

Watchman ●

BUSINESS PLAN 2024



TABLE OF CONTENTS

| | |
|---|----|
| 1.0 Company Overview | 3 |
| 1.1 Company Profile | 3 |
| 1.2 Company Vision and Mission Statement..... | 3 |
| 1.3 Company Offerings..... | 3 |
| 1.4 Target customer profiling | 5 |
| 2.0 Industry Analysis | 7 |
| 2.1 SWOT Analysis | 7 |
| 2.2 Porter's 5 forces analysis | 8 |
| 3.0 Marketing Plan..... | 9 |
| 3.1 4 P's Marketing Mix | 9 |
| 4.0 Operations Plan..... | 10 |
| 4.1 Key operational processes..... | 10 |
| 4.2 Recruitment Plan..... | 11 |
| 5.0 Financial Plan..... | 13 |
| 5.1 Revenue Model | 13 |
| 5.2 Financial Highlights..... | 14 |
| 5.2.1 Income Statement..... | 14 |
| 5.2.2 Cash flow | 16 |
| 5.2.3 Balance Sheet..... | 16 |
| 5.2.4 Breakeven analysis..... | 17 |
| 5.3 Funding requirement and use of funds..... | 19 |

1.0 COMPANY OVERVIEW

1.1 COMPANY PROFILE

Watchman, established in 2024 and headquartered in Chicago, USA is a pioneering cybersecurity firm dedicated to providing advanced, cloud-based vulnerability monitoring solutions. The company specializes in a comprehensive service that emulates an alarm system for information systems, scanning continuously for vulnerabilities, alerting IT managers with actionable intelligence, and offering tools for rapid response to cyber threats.

Watchman sets itself apart in the cybersecurity market with its innovative use of advanced algorithms and real-time monitoring capabilities, tailored specifically to the unique challenges of the American market where it initially focuses.

1.2 COMPANY VISION AND MISSION STATEMENT

Vision

"To be the global leader in cybersecurity, safeguarding the digital landscape by pioneering innovative solutions that protect businesses and empower them to thrive in an increasingly connected world."

Mission

"To be a model in a rising industry of the USA."

1.3 COMPANY OFFERINGS

Key services include real-time alerts, risk prioritization, Proof of Concept (PoC) demonstrations, and domain name monitoring to prevent cybersquatting and protect online reputation. However, more details of the core offerings of the company include:

Table 1 - Core offerings of the company.

| | |
|-----------------------|---|
| Continuous Monitoring | Watchman excels in continuous monitoring of clients' information systems to detect vulnerabilities and security gaps. This service ensures that |
|-----------------------|---|

| | |
|--|---|
| | businesses are always aware of their security stance and can react promptly to potential threats. |
| Real-Time Alerts | Users receive instant alerts when new vulnerabilities are detected, enabling them to take immediate action. This feature is essential for maintaining high levels of security and ensuring that all systems are protected from emerging threats. |
| Periodic Reports | Detailed and customizable reports are generated periodically, providing businesses with a comprehensive view of their security health over time. These reports are invaluable for auditing purposes and for tracking the effectiveness of security protocols. |
| Patch Management | Watchman provides tools and support for effective patch management, helping businesses apply security patches and updates promptly. This service is crucial for protecting against vulnerabilities that could be exploited by cyberattacks. |
| Proof of Concept (POC) | The POC feature offers real-life demonstrations based on current vulnerability trends, helping IT teams understand and mitigate risks effectively. These demonstrations serve as valuable learning tools for improving security measures and response strategies. |
| Phishing and Security Patch Management | Beyond traditional vulnerability scanning, Watchman extends its monitoring to include phishing attempts and the management of security patches. |

| | |
|--|---|
| | This rounded approach ensures that multiple facets of cybersecurity are addressed, from direct cyber threats to human-factor vulnerabilities. |
|--|---|

1.4 TARGET CUSTOMER PROFILING

Watchman's cybersecurity solutions are designed to cater to a broad range of industries and organizations that require robust, real-time monitoring and management of information system vulnerabilities. The following customer profiles illustrate the specific target segments:

1. Small and Medium-sized Enterprises (SMEs):

- Industry: Varied, including finance, healthcare, retail, and technology.
- Size: Businesses with 10 to 250 employees.
- Need: SMEs often lack the resources to maintain a large, specialized IT security department but face significant risks from cyber threats due to less sophisticated defense mechanisms.
- Benefit: Cost-effective, comprehensive cybersecurity solutions that allow SMEs to achieve a higher level of security without the need for extensive in-house expertise.

2. Large Corporations:

- Industry: Primarily in sectors such as finance, healthcare, and government, where data sensitivity is high.
- Size: Companies with more than 250 employees.
- Need: These organizations often face complex cybersecurity challenges and require advanced, scalable solutions that can be integrated with existing IT infrastructure.
- Benefit: Advanced threat detection, real-time alerts, and detailed reporting that integrate seamlessly into large-scale operations, enhancing existing security measures.

3. E-commerce Platforms:

- Industry: Online retail and services.

- Size: From emerging startups to established platforms.
- Need: High susceptibility to cyberattacks such as data breaches, DDoS attacks, and phishing due to the high volume of transactions and data handled.
- Benefit: Specialized monitoring tools that protect customer data and transaction information, maintaining trust and compliance with data protection regulations.

4. Educational Institutions:

- Industry: Schools, universities, and educational services.
- Size: Ranges from small private schools to large universities.
- Need: Need to protect student and faculty data and maintain secure online learning environments.
- Benefit: Easy-to-manage, comprehensive cybersecurity solutions that safeguard sensitive information and ensure uninterrupted educational services.

5. Government Agencies:

- Industry: Public sector entities that manage sensitive information and critical infrastructure.
- Size: Can vary from small local offices to national agencies.
- Need: High targets for cyber espionage and sabotage requiring top-tier security protocols.
- Benefit: High-level security solutions that ensure compliance with strict regulatory standards and protect against sophisticated threats.

6. Healthcare Providers:

- Industry: Hospitals, clinics, and healthcare systems.
- Size: All sizes, from small clinics to large hospital systems.
- Need: Protection of sensitive patient data and compliance with health information privacy regulations.

- Benefit: Robust security solutions that secure patient data against breaches, enhancing patient trust and regulatory compliance.

2.0 INDUSTRY ANALYSIS

2.1 SWOT ANALYSIS

Table 2 - SWOT Analysis

| Strengths | Weaknesses |
|--|--|
| <ul style="list-style-type: none"> Utilizes state-of-the-art vulnerability detection and real-time monitoring algorithms. Offers extensive services including alerts, reports, patch management, and PoCs. Competitive pricing model, making it accessible for SMEs and other budget-conscious organizations. | <ul style="list-style-type: none"> Limited brand recognition and customer base compared to established competitors. Currently limited operational scale which could affect service delivery and client acquisition in global markets. This can change with the desired funding requirement. Heavy reliance on cloud-based services may pose risks in regions with unreliable internet infrastructure. |
| Opportunities | Threats |
| <ul style="list-style-type: none"> Growing global concern about cybersecurity may lead to higher demand for monitoring solutions. Opportunity to form alliances with local and international IT companies to enhance service offerings. Can develop training programs for clients, adding an additional revenue stream. | <ul style="list-style-type: none"> The cybersecurity field is highly competitive with numerous well-established players. Rapid changes in technology and new types of cyber threats could outpace Watchman's current offerings. Potential for stringent regulations which could increase operational costs or affect business practices. Economic instability could reduce IT budgets and the willingness of companies to invest in advanced security solutions. |

2.2 PORTER'S 5 FORCES ANALYSIS

Table 3 - Porter's 5 forces analysis.

| Force | Impact | Reasoning |
|-------------------------------|--------|--|
| Threat of new entrants | Low | While the initial investment and technical expertise required to start a cybersecurity company can be substantial. Moreover, established relationships and advanced technology serve as barriers to new competitors. |
| Bargaining power of buyers | High | As cybersecurity becomes more critical, customers (businesses and governments) may demand more tailored solutions, competitive pricing, and high service levels. In a growing market with multiple providers, customers can often negotiate better terms. |
| Threat of substitutes | Medium | The primary substitutes for Watchman's services are in-house security solutions or different types of security technologies like AI-driven threat detection systems. The availability of DIY security solutions or bundled services from large IT firms could pose a competitive threat. |
| Bargaining power of suppliers | Low | In the cybersecurity industry, the suppliers are typically providers of technology platforms, hardware, and software. Given the global availability of these technologies, Watchman likely has multiple options to choose from, reducing the bargaining power of any single supplier. |
| Industry Rivalry | High | The cybersecurity market is highly competitive with both global giants and niche players. Competitive factors include pricing, innovation, reputation, and the range of services offered. |

3.0 MARKETING PLAN

3.1 4 P'S MARKETING MIX

Table 4 - 4 P's Marketing Mix.

| | |
|------------------|---|
| Product | Watchman offers a cloud-hosted cybersecurity solution that continuously monitors information systems for vulnerabilities, similar to an alarm system for digital infrastructure. The product includes features like real-time alerts, detailed reports on detected vulnerabilities, proof of concept (PoC) demonstrations, and patch management. Watchman differentiates itself from competitors by providing advanced algorithms for real-time monitoring and a significant reduction in false positives, which ensures continuous protection and efficient security management. |
| Price | Watchman employs a value-based pricing strategy that reflects the sophisticated nature of its technology and the high level of service it provides. |
| Place | The primary sales channel for Watchman is its digital platform, where customers can subscribe directly to the service. Watchman also expands its market reach through strategic partnerships with other companies that resell its licenses, thus leveraging their sales infrastructure and customer networks. |
| Promotion | Watchman adopts a diversified communication strategy to promote its services. This includes direct marketing efforts such as cold calling and emailing, which are designed to generate leads and build customer relationships. Public presentations and participation in digital exhibitions help to increase brand visibility and establish thought leadership in the cybersecurity domain. Strategic partnerships for license reselling also play a crucial role in promotional activities, expanding reach and influence across different markets. Additionally, the freemium model serves as a promotional tool by allowing potential customers to experience the product's value firsthand, thus facilitating conversions from free users to paid clients. |

4.0 OPERATIONS PLAN

4.1 KEY OPERATIONAL PROCESSES

Product Development and Management

The CEO of Watchman, who also serves as the Product Owner, is responsible for the strategic direction of the product's development. This includes defining the development roadmap based on direct customer feedback and industry benchmarking. The CEO prioritizes features and sets production deadlines to ensure the product continuously evolves to meet market demands while maximizing value.

System Architecture and Maintenance

The Chief Technology Officer (CTO) at Watchman oversees the system architecture. This role is crucial for maintaining the integrity and efficiency of the Watchman platform. The CTO ensures that deployments are executed flawlessly and that the system is optimized for resource usage. This position embodies the principles of the DevOps culture, utilizing its best practices and tools to streamline operations and enhance performance.

Software Development

The software development team at Watchman is split into two focused groups: backend developers and frontend developers. Backend developers are tasked with building and maintaining the technical infrastructure necessary for the application's operations. Frontend developers, guided by specifications from the UX/UI Designer, create intuitive and ergonomic graphical interfaces that enhance user interaction and overall experience.

User Experience Design

The UX/UI Designer plays a vital role in ensuring that the user interface is clear, navigable, and optimized for user journeys. This role involves continuous improvement of the interface design to enhance user satisfaction and engagement.

Sales and Marketing Execution

The sales team at Watchman is tasked with implementing the company's marketing strategies and driving customer acquisition. Their responsibilities include developing partnerships and directly managing client relationships to achieve specific sales targets.

Security and Compliance

The Chief Information Security Officer (CISO) is tasked with overseeing the overall security of the Watchman solution. This includes implementing necessary security tools and processes to protect the infrastructure and ensure compliance with various industry standards and requirements. The CISO also leads efforts in business continuity planning and risk management, crucial for maintaining trust and reliability among clients.

Customer Support and Service

Watchman provides continuous customer support to ensure clients can fully leverage the platform. This includes 24/7 technical support to address any issues that may arise, ensuring clients receive timely and effective solutions to their inquiries and problems.

4.2 RECRUITMENT PLAN

Objective:

Watchman's recruitment plan is designed to build a robust and agile team capable of driving innovation and growth in the cybersecurity sector. The focus is on attracting top talent in software development, system architecture, product management, and customer support to solidify Watchman's market presence in Africa and prepare for expansion into European and American markets.

Phase 1: Initial Team Strengthening

In the first year, Watchman's recruitment strategy prioritizes strengthening the core team with essential technical and management roles. Additional backend and frontend developers will be hired to enhance the product's scalability and user interface, respectively. A product manager will

be appointed to assist the CEO in roadmap development and feature prioritization. The customer support team will be expanded to ensure 24/7 service availability as the customer base grows.

Phase 2: Enhancing Expertise and Operational Efficiency

During the second year, the focus will shift towards enhancing expertise in security, compliance, and system optimization. Watchman plans to recruit a compliance officer, a cybersecurity analyst, and a DevOps engineer. These positions will ensure that the products not only meet industry standards but also lead in security and operational efficiency. A human resources manager will also be brought on board to streamline internal processes and foster employee development.

Phase 3: Strategic Expansion

The third year of recruitment will focus on preparing for strategic global expansion.

Recruitment Methods:

Watchman's approach will utilize a combination of online job portals, professional networking sites like LinkedIn, university partnerships for fresh graduates, and headhunting for senior positions. Referral programs will be implemented to leverage existing employees' networks, with incentives for successful placements.

Selection Process:

Candidates will undergo a multi-stage selection process starting with resume screening, followed by technical assessments and behavioral interviews to gauge cultural fit. Strategic roles will involve additional rounds of interviews with senior management.

Training and Development:

New hires will receive comprehensive onboarding to integrate smoothly into their roles, with ongoing training programs designed to keep the team updated with the latest cybersecurity trends and technologies. Regular feedback and career development sessions will be part of the effort to ensure continual growth and job satisfaction.

Monitoring and Adjustments:

The effectiveness of the recruitment plan will be regularly evaluated against company performance and strategic objectives. Adjustments will be made based on feedback from department heads and HR analytics, ensuring the recruitment strategy remains aligned with market conditions and company goals.

5.0 FINANCIAL PLAN

5.1 REVENUE MODEL

Watchman ensures a robust revenue model that supports both initial market penetration and sustainable long-term growth through a blend of strategies.

Subscription-Based Model:

Watchman employs a subscription-based revenue model, charging customers on an annual basis per machine. This approach provides a predictable and steady stream of income while allowing customers to budget their cybersecurity expenses effectively.

Freemium Model:

To attract new customers and allow them to assess the utility and effectiveness of the service without initial financial commitment, Watchman offers a freemium model. This strategy is designed to convert users to the paid subscription as they experience the benefits and capabilities of the system firsthand.

Value-Added Services:

Beyond the basic subscription, Watchman offers additional services that can generate extra revenue. These include customized reports, enhanced security consultation, and tailored solutions for specific industries such as finance and healthcare, which have stringent compliance requirements and may require more sophisticated security solutions.

Strategic Partnerships and Reseller Agreements:

Watchman plans to establish partnerships with other companies that can resell its licenses. This will help in penetrating markets where direct sales might be less effective and will provide a commission-based revenue from resellers. This broadens the market reach without corresponding increases in sales force expenses.

Scalability:

The cloud-based nature of the service ensures scalability, allowing the revenue model to easily adapt as demand increases. The infrastructure can support a growing number of users without significant additional investment, ensuring that increased revenue translates effectively into profit.

5.2 FINANCIAL HIGHLIGHTS

5.2.1 INCOME STATEMENT

Detailed breakdown of the finances is provided in the table below.

Table 5 - Income Statement.

| Description | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 |
|---------------------------------|-------------|-------------|-------------|-------------|-------------|
| Revenue | \$2,640,000 | \$3,300,000 | \$4,125,000 | \$5,156,250 | \$6,445,313 |
| Costs | | | | | |
| Salons | \$598,435 | \$658,279 | \$724,107 | \$796,518 | \$876,169 |
| Payroll | \$200,880 | \$220,968 | \$243,065 | \$267,371 | \$294,108 |
| Tour | \$158,960 | \$174,856 | \$192,342 | \$211,576 | \$232,734 |
| Real Estate | \$29,886 | \$32,875 | \$36,163 | \$39,779 | \$43,757 |
| Utilities & Telecoms | \$49,809 | \$54,790 | \$60,269 | \$66,296 | \$72,926 |
| Professional Services | \$27,000 | \$29,700 | \$32,670 | \$35,937 | \$39,531 |
| Insurance | \$12,960 | \$14,256 | \$15,682 | \$17,250 | \$18,975 |

| | | | | | |
|--|-------------|-------------|-------------|-------------|-------------|
| Technology & IT | \$59,400 | \$65,340 | \$71,874 | \$79,061 | \$86,967 |
| Marketing & Advertising | \$108,000 | \$118,800 | \$130,680 | \$143,748 | \$158,123 |
| Administrative Charges | \$10,800 | \$11,880 | \$13,068 | \$14,375 | \$15,812 |
| Compliance | \$75,600 | \$83,160 | \$91,476 | \$100,624 | \$110,686 |
| Maintenance & Updates | \$100,000 | \$110,000 | \$121,000 | \$133,100 | \$146,410 |
| Customer Support | \$100,000 | \$110,000 | \$121,000 | \$133,100 | \$146,410 |
| Team Training & Development | \$100,000 | \$110,000 | \$121,000 | \$133,100 | \$146,410 |
| Public Relations | \$50,000 | \$55,000 | \$60,500 | \$66,550 | \$73,205 |
| Sales Team Expansion | \$250,000 | \$275,000 | \$302,500 | \$332,750 | \$366,025 |
| Infrastructure | \$150,000 | \$165,000 | \$181,500 | \$199,650 | \$219,615 |
| Total Costs | \$2,081,730 | \$2,289,903 | \$2,518,893 | \$2,770,782 | \$3,047,860 |
| Net Profit | \$558,270 | \$1,010,097 | \$1,606,107 | \$2,385,468 | \$3,397,453 |

5.2.2 CASH FLOW

Table 6 - Cash Flow.

| Description | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 |
|-------------------------|--------------------|--------------------|--------------------|--------------------|---------------------|
| Cash Inflows | | | | | |
| Initial Funding | \$2,000,000 | \$0 | \$0 | \$0 | \$0 |
| Revenue from Operations | \$2,640,000 | \$3,300,000 | \$4,125,000 | \$5,156,250 | \$6,445,313 |
| Total Inflows | \$4,640,000 | \$3,300,000 | \$4,125,000 | \$5,156,250 | \$6,445,313 |
| | | | | | |
| Cash Outflows | | | | | |
| Operating Expenses | \$2,081,730 | \$2,289,903 | \$2,518,893 | \$2,770,783 | \$3,047,861 |
| Capital Expenditures | \$150,000 | \$165,000 | \$181,500 | \$199,650 | \$219,615 |
| Total Outflows | \$2,231,730 | \$2,454,903 | \$2,700,393 | \$2,970,433 | \$3,267,476 |
| | | | | | |
| Net Cash Flow | \$2,408,270 | \$845,097 | \$1,424,607 | \$2,185,817 | \$3,177,837 |
| | | | | | |
| Cumulative Cash | \$2,408,270 | \$3,253,367 | \$4,677,974 | \$6,863,791 | \$10,041,628 |

5.2.3 BALANCE SHEET

Table 7 - Balance Sheet.

| Description | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 |
|----------------------|--------------------|--------------------|--------------------|--------------------|---------------------|
| Assets | | | | | |
| Cash | \$2,408,270 | \$3,253,367 | \$4,677,974 | \$6,863,791 | \$10,041,628 |
| Accounts Receivable | \$660,000 | \$825,000 | \$1,031,250 | \$1,289,063 | \$1,611,329 |
| Inventory | \$0 | \$0 | \$0 | \$0 | \$0 |
| Equipment & Software | \$150,000 | \$315,000 | \$496,500 | \$696,150 | \$915,765 |
| Total Assets | \$3,218,270 | \$4,393,367 | \$6,205,724 | \$8,849,004 | \$12,568,722 |
| | | | | | |
| Liabilities | | | | | |

| | | | | | |
|-------------------------------------|-------------|-------------|-------------|-------------|--------------|
| Accounts Payable | \$520,433 | \$572,476 | \$629,724 | \$692,696 | \$761,966 |
| Long-Term Debt | \$1,000,000 | \$800,000 | \$600,000 | \$400,000 | \$200,000 |
| Total Liabilities | \$1,520,433 | \$1,372,476 | \$1,229,724 | \$1,092,696 | \$961,966 |
| | | | | | |
| Equity | | | | | |
| Contributed Capital | \$2,000,000 | \$2,000,000 | \$2,000,000 | \$2,000,000 | \$2,000,000 |
| Retained Earnings | (\$302,163) | \$1,020,891 | \$2,976,000 | \$5,756,308 | \$9,606,756 |
| Total Equity | \$1,697,837 | \$3,020,891 | \$4,976,000 | \$7,756,308 | \$11,606,756 |
| | | | | | |
| Total Liabilities and Equity | \$3,218,270 | \$4,393,367 | \$6,205,724 | \$8,849,004 | \$12,568,722 |

5.2.4 BREAKEVEN ANALYSIS

Assumptions and Calculations:

1. Fixed Costs: Sum of all annual costs that do not vary with the number of customers:

- Salaries: \$200,880
- Digital Trade Shows: \$598,435
- Real Estate Charges: \$29,886
- Utilities & Telecoms: \$49,809
- Professional Services: \$27,000
- Insurance: \$12,960
- Technology & Computer Science: \$59,400

- Marketing & Advertising: \$108,000
- Administrative Costs: \$10,800
- Compliance Expenses: \$75,600
- Maintenance Costs: \$100,000
- Customer Support: \$100,000
- Team Training and Development: \$100,000
- Public Relations: \$50,000
- Sales Team Expansion: \$250,000
- Infrastructure: \$150,000

Total Fixed Costs = \$1,922,770

2. Variable Costs: Considering minimal variable costs for the sake of simplicity, as the major costs have been outlined and appear largely fixed.

3. Revenue Per Unit: \$240 per machine annually.

Breakeven Analysis:

The breakeven point in units (subscriptions) can be calculated with the formula:

$$\text{Breakeven Point (units)} = \frac{\text{Total Fixed Costs}}{\text{Revenue Per Unit}}$$

$$\text{Breakeven Point (units)} = \frac{1,922,770}{240} \approx 8012 \text{ machines}$$

This calculation suggests that Watchman needs to secure about 8,012 annual subscriptions to cover all its fixed costs under the given assumptions. Any subscriptions beyond this number would contribute to profit, assuming variable costs remain minimal or are absorbed into the calculation.

5.3 FUNDING REQUIREMENT AND USE OF FUNDS

Total Funding Required: **\$2 Million**

Majority of the funds shall be dedicated to covering first year and start up costs as mentioned in the income statement. This strategic allocation of funds is designed to ensure robust development of Watchman's product and service offerings, effective market penetration, and a strong foundation for scaling operations while maintaining the highest standards of cybersecurity and client service.