Whitenoise Laboratories

Investment Proposal

Contact : André Brisson, Director Business Development

Telephone : 604-724-5094

Email : abrisson@wnlabs.com

www.wnlabs.com

Summary

Whitenoise technology has a unique, patented identity management, continuous authentication and verification, and encryption capability that differentiates itself from other competitor products. One single one-time-pad key is not only unbreakable but provides all network and data security controls.

The robust extensible core product will provide flexibility of future market expansion into telecoms, banking, medical, smart city and the military.

Introduction

This proposal outlines methods and costs of developing Whitenoise technology to meet the needs of current and future trends in cloud and mobile computing. It outlines a structure that leverages the large and growing existing cloud services user base as a means of rapidly gaining market share and producing significant ROI for investors.

The development costs of the technology forms only part of any investment proposal.

Technology

The Whitenoise technology is a unique Identity Management, authentication and encryption system that generates effectively infinite length (> 10^{18} Bytes) one-time pad (OTP) keys from a much smaller user key.

The nature of the OTP key makes it unbreakable by all currently known cryptographic techniques, and allows it to be exploited for user authorization, continuous verification, and network intrusion detection.

It is not susceptible to man-in-the-middle, side channel or botnet attacks. If implemented as intended, its use is seamless to the user.

Differentiators

Whitenoise Technologies
Total Information Security

Simple to deploy

One-time key download from server.

Efficient

Little power consumption, ideal for mobile devices.

Effective

No additional hardware, low cost of manufacture, high profitability.

Friendly

No additional passwords for users to remember.

Protected

Patented in all major economic zones (including China).

Vision

Develop a strong and flexible core security capability that can be applied to any network topology, or cloud service.

Position the product as a disruptive technology in the cloud services sector, and leverage a large (>300M) existing user base to generate initial cash flow.

Leverage design, incorporating future modules in order to create key differentiators in the market, and allow ongoing product development.

Ensure applicability to a broad range of vertical markets such as banking, medical, commercial, and developing networks, including smart cities, internet of things, etc.

Approach

Any security system must be applicable to modern distributed mobile working and static private networks. Whitenoise is capable of identity management, authentication and continual verification, and encryption, and works well across all mobile platforms including iOS, Android, Windows, and Blackberry, as well as desktop environments including Windows, Linux (popular in servers) and OS-X, a growing market.

The core library will be extensible. This allows development into new markets while also accommodating change, as new working modes develop in this dynamic technological area.

Market Development

The easiest market to leverage is the growing consumer and business cloud services sector. It requires little certification, and offers the fastest route-to-market with the quickest, and the highest, ROI.

In this light, Whitenoise is a hugely disruptive technology that creates hard security around existing incumbent products with large user bases, bypassing or excluding any existing systems in place, thus leveraging a huge user base with little effort.

This frees WNL from competing with FileLocker and similar companies who offer secure file cloud services to avoid server-based facilities with their obvious incumbent capital and overhead costs.

Market Development

Secondary development of Whitenoise equivalent services would rapidly follow, opening up the large SME market for private (non 3rd party) cloud and hybrid secure file services.

Future technological expansion into other markets will follow through subsequent development. Financial services, medical data, and military markets will require increasing levels of certification and will be penetrated in turn, as confidence and user base grows. These markets generally have longer lead times and as such, will eventually and naturally lead to an organic fast-growth path.

Go To Market

It is recommended that sales are made through the application (“app”) stores of the major computer companies. This minimizes overhead cost, with little need for infrastructure, advertising, etc., thus maximizing profitability (>80%). The cost is appropriately 30% of gross price.

The nature of the proposed market dictates leveraging social media and web-based marketing, build hacks, Google and Facebook ads, Twitter, etc. Employment of specialist social media and web marketing personnel is recommended to maximize the download profiles of app store offerings.

More details can be found in the section at the back of this presentation.

Massive Market

Name	Users	Notes
Dropbox	~170,000,000	Security Issues
Google Apps	54,000,000	Google quoted figures.
Microsoft 365	10,000,000	
Box	10,000,000	Similar to DropBox. Offers application building.

695M cloud business users by 2022 Gartner report

Cloud & Collaboration Costs

Name	Service	Cost per user per annum	Notes
Dropbox	Cloud-based files + 3rd party app integration	£114	Security issues
Google Apps	Files + SaaS Apps	£33	
Microsoft 365	Cloud-based files + apps (SaaS + local)	£100	
Box	Cloud-based file sharing	£94	
SharePoint + Yammer + Office 365	Collaborative	£75	Plus $7000 server license for SharePoint

Cost vs Market summary

Component	Indicative Development Cost	Target User Base(2014)	Notes
Core	$1,100,000		
DropBox	$300,000	200,000,000	Drop Box encryption $15
Box, Cubby etc.	$230,000	30-50,000,000	
Private disk storage	$420,000	200,000,000	DropBox like facility using open source integrated with Whitenoise designed for SMEs in US, UK and EU
Heuristics	$175,000	2,000,000	Add on for private or corporate systems

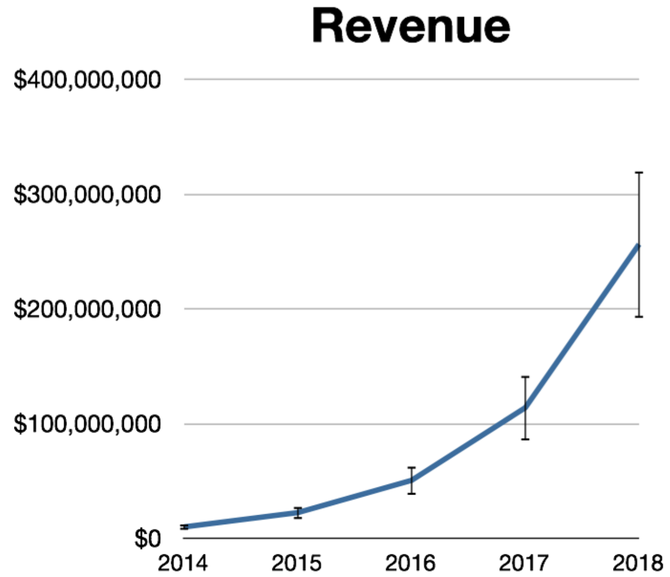
Revenue Growth

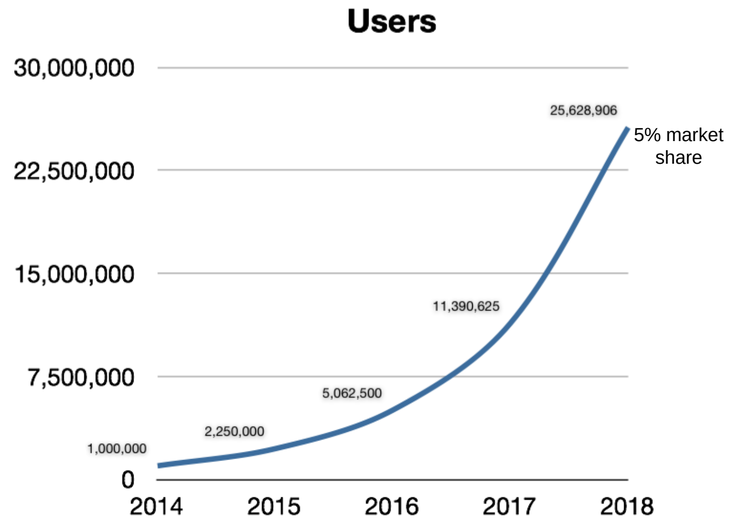
Projected 5-year revenue growth is anticipated for overall personal cloud services, based on conservative estimates of between 0.5 - 5% per annum market penetration and 50% user retention rate. Existing markets suggest an minimum application price of $10 per user (renewable per annum).

Overall user growth in the cloud market is estimated at 25% per annum.(Gartner)

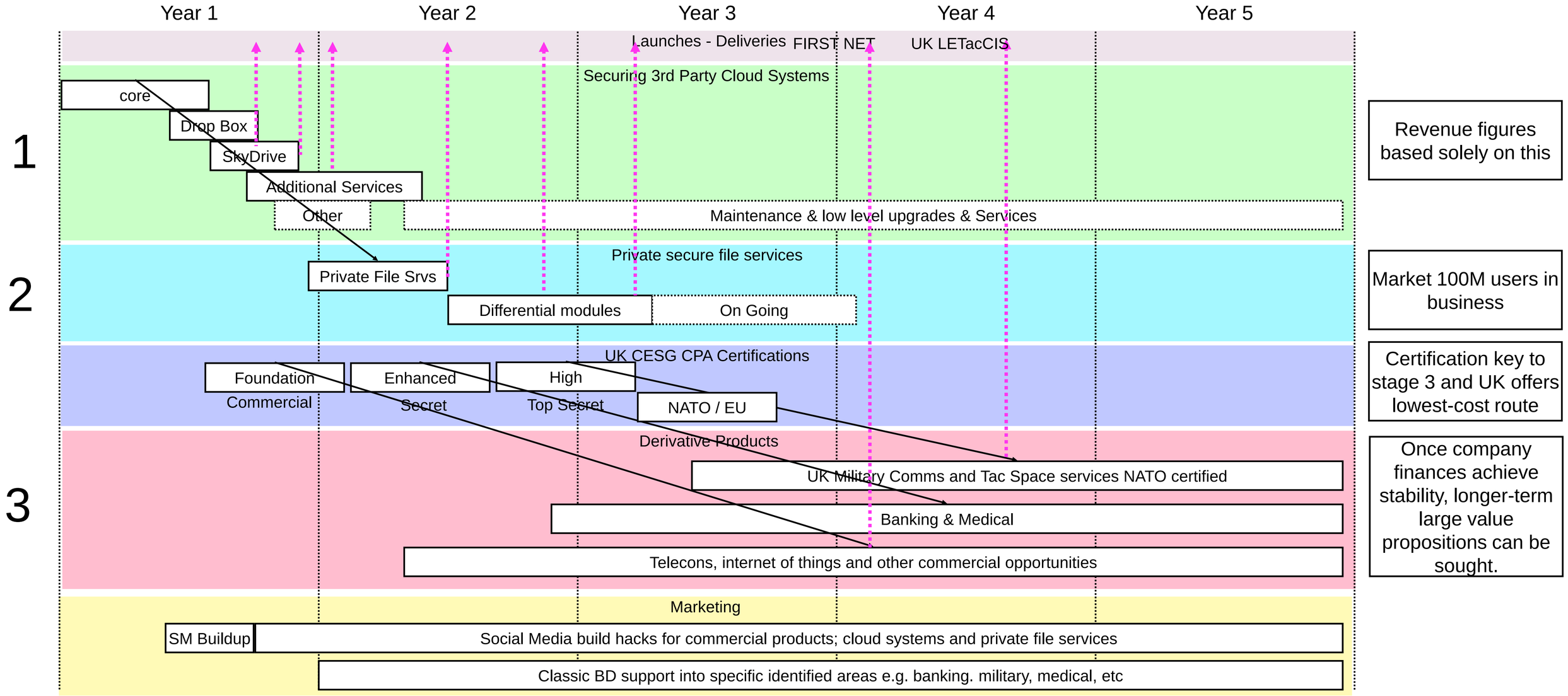
Approximately 30% (Google) of cloud services users are business-based. Leveraging these users with additional services could increase revenue by 30-50%.

An analysis of revenue potential in other, longer term markets should be undertaken.





Business Plan



Revenue figures based solely on this

Market 100M users in business

Certification key to stage 3 and UK offers lowest-cost route

Once company finances achieve stability, longer-term large value propositions can be sought.

References

The following persons can all supply technical references for the validity of Whitenoise capability. Contact details are publicly available or can be supplied on request.

Abbie Barbir - VP, Senior Security Architect, Bank of America – OASIS standards

Daniel Wevwrick - Communications Security Establishment – crypto mathematician

Proof of Concept Products

Solutions can be downloaded from the the following sites.

www.wnlabs.com

AT&T Certified Solution

ProgramBase

Whitenoise is available as shareware products for file and email encryption.

Investment

Item	Value
Product development costs, including early stage UK certification	$2M
Executive Board Expansion, Marketing, etc.	$1M
Total investment sought	$3M

Conclusion

Rapid development of a strong product, and leveraging of existing cloud markets, provide rapid ROI for investors with large upside potential. Large ROI with small market penetration minimizes risk of the relatively small investment necessary to develop a key product.

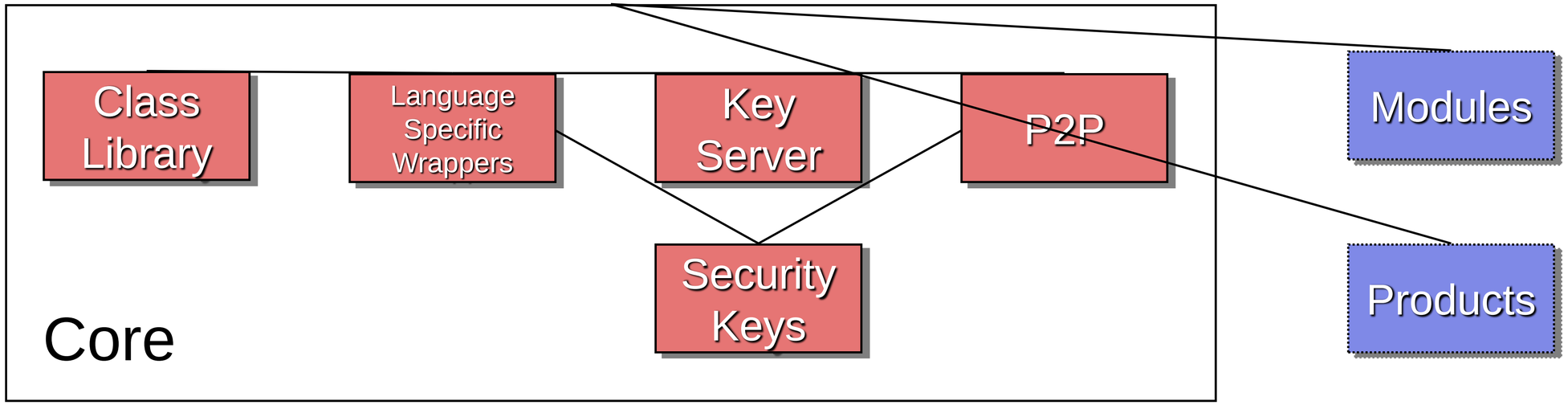
Once established, the company and product can develop in several directions, making use of new markets in both civilian and military spaces.

App Development

Cost Breakdown

Development

Core development is split into several key stages, each building on the capability of the previous one with some dependencies.



The final core capability will be a set of cross platform components (API, DLL, browser plug-ins, etc.), allowing rapid development of future work.

Class Library

C++ APIs

- Base Types
- Encryption & Decryption Classes
- Multithreading support
- Key generation, management, support
- DLLs
- UDP classes

Testing

- Against test rig
  (at contracted partner - www.wavefrontac.com)
- Performance testing
  (an offer has been presented by Rick Pierson of JTGlobal for testing in conjunction with banking partner - Rick.Pierson@jtglobal.com)

Documentation

Language-Specific Wrapper

Language-Specific Wrappers take the core library components and extend the capability to other major desktops:

- .NET - Windows
- Java - cross platform operation
- Objective C - OS X

and browsers:

- IE (versions 7-10)
- Chrome
- Firefox
- Safari

Key Server

Create a cross platform KeyServer with ability to add in additional security modules developed later, such as heuristic anomaly detection

- Windows
- Linux
- OS-X

Administrative Console for KeyServer management

- Browser-based
- Secure key distribution
- Mobile Apps (iOS, Android, Windows)

Security Keys

Develop proximity-based login using Bluetooth from mobiles. Integration of GPS and on-device biometrics including iris scans, fingerprints, face recognition, etc.

- iOS
- Android
- Windows

USB-based keys for failsafe

P2P Secure link

The P2P secure link is the basic networking capability of the system, allowing data to be moved across private and public networks (Internet), cloud systems, and ad-hoc distributed mesh networks.

Available on all major OS

- Windows
- Linux
- OS X

Additional Costs

It must be recognized that a development of this nature will not consist entirely of a few programmers in a room. To create commercial grade software, fully tested and with a ISO9001 QA assurance requires testing facilities, management overhead and, given the geolocation of the client, some travel and living expenses.

We have quoted for UK certification as a start. US certification may be required later after analysis. EU certification should be investigated.

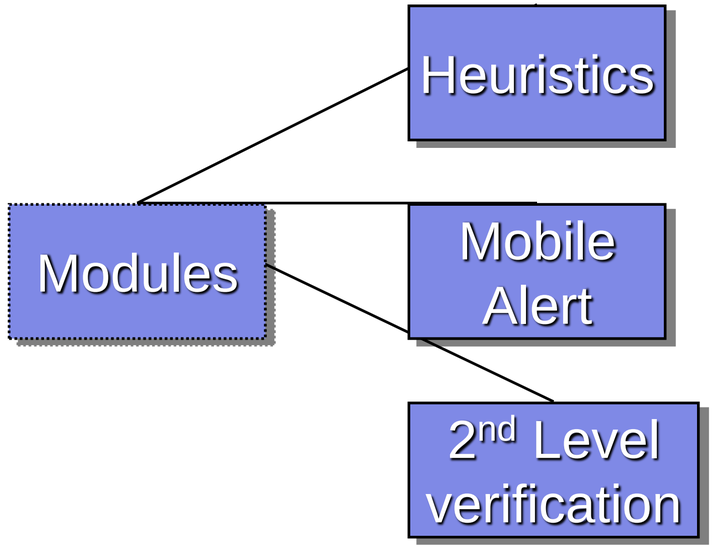
Costs - basic development

Component	Duration (Months)[1]	Cost £ GBP	Cost $ USD
Core Library	3	£138,438	$222,885
Language Specific Wrappers	2	£101,521	$163,449
Key Server	2	£110,750	$178,308
Security Keys	1	£57,693	$92,886
P2P Secure Link	1	£43,269	$69,663
Project specific h/w, s/w		£24,721	$39,801
Management & Support		£153,400	$246,974
Certification (UK)		£16,000	$25,760
T&L		£30,000	$48,300
TOTAL Basic Development	9	£675,792	$1,088,025

1. Duration is based on small team with contracted in specialists as required.

Modules

Our underlying philosophy of development is to allow extension of the basic capability, reflecting changes in market trends and technological development. One of our core beliefs is, “He who does not innovate dies.” The unique modular aspect of development allows the addition of differentiators and Key Selling Points to the product.



Heuristic AD

Heuristic Anomaly Detection is a type of development most prevalent in present day security systems. A pattern of life is built for each user that reflects their normal behavior. This allows for such things as outside influences, weekends, holidays, bad weather, geolocation, etc., and monitors network access. Access outside of these normal bounds will flag an alert to a supervisor.

Mobile Alert Monitoring

It is important that any security breaches are made known to those in authority as soon as possible. This module runs as an app on major mobile operating systems (eg., iOS7, Android), and links to the heuristics supervisor.

Second level verification

Although WN is secure, in the event of a stolen key being used and triggering an alert flag by the heuristics module, a second question and answer can be set up for user verification.

The question will accept two answers, one to be used under duress. The latter does not lock the user out of the system for safety reasons, but alerts a supervisor and gives access to dummy false data or adds warnings to messages, etc.

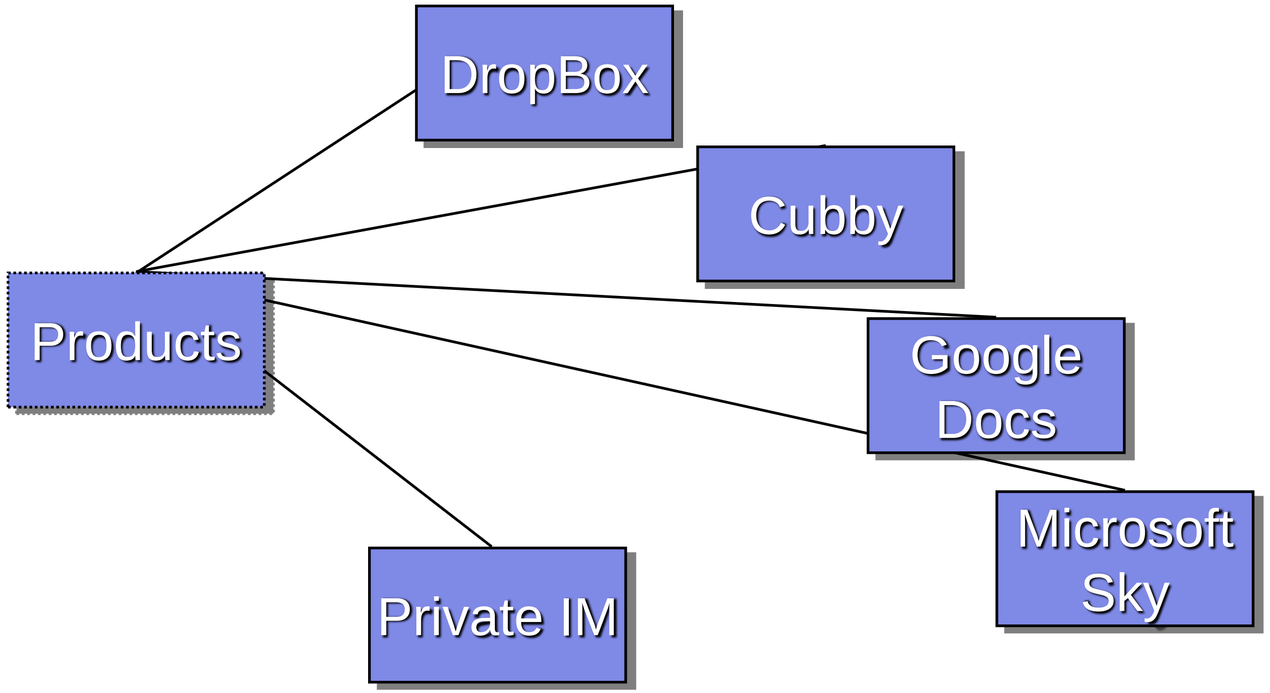
Costs - Modules

Module	Duration (Months)	Cost £ GBP	Cost $ USD
Disk Storage	4	£261,040	$420,274
Heuristic Anomaly Detection	variable	£104,677	$168,530
Mobile Alert Warning	1	£53,531	$86,185
Second Level Verification	1-2	£148,594	$239,236

These cost estimates are for example only, and will change if a full quotation is requested.

Products

The following give an indication of the potential costs of sample products that could be developed using the core system.



Commercial cloud service

Commercial cloud services are inherently insecure. In particular, Google has a business need to analyze client data. DropBox has had confidentiality issues in the past. Some services offer encryption at a cost, but is it truly safe?

This application creates a seamless front-end to the user's data, encrypting and decrypting on the fly.

P2P IM cross platform

Blackberry's famous IM service has now been revealed to be unencrypted on servers. We could offer a P2P IM service with total security and no servers. This does present some problems, such as knowing users' IP addresses in a variable mobile situation and may require backend capability to maintain these links but not store any data. The costs quoted is for software development only, and is very speculative at this stage.

WNL Products

The cost and effort of creating of WNL products such as disk encryption, file store, etc., is not dissimilar to the costs associated with the creation of a commercial cloud front end.

Costs - Applications

Application	Duration (Months)	Cost £ GBP	Cost $ USD
Commercial Cloud Front End		£181,467	$292,162
Cross Platform IM		£239,043	$384,859
Additional own products		See Commercial Front End	

These costs are an estimate, and will change if a full quotation is requested.

Route To Market

Commercial App-based systems

Social Media Hacks

Social Media Hacking

Social Media Hacking is a type of marketing that employs customer's social media contacts to increase market presence. It is particularly effective in the Apps market, where initial popularity and ongoing downloads are the key to success.

The principle is that you take more notice of what your friends are doing/using, rather than advertising. In a fragmented marketplace, social media connects like-minded people quickly. One person recommends a product to 10 others, 2 of which convert to sales. These 2 sales recommend the product to 20 others, which converts to 4 sales, etc. Referrals are the key.

Process

Stage 1: Pre-launch build up

Stage 2: Launch - social media and tech blogs, news outlets synchronized

Stage 3: Post launch - maintain referral at every opportunity, e.g. license renewal etc.

Pre-Launch

Generate website interest and encourage people to sign up. Support with tech blog articles, **Pinterest**, **DiggIt**, **LinkedIn**, **Facebook**, etc. all pointing to signup page on website.

Acquire email address for signup, while encouraging **Twitter** or **Facebook** logins to register interested users.

Target 10 - 30,000 sign-ups by launch.

Identify target tech blogs, tech news outlets, etc., ready to run articles on Day 1.

Launch

Launch on all platforms simultaneously.

Target all signed-up users. Offer free to first 5,000 users? Key is to rapidly grow user base.

Offer discount for referrals. Start at $25, offer $10 discount for full contact list referral. Create Incentives for grass-roots marketing efforts by users: $5 for SM referral or posting, $2 for a like or tweet, etc. This maintains our desired revenue stream even while offering discounts.

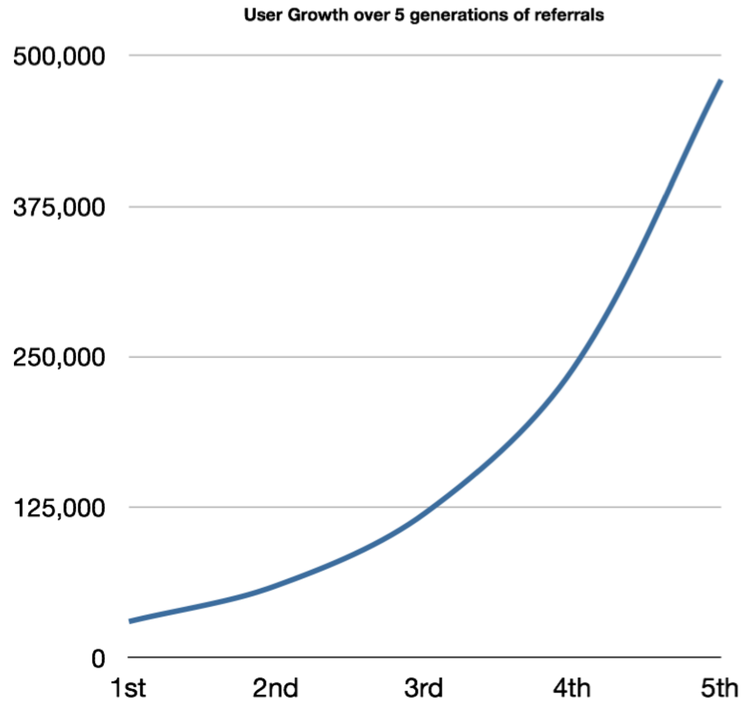
Media outlets may not run articles fast enough to meet the 1-week timeframe and so must be considered secondary to referrals.

User Growth

Social media hacking is key to creating substantial user growth during the important 1st week after launch.

App stores display new apps prominently for 1 week. Display is based on downloads thereafter.

4,000 downloads per week maintains an app in the Top 10 of the paid section in the Apple App store[1]. User base, word of mouth, and referral rate must sustain this.



1. http://techcrunch.com/2013/09/24/download-rate-for-top-ios-7-apps/

Technology note!

Dynamic Identity Verification and Authentication (DIVA) exploits the one time pad (OTP) characteristics of Whitenoise creating dynamic, continuous authentication and identity verification throughout a network session.

DIVA and Whitenoise work seamlessly with public key systems to fix their fatal flaws creating a two-channel-multi-authentication-factor framework. A hacker needs to break two different systems simultaneously, one of which is dynamic (DIVA).

Whitenoise and DIVA are usually used for Identity Management.

Whitenoise One time pad keys are unbreakable. Current encryption algorithms are proven to be insecure but with Whitenoise and DIVA you can continue to use your current encryption modules safely.

Investor Note!

Direct licensing to foreign governments/military

- one-time flat rate – non-commercial use i.e. $20 million small country

Direct licensing of WN as a random number generaror1 exclusively

- one-time in perpetuity flat fee

Use of Whitenoise to randomize biometrics on all devices

- Problem – biometrics create permanent identity vulnerabilities
- Whitenoise turns biometrics into a dynamic one-time-pad

•Note 1 Microsoft and PGP have indicated their intention to discontinue the use of the US NIST Random Number Generator. It is NOT random enough and is creating unnecessary security vulnerabilities. Whitenoise is the most random data source ever created, orders of magnitude more random than radio active decay. This provides a blanket licensing opportunity to both governments and global service providers. FULL PROPOSALS AVAILABLE UPON REQUEST!

.

Contact Information

Contact: André Brisson, Director Business Development

Telephone: 604-724-5094

Email: abrisson@wnlabs.com

www.wnlabs.com