First Challenge:

SMEs might not be able to adopt the new technologies fast enough, they have limited funding, limited talent, limited time along with limited space to be able to transition from one technology to another, this results in them lagging behind and as such losing more funds, this only results in a vicious cycle in which companies would not be able to get back from. With this, they also lose their customers and thus, their business might be driven to bankruptcy.

Research:

This is particularly evident when AZ Central states that,"The first major issue with not having enough inventory to meet demand is lost sales. Customers usually approach your business with an intent to buy. This in itself is an accomplishment. When consumers realize you are out of stock, they have to seek out other providers or brands to meet their needs." From this, it can be related to not having the resources to adopt technology fast enough, resulting in loss of customers, eventually leading to what AZ Central has stated, the customers will look towards bigger companies and SMEs will lose business.

Second Challenge:

Inflation will be even worse in the future. When inflation happens, the issue of prices becoming spiked up is very much a probability, even a necessity for the sellers. As this happens, cost of living follows and rises. Prices will slowly become either too high to maintain the business, or that the prices are so high customers can't afford to buy them and companies lose business. Even when prices drop, sales rate may not be high and no one will buy anything. Even with high sales, loss will be higher than any revenue made due to cost price being overpriced. Currently, we are headed towards a second Great Depression, however, whether it is more serious or less, we cannot give an answer to it. What we can confirm is that most SMEs will not be able to make it past such an obstacle. As mentioned before, they have limited funding and thus probably will not make it past this.

Research:

Evidence like, "Despite fall in the inflation rate, prices are still rising. The rise in prices is partly a reflection of generally positive economic growth. As demand expands, we tend to get a moderate amount of inflation.The last period of deflation in the UK was during the 1920s and 1930s. Of course, this was mainly a period of economic depression. When we are economically sound, the inflation of prices is bound to happen," as shown by Economics Help, we can see that inflation is a real threat that is approaching. Of course, it isn't coming in drastic proportions. However, Inflation.data shows that the threat exists, whether or not we see it or not, with evidence like "This is the most obvious impact to businesses. Rapidly rising prices will cause consumers to "stay away in droves". There are ways for businesses to plan for inflation to reduce the chances of revenue loss. Gradually increasing prices will prevent a sudden price hike, and if your competitors don't respond similarly, they'll have to increase their own prices suddenly, which will cause "sticker shock" for their consumers causing them to look for more affordable alternatives. Another sneakier option that businesses often resort to, is to shrink the package size while keeping the price the same. This is sort of "stealth inflation" because most consumers won't notice the quantity change because they are more focused on price."

Third Challenge:

Data Piracy.When the Fourth Industrial Revolution happens, there is bound to be a lot of personal data being put online. E-commerce is becoming more and more active lately, with places like Amazon and Carousel letting people sell and buy stuff, some of which requires personal information. Hackers can easily aim for these things and use them for malicious purposes. The presence of hackers is real, so there is bound to be hackers going after these data which is worth a lot of money.

Research:

This can be proven through several different events where even a Raspberry Pi, which isn't a supercomputer, managed to hack into the NASA database. This website shows it:https://www.zdnet.com/article/nasa-hacked-because-of-unauthorized-raspberry-pi-connected-to-its-network/ Another evidence would be an article about Hundreds of personal user IDs and passwords belonging to individuals working in multiple government organisations, along with the information of nearly 20,000 cards from local banks, have been harvested by hackers and put up for sale. This website shows it:https://www.businesstimes.com.sg/government-economy/singhealth-hacked-records-of-15m-patients-including-pm-lee-hsien-loong-stolen

Fourth Challenge:

Limited funding. SMEs cannot afford the necessary stock and equipment needed to maintain their machinery and automation, this lack leads to a decrease of efficiency among the SMEs and thus they may not be able to keep up.

Research:

LACK OF FUNDING, A MAJOR CHALLENGE FOR SMES TO ADAPT AND INNOVATE: AON STUDY | SME HORIZON

In-text: ("Lack of funding, a major challenge for SMEs to adapt and innovate: Aon study | SME horizon", 2019)

Your Bibliography: Lack of funding, a major challenge for SMEs to adapt and innovate: Aon study | SME horizon. (2019). Retrieved 6 August 2019, from https://www.smehorizon.com/lack-of-funding-a-major-challenge-for-smes-to-adapt-and-innovate-aon-study/

LACK OF FUNDS HINDERS SMES' GROWTH

In-text: ("Lack of funds hinders SMEs' growth", 2019)

Your Bibliography: Lack of funds hinders SMEs' growth. (2019). Retrieved 6 August 2019, from https://vietnamnews.vn/economy/423399/lack-of-funds-hinders-smes-growth.html#v6dbFWWu4Om1D7ES.97

MATTERS, B.

Lack of funding puts growth of SMEs at risk

In-text: (Matters, 2019)

Your Bibliography: Matters, B. (2019). Lack of funding puts growth of SMEs at risk. Retrieved 6 August 2019, from https://www.bmmagazine.co.uk/news/lack-funding-puts-growth-smes-risk/

Fifth Challenge:

Stiff Competition. This is a problem that happens regardless of age but with more and more SMEs and more and more big tech giants along with huge retail chains, SMEs face extremely stiff competition as they have to compete with many other companies, selling the same products in the same way.

Research:

SHIAO, V.

SMEs grapple with rising costs, stiff competition: survey

In-text: (Shiao, 2019)

Your Bibliography: Shiao, V. (2019). SMEs grapple with rising costs, stiff competition: survey. Retrieved 6 August 2019, from https://www.businesstimes.com.sg/government-economy/smes-grapple-with-rising-costs-stiff-competition-survey

COLEMAN, A.

How can SMEs compete with big businesses?

In-text: (Coleman, 2019)

Your Bibliography: Coleman, A. (2019). How can SMEs compete with big businesses?. Retrieved 6 August 2019, from https://www.theguardian.com/small-business-network/2013/jan/10/sme-compete-big-business

SMES GRAPPLE WITH RISING COSTS, STIFF COMPETITION: SURVEY

In-text: ("SMEs grapple with rising costs, stiff competition: survey", 2019)

Your Bibliography: SMEs grapple with rising costs, stiff competition: survey. (2019). Retrieved 6 August 2019, from https://www.sgsme.sg/news/smes-grapple-rising-costs-stiff-competition-survey

Underlying Problem:

In the end, we decided that our underlying should be:SMEs play a profound role in the economic development of Singapore. Due to the constant inflation of prices, it appears that our SMEs may not be able to cope with the fast-paced evolution of technology and the constant inflation of prices. On top of that, there is the chance that data may be lost to hackers, which will be a huge setback for the company. How might we increase the SMEs' profits and improve their network security so that that they can become organisations that are sustainable in the years 2030 and beyond?

Why we phrased it that way:

We specified that the SMEs were extremely important and that they had several different threats. However, in the end we decided the most crucial problem at hand was data piracy. Data piracy is extremely common and loss of information in an SME is an extremely big problem as the company would stand to lose thousands or even millions, which takes a big toll on them, having to take care of their losses along with trying to keep up to date.

First Solution:

We, the Singapore Biometric Security Company will implement biometric security in Singapore for all the SMEs with their collaboration. All SMEs will change their security systems to biometric security within 24 hours. Hackers will be unable to obtain biometric information in merely one day and the chances of data piracy will significantly decrease in Singapore, by 2025.

Research:

It was extremely important to specify SMEs with their collaboration as this was a form of showing that it would be done with an SMEs agreement and it was not something forced, thus it could be more acceptable. We also had to specify the type of security, where we chose biometrics, which is basically a password that is unique and cannot be duplicated. If changed within 24 hours, hackers would then be rendered unable to access any of the information and would ensure concrete security.

CNBC. (2019). *Biometrics: The future of digital security*. [online] Available at: https://www.cnbc.com/2016/04/05/biometrics-future-of-digital-cyber-security.html

THOMPSON, E.

Understanding The Strengths And Weaknesses Of Biometrics | Information Security Buzz

In-text: (Thompson, 2019)

Thompson, E. (2019). Understanding The Strengths And Weaknesses Of Biometrics | Information Security Buzz. Retrieved 6 August 2019, from https://www.informationsecuritybuzz.com/articles/understanding-the-strengths-and-weaknesses-of-biometrics/

HOW SECURE IS BIOMETRIC DATA | VERIDIUM

In-text: ("How Secure Is Biometric Data | Veridium", 2019)

How Secure Is Biometric Data | Veridium. (2019). Retrieved 6 August 2019, from https://www.veridiumid.com/how-secure-is-biometric-data/

Second Solution:

We, the software engineers of Firewall X, will create a 6th generation firewall known as meta-firewalls and implement it for the SMEs in Singapore. This firewall serves 4 purposes. Firstly, it fulfils the role of a traditional firewall. Secondly, it can secure areas that the 5th generation firewall could not, for example, containers, Cloud and SDN. Thirdly, it removes phishing links and suspicious files from the servers before they reach the email of the staff. Lastly, it learns, this firewall is capable of changing its own code to adapt to different viruses and hacking tools. Hackers will be unable to bypass the firewall, significantly decreasing the chance of data piracy in Singapore by 2030.

Research:

This solution leverages on further development of Application Firewalls, It operates by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall. Basically, it detects any anomalies within the systems and is able to choose whether to let it pass.

However, the information has to follow a certain policy in order to pass. These meta-firewalls make use of Machine Learning, allowing these firewalls to adapt to different threats and make new policies along the way, meaning security in the internet only gets more strict the more attacks it faces, this firewall adapts to its strongest everytime it is attacked. This means it is capable of predicting different threats before they even strike and only become more effective in the long run.

WHAT IS AN APPLICATION FIREWALL? | GLOSSARY | F5

In-text: ("What Is an Application Firewall? | Glossary | F5", 2019)

Your Bibliography: What Is an Application Firewall? | Glossary | F5. (2019). Retrieved 6 August 2019, from https://www.f5.com/services/resources/glossary/application-firewall

MACHINE LEARNING: WHAT IT IS AND WHY IT MATTERS

In-text: ("Machine Learning: What it is and why it matters", 2019)

Your Bibliography: Machine Learning: What it is and why it matters. (2019). Retrieved 6 August 2019, from https://www.sas.com/en_sg/insights/analytics/machine-learning.html

Next-Generation Firewalls: A History of the Firewall Part 4., , from https://www.firemon.com/practical-history-firewall-part-4-generation/

Third Solution:

We, the software engineers of CloudTech, will improve and increase the efficiency and security of Cloud technology to make all SMEs use and trust Cloud technology. SMEs will store backup data in Cloud and in their own databases. SMEs will not have to focus as much on security with Cloud technology helping them, this also greatly relieves financial stress on SMEs in Singapore to afford new technology to secure their data from 2025 onwards.

Research:

This solution particularly focuses on the new Cloud technology that will be commonly used. This kind of technology basically stores information into one concentrated,extremely protected network, this can increase concentrated security and companies will be less strained in funding when it comes to this.

WHAT IS CLOUD COMPUTING?

In-text: ("What Is Cloud Computing?", 2019)

Your Bibliography: What Is Cloud Computing?. (2019). Retrieved 6 August 2019, from https://www.pcmag.com/article/256563/what-is-cloud-computing

WHAT IS CLOUD COMPUTING? A BEGINNER'S GUIDE | MICROSOFT AZURE

In-text: ("What Is Cloud Computing? A Beginner's Guide | Microsoft Azure", 2019)

Your Bibliography: What Is Cloud Computing? A Beginner's Guide | Microsoft Azure. (2019). Retrieved 6 August 2019, from https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

How can SMEs protect their data by using the Cloud? (n.d.). Retrieved from https://mybusiness.singtel.com/techblog/how-can-smes-protect-their-data-using-cloud

Fourth Solution:

We, the Employees of McAfee will create a package which will educate the employees among SMEs to exercise more cyber-awareness. This way, SMEs will not have to lose information due to their own employees exposing personal information and causing data breaches amongst the company, this is a cost efficient way that does not require actual software but only asks for the awareness of the employees.

Research:

SECURITY AWARENESS STATISTICS

In-text: ("Security Awareness Statistics", 2019)

Your Bibliography: Security Awareness Statistics. (2019). Retrieved 6 August 2019, from https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-awareness-fundamentals/security-awareness-statistics/#gref

WHY EDUCATING YOUR EMPLOYEES ON CYBER INTELLIGENCE AND SECURITY WILL REDUCE RISK

In-text: ("Why Educating Your Employees on Cyber Intelligence And Security Will Reduce Risk", 2019)

Your Bibliography: Why Educating Your Employees on Cyber Intelligence And Security Will Reduce Risk. (2019). Retrieved 6 August 2019, from https://www.cybintsolutions.com/employee-education-reduces-risk/

How to Reduce Data Breaches with Effective Employee Training. (n.d.). Retrieved from https://cyberscout.com/education/blog/how-to-reduce-data-breaches-with-effective-employee-training

Fifth Solution:

We, the employees of anti-virus companies will work together to standardise a bot known as I-Bot, an online helper that will monitor and give advice to the surfer and will also help to scan for viruses and remind them. This I-Bot will help to prevent data piracy from occurring through constant reminders. This will help to decrease the amount of data piracy from 2023 and beyond.

Research:

Wax, D. (2019, June 18). The Importance of Reminders (And How to Make a Reminder That Works). Retrieved from https://www.lifehack.org/articles/featured/back-to-basics-reminders.html

Blood, E. (2017, August 26). Why Reminders Matter. Retrieved from https://www.theodysseyonline.com/why-reminders-matter

10 best reminder apps for Android! (2019, June 08). Retrieved from https://www.androidauthority.com/best-reminder-apps-for-android-654628/

All of these are to prove the importance of reminders and how they can impact us along with how common reminder bots are nowadays to help people

Criteria:

Firstly,Which solution is the most cost effective?
Secondly,Which solution can secure the data most effectively?
Thirdly,Which solution is most available to the mass SMEs?
Fourth,Which solution requires the least amount of time to implement?
Fifth,Which solution will receive the most acceptance from the SMEs?

Our reasoning:

All of the criteria were mainly focused on allowing the most SMEs to be affected and within the shortest time. Of course, the effectiveness was also extremely important in the criteria because a security system would not be one if it did not do very well securing information.

Action Plan:

Our conclusion for the best solution was Solution 2, the Meta-Firewalls. These meta-firewalls will begin developing in 2020 with the help of several cyber-security organisations like Firewall X and the NSA and the first prototype will be finished by 2023 or earlier. They will first launch it to a small group of SMEs to be the first beta-testers and white hackers will attempt to breach the firewalls systems. These white hackers will repeatedly attempt to hack. If they succeed, development will proceed and the hackers will tell the software engineers where the bugs are and what improvements must be made. Upon succession, the first batch will be sold to the public and will be done so in 2025. Around this time, the Fourth Industrial Revolution will probably have begun or is beginning and from 2025 onwards, data piracy will be uncommon.

Evaluation:

Our backing towards these claims is that these Meta-Firewalls consist of 2 components for it to succeed. Firstly, it requires the existence of an Application Firewall, which already exists. What we think is that if we combine this with the second component, Machine Learning, we can create an adapting, changing, strict and sturdy firewall. Machine Learning is also something that exists and is easy to do, however, it is currently being developed and still has not hit a peak. We believe Machine Learning can become faster, it can evolve to the point where it can predict and react to even the most aggressive virus attack. In addition, the merging of the Application Firewall and Machine Learning requires time, and we predict that there may even be a chance for it to be ready by 2022. Of course, the earlier it finishes, the better. The Fourth Industrial Revolution will happen very soon and if we finish the Meta-Firewall by then, we will be able to counter hacker attacks extremely early. We think this idea is extremely feasible as Machine Learning and Application Firewalls already exists, all we need to do is to merge them together and develop it further to create, the Meta-Firewall. However, we have identified two problems, the firewall might be weak at first as it has not yet adapted yet, thus, if hackers do take advantage of this, they may be able to breach the systems. Secondly, Firewalls depend on the employees too, if a hacker manages to hack an employee's phone instead of the database, they still might find a loophole. Luckily, all of these are just temporary issues before the firewall begins to adapt and learn.

Research:

WHAT IS AN APPLICATION FIREWALL? | GLOSSARY | F5

In-text: ("What Is an Application Firewall? | Glossary | F5", 2019)

Your Bibliography: What Is an Application Firewall? | Glossary | F5. (2019). Retrieved 6 August 2019, from https://www.f5.com/services/resources/glossary/application-firewall

MACHINE LEARNING: WHAT IT IS AND WHY IT MATTERS

In-text: ("Machine Learning: What it is and why it matters", 2019)

Your Bibliography: Machine Learning: What it is and why it matters. (2019). Retrieved 6 August 2019, from https://www.sas.com/en_sg/insights/analytics/machine-learning.html

Next-Generation Firewalls: A History of the Firewall Part 4., , from https://www.firemon.com/practical-history-firewall-part-4-generation/

What Happens When a Business Does Not Meet the Demand of Consumers?. (2019). Retrieved from https://yourbusiness.azcentral.com/happens-business-not-meet-demand-consumers-13978.htmSchwab, K. (n.d.). The Fourth Industrial

World Economic Forum. (2019). *The Fourth Industrial Revolution: what it means and how to respond*. [online] Available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Investopedia. (2019). *Inflation Definition*. [online] Available at: https://www.investopedia.com/terms/i/inflation.asp

Singapore Business Review. (2019). *Singapore remains at risk from high-profile hackers*. [online] Available at: https://sbr.com.sg/information-technology/in-focus/singapore-remains-risk-high-profile-hackers

Security Today. (2019). *The Average Cost of a Data Breach -- Security Today*. [online] Available at: https://securitytoday.com/articles/2018/07/17/the-average-cost-of-a-data-breach.aspx?m=1

Cybint. (2019). *13 Alarming Cyber Security Facts and Stats | Cybint*. [online] Available at: https://www.cybintsolutions.com/cyber-security-facts-stats/

Pettinger, T. (2019). *Why do prices always go up in an economy? | Economics Help*. [online] Economicshelp.org. Available at: https://www.economicshelp.org/blog/86/inflation/prices-go-up/

McMahon, T. (2019). *Effects of Inflation on Businesses*. [online] InflationData.com. Available at: https://inflationdata.com/articles/2017/06/07/effects-of-inflation-on-businesses/

NBCNews(2019) The total cost of a data breach — including lost business — keeps growing[online] Available at:https://www.nbcnews.com/business/consumer/total-cost-data-breach-including-lost-business-keeps-growing-n895826