WEBACCESSPRO: AN ARTIFICIAL INTELLIGENCE START UP IN CROWDED MARKET

Dr. Prem Prakash Dewani, Indian Institute of Management, Lucknow
Karnika Bains, FPM Scholar, Indian Institute of Management, Lucknow

ABSTRACT

WebAccessPro, a cyber-security start-up with less than 100 employees and faced the issue of the product's adoption, while also wanting to expand. Most of its revenue was currently being obtained by government departments, denting the cash flow of the business. The business wish to move to a more liquid market and the management was wondering if they should foray into an aggregator marketplace platform, listing suppliers and customers worldwide, while also selling its own products via this platform. The brand is relatively newer and lesser known, and hence, the customers were skeptic of moving away from other established global brands. While the competition in the market offered multiple solutions and products, WebAccessPro specialized in an AI-enabled security product for websites, applications, and against data leak threats. It is a self-learning and self-healing product based on machine learning. The case deals with a high-technology product facing an adoption challenge in the market. The company is struggling with customer acquisition for trial, and customer retention for repeat purchase.

Keywords: Business Development, Cyber Security, AI, Brand Awareness.

INTRODUCTION

We're all Connected! The creation of the internet brought the world closer, and linked all of us up. While little surpasses the ease and convenience of online shopping, an inhibitor for some potential users is the need to share personal information. In addition to being bombarded with advertisements, and spam mails, there is also the risk of sensitive information being leaked online. Imagine the plight! One Mr. Dhruv Banerjee fell into such a trap, and played part to the fraud which followed next. Mr. Banerjee received a phone call from a cybercriminal portraying to be from a mobile service provider. The fraudster enquired if Mr. Banerjee was using a 3G sim card, and if he would like to swap that with a 4G sim card and with some additional exciting ongoing offers. Mr. Banerjee agreed. After the call, the culprit sent a 20-digit number to the 3G sim, and Mr. Banerjee, unfortunately, followed the criminal's instructions and sent this 20-digit number to the service provider's helpline. Soon after, the 3G sim was deactivated, while the 4G sim which the cybercriminal had already bought and obtained, was activated. In the next 24-hours, he used the new sim for various OTPs, and used Mr. Banerjee's bank account for buying electronics worth 2 lacs. Sadly, Dhruv wasn't the only such victim in this ploy, and the criminals ended up transferring nearly 4 crores from about 50 different individuals.

Brands like Yahoo!, LinkedIn, Facebook, Dropbox, Zomato, HBO, WhatsApp, Telegram have also not been able to stay clear from such risky cyberthreats. Websites are often attacked, hacked, and Gigabytes of data pertaining to customers' personal information are leaked online. This information can then be used by the cybercriminal in multiple ways. Attackers don't just attempt to gain information, but they may even send fake traffic to websites, thereby increasing

load onto the server, and thus leading to a crash, not allowing legit customers to enter the website.

'Cybersecurity is now a boardroom issue'- read one article published in The Hindu, April 2019. While a Union Minister addressed a gathering in 2018 as follows,

"There is phenomenal increase in cyber espionage to steal state secrets, corporate information, intellectual property or military superiority. Cyber attackers are more organised and many have significant funding."

He estimated the threat to cost the world trillions of dollars per year, by 2021. As technical as the risk is, some still don't fathom the threat Figure 1.

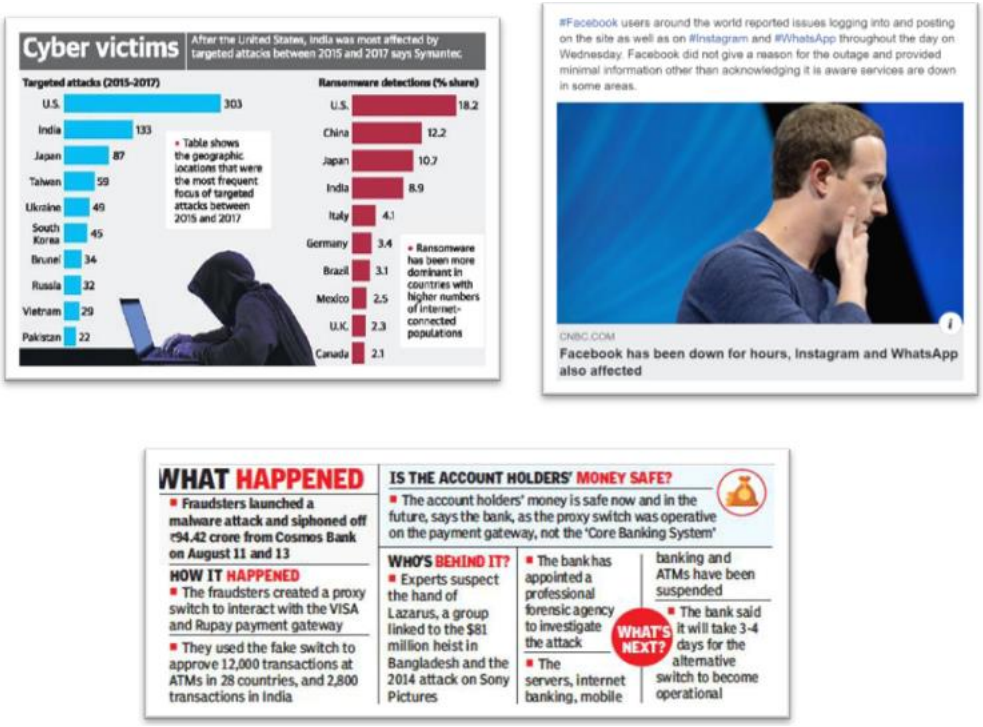

FIGURE 1
CYBER-ATTACKS

We are at Risk

We do what bouncers do at night clubs. We provide the first line of defence to ensure enterprise websites stay online and secure - always said the CEO of WebAccessPro. Although, there were multiple cybersecurity products available in the market, WebAccessPro had created a product unlike others. They catered to several government and state-owned departments, national banks, manufacturing firms, energy companies, transport businesses, telecom providers, etc. While all other existing products required human intervention in implementing security solutions, WebAccessPro pioneered with an AI (Artificial Intelligence) – powered product, which was not only self-learning, but also self-healing. It worked on the properties of machine learning and generated appropriate configurations by observing incoming traffic. The product would observe and understand genuine customers' usage pattern and instantly catch fictitious

traffic on accounts of spurious behaviour. It also tested these configurations and implemented them if everything in the solution seemed alright.

History

WebAccessPro was birthed from its parent organization, FNP IT Services, which had been operating since 2006. FNP provided multiple security services and products like- Web Application Security Auditing, Network Security Auditing, Information Risk Management, Cyber Forensics, Mobile Forensics, Cyber Crime Investigation, Information Security Training, Computer Security Incident Response Team and Security Operations Centre. In addition, they also provided software solutions and infrastructure testing. To establish a differentiated product with a new and younger brand, FNP launched WebAccessPro under the *'Make in India'* initiative in 2015, as India's first home-grown and comprehensive DDoS solution for managing current and future attacks. WebAccessPro was established to cater to start-ups, while FNP had dealt with B2G and MSMEs (micro, small and medium enterprises). WebAccessPro was the first Indian-based network security start-up providing customizable solutions to its clients with its flagship product, WebAccessPro, an AI-enabled tool, which intelligently and automatically detected and mitigated all kinds of DDoS attacks (HTTP Flood, SYN Flood, SSL Attack, Slowloris, etc.) in real time. It offered multi-layered and multi-vector protection which ensured that the client's website always stayed online and accessible to its real customers. Its multi-layer mitigation provided the widest range of protection to application servers, required minimum human intervention and generated zero false positives. The product was an anomaly detection-and-mitigation system and did not rely on attack signatures, which were usually defined as *"rules"* for any security product or software. This made it harder for the attackers to bypass the firewall, as there were no rules to break. The software would study incoming data and understand the behaviour of a genuine customer and then identify bogus traffic depending on behaviour anomalies. The self-learning software ran on custom configured hardware, which made it extremely flexible to update to newer technologies without needing any hardware upgrade.

The company's vision was *"Simplifying IT Security"*, while its mission was *"To make the IT Security Simple, Effective and Affordable to Businesses - Small and Large"*. WebAccessPro was the only indigenous and an Indian company to offer such a product in the entire Asia-Pacific region. While the international products were highly expensive, WebAccessPro was a cost-effective solution which sold at nearly three-fourth of the price of imported products. So far, the business had been funded by the parent organization itself, and FNP had also secured funding from the Technology Development Board (TDB) for its DDoS-WAF project, WebAccessPro.

Product and Services

FNP offered cyber security products, some of which were even physical in nature and required space in the customer's business premises, whereas, WebAccessPro was established keeping in mind the cloud-based offerings only. Products included cloud-based products, and software as a service- DDoS, Web Application Firewall, etc., while services offered were auditing, training and certifications. These products and services were offered in different business model formats Table 1.

Table 1 WEBACCESSPRO BUSINESS MODELS		
BUSINESS MODEL	**OFFERING**	**PAYMENT MODEL**
Software As a Service	Managed Security	Monthly Subscription
Hardware Appliance	24x7 Enterprise Support	Perpetual Licensing
Hardware As a Service	Managed Security	Quarterly Subscription

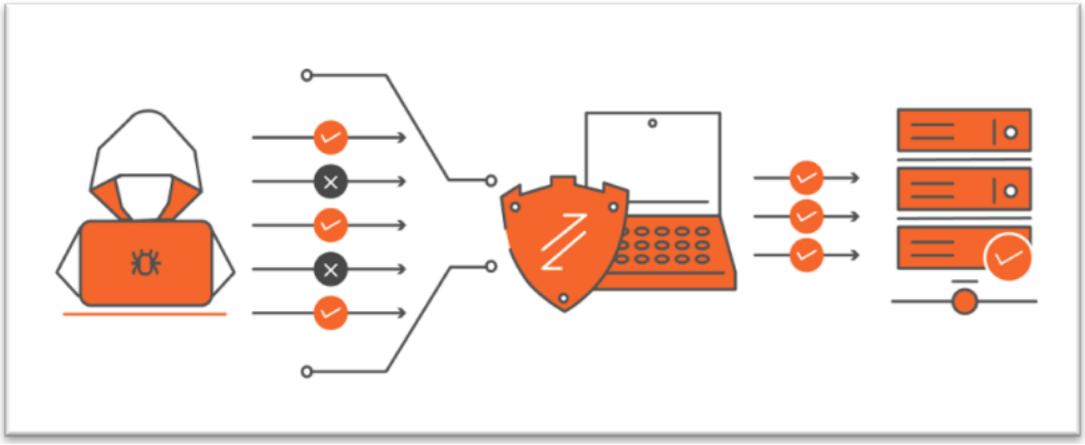

FIGURE 2
WEBACCESSPRO DISTRIBUTED DENIAL OF SERVICE (DDOS)

MITIGATION

DDoS Mitigation Solution- Protection for IT Network Resources

In a distributed denial of service attack hackers generated multiple fake users to overwhelm a website's server. These attacks were evolving in scale, sophistication, and complexity and a successful attack could lead to revenue loss, brand loss, hurt customer sentiments and satisfaction, and could also enhance the company's IT infrastructure cost.

WebAccessPro DDoS Mitigation Solution automatically detected and accurately mitigated cyber-attacks on websites and IT Networks in real time Figure 2. It combined NBA (network behavioural analysis), heuristics, and reputation techniques to self-detect, round the clock, and operated without the need of human intervention. WebAccessPro provided security for multiple types of DDoS attacks and the solution was offered based on the size of the data centre:

1. SWIFT Series- Upto 1Gbps (small enterprise)
2. FREGATA Series- Upto 5Gbps (small & medium enterprise)
3. FALCON Series- Upto 10Gbps (medium & large enterprise)

Web Application Firewall- Protection for Websites and Applications

The WAF was a product designed specifically for applications. Companies used applications for their business, and to connect with their customers, suppliers, and at times even with the employees. This increased use of applications put its assets on the web in a more vulnerable and risky manner. The Firewall prevented data breaches via applications, which were

a host to sensitive and confidential information about the customers and the business Figure 3. The Firewall could:

1. Protect against volumetric DDoS attacks to reduce service outages
2. Protect applications and APIs (Application Programming Interface) against web-attacks like zero-day threats, data leakage, etc.
3. Block malicious bots with built-in detection to separate good bots from the bad, and ensure optimal application performance
4. Defend against automated attacks from non-human traffic, data theft, or content scraping
5. Secure application delivery with Instant SSL (Transport Layer Security) capabilities, enabling quick and easy HTTPS (Hypertext Transfer Protocol Secure)
6. Identify genuine requests and block risky ones to provide API interaction protection

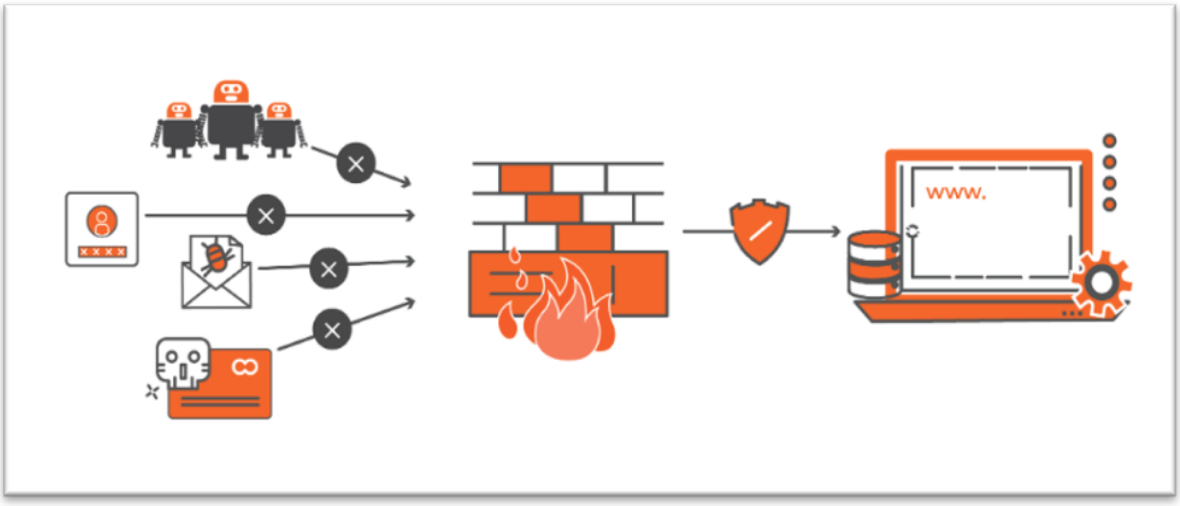

FIGURE 3
WEBACCESSPRO WIRELESS APPLICATION FIREWALL (WAF)

Integrated WAF & DDoS

This solution integrated the Firewall and DDoS mitigation to ensure ultimate protection against data loss. With strong authentication and access control capabilities, it could block network layer as well as application layer DDoS and other attack vectors directed at web-facing applications and those directed towards a network Figure 4. The integrated WAF & DDoS product restricted access to sensitive data as well as to applications.

Security Auditing & Compliance Services

Multiple services were offered to uncover system risks, ensure protection, integrating risk management, while also ensuring policy compliance:

1. Security audit
2. Vulnerability assessment
3. Testing for Penetration, Network Security
4. Compliance and risk management
5. ISO implementation (ISMS- Information Security Management System)

Security Training & Certifications

Various security training programs fo professionals and certifications for auditors were available for email security, password security, social security, etc. These short programs were offered to IT personnel, professionals, and enthusiasts (Table 2).

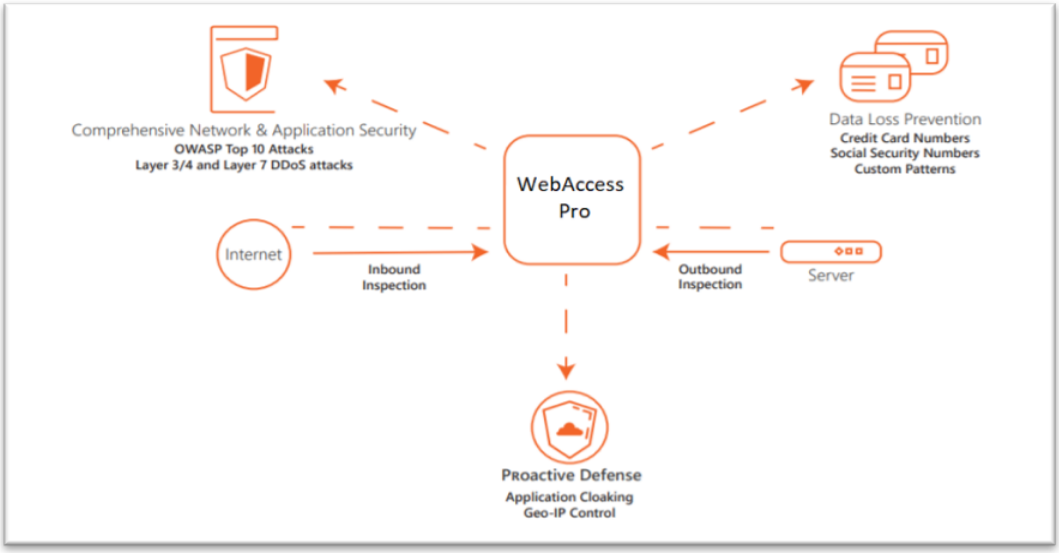

FIGURE 4
WEBACCESSPRO INTEGRATED SOLUTION- WAF & DDOS

Table 2
TRAINING AND CERTIFICATION BY WEBACCESSPRO

Course or Certification	Duration	Prerequisite to Attend	Useful For
Cyber Security Awareness Testing	7 hours	Basic Computer Knowledge	IT Users like web/mobile developers, Security enthusiasts, and more
Certified Ethical Hacking (CEH)	5 days	Basic Computer Knowledge	System Engineer, System Administrator, Security Enthusiasts, IT Security Professionals
Certified Information Systems Auditor (CISA)	5 days	Experience in systems auditing, control or security	IT Audit Manager, Internal Auditor, IT Risk and Assurance Manager, Security Enthusiasts
Certified Information Systems Security Professional (CISSP)	5 days	Experience in domains of CISSP - CBK 2018	CISOs, Security System Engineers, Network Architects, Security Enthusiasts
Certified Application Security Professional (CASP)	3 days	Basic understanding of web application, MCA, degree/diploma in CS/IT/ECE	Web/Mobile developers, Penetration Testers, Security Enthusiasts, IT Security Professionals
Certified Network Security Professional (CNSP)	3 days	Basic IT skills and networking understanding	Network/System Administrators, Penetration Testers, Security Enthusiasts, IT Security Professionals

Pricing

WebAccessPro DDoS had a variable pricing method:

1. Small Enterprise (personal websites, blogs, small enterprise websites): $30/month
2. Medium Enterprise (enterprise websites, e-commerce platforms): $60/month
3. Large Enterprises would get in touch with the vendor and obtain a quote, based on the website's size and audit requirement

In addition, they also offered a 15-day free trial. Other players in the market were international and their products were sold after a currency conversion, and hence were more expensive than WebAccessPro. However, these brands with deep pockets had the capacity and appetite to go low in their prices to ensure a sale. They also offered local support for the businesses, which was another benefit for the customer. Competitors like Arbor, Radware, F5, and A10, offered heavy discounts, up to 80-90%, while WebAccessPro usually gave 40-50% discounts, since the product was already cost-effective. The Indian customer, however, was lured by discounts and trusted established brands more than a newly launched brand for something as sensitive as security.

WebAcessPro's next price offering was to be a subscription-based model for their cloud-based services, with no heavy investment or equipment requirement. In such a subscription, the customer would subscribe on to the required software for- a month, or a quarter, or a year, depending on their need, and would pay at the end of the month for the amount of services used. The CEO was certain that this model would bring down the customer's IT infrastructure cost as they would only pay for the actual usage, compared to buying a software with an upfront payment (Table 3).

Table 3
AWARDS WON BY WEBACCESSPRO

YEAR	AWARDS
2019	Winner of the StartVille program - WebAccessPro at NullconX International Security Conference
2019	"The 30 Young and Dynamic Entrepreneurs to watch in 2019"- Insights Success Magazine
2018	Best Cyber Security Product Solution- WebAccessPro at GESIA Annual Awards
2018	The Best Innovation Award- WebAccessPro at InSpRENEUR Summit, Singapore
2018	"Top 20 Tech Brands to Watch in 2018"- CEO Magazine
2017	Top Ten Innovator Award- WebAccessPro at IIT Delhi
2017	10 Most Trusted Cyber Security Companies in 2017- Insights Success
-	Most Innovative Leader Award - Awarded by World Innovative Congress
2016	First Cohort of Cisco LaunchPad- CISCO Launchpad Accelerator Program
2016	Runner up "DSCI Excellence Awards", Recognition as the "Security Product Company of the Year"
2015	Express IT Best Innovation Award of the Year- Express IT

Competitors

In addition to Training and providing Certifications, each of WebAccessPro competitors offered multiple products other than security. These global brands had their respective distribution networks and some were long-running brands (Figure 4-9 & Table 4). Some products and products categories are mentioned below.

Radware

Radware's mission was to be at the forefront of technology/service advances so their customers could be at the forefront of their respective industries. Their product solutions claimed to optimize business operations, minimize service delivery degradation and prevent downtime, with the following product offerings:

1. Application Delivery & Load Balancing
2. Management & Monitoring
3. Application & Network Security
4. Cloud Services- Cloud WAF Service, Cloud Web Acceleration Service, Cloud DDoS Protection Service, Cloud Malware Protection Service, Cloud Workload Protection Service, Bot Manager.

NETSCOUT Systems Inc

Arbor's Smart Data technology distilled real-time, precise, and relevant intelligence from all connected services and their interactions. Arbor helped build and implement digital strategies and deliver optimal application and service performance, provide unmatched user experience, and find and fix advanced cyber and DDoS threats with the following solutions:

1. Enterprise Application & Network Performance Management
2. Carrier Service Provider Products
3. Cyber Threat & DDoS Protection
4. Smart Visibility
5. Handheld Network Tools

F5 Networks

With more than 20 years of application service experience, F5 provided the broadest set of services and security for enterprise-grade apps, on-premises or across any multi-cloud environment:

1. Traffic Management
2. Application Security
3. Infrastructure Security
4. Automation, Orchestration, and Management
5. Cloud Services (as-a-Service)- DNS Cloud Service, DNS Load Balancer Cloud Service, Security Cloud Services
6. Cloud Software
7. Hardware
8. Managed Services

A10 Security Solutions

A10 Networks' application networking, load balancing and DDoS protection solutions accelerated and secured data centre applications and networks of enterprises, service providers, and hyper scale web providers.

1. Products- Application Delivery, Application Delivery for Cloud, DDoS Protection, SSL Inspection, Firewall, VPN, Secure Web Gateway

2. Management- DDoS Monitoring & Management, Service Analytics & Management
3. Services- DDoS Cloud Scrubbing, DDoS Threat Intelligence, DDoS Security Incident Response Team, Training, Professional Services

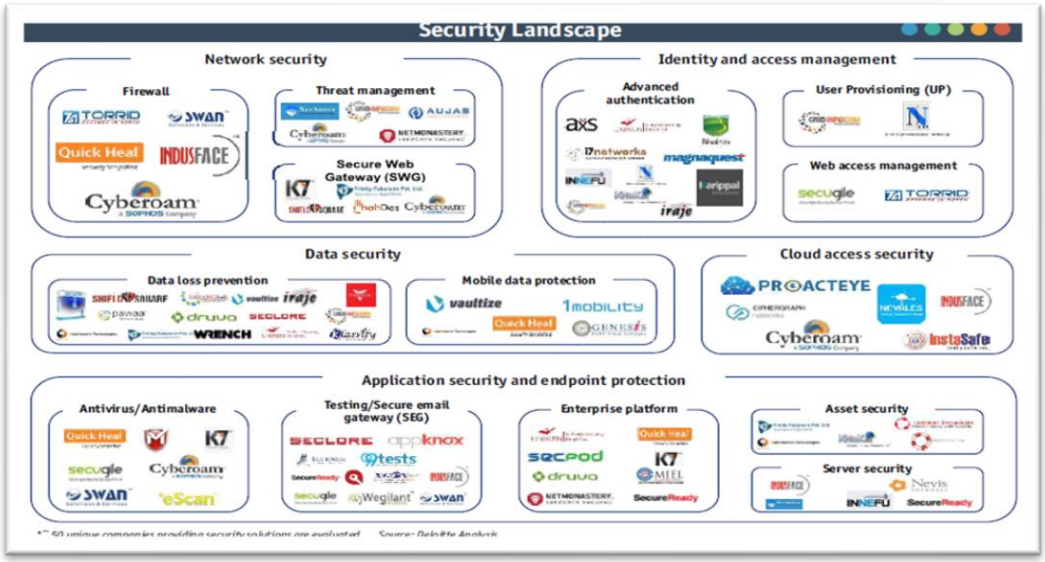

FIGURE 5
INDIAN CYBER-SECURITY SOFTWARE MARKET 2017

FIGURE 6
RADWARE SOLUTIONS & CUSTOMERS

FIGURE 7
NETSCOUT ARBOR DDoS SOLUTION

FIGURE 8
F5 REACH

FIGURE 9
A10 SOLUTIONS

Table 4
COMPETITOR ENVIRONMENT

PLAYER	YEAR ESTD.	REVENUE '18-'19 (US$)	NETWORK CAPACITY	GEOGRAPHIES	INTEGRATORS	EMPLOYEES
F5	1996	2161 million	< 1 Tbps	USA, APAC, Europe	AWS, Microsoft, Red Hat, VMware, Cisco, OpenStack, OpenShift, Google Cloud	4400
A10	2004	232 million	(unknown)	USA, APAC	AWS, Cisco, Google Cloud, Microsoft, Oracle, Red Hat, VMware, Ericsson	800
RADWARE	1997	300 million	< 3.5 Tbps	USA, APAC, Europe, Middle East, Africa, Australia	Blackboard, Cisco, Citrix, Microsoft, Oracle, SAP, VMware	900
NETSCOUT	1984	1160 million	< 1.14 Tbps	USA, APAC, Europe, Middle East, Africa	AWS, VMware, Microsoft, Citrix, Cisco	3000
CLOUDFLARE	2009	120 million	30 Tbps	USA, APAC, Europe, Middle East, Africa	Microsoft, Google, Qaulcomm, Baidu, IBM	750

WEBACCESSPRO Product Differentiation

With multiple threats and respective products in the environment, it was important to differentiate a product to stand-out in the market and provide the customer with a novel solution. WebAccessPro products generated outputs in standard format, which enabled easy integration with other security information and event management (SIEMs) systems. Most other products relied on rules to detect anomalies, while WebAccessPro had a rule-less solution which made risk detection and mitigation more comprehensive and effective. Its distinctive integrated solution combined DDoS mitigation, Web Application Firewall, and Load Balancer into one and provided full attack defence for data and websites. Since it was AI-enabled and a real-time solution, threats that other manually operated solutions solved and eradicated in hours, WebAccessPro mitigated them within a few milliseconds. During the attack, the customer received a system alert, and an e-mail or SMS alert, depending on what the client had signed up for. Furthermore, once the attack was resolved, the system sent out a status report with information like- start time, end time, attack direction, time taken to mitigate, pictorial representation of the traffic (charts, graphs), etc. The process of detecting the cyber-risk had been patented by the firm in 2017, and the patent was good for a time period of ten years. In addition, the company had also applied for two more patents and they were in the pipeline for approval. The product differentiated itself as per the following:

1. The product was AI-powered, based on a rule-less algorithm
2. No manual interventions were required to detect and correct vulnerabilities
3. The company had 3 patents (one approved, two pending) in DDoS and WAF technology
4. It could defend against Zero-Day attacks
5. Provided Layer 3 to Layer 7 protection in a single solution
6. It was time efficient as other products took about 6 hours to mitigate DDoS, while WebAccessPro took only a few milliseconds for the same task
7. The system reported attack statistics post mitigation

Marketing

Being a new and an Indian-origin brand, brand awareness was a major challenge being faced by the company. Most customers wished to buy products which they knew were being used by their competitors or network partners. The company had managed to acquire customers and was also gaining demand traction in other countries via conference participation as well. The

Indian market was not as open to the product as were other nations like Singapore, Bahrain, UAE, etc.

For communication and promotions, WebAccessPro had been using: Blogs, Whitepapers, SEO Marketing, and Social Media Marketing. For most sales they had relied on direct marketing and had obtained clients via sales staff and the established FNP brand itself Figure 10. The company had also participated in multiple technology conferences for product exposure, *viz.*, GISEC '19 (Gulf Information Security Expo & Conference) - Dubai UAE; FINSEC '19 (Financial Security Conclave) - Mumbai India; NULLCON '19 - Goa India, etc. The brand used social media platforms like LinkedIn, Facebook, Twitter, and Instagram for general communication, product promotions, and also for product information (Figure 11 & Table 5, Table 6, Table 7A, Table 7B). Occasion-based marketing was employed on days and festivals like- Earth Day, Women's Day, Mothers' Day, International Workers' Day, Holi, Ramadan, Navratri, Good Friday, etc. The marketing team's objective was two-fold: to generate leads, and to develop the brand. The Vice-President, Sales & Marketing, gave equal importance to both, but also felt that the right kind of customer needed to be targeted, in saying, *"Having 20 thousand followers is not my job. These followers must also buy my product."* The marketing team was small, but, included a graphic designer, one content writer, a digital marketing associate, and additional salesforce. The marketing team had also recently ventured into paid advertising with major search engines.

However, with a new subscription-based marketing offering being launched in June 2019, the CEO knew he would now have to focus on other techniques as well to acquire new customers.

WebAccessPro's existing customers were happy with the brand and its products. One such customer quoted, *"Sincere efforts lead to success. Congrats WebAccessPro team. You're good!"* However, there was no structured mechanism to capture customer feedback. In cases where one technical support staff was always deployed at the client's site, there was day-to-day ongoing feedback, which was mostly reactive and not proactive. Additionally, reactive feedback was obtained at the end of the billing period, by some customers.

Market Potential

Internet's penetration in India crossed the 500 million mark in March 2019, of which 40% were rural active users, and 97% of these users accessed the internet using their mobile devices. Not only were the rural-urban demographics balanced, women were also as active as the men, comprised of 42% of the total internet users, and were actively engaged in the digital world - spending time and money on the internet, for entertainment and communication, and even consumption. With this increase of internet usage, people shifted to online transactions for buying groceries, clothes, books, etc. Similarly, the lesser educated and unemployed individuals, who would steal to make a living, also moved their crime to this virtual place from the physical. The rural market had driven the internet growth in India, and 290 million rural active customers were expected to use the internet by the end of 2019. Usage increased business, and business increased the risk. The growth of internet was initiated by the increasing sales of smartphones, and was later supported by telecoms offering low-cost internet services.

The cyber-security market was an oligopolistic market with a bright future potential. The DDoS world market stood at $1b in 2018 and was expected to grow at 38% CAGR to $2.6b by 2021. The Indian market was at $28m in 2018, with an expected CAGR of 42% till 2021. The Asia-Pacific DDoS and WAF markets were expected to grow at the fastest rate. The WAF world

market was $3.4b in 2018 and was expected to grow at a CAGR of 18.3% to $5.6b by 2021, while the Indian market was $34m in 2018, and was expected to grow with a 107% CAGR.

Customers

Most of WebAccessPro's business came from government offices and its departments. The product was customizable and hence could cater to the needs of multiple industries. Their clients belonged to the following sectors- transport, manufacturing, PSUs (public sector undertakings), energy, government departments, national banks, law enforcement (Police), medical & healthcare (pharmaceutical firms), and educational (institutes like colleges, universities, etc.). 75% of the business was obtained from the government, while 24% contributed to the B2B segment and less than 1% contribution was being made by international sales. B2G transactions were highly influenced by geopolitics and had the infamous modus operandi of delayed payment cycles. Other medium-sized enterprises preferred and trusted known brands for their cyber-security needs.

A major lead in the pipeline for WebAccessPro was from a leading infrastructure firm, who had partnered with a state government. The project was worth $150 million, which would materialize over the next financial year. Smooth and successful execution of this product would ensure similar projects which would then be replicated across five or six more states. WebAccessPro had also recently partnered with the biggest data centre in India, which had about 4,000 customers. A contract with the data centre meant that business would also trickle down to their customers for their individual firm's security needs.

One major problem being faced by the WebAccessPro's customers was the lack of human intervention in problem solving. They felt assured at the sight of an *'IT personnel'* working to fix the problem. However, in the case of WebAccessPro products, it wasn't possible for one person to gain working knowledge about the existing and potential types of threats, and additionally there was no need of human intervention on the account of artificial intelligence, and interestingly, some wouldn't trust machines to fix machines. However, no one person could master and mitigate the innumerable types of cyber threats persistent and possible in the future. An estimate from the marketing head stated that of the business raised by a new customer, 10-15% of the amount was used to acquire the new customer. The costs to acquire a new customer included sourcing the lead plus the resources expended on the customer. Approximately 60 thousand dollars were spent in gaining a new client.

Way Ahead

WebAccessPro was operating as a subsidiary of the parent organization, using their network and referrals, and the CEO was now wondering if he should offer his product and services via a self-owned and self-operated platform. The company would list other security audit providers on its platform as well, and charge them a commission for providing them with the business opportunity. He wished to create a service and product marketplace and leverage its cloud-based SaaS model. This way the business could also acquire customers worldwide. The investment required in setting up an online marketplace platform was $300,000 with an additional $6,000 for an application of the platform. In addition, an annual $50,000 would be required for maintenance and smooth functioning of this platform.

International expansion was also on his mind as the South East Asia, Middle East, and African markets were yet to see their boom in cyber security needs, however, visit to a Dubai

conference had given him mixed responses for the product. The potential customers wished for a physical presence of the brand in their location, and he was expecting good demand traction from Qatar, Bahrain, Turkey, etc. These potential clients liked the product, and System Integrators (distributors) were already approaching the company for business.

So far, the revenue collected was being invested in R&D for the product, and payments from the B2G business were often delayed by anywhere between 15 days to 8 months. Hence, there was a lack of working capital in the business operations. In addition to a financial crunch, WebAccessPro was also facing a churn rate challenge among valuable employees. Graduates were hired fresh out of college and were trained for 6 months to become professional auditors. Valued resources and time were spent on these trainees and some were then poached by bigger companies at three or four times the salaries being paid by WebAccessPro.

Another challenge being faced was the mere fact that the customer could not differentiate between multiple brands which sold highly technical products. Since the customer could not make out the difference between various market offerings, she or he did not know which product was better. Acceptability of the product in international markets was also a task as Indian markets were better known for their services, than they were for their products.

Lastly, the CEO was thinking about the upcoming launch of a monthly subscription SaaS model which was to debut in June 2019. The business would buy a subscription instead of a hardware appliance or a license, and it could be for a month, a quarter, or a year, as per the customers' needs. All traffic coming to the website would first go through WebAccessPro systems and only the verified customers or users would be sent to the client website. This way customer would pay for only what he required and used throughout the month, rather than a fixed fee which seemed like sunk cost to the customer in the case where no attacks happened. This subscription-based model was also expected to further bring down the customer's IT security cost, and make the product seem more affordable to the customer.

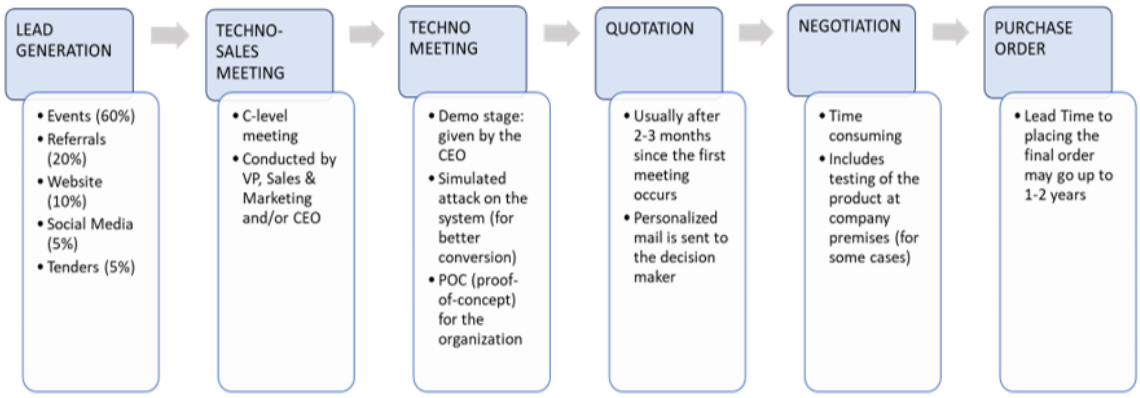

FIGURE 10
WEBACCESSPRO CUSTOMER JOURNEY MAP

FIGURE 11
WEBACCESSPRO MARKETING- FACEBOOK, LINKEDIN, etc., & BLOGS

Table 5
WEBACCESSPRO CUSTOMERS

CHARACTERISTICS	B2G CUSTOMERS	B2B CUSTOMERS
MODE OF BUYING	Via floating tenders Via GeM (Government e Marketplace)	Website Digital Marketing initiatives
PREFERRED MODE OF COMMUNICATION	Prefer to meet in person	Open to WebEx interactions to reduce time consumed
BUYING NEEDS	Need to recognize cyber-threat and form policies	Understand product need as they are accountable to their customers

Table 6
WEBACCESSPRO EMPLOYEES

EMPLOYEES	NUMBER	REMARKS
Administrative Staff	15	-
Sales & Marketing	10	Includes sales force members who would travel to garner orders
Technical Staff (Auditors, Engineers, etc.)	65	Out of which, 15-20 would often stay on client premises, to ensure functioning of the equipment
Managerial and C-level	10	-

Employees		
	Total = 100	

Table 7A WEBACCESSPRO BALANCE SHEET AND PROFIT & LOSS STATEMENT			
($1=INR70)	**WEBACCESSPRO PRIVATE LIMITED**		
	BALANCE SHEET AS ON 31st MARCH, 2019		
Particulars		**Figures at the end of the Current reporting period (INR)**	**Previous Year (INR)**
I.	EQUITY & LIABILITIES		
1)	Shareholders' Funds		
	a) Share Capital	5712000	5700000
	b) Reserve & Surplus	7584628	50261978
		13296628	55961978
2)	Share Application Money (pending allotment)	0	0
3)	Non-Current Liabilities		
	a) Long Term Borrowing	24000000	33697968
	b) Other Long Term Liabilities	0	0
	c) Long Term Provisions	0	0
		24000000	33697968
4)	Current Liabilities		
	a) Short Term Borrowings	27726210	6661653
	b) Trade Payables	18585972	1989411
	c) Other Current Liabilities	3504997	9686936
	d) Short Term Provisions	0	0
		49817179	18338000
	TOTAL	87113807	107997946
II	ASSETS		
1)	Non-Current Assets		
	a) Fixed Assets		
	Tangible Assets	4844951	62733073
	Intangible Assets	0	0
	Capital Work in Progress	2780654	0
		7625605	62733073
	b) Non-Current Investments	0	0
	c) Long Term Loans & Advances	0	0
	d) Other Non-Current Assets	0	0
		7625605	62733073
2)	**Current Assets**		
	a) Inventories	0	0
	b) Trade Receivables	0	32348640
	c) Cash & Cash Equivalents	7318742	3265269
	d) Short Term Loans & Advances	72169460	9650964
	e) Other Current Assets	0	0
		79488202	45264873
	TOTAL	87113807	107997946

Table 7B WEBACCESSPRO BALANCE SHEET AND PROFIT & LOSS STATEMENT			
($1=INR70)	**WEBACCESSPRO PRIVATE LIMITED**		
	STATEMENT OF PROFIT & LOSS FOR THE YEAR ENDED ON 31st MARCH, 2019		
Particulars		**Figures at the end of the Current reporting period (INR)**	**Previous Year (INR)**
A)	REVENUE		
i)	Revenue from Operations	18,09,82,921	10,93,52,215
ii)	Other Income	11,77,162	8,92,261
		18,21,60,083	11,02,44,476
B)	EXPENSES		
	Purchases	7,54,49,467	1,85,03,355
	Employees' Benefit Expenses	7,26,70,903	5,84,18,079
	Finance Cost	38,50,985	64,65,519
	Depreciation & Amortization Expenses	26,70,607	19,53,278
	Other Expenses	3,14,88,615	3,12,89,414
		18,61,30,577	11,66,29,644
	Profit before Exceptional & Extraordinary Items		
	(A)-(B)	-39,70,494	-63,85,168
	Exceptional Items	-	-
	Profit before Extraordinary Items	-39,70,494	-63,85,168
	Extraordinary Items	-	-
	Profit Before Tax	-39,70,494	-63,85,168
	Tax Expenses		
	Tax for Current Year	-	-
	Less: Adjustment for Previous Year Provision	-	-
	Net Current Tax	-	-
	PROFIT AFTER TAX FOR THE YEAR	-39,70,494	-63,85,168