USF | Muma Case Review
A publication of the Muma College of Business | University of South Florida

Volume 8 Number 4 20 DECEMBER 2023

GARRETT BRIDENBAUGH, DANIEL BELLINGER, SOUJANYA NOMULA, AJAY SIKHA, ERIC PANDORF, JAY STRATTON

CASK SYSTEMS SEGMENTATION TO GROW PROFITS[1]

Cask implements market segmentation strategies to discover potential profits.

“Any questions?” Melvin Johnson, Public Sector Sales Director for Cask Systems, scanned the room full of his regional sales managers. Met with silence, he pointedly made eye contact with each of them. He could see the concern and questions on their faces. These were competent professionals. They knew stagnation in the small to midsize market was a real threat. They could also see the data that showed the growth potential of untapped small market accounts. The looks on his regional managers' faces told him they had reached the same conclusions. Do we break the small accounts out into their own separate sales team? Do we follow the segmentation blueprint utilized by the Commercial Sales team that was tried previously? Do we leverage sales technology and risk losing our connection with these smaller customers? One thing was certain; he needed to get this decision right.

As his managers shuffled out of the room, he saw Dan, his most senior and trusted manager, still scribbling in his notes. Over the past 15 years, Dan has done it all at Cask, an IT hardware, software, and services provider specializing in networking, security, collaboration, and data center solutions. He glanced up, making eye contact, a clear sign he had concerns he wished to discuss. Dan immediately asked when they were alone, “What are we going to do when these small accounts become mid-size? If we use sales AI technology for these smaller customers, we risk losing them to more hands-on sales opposition. What about the loss of commission for the midsize sales team when these smaller accounts are carved out?” Melvin had been asking himself these same questions. He assured Dan that he was aware of these issues and encouraged him to engage with his team for feedback as he continued to formulate his plan.

As Dan left, Melvin knew he had more unknowns to work with than knowns at this point. One thing he did know was that the data backed up the necessity for segmentation. He just needed to show his team quickly that there is a lot of untapped potential in the small and midsize accounts. He needed to make the decision on how this market segmentation would look to demonstrate that it would result in sales growth for everyone. He needed to do it fast or risk his team’s morale plummeting over lost revenue and internal squabbling over lucrative smaller accounts.

[1] Copyright © 2023, *Garrett Bridenbaugh, Daniel Bellinger, Soujanya Nomula, Ajay Sikha, Eric Pandorf, Jay Stratton.* This case was prepared for the purpose of class discussion and not to illustrate the effective or ineffective handling of an administrative situation. Names and some information have been disguised. This case is published under a Creative Commons BY-NC license. Permission is granted to copy and distribute this case for non-commercial purposes, in both printed and electronic formats.

Editor: Grandon Gill

Enterprise Networking Industry

Enterprise network denotes the IT infrastructure that midsize and large organizations use to provide connectivity among users, devices, and applications. The goal is to support the organization's objectives by consistently delivering connected digital services reliably and securely to workers, partners, customers, and the IoT (the internet of things).

Advantages of enterprise networking

1. Always-on connectivity: A well-designed enterprise network provides the proper connectivity for all users, things, devices, and applications in an organization, as appropriate for the role, purpose, and location.
2. Optimized user experience: An enterprise network can help improve the user experience through proactive network optimization, faster issue resolution, proper prioritization of essential traffic, and helping to ensure security and privacy.
3. Readiness for digital transformation: An enterprise network can be designed to support digital initiatives needed to quickly adapt to rapidly evolving needs, including expansion, scaling, growth, and introduction of new services.
4. Easier Network Management: Network management tools such as network controllers give administrators the ability to set access rules and permissions for users and departments, add new users or functions easily, monitor performance, and take corrective action, all from a central interface.
5. Enhanced Security: In addition to security applications and devices, such as firewalls and secure Internet gateways, an enterprise network becomes a primary detector of threats and an enforcer of security and compliance. It does so with device identification, profiling, verification, network monitoring, authentication, access controls, segmentation, and device and account management.
6. Seamless cloud Integration: As more and more data and applications are developed, deployed, and delivered across multiple public clouds, enterprise networks provide seamless connectivity between users and cloud applications. They also optimize workloads between on-premises locations and public clouds.

The enterprise network equipment market was valued at USD 9.83 billion in 2020 and was expected to reach USD 15.48 billion by 2026, at a Combined Annual Growth Rate (CAGR) of 7.85% forecast period 2021 to 2026. An enterprise network was an enterprise's communication backbone that helps connect computers and related devices across departments and workgroup networks, facilitating insight and data accessibility. It reduces communication protocols, promotes system and device interoperability, and improves internal and external enterprise data management. The increased need for enterprises to become digital to remain competitive was expected to increase the impetus for agile networking and the value and importance of virtual and software-defined networking. Companies are focused on upgrading their networks to increase wireless capacity. Moreover, they were spending money to modernize their system, which was expected to fuel enterprise network demand over the forecast period.

The industry anticipated to witness growth owing to ongoing technological innovations in wireless LAN technology and high-speed Ethernet switches. This technology led to developing smaller and more efficient chipsets and modules with added functions. Escalating needs for implementing high-speed Ethernet switches was expected to provide new growth avenues over the next eight years.

The increased shift towards wireless adoption, expanding the mobile workforce, increased bandwidth requirements, and growing base of mobile internet devices are the key factors that were expected to drive demand. Growing adoption of virtualization technology and high demand for internet-enabled devices was expected to contribute efficiently to industry growth.

Please refer to Exhibit 1 for details on the enterprise networking market, 2012-2024.

Enterprise Network Security

Network security is a broad term that covers a multitude of technologies, devices, and processes. In simplest terms, it is a set of rules and configurations designed to protect the integrity, confidentiality, and accessibility of computer networks and data using software and hardware technologies. Every organization, regardless of size, industry, or infrastructure, requires a degree of network security solutions to protect it from the ever-growing landscape of cyber threats of the time. Cybercriminals saw the pandemic as an excuse to increase their immoral behavior by leveraging the weakness of remote workers and tried to capitalize on public interest in coronavirus. These factors encouraged organizations to further increase their security spending and improve their network security infrastructure to adapt to remote working environments. This promised a stable growth opportunity for the global network security market.

Over the previous 3 years the global network security market share has been dominated by network security. It was expected to maintain its dominance in the upcoming years. Network security solution types primarily focus on various system parts, from network security device management network packet analysis, and embedded security, thereby creating a highly profitable scenario for market growth. The increased number of cyber-attacks on enterprises caused considerable losses in both social and economic scenarios. The increased attacks continued to cause organizations to increase their spending on security conditions, creating a lucrative growth foundation for the overall market. Furthermore, the heavy reliance on cloud and online systems, owing to work from home policy, which increased the risk of cyber threats. Please refer to Exhibit 2 for the market share based on cloud and on-premises components.

The **global network security** market was projected to grow from USD 22.60 billion in 2022 to USD 53.11 billion by 2029, at a CAGR of 13.0% during the forecast period.

Key Market Players:

- Cask Systems
- Solarwinds - was an American company that developed software for businesses to help manage their networks, systems, and information technology infrastructure.
- IBM - The International Business Machines Corporation, nicknamed Big Blue, was an American multinational technology corporation headquartered in Armonk, New York and present in over 175 countries.
- Trend Micro - was a Japanese multinational cyber security software company with global headquarters in Tokyo, Japan and Irving, Texas, United States, and global R&D headquarters in Taipei, Taiwan.
- FireMon - provided security manager, policy planner and optimizer, lumeta, global policy controller, and risk analyzer. FireMon served customers worldwide.
- Symantec - was a client-server solution that protects laptops, desktops, and servers in your network against malware, risks, and vulnerabilities.
- FireEye - was an intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offered a single platform that blends innovative security technologies, nation-state grade threat intelligence, and Mandiant consulting.
- GFI Software - was a leading network security scanner and patch management solution that acted as a virtual security consultant. It gave a complete picture of the network setup, provided risk analysis, and helps maintain a secure and compliant network with minimal effort.

- Avast Software - was a Czech multinational cybersecurity software company headquartered in Prague, Czech Republic that researched and developed computer security software, machine learning and artificial intelligence.
- Juniper Networks - was an American multinational corporation headquartered in Sunnyvale, California. The company developed and marketed networking products, including routers, switches, network management software, network security products, and software-defined networking technology.

Please refer to Exhibit 3 for a breakdown of the top market players in Networking and Security Industry.

Cask Systems, Inc.

Cask Systems, Inc., commonly known as Cask, was a multinational company headquartered in San Jose, California. Cask developed, manufactured, and sold networking, hardware, software, telecommunications, and other hi-tech services and products. It was one of the world's largest technology companies, ranking 63 on the fortune 100 with over $51 billion in revenue and nearly 80,000 employees.

Cask Systems was founded in 1987 by John Smith In 1995, when the company went public, Cask had a market capitalization of $224 million, on and as of August 2022, it was around $236.2billion.

Brand

Cask was one of the most trusted names in networking technology. As it continued to expand its portfolio of products, it focused on providing its users with tools that allowed them to grow its network infrastructure, connect with cloud applications and services, and ensure that security was at the forefront of what they do. By partnering with a professional team that understood how to design, implement, and support network infrastructure solutions and relying on top-of-class tools to build that network, businesses could worry less about downtime, crashes, and bottlenecks and focus more on their business.

Operations

Cask offered simple, flexible, and secure networks for small and medium businesses that fit business owners' needs, were simple to set up and maintain, and were cost-effective for small businesses.

Switches – Cask switches were key building blocks of networks. They connected multiple devices, such as computers, wireless access points, printers, and servers, on the same network within a building or campus. A switch enabled connected devices to share information and talk to each other.

Routers – A router receives and sends data to computer networks. Routers were sometimes confused with network hubs, modems, or network switches. However, routers could combine these components' functions and connect with these devices to improve internet access or help create business networks.

Wireless – The Cask Wireless Network Solution supported client data services, client monitoring and control, and all rogue access point detection, monitoring, and containment functions. It used lightweight access points, controllers, and the optional ECS to provide wireless services to service providers.

Voice – Cask provided call-processing solutions for organizations of all sizes and types to manage voice, video, mobility, and presence services between IP phones and endpoints, voice-over-IP (VoIP) gateways, mobile devices, and multimedia applications.

Network Manager – The very purpose of business use of Cask management was to identify and troubleshoot faults in a network environment before the faults turned into potential business losses.

Customer Transformation

Small and Mid-size businesses were investing in digital transformation for the future, this represented a significant market opportunity. According to TechAisle, "Worldwide small and medium business IT spend is forecast to reach US $700B in 2020, growing at 6% over 2019". Cask had three great new reasons to expand business with small and mid-size customers.

Reason #1: Financing. Cask offered financial support for business partners with a predictable payment schedule, no up-front costs, and low, competitive rates. They also rewarded clients with cash rebates for overall growth, expanded across architectures, and provided further options to choose from specific SaaS and product solutions in targeted campaigns.

Reason #2: Cask made operating software easy. The hardware and the power network infrastructure all required operating system software so it could do its job. Cask's ONE software for data center wide area network (WAN) and access domains with the freedom to deploy this software on both physical and virtual machines. And because these licenses were portable and not tied to any specific hardware, they made it much easier for the company to grow, whether they needed to expand access, WAN, or data center capabilities.

Reason #3: Each component on the network provided attackers with a point of entry into the systems. Cask helped detect anomalies in network traffic by embedding intelligent sensors and enforcers into the switches, routers, and wireless solutions that made up network infrastructure to give enhanced visibility and a better opportunity to spot incorrect things.

Digital Transformation

According to a Gartner report, 55% of employees say their ability to work flexibly will impact their decision to stay at their jobs. 96% of businesses wanted to improve their work environment with intelligent workplace technology, and 50% of small and medium businesses would need to re-organize to deploy remote and virtual distributed structures through technology. This showcases the people and technologies propelling small and medium businesses. Cask celebrated the ingenuity and perseverance of entrepreneurs and innovators—and the partners who help their success, explore their unique journeys, and offer insights to help them thrive.

There are several technologies that would be critical to enabling a flexible workforce. Companies would have to prioritize integrated technology in security, communication and collaboration, smart offices, people analytics, customer engagement, document management, employee learning applications, digital training, and leverage the power of the AI renaissance. Cask would be uniquely positioned to support the transition to a hybrid workforce.

Cask Technologies

Cask's Four Architectures

Cask's bread and butter was in Information Technology (IT). They provided a wide variety of IT services to large-scale and small-scale businesses, municipalities, government agencies and services, and within the public and private sector. Most of the modern world ran on the internet and was heavily involved in IT services. From the Internet of Things (IoT) to cloud computing, technology, and the services that Cask provided were crucial for the success of modern business. Cask's primary services were in four architectures of IT: Enterprise Networking, Security, Collaboration, data center, and cloud computing. these four architectures are discussed.

Enterprise Networking

The first architecture was enterprise networking. Networking was the hardware and software that was physically and remotely connected to ensure all the systems can communicate and function within the network. A network comprised of products like switches, routers, wireless access points, Wide Area Networks (WAN), and Local Area Networking (LAN). A WAN was a large network of information that spanned a vast geographical area. It was not tied to a single physical location and can share information globally. Access to the WAN could be granted through a wide variety of means such as internet connections, wireless access, virtual private networks (VPNs), and hardlines. Many international organizations, large corporations, schools, and large and small municipalities used WANs to relay data and information back and forth to one another. If they were set up and communicating within the WAN, they would be able to have access to the information no matter the distance between them.

Local Area Networks (LANs) were essentially the same as a WAN, just on a smaller scale. A LAN provided data communication within a limited geographical area. Think of the systems set up within a house as a LAN and a connection to a cloud or the internet as a WAN. All the devices within a home are called the Internet of Things (IoT). Many objects those days could connect to the internet and make up a LAN. This can be everything from a smartphone, laptop, refrigerator, or any device that ran an IP address and connected to the network. This system of networks was Cask's first architecture that could be set up to provide communication and data sharing capabilities to its clients.

Security

The second architecture was security. Being able to secure a network was vital in the world at the time. Suppose Cask was responsible for setting up a public or private sector LAN or WAN that could contain sensitive information. In that case, the ability to secure that data was paramount. There are many ways to provide security for systems. With billions and billions of IoTs within networks, how can Cask monitor who should or should not be allowed within a network, and are the devices secure? Cask used a "Zero Trust" philosophy. This philosophy began with every device trying to gain access to a network at zero trust. Trust in the network was established, not given. Trust was ensured over time by establishing trust, enforcing trust-based access, and maintaining trust. Cask's trust-based approach was dynamic and comprehensive.

One of the biggest challenges in maintaining cybersecurity was the end user. Most of the time, unwanted access to a network was gained by endpoint behavior. Someone may receive and open a phishing email with ransomware or in some way provide access for a virus or a Remote Access Trojan (RAT) to gain access to the network. Cask was dedicated to protecting the network at all costs. Cask provided a secure software defined (SD) limited access. Cask SD access established and automatically enforced endpoint access through the zero-trust philosophy. If an endpoint began to act suspiciously, Cask SD access could contain and correct the behavior before a breach occurred within the network.

Another way Cask provided an element of cybersecurity was through Secure Access Service Edge or SASE. A significant issue in the post-COVID era was that businesses and individuals move remotely. More and more information was being stored in the cloud instead of in complex data centers. As more and more services became available for remote access and out of the data center and into the cloud. Most apps would work in the cloud. SASE was a framework that combines WAN and zero trust solutions into a cloud platform that could connect endpoints, user systems, apps, and remote networks. It contained four parts: Identity driven security, Cloud delivered, physical, logical, and digital support and protection, and globally distributed. SASE was not one size fits all. SASE could be scaled up or down to fit the needs of the organization that Cask was providing services.

Collaboration

The third architecture was collaboration. As with security, remote collaboration was being used more and more. The post-pandemic pandemic changed much of how the world worked. Businesses moved remotely, and people communicated at greater distances than ever before. Cask was one of the leading providers of remote connections. The future of work was moving towards a hybrid approach. Some of the time was spent in the office and some remotely. Cask provided conferencing, messaging, live polling, and live translation meetings to ensure everyone was involved. Cask used a platform called WebView to provide a platform for remote work to occur and keep up with the ever-changing world. The ability to connect others through video, live polling, and messaging ensured that everyone's voice was heard and enabled access to a hybrid learning and working environment.

Data Services and Cloud Computing

Lastly, they provided data center and hybrid cloud services. As Cask was looking to expand into more areas and municipalities, they realized that not all businesses are the same, nor did they need the same data and cloud services. A public-school service and a small city or town may need similar but different services. Cask realized this and developed a way to provide hybrid services that fit the client's needs. They could provide the ability to connect to a public or private cloud and to stay in control of cloud services. This capability could automate typically repetitive tasks, provide the instruments to connect and optimize the teams and infrastructure and adapt to the future. Applying all four of these architectures in concert with each other, Cask could provide comprehensive products and solutions that could expand across the needs of any size client to achieve optimal IT services.

Market Segmentation Transition

Cask Systems sold technology solutions to several business industries, categorized internally as Large Enterprise, Commercial, and Public Sector. Public Sector was comprised of Federal agencies (Fed) and State/Local government and Education (SLED). Commercial and Public Sector were further broken down by revenue (Commercial) or headcount (Public Sector).

Commercial customers were generally firms with annual revenue below $10M. Those firms could range in size from 100 employees to several thousand. As the firms were in the private sector, many start with small annual revenue and grow quickly. Every day, new businesses were created that required technology that connected them to the Internet, allowed them to collaborate, and kept their data available and secure. This business industry was always growing.

Conversely, Public Sector was more static than the Commercial business. No new states were being created, and a new city was rarely created. Several new schools opened every year, but they usually resulted from a reduction in students elsewhere. Also, even if a new school opened, no new school districts were founded.

Cask's SLED team faced an implementation challenge in deciding the go-to-market plan for their smallest customer base. Small accounts were typically local municipalities with populations below 100,000, school districts with enrollments below 100,000, or small colleges and trade schools. These were managed by a specific group of Virtual Sales Executive (VSEs) for years with quantifiable success. VSEs took pride in identifying prospective customers who did not purchase Cask solutions, introducing their prospects to what Cask had to offer, and ultimately gaining new customers. Occasionally there were financial incentives for sourcing new accounts, which served as additional motivation for sales reps. The small customers who were already Cask customers felt comfortable knowing their sales rep and building rapport over the years.

Another benefit of keeping the small and midsized sales accounts together was maintaining continuity. Melvin attempted to avoid customer disruption whenever possible and making this change would have introduced a new team of sales reps into the account base. This new sales team consisted of early sellers from two programs, Cask's TechAccelerate program and the Cask Sales Training Program (CSTP), already funded without impacting Melvin's funding allocations. TechAccelerate was a program that aligned top Black/African American talent in tech with industry-leading companies. These new employees had little to no experience selling Cask solutions (*Closing Job and Opportunity Gap for Black Talent*). CSTP was an internal Cask program focused on exceptional talent graduating from university (. These sellers had more Cask sales experience than TechAccelerate; the program was a yearlong "graduate" course in Cask that prepared sellers for their first sales job in the company. It focused on teaching the four architectures Cask sold from a technical perspective, then reinforced the sales skills required to be successful. The CSTP program had also been a feeder program for the VSE role at Cask. While TechAccelerate and CSTP could be effective strategies for building another sales team, there were questions about their efficacy.

One downside of the Small & Midsize combined account strategy was the large number of accounts assigned to one sales rep. This made it difficult to establish more than surface-level relationships with most of the customer base. According to Melvin, a productivity per full time full-time (FTE) score showed how productive a VSE could be in each territory. Ideally, he wanted his VSEs below a $7M sales quota mark to give the best chance of success. Looking at small and midsized accounts combined, there were sales reps with $11M+ sales quotas. Johnson also wanted to reduce the number of sales accounts per VSE. There were VSEs with over 800 sales accounts where he thought the max should be around 200. With such a large sales quota, most sales reps gravitated toward larger municipalities and schools that provided a higher chance of large sales opportunities. And with several hundred sales accounts the VSE was responsible for, it was impossible to connect with everyone. In turn, this left an entire subset of potential customers without someone to provide them assistance.

By extension, additional problems surfaced when considering the bandwidth and time constraints of technical resources and subject matter experts. Since the Cask portfolio was so vast, it would be impossible for a VSE to have deep knowledge of all the nuances of the solutions they sold. Cask employed sales engineers and specialists with the requisite knowledge for their respective Cask architectures. These specialists covered several states and had responsibility for thousands of sales accounts. They were stretched thin and did not have time to do anything more than hop from one sales call to another to support all their VSEs.

Melvin Johnson was familiar with other parts of the business that had similar challenges. He reached out to his counterpart who led Cask's commercial business for insight into their strategy. He learned that Cask's commercial business went through a 2-year pilot program, separating small and midsized accounts. The small accounts were still supported by a VSE – the same way they always had been, while the midsized accounts took a different approach based on Cask architectures. This model was called the Virtual Technology Sales (VTS) model. Initially, the pilot program was well received, and the Global Executive VP of Sales backed it. Instead of midsized accounts having a sales rep supported by specialists, the specialists were all responsible for connecting directly with the customer base and getting new business. There were specialists specific to collaboration sales, one for enterprise networking, one for data center, and another for security.

Early days were faced with lots of headwinds, Johnson was told. One of the most challenging adjustments was explaining how the specialists worked with customers. Customers didn't understand who they turned to for pricing or to learn more about Cask. For example, a large enterprise networking customer ask would likely only talk to the enterprise networking specialist. In that customer's mind, the specialist was his only sales contact. Conversations became awkward when that specialist had to introduce his customer to a different sales rep to sell a different Cask architecture. Another problem that was uncovered was around internal competition. Since SLED customers typically worked with very tight budgets, the specialists often competed for the same dollars without knowing it. There was little communication across architectures since each specialist focused on their part of the business. Conflict often wasn't recognized until the customer notified the specialists of each other's existence in the same sales account.

Ultimately, these concerns subsided; the customers grew accustomed to having more resources at their disposal and saw the move as a net positive. Some of the internal conflicts between sales specialists were mitigated through a change in the compensation plan. Specialists would have two sales goals: one for their own Cask architecture sales and another shared goal based on the team's overall success. The pilot started to work well, and the VTS model started to outperform Cask's standard model. So, what happened? Melvin was curious about why the pilot did not make it out of its test stage. Several factors led to the end of the pilot. First, the EVP who blessed the project, and other leaders with a vested interest in the program's success left Cask. New leadership did not see the model scaling to the number of sales reps needed to make the project successful. The VTS pilot was eight sales specialists for only 350 customers, whereas Johnson's midsized accounts totaled around 3,500 nationally. This would be an expensive undertaking, nearly doubling the number of sales reps he planned to have in midsize sales, not including the sales reps required to cover small accounts.

Implementation Strategies

Melvin knew that capitalizing on the growth of small and mid-sized businesses was a strategic initiative to capture new revenues and market share. Cask was convinced it could be the best solution for these customers in network infrastructure, cloud application connections, and network security. In addition, the digital transformation of the office space was ripe for Cask to be the trusted name for more small and medium-sized commercial customers.

But the decision remained for Johnson, not if they need to go after these customers, but how to successfully implement the initiative with the sales plan. Melvin has been around long enough that anything short of a win-win situation would not fly with tenured sales employees. Poor implementation would easily slow new candidates' interest in joining a well-operated Cask Systems.

As Melvin pondered his options, he wanted to ensure that he was clear on the choices at hand.

Option 1 – Implement the blueprint used by the commercial sales team previously. Segment the accounts into two sales teams based on size and region. Small accounts would be managed by a new group of sales reps, and midsize accounts would continue to be supported by the existing VSEs. By segmenting the accounts, you can save money on labor costs by not having to increase the amount of personnel in the sales teams. Cask can increase their use of their internal predictive analysis for the current sales teams to provide more accurate and targeted sales of the small accounts.

Option 2 – Utilize data analytics and leverage internal technologies and external products to better service small-size accounts. The current sales team could be used, removing the need for an entire additional team. They could leverage historical data to identify customers who will continue to increase sales. Cask could operate more efficiently and maximize the sales reps' time spent with each account. Invest in further developing Z-Score Productivity Model to measure an optimum number of accounts serviced by each sales rep. Additionally, expand the use and implementation of the IT Potential Spend Model to maximize sales revenue in each segment.

Option 3 – Offer limited technology capability bundles to small-size accounts. This would increase the sales capability for midsize accounts. On the other hand, this could result in limited sales capabilities for small-size accounts. Additionally, it could result in limited customer satisfaction and sales growth for the small size accounts.

Option 4 – Do nothing. Maintain the current sales model and utilize a single sales rep for small and mid-size accounts.

Within any of these options, it will take at least a quarter to see how things would go. The company would keep an eye on standard company metrics with a long-standing history of reliability, such as customer complaints, partner complaints, customer case open rate, and case time outstanding. With the proper implementation, Melvin could tap the deeper wallets of the small and midsize companies while maintaining continuity in the support, solutions, and innovation that Cask expected the customer to receive.

Biographies

Garrett Bridenbaugh is a project manager at the USF Institute of Applied Engineering. He is responsible for managing the cost, schedule, and performance of multiple projects and has worked to establish the Academic Consortium partnering with more than 17 universities nationwide. Garrett received his bachelor's degree from the Florida Institute of Technology in Melbourne, FL. Previously, he was a US Army Engineer Officer with the 101st Airborne Division, a structural engineer, and an operations supervisor. He is currently completing his Executive MBA at the University of South Florida.

Daniel Bellinger is the southeast Public Sector Territory manager with Cisco Systems covering Florida, Georgia, and other states along the Gulf Coast. In this role, he leads a team of four account managers and four technical specialists. He has been with the company since 2018 and is responsible for setting the go-to-market strategy for Public Sector sales. He is a founding member of Cisco's Advisory Council for Change. Daniel received his bachelor's degree in communication studies from University of Texas at Austin and is currently completing his Executive MBA at the University of South Florida.

Soujanya Nomula is the associate director for RISK Business with the Depository Trust and Clearing Corp., responsible for the end-to-end deliveries of critical risk projects which are regulatorily mandated and subject to rule filing by the Federal Reserve. She is a multi-faceted professional with a unique mix of strategic vision, tactical execution, and a high level of learning agility. Soujanya received a bachelor's degree from Osmania University, India. She is currently completing her Executive MBA at the University of South Florida.

Ajay Sikha is the Director of Business Innovation, Strategy, and IT Operations at Tampa Electric (TECO) responsible for managing the company's information technology infrastructure and applications. He is a seasoned IT executive with global experience in business transformation and operations across multiple industries such as Utility, Automobile, Electronics, Aviation, and Manufacturing sectors. He is responsible for a diverse portfolio of technology assets, and is keenly focused on operational excellence, as he seeks to streamline the IT organization and leverage strategic partners to deliver cost-effective technology solutions.

Eric Pandorf is the vice president of finance for U.S. Saws. He is responsible for the execution of the company's vision, mission, and values. He reports directly to the CEO and uses his leadership skills across multiple departments to bring success. Prior to working at U.S. Saws, he served as senior financial and operations analyst with National Home Builder and Land Developer, where he oversaw the financial review of two division's monthly financial statement packages. Eric received his bachelor's and is completing his Executive MBA at the University of South Florida.

Jay Stratton is the clinical skills director and security officer for the Vein and Vascular Institute of Tampa Bay. He trains managers and staff members for all six of the clinic's offices. He is responsible for training administrative and clinical personnel, as well as, ensuring the company stays in compliance with security and HIPAA. He has over 20 years in the US Army as a combat medic working with a variety of conventional and special operations units. Jay received a bachelor's degree in science with a concentration in health care administration/health information technologies and is currently completing his Executive MBA at the University of South Florida.

Bibliography

Business Market Segmentation. (2022). Retrieved from www.iedunote.com: https://www.iedunote.com/business-market-segmentation

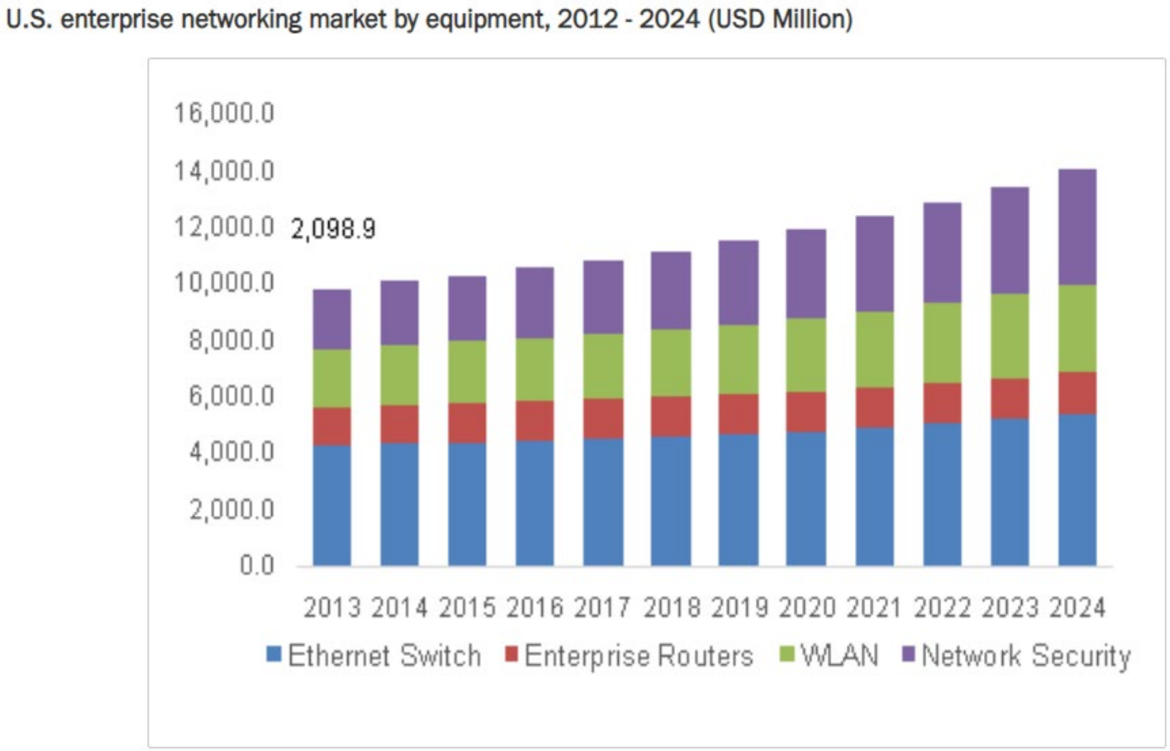
Closing Job and Opportunity Gap for Black Talent. (n.d.). Retrieved from https://oneten.org/about/mission/

Enterprise Networking Market Analysis By Equipment (Ethernet Switch, Enterprise Routers, WLAN, Network Security) And Segment Forecasts To 2024. (2022). Retrieved from www.grandviewresearch.com: https://www.grandviewresearch.com/industry-analysis/enterprise-networking-market

Jendrasiak, G. (2022, August 18). USF EMBA Call w/Gordon Jendrasiak. (D. Bellinger, G. Bridenbaugh, & E. Pandorf, Interviewers)

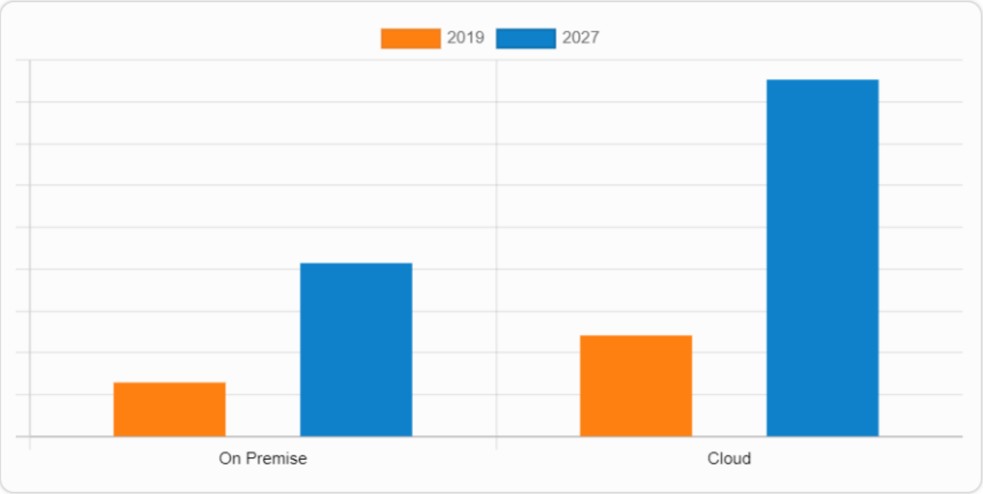
Leading cybersecurity vendors by market share worldwide from 2017 to 2020. (2022). Retrieved from www.statista.com: https://www.statista.com/statistics/991308/worldwide-cybersecurity-top-companies-by-market-share/#:~:text=Cisco%2C%20Palo%20Alto%20Networks%20and,7.8%20and%205.9%20percent%20respectively.

Exhibit 1: U.S. Enterprise networking market by equipment, 2012-2024



(Enterprise Networking Market Analysis by Equipment)

Exhibit 2: Network Security Market by Component



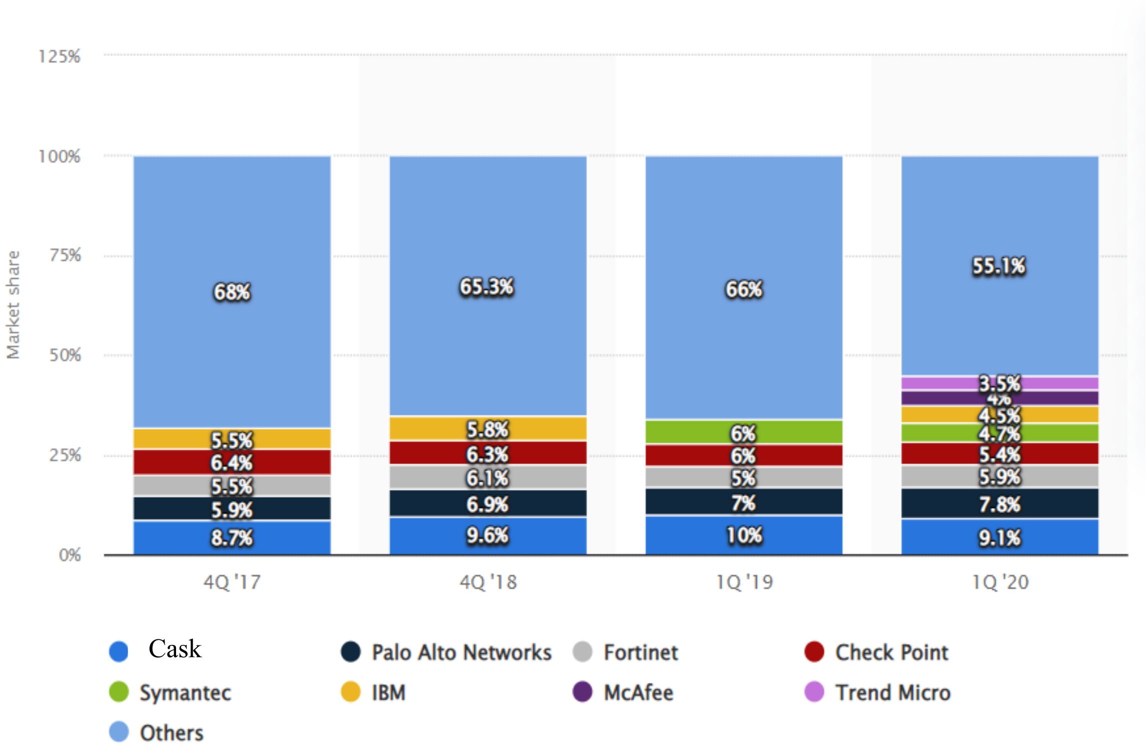
Network Security Market

By Component

Cloud segment is projected as one of the most lucrative segments.

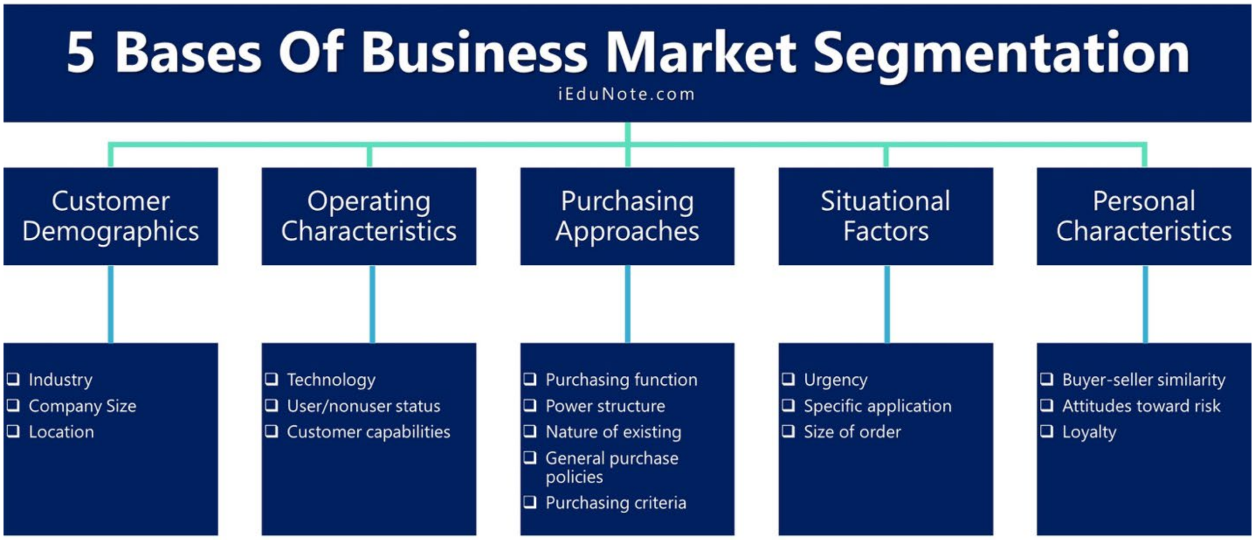
(Leading cybersecurity vendors by market share worldwide from 2017 to 2020)

Exhibit 3: Network Systems by Market Share



(Leading cybersecurity vendors by market share worldwide from 2017 to 2020)

Exhibit 4: 5 Bases of Business Market Segmentation



5 Bases Of Business Market Segmentation

iEduNote.com

Customer Demographics

- □ Industry
- □ Company Size
- □ Location

Operating Characteristics

- □ Technology
- □ User/nonuser status
- □ Customer capabilities

Purchasing Approaches

- □ Purchasing function
- □ Power structure
- □ Nature of existing
- □ General purchase policies
- □ Purchasing criteria

Situational Factors

- □ Urgency
- □ Specific application
- □ Size of order

Personal Characteristics

- □ Buyer-seller similarity
- □ Attitudes toward risk
- □ Loyalty

Exhibit 5: Annual Revenue Per Market Segment

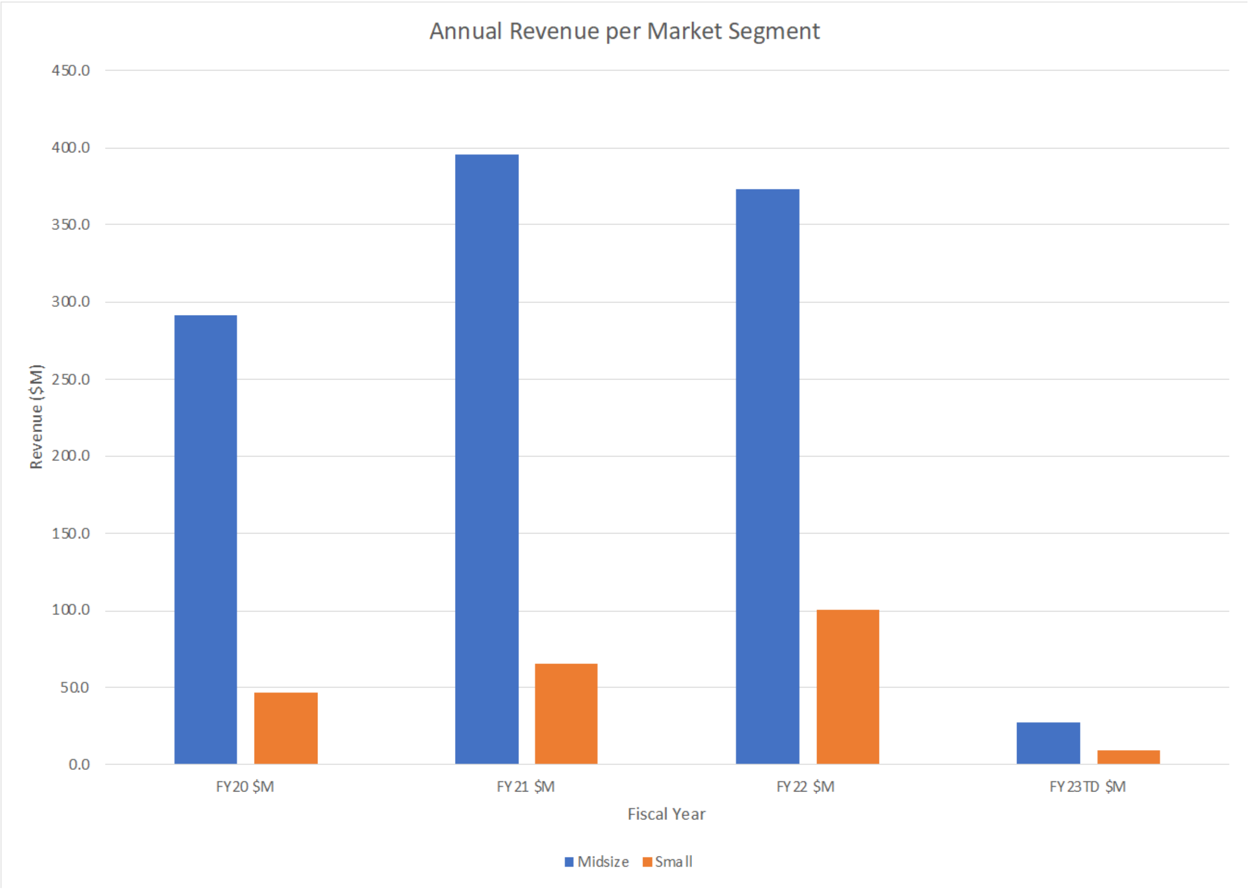
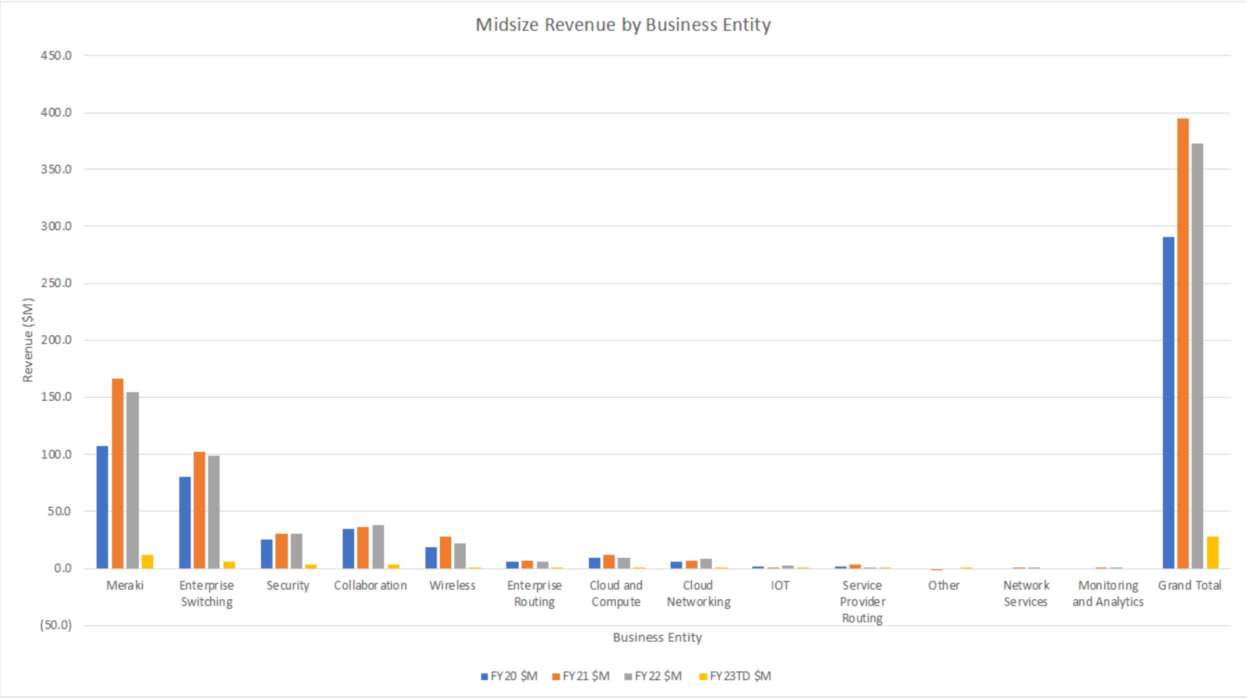


Exhibit 6: Segment Revenue by Business Entity



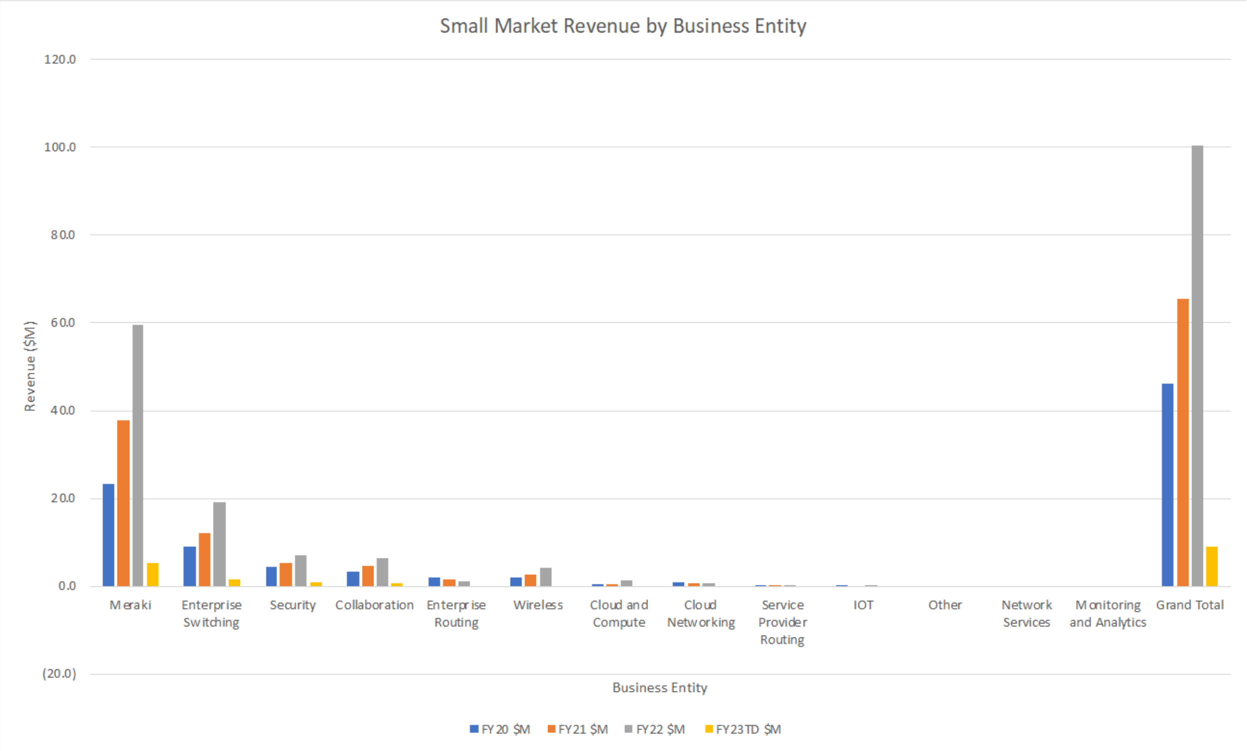
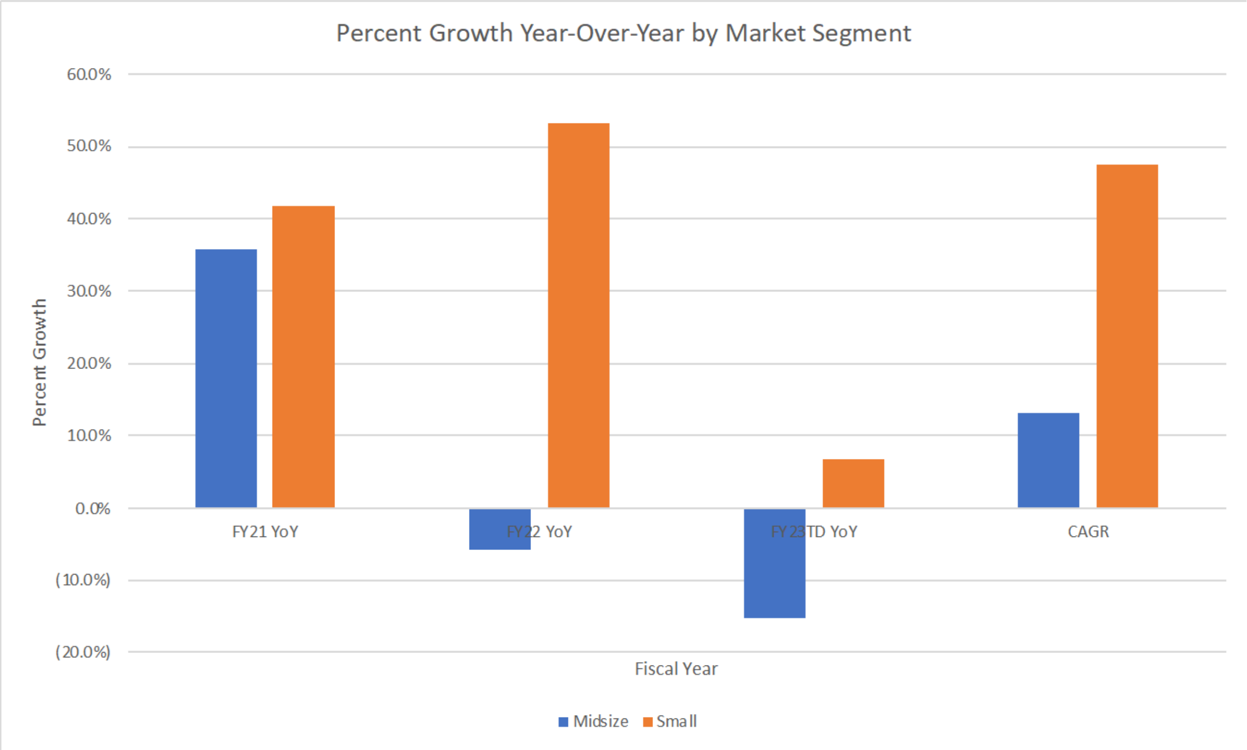


Exhibit 7: Growth Year-Over-Year by Market Segment



(SLED Territory Data, 2022)