DigiServe Forensics

"From Chaos to Clarity - Digitally Served"

Danielle Caplinger
dcapl002@odu.edu
(434) 200-0441

Table of Contents

Executive Summary

In today's technological society, almost every business relies on technology to increase efficiency, operate, and provide necessary services to their customers. With this new reliance on cyberspace, though, comes an increased risk for cybercrimes and incidents that can have crippling damage to small-to-medium sized businesses (SMBs) that don't have access to in-house or retained digital forensics experts. My business, DigiServe Forensics, is designed to make this increasingly prevalent problem easily solvable. We do this by providing immediate access to automated professional digital forensics triage, evidence analysis and documentation, and reporting based on current regulations and legal requirements. On their own, most businesses do not have the resources to have in-house personnel to handle this or to hire a retained digital forensics firm. With DigiServe, however, businesses need to; they can instead use our product to respond efficiently when cyber incidents happen while complying with all necessary legal or insurance requirements and minimizing the financial or operational impact such an incident can cause.

At DigiServe, our mission is to provide immediate, efficient, and professional digital forensics support services to SMBs. We turn digital chaos into clarity, one incident at a time. DigiServe Forensics' vision is to change the technological landscape, making digital forensics affordable and accessible for every business' incident needs. DigiServe Forensics will be headquartered in Charlottesville, Virginia as it is a hub between major east coast technological capitals in the DC-Maryland-Virginia (DMV) area. Due to its digital nature, services will be able to be administered virtually for clients across the country and eventually, globe.

By combining automated triage, digital evidence analysis and documentation, insurance reporting, and legal or compliance regulatory guidelines, DigiServe will be the one-click service for SMBs facing a cyber incident without breaking the bank. Its automation and evolving responses to new cyber threats will allow DigiServe to scale rapidly across industry and location to remediate cyber incidents across cyberspace.

Business Description

DigiServe Forensics is an on-demand digital forensics service platform for SMBs that are victim to cyber incidents or breaches. DigiServe does things differently by separating itself from the traditional managed service providers (MSPs). Rather than being continuous support, we act as a singular scalable platform that is only activated when necessary to automate the necessary processes needed immediately after a breach is detected. This platform includes post-incident triage, recovery operations, evidence preservation, data analysis, incident reporting, and verified regulatory compliance requirements documentation.

Our target market is for small-to-medium sized businesses (SMBs) that do not have the resources for in-house digital forensics personnel or a budget necessary to keep an external firm on retainer. These businesses often are at an increased risk for cyber threats, and as such, are in need of these kinds of services despite the lack of resources allocated towards them. DigiServe's pricing model solves this by allowing for an incident-based pricing scheme with optional subscription monitoring for post-breach assurance. In addition to flexible pricing, DigiServe's have a unique strength in the platform's ability to evolve to cyber threats as they emerge, giving clients reassurance that they are as up-to-date as possible.

DigiServe's Forensics' value proposition lies in its ability to turn digital chaos into forward-focused clarity. A cyber incident can be crippling to a small business, and we make that risk mitigatable for when the inevitable does happen. By empowering these businesses to respond quickly, simply, and with the professional expertise of digital forensics experts through a unified platform, DigiServe Forensics adds value back to every SMB facing the possibility of a cyber incident.

Organization and Management

DigiServe Forensics' organizational structure will be as a Limited Liability Company (LLC) headquartered in Charlottesville, Virginia. The LLC structure will restrict the owner's liability from business liability while also allowing for flexibility in management structures. These benefits will be extremely useful for a service-based technology company like DigiServe where legal protections and adaptability are paramount.

DigiServe Forensics will operate with a specialized leadership team to include a CEO, CTO, Director of Operations and a Lead Digital Forensics Specialist. As founder, I will also take over as Chief Executive Officer to lead the strategic direction and growth of the company as well as fostering partnerships with MSPs and other partner clients. With my knowledge of digital forensics, risk management, and automating complex IT systems, I'll be able to drive the company forward on goals with the necessary experience. The Chief Technology Officer (CTO) will be responsible for overseeing the platform's development from a technical standpoint including automation tools, integration with new forensic techniques, and adapting to emerging cyber threats. They will work closely with the Lead Digital Forensics Specialist to make sure the platform is adhering to proper digital forensics protocols and adheres the necessary legal, compliance, and regulatory standards. The role of Director of Operations will handle the day-to-day of client onboarding, incident workflows, and subscription monitoring.

As DigiServe grows, a dedicated Compliance Manager, and Cyber Insurance Litigator will be needed. Additionally, support staff of software engineers, customer representatives, and forensics specialists can be onboarded as needed. However, keeping the leadership team small at first will allow for a more flexible DigiServe that can scale rapidly while maintaining the high-quality service needed for such work.

Business Goals

At its core, DigiServe's Forensics has the business goal to become the leading on-demand digital forensics platform for SMBs through high-quality, efficient and accessible services. By doing so, we can close the gap between a cyber threat and cyber response to keep businesses more secure.

As far as short-term goals from inception to the first two full years of operation, DigiServe Forensics has identified a few strategic goals:

- Launching the DigiServe platform to have automated triage, collection, and reporting capabilities.
- Aligning infrastructure to CMMC guidelines necessary to operate with clients that handle government information.
- Build strategic partnerships with Managed Service Providers to grow referral rates.
- Strengthen credibility with industry certifications, compliance requirements, and partner MSPs and digital forensic integrations

Long-term goals for the third year of operations past five years include:

- Expanding capabilities to include AI-enhanced analysis (where regulatory feasible) and constantly evolving automation and threat detection as cyber threats emerge.
- Scaling nationally and increasing legal integrations to handle international clients.
- Grow the forensic engineering teams to handle higher demand for complex automation.

Products & Services

Our core offering will be the DigiServe Forensics Platform that will handle the base functions that are necessary to conduct a digital forensics investigation post-incident. This will include evidence preservation like imaging, chain of custody, and artifact collection as well as log analysis, timeline reconstruction, and incident maps. All of this will be done via automation inside the platform that can then create forensic reports that comply with whatever user-selected legal or insurance requirement is necessary. During this process, the client will be informed of standard action-items to remediate incidents and vulnerabilities based on all of these findings. The production cost for this is predicted to be about eight to fifteen dollars per endpoint (depending on type of endpoint) to account for cloud processing, licensing, encryption and bandwidth costs, and compute times. To account for production cost as well as personnel cost to keep the platform as high in quality as possible, the sale price will be $150 per endpoint with bigger systems having the ability to bundle as pricing metrics are better understood.

A supplementary offering will be post-incident forensic monitoring service called DigiServe Forensics Monitoring. This will conduct continuous log reviews and anomaly detection based on the findings by the platform as well as follow-up forensic checks. This model can be done as a subscription at the monthly, quarterly, or annual levels to allow SMBs to be assured their systems are secure post-incident. The production cost of this would be estimated at ten to twenty dollars per endpoint per month depending on the endpoint and incident-type. As such, sale price will be $75 a month with a 8 and 12 percent discount, respectively, for quarterly and annual subscriptions.

DigiServe will work based on a proprietary agent that can be deployed to a system once a system is infected and clients buy the product. It will be able to forensically image the system to account for legal requirements and forensic best-practices and make copies of relevant artifacts that the platform can then use to triage, analyze, and report accordingly. Chain-of-custody will be handled based on built-in hashing capabilities and secure cryptographic chains. Unique features of the DigiServe product line will be a lack of disruption to operations while handling forensic analysis, as well as its scalability and accessibility to SMBs across industries.

Market & Industry Analysis

The digital forensics and incident response (DFIR) industry has expanded quite quickly in the last few years due to the increase in cyber incidents and cybercrimes, specifically against SMBs. However, most products in this industry only address one facet of the overarching situation: incident response, vulnerability remediation, evidence collection, artifact analysis, or reporting. There is not a single platform that can handle all of these, and most are using subscription-only models that DigiServe will not require. Competitors like these include Magnet Forensics, Oxygen Forensics, and SentinelOne. There is additional competition from traditional digital forensics firms that tend to cater to larger companies and are held on retainer. Based on these differences when compared to DigiServe, and many of these competitors being out-of-target for our intended market, DigiServe Forensics is in a unique position to not have any true competition.

The key demographic for DigiServe customers will be in small-to-medium sized businesses that operate with limited IT budgets or even contract out their IT staff. These organizations tend to only have 10-300 employees, but are at an increased risk for cyber incidents. Customers that handle sensitive customer data including financial, health, proprietary, or controlled unclassified information (CUI) are the niche SMBs that we will cater most towards. Their needs that we can fulfill will be the need for quick and compliant evidence preservation and incident response but cannot afford a full-time digital forensics staff in-house or on retainer. The key sectors that these SMBs fall under would be healthcare clinics, smaller law firms, local government contractors, small e-commerce businesses, manufacturing companies, and any SMB that has a cyber insurance requirement necessitating a digital forensics plan.

Due to its scalability from being an automated, cloud-based delivery model, DigiServe Forensics has tremendous growth potential. Once the agent and analysis algorithms are completed, the service could scale to thousands of endpoints practically immediately with minimal new operational costs. Growth will be entirely determined at that point by how quick cyber threats emerge, and DigiServe can add the necessary responses to our automation.

Marketing & Sales Strategy

DigiServe's target audience is at the small-to-medium sized businesses (SMBs) that do not have the resources for traditional digital forensics offerings. Additionally, managed service providers (MSPs) will be a secondary audience if they need forensic support of the same nature. MSPs wanting to offer digital forensics services through our platform will also be a target market as we scale. Customers will be able to purchase DigiServe's platform and monitoring services directly through our web portal or through reseller distribution with MSP or insurance partners. This will allow for a one-time instant download of the forensic agent.

Our main promotional and sales strategies will rely on our transparent, efficient, incident-based pricing with sample forensic reports to demonstrate quality. Lead generation can be done through traditional tech industry practices like educational resources, webinars, and tech expos. Discounts and incentives will be applied for MSP or insurance partners based on referral generation. Persuasion strategies will showcase the affordability of the platform when compared to traditional forensic firms while highlighting its ease and speed of use. The ability to customize reports based on insurance, regulatory, or other compliance requirements will also be emphasized. Testimonials and case examples will be crucial in these areas.

For marketing, search engine optimization content and LinkedIn advertising while be the standard for traditional marketing. Educational webinars, posts, guides, and resources can be used to spread name-recognition as well as increase brand credibility. Being present at cybersecurity, MSP, cybercrime, and insurance tech events will also be integral to this marketing strategy. Social media campaigns would consist of incident response awareness as well as showcasing customer reviews and simulated demonstrations of the tools.

Funding Request

DigiServe Forensics is seeking an initial funding request for $75,000 to support platform development, base infrastructure, and early-stage operations as clients are onboarded. This funding will be responsible for the infrastructure costs and personnel costs to build the platform as well as base marketing to draw in prospective customers.

A cost breakdown for product development would be $30,000 for a contracted software engineer that can do what I could not build alone. This engineering effort will build the forensic collection agent that supplies information to the platform and triggers automation workflows, logs, report generation, and ensures high quality and security. Digital forensics tools that will be integrated into this agent will be primarily open-source, so the only costs associated with those would be in compute power. From an infrastructure perspective, costs are predicted to grow to $20,000 in the first year to handle cloud hosting and infrastructure that can handle backend functions for the platform as well as storage. Since encrypted storage, chain-of-custody requirements, and law enforcement regulations require higher compliance standards, this infrastructure must be built and assessed to those standards, requiring a higher cost.

From our initial request, $12,000 will be allocated towards marketing and acquisition using efforts defined in our marketing and sales strategy. Funds will be used for website and client portal development as well as basic content production. This will then be used for Search Engine Optimization and LinkedIn ads that will also be budgeted under this category. An additional $8,000 will be set aside for legal and administrative costs related to forming the business, filing trademarks and patents, and an initial legal review. This will allow us to comply with necessary legal requirements before engaging with MSPs and insurance agencies. The remaining $5,000 will be set aside as a buffer for cost overruns and a contingency in case technical requirements need to change quickly. This will ensure an efficient and adaptable starting phase that emphasizes security and reliability.

Appendix

Flow Showing traditional DFIR process versus DigiServe: