, it's one of the best cloud security vendors on the market right now. It has a patent on virtually all of its products. It's very scientific and technical in its solutions, unlike many other new cybersecurity vendors. It takes pride in its engineering prowess and is known for its best-in-class engineering when it comes to accessing the internet or inbound gateways for the cloud.

A lot of these legacy organizations want to have a piece of the new business. Although their transitioning to Zscaler's model is inevitable, there's still some time before it happens. The other elephant in the room is the large cloud vendors. It's not too much of a stretch for

Microsoft, which is a hyperscale cloud vendor, to enter into this security market, especially the multi-tenant security. This is a giant tech company with almost unlimited resources, so it would be an issue if it sets its sights on this market.

The investment thesis is quite straightforward from our perspective. There's a significant secular growth story here. Cloud computing isn't new, but the transformation of the enterprise with cloud-based architecture for mission-critical workflows will grow exponentially. Despite their resources, legacy competitors face significant opportunity costs to transition to Zscaler's model, and it will take years and a significant amount of focus, whereas Zscaler has a strong head start. The legacy operators also lack the expertise and the patents Zscaler has. The other thing is ZPA, which can completely displace VPN networks over time. If enterprises are shifting to cloud-based architectures, this may create an opportunity for ZPA to effectively control the network. The company has security partnerships with Microsoft, which recognized Zscaler's prowess early, and AWS, so this does reduce vendor risks.

Finally, the business has fully recurring revenue, highly complex, sticky infrastructure software, very high free cash flow/sales, and rapid growth. We expect strong revenue and gross margin growth as the company continues to expand and reduce the amount of CapEx required. Last quarter, it reported a 61% increase in revenue and gross margin at 82%. It is a potential acquisition target because of its focus in the market and strong execution. Being a software company, it will naturally have a defensive nature given its advanced and sticky infrastructure software. Therefore, there will be high returns on capital. It's in the cloud, so there's less cost versus other security vendors. We also have the network effects, which make unit economics highly favorable.

No matter what the investment thesis or the story may be, there's always going to be the price paid. When I wrote this presentation, it was a little over 33x sales and is probably closer to 35x now. We believe Zscaler is on the high end and slightly overvalued given the return on capital profile and the growth, and the secular story we believe is for a decade and over. However, given the current market cycle and execution, we don't see true signs of excess just yet. We view it as slightly overvalued or a bit on the expensive side. Free cash flow grew from \$2 million to over \$31 million in one year, and we expect \$55 million by the end of the year. Book value per share is also growing tremendously. It was at \$2 at the beginning of 2018 and \$2.23 by the end of 2018. We expect close to \$4 by the end of the 2019. With 84% gross margin and 32x to 34x price-to-book range, which may be higher or lower depending on what interest rates do and what the demand for sticky secular growth names is, we expect it to touch close to \$120 a share.

*The following are excerpts of the Q&A session with Peter Mantas:*

**Q:** It sounds like the company has plenty of reinvestment opportunities. Could you expand a bit on capital allocation? Do you expect it to retain all the capital for the foreseeable future, and where do you think it gets deployed?

**A:** In the short term, there's a level of education in the market about the solutions, particularly around ZPA. I don't think organizations will displace VPN through the ZPA solution any time soon. Although there's a significant runway for ZIA, it does have slightly longer sales cycles because you have organizations which have invested hundreds of millions, maybe billions, in the IT infrastructures they've had since the 1980s or 1990s. I think the allocation will be towards revenue growth, so investing in the business, hiring more account managers, and increasing the SG&A line of the income statement to get out there in the market and continue to talk to CTOs and CIOs in order to show the benefits of what Zscaler does.

The market is starting to realize the business opportunity and the real use cases it's solving from clients like Concho Resources to Anheuser-Busch. Over the next little while, the allocation will be towards growth to attain more market share of the Fortune 2000. I think the second aspect will be around expanding the ZPA platform to effectively use it as a complement or a replacement of some sort for corporate VPNs. Maybe in 10 years or longer, the price-to-sales will come down to what Checkpoint might be, like 8x, 9x, 10x, or 11x sales, depending on what interest rates do. There may be more focus on acquisitions and potentially return of capital. In the short term, I think it's about executing the ZIA and educating the market about the benefits of the ZPA.

**Q:** Could you elaborate on the management team and their incentives?

**A:** Like any technology company, there's a lot of stock options outstanding for the talent the company has. The CEO, who was a co-founder, is a very well-educated guy. We think the stewardship for management is there. It's standard. The compensation is in line with other tech vendors. We do find management slightly humbler compared to other software companies we've studied in the past. We believe they are aligned with shareholders and know exactly where they are in the market. Obviously, we pay attention to the dilution of stock options and how they impact equity being issued, but we don't see any concern regarding management and their plans for the company.

**Q:** What would be some key data points to track over time to either validate or challenge your thesis?

**A:** Some of the data points will be revenue growth and gross margin. If gross margin starts to come down a bit, and if revenue growth isn't consistent with our expectations, there may be a twofold issue. Although the company has gained some traction in the market regarding its ZIA platform, it may take longer than we thought. If gross margin comes down, we'll be a little concerned about whether there is increased competition somewhere or an erosion of the growing moat given increased costs without the requisite revenue growth. If we start to see declines in those areas, we will question what may be going on. If those remain steady, then the story is about execution and the continued development of the ZIA and ZPA platforms.

*About the instructor:*

Peter Mantas serves as a general partner of Toronto-based investment firm Logos LP. Peter has an assortment of business and financial experience at global institutions. Peter's prior experience includes senior managerial roles at large information service and enterprise technology companies in addition to legal experience within the capital markets, alternative investments and tax groups at McCarthy Tetrault LLP. Peter has also been involved in a variety of private equity transactions, ranging from retail to renewable energy, in addition to leading a proprietary trading team for a boutique desk. Prior to this, he held various economic research positions at the Export Development Bank of Canada, Statistics Canada and other various federal government departments. Peter has both an LL.B. and B.C.L. from McGill University's Faculty of Law. Prior to studying law he obtained an Honours Baccalaureate in Commerce, Magna Cum Laude, from the University of Ottawa, Telfer School of Management, where he received several awards of excellence.