iWebGate Limited (IWG) has developed a IT security software solution, intended to add a critical layer of security and significantly simplify the delivery of solutions across all networks. IWG has created a Virtual Services Platform (LaunchPad), which deploys a network of service in front of an existing network and its firewall. This new virtual network separates core networks from other dangerous networks via a virtual “reception area”. Network environments thus become safer with no direct access points and more control over access points. Additionally, IWGs technology can install secure containers on connected devices that ensure all applications connect to LaunchPad in a highly secure manner. Ideal for mobility initiatives, this establishes a vibrant app marketplace for third-party applications to be integrated and securely delivered across networks. This technological advancement could replace old-style Virtual Private Networks (VPNs) and relegate traditional firewalls to a secondary level of security. Given the large size of the IT security industry, IWG is in a position to establish itself as an industry standard for security and leverage off this fast growing market. Additionally cloud providers, like Telstra, is now capable of providing many Software-as-a-Service (SaaS) solutions to its customers, which were often too complicated and expensive to implement. IWG’s software overcomes this barrier and enables cloud providers to generate tighter security, more revenues and deeper customer relationships instead of over-the-top (OTT) providers. IWG is currently in advanced negotiations globally and has launched its product suite in Australia via agreements with Telstra. We believe there are numerous near and medium term catalysts for IWG but, given that the risks associated with the fact that the product is yet to be fully commercialised, we initiate with a Speculative Buy rating.

- **Operations Globally:** IWG has operations in Australia and the USA and most recently has expanded to Europe. The Company is at different stages of commercialisation in these geographies and has differing strategies in each, with Australia being the most advanced with its software products being available to Telstra serviced Small and Medium Businesses (SMB) via the partnership with AppDirect and the Telstra marketplace. IWG is in advanced stage of negotiation in the USA, with both government agencies and Universities. In Europe, IWG is at early stages with a leading European Telecommunications and Services provider, and hopes to establish itself at the cornerstone software technology for virtual segregation security and delivery of enterprise-ready applications.

- **Software products built synergistically:** IWG has built and developed its Virtual Segmentation Platform (LaunchPad – securely isolates core networks from direct exposure and provides strong access controls), Virtual Invisible Networking (Network Linkup – faster more secure connectivity tunnels than VPN) and Device Containers (Device Linkup – creates secure work environments across many different user devices). Given the modular nature of the software products, different users will request to implement different combinations of the software suite. We note that pricing is thus dependant on the final package assembled and the quantum of users, which has the potential to be very large, based solely off the current operations in negotiation.

- **Large and Growing IT security market:** The global IT security market spend is currently estimated at cUS$76.0bn and is set to experience double digit growth to cUS$173.0bn by 2020. This is driven by the increase in cyber-security incidents, which have increased globally from 3.4m incidents in 2009 to 42.8m incidents in 2014 and is expected to grow further.

- **Corporate:** IWG currently has c$3.2m of cash on hand, following the Share Placement in October of $2.0m, at $0.17/sh, and the debt facility draw down of $1.0m. Given the current quarterly cash burn of $1.5m, we estimate IWG will need to return to market within 3-6 months.
COMPANY OVERVIEW

iWebGate Limited (IWG) is a technology company, focussed on cyber and mobile security, which provides sophisticated network solutions to organisations of all sizes. IWG was founded in 2004 in Perth, Australia, has a global operations office in Maryland, USA and has recently established operations in Europe. The Company has won a number of prestigious awards, including the worldwide winner of the Global Security Challenge, and has earned the highest NIST Compliance rating awarded by CyerRx.

IWG’s software creates a new network communication environment that sits on top of, and in front of, the traditional firewall set-up. This acts as a virtual, secure and collaborative “reception area” for all connected networks. To compliment this innovation, IWG has also created an interlinking technology for connecting and commanding related devices, application and users to the network via this best practice design. This allows for the virtualised segmentation of connected networks.

The software enables organisations to connect, implement and manage 3rd party security and Software as a Service (SaaS) applications and procedures via IWG’s platform. IWG’s software is currently available through the Telstra Marketplace with imminent plans to rapidly expand its offerings in the US and Europe.

OPERATIONS

Australian Operations via Telstra Marketplace

IWG has had extensive development and beta testing with Telstra, spanning close to a year, which has proven successful. Subsequently the Company has working with many Telstra Channel Partners to provide its cyber-security services to potentially hundreds of thousands of Telstra customers, ranging from small to enterprise-level organisation, across Australia via the online marketplace. Telstra will actively promote IWG’s suite of services and products to its end user customers. The Company anticipates that the revenue share agreements will drive significant revenue growth in the current financial year and beyond.

European Pilot Programs

IWG has recently set up European operations and has begun discussions with pan-European service providers and major telecommunications organisations. IWGs products and services are currently undergoing extensive product evaluation at an unnamed global telecommunication company. The Company has also deployed a proof-of-concept of its technology in an effort to establish itself as the core component of the security framework for a pan-European service provider's software application platform.

US Expansion

In the USA, IWG is participating in three major Government agency tender processes as a preferred partner to a leading provider of IT security services to the US Federal Government. IWG has tendered for projects to provide secure communications and networking, data transfer/storage and remote access technology to three separate Federal Government agencies. These tenders are ongoing and an outcome for each project is expected early to mid 2016.
IWG is also expanding its technology to a leading North American University, where it provides network security services. Having successfully completed the first phase to provide its network services to the University system’s administration, IWG will now extend its services to encompass the University faculty, which may include the university’s students and alumni. If successful, this project will open up the opportunity for IWG to provide similar services to other US universities.

The Company also hopes to obtain final certifications with the region’s largest telecommunications company and the leading hybrid cloud provider. It has also secured "proof of concept" pilots beginning in November 2015 to launch enterprise solutions for Windows and Android devices.

PRODUCTS

IWG’s software establishes software abstraction layers at the network perimeter, between Internet connections and across user devices. This creates an additional layer of protection for IT networks, ultimately relegates firewalls to a secondary security asset and replaces, thus making obsolete, the old-style Virtual Private Networks (VPNs) within most networks.

IWG has created three core synergetic technological products, namely LaunchPad, Network LinkUp and Device LinkUp.

The LaunchPad software creates a “Virtual Network of Services” or Virtual Segmentation Platform (VSP) between a primary network and all other networks. This powerful software creates an abstraction layer which uses the principle of separation to re-define a networks perimeter. This creates a funnel point or virtual reception area where all connected devices and networks interact. The virtualisation of these network services allows the virtual networks to be hosted on the cloud and thus allows authorised network administrators easy and secure access remotely from a range of connected devices.

Network LinkUp establishes a secure connection between LaunchPad and a remote network. Customers use LaunchPad to establish “security zones” in cloud environments and seamlessly connecting them to on-premise and/or other cloud networks using Network LinkUp.

Device LinkUp is the container for an array of computer and mobile devices. Once installed, the container ensures a device securely connects to any given network via Network LinkUp and/or the LaunchPad. Additional security features include encryption at rest and in transit, multi factor authentication and remote retrieving of application data. This is becoming a greater need in many organisations given the increase in connected mobile devices and the rise of Bring Your Own (BYO) devices, capable of compromising traditional networks with multiple touch points.
**iWebGate Workspace Suite**

The IWG Workspace Suite (WSS) is the collective name for IWG’s three products.

Integrating other security and business applications into IWG’s technology transforms them from “enterprise friendly” products into “enterprise ready” solutions. The result is improved security, deployment processes and distribution capabilities. Currently, IWG is offering three WSS solution offerings through Telstra and its channel partners. These solution offerings can be deployed individually or together, and supports a user’s device of choice, using any network and cloud.

This blend of greater security and collaborative capability creates new commercial capacity for any organization without altering or interrupting existing ICT infrastructure.

**Figure 3: iWebgate Workspace Suite**

VPN LP establishes an encrypted Virtual Local Area Network (VLAN) over a multi peer-to-peer (P2P) connection framework. VPN LP’s strength is the ability to easily create layered tunnels (VLANs) between computer devices and networks using software only. This new form of VPN secure connectivity obfuscates the true identity and location of the virtual network across private and public networks like the Internet.

Desktop LP facilitates remote desktop services (RDP, SSH and VNC) across a wide range of computers and mobile devices. Additionally, Desktop LP supports concurrent connections via gateway services to ensure network isolation for on-premise and remote location usage.

Proxy LP includes a number of proxy services integrated with multi factor authentication and certificate management tools. It ensures web services are never directly exposed to internal and external networks. Cost and complexity is significantly reduced when activating Multifactor Authentication and single server certificates to protect entire network servers.

### Pricing

Given the modular nature of the software products, different users are likely to request to implement different combinations of the software suite. We note that pricing is, thus, dependant on the final package assembled and the quantum of users.

Using the package and pricing shown in Figure 4 as an example; a 100 person organisation would spend $6,500 per month for IWG’s software and licences. This is notably cheaper than contracting a managed Security Services Provider (MSSP) or using some of the incumbent software available in the market.
Using this pricing example we could extrapolate the large revenue potential for IWG based just on its current operations. Telstra’s marketplace puts IWG’s software in front of thousands of organisations which would have hundreds of employees (on average) each. Replicating this Telstra Agreement in Europe should allow for a significant increase in the potential number of users, given the size of the market. Additionally, securing the US Government tenders and the US University has large potential given the number of government employees (c.2.8m workers in 2009) and student and alumni at the institution (c.5.0m).

Figure 4: Pricing Example

VALUE PROPOSITION:

- **Internet Services Providers (ISP):** to the ISP, like Telstra, IWG provides a platform that allows it to sell Software-as-a-Service (SaaS) to its existing customers where it has not been able to do previously. The ability to provision these services remotely opens up a revenue channel that has been beyond the scope of most ISPs globally due to the very difficult and costly nature of installing and configuring these services. The ISP creates a large revenue opportunity from a customer base where they are seeing otherwise diminishing margins from traditional offerings (landline, mobile, internet, data). The IWG platform locks in existing customers but also allows for an ability to win new customers that can easily be spun into the ISP’s cloud network. This is extremely valuable territory to any ISP, as the architecture and challenges are ubiquitous globally.

- **The Channel Partner:** for the channel partner linked directly to the ISP or third party groups, a new product sales channel is being established where it can get trailing revenues on a monthly basis. Currently, trailing revenue products have been non-existent for channel partners of ISPs, due to products traditionally being one-off purchases, rather than plan or subscription based. For instance, the margin to a channel partner for the sale of an iPhone would be in the order of $20, whereas selling that product with an attaching monthly rental option becomes extremely compelling. IWG has stated that through the first two months of educating the channel partners on the product; the interest in deployment to its customers has been very positive.

- **The Consumer:** the IWG platform offers the very highest level of network security that is available to every business, large or small. The charging model is such that the customer pays a monthly subscription for the services deployed on the network that have been deployed remotely. This removes the high-cost nature of installing expensive remote access, rapid acceleration, cyber threat analysis, encryption and the like. In the traditional supply chain model, the business user would be required, for every separate installation of software, to pay large upfront costs and have a technician make a manual installation behind the firewall that adds to the cost and timeframe to deploy. For these reasons, most businesses do not implement “best practice” security solutions, which then lead to increases in cyber security breaches. IWG protects the primary network of an organisation through the virtual network in front of the firewall and redefines connectivity through the VPN replacement that is undetectable through the peer to peer connection. In short, the Virtual Services Platform locks down networks, protects assets from attacks through all devices (phones, iPads, laptops, desktops) and is the most cost effective method of doing so. This greatly reduces the IT spend for businesses.
MARKET OPPORTUNITY

The Internet and connected devices has increasingly become an integral part of daily life and business. This is due to the increase in personal connected devices, such as smartphones, and mobile business devices such as laptops or tablets. Recently we have also seen an increase in global data consumption and storage, with the latter being highly facilitated by the migration to the cloud.

Given the importance of the information individuals and businesses store online and in networks, such as banking details, business secrets, etc, the amount of attacks or hacks have increased. Security breaches have also received increased time in the media, such as the AshleyMadison.com hacks. Notably, security breaches are not only via external sources and hackers but are rather internal data breaches, due to the lack of best practice in the internal networks or over the top administrative security. It is estimated that 60% of malicious data breaches are internal. Globally detected and reported security incidents have increased from 3.4m in 2009 to 42.8m in 2014 and is expected to grow further. (Figure 5)

**Figure 5: Global detected and reported security incidents**

![Global detected and reported security incidents](chart)

*Source: PwC: Global State of information Security*

The need to increase information security both internally and externally has seen spend on IT security increase substantially. The global IT security market is currently estimated at US$76.0bn and is expected to grow at 15% per annum to reach US$173.0bn by 2020. (Figure 6)

**Figure 6: Global Security Spend Forecast**

![Global Security Spend Forecast](chart)

*Source: Gartner: Information Security Forecasts*
We note that a large portion of IT security spend is on Managed Security Services Providers (MSSP), who act as consultants to business and organisations and remotely manage the security needs. However, given the unique nature of security needs for each individual business, this has increased the costs needed to contract a MSSP. The managed Security market is currently worth $14.1bn globally and is set to increase to $24.6bn by 2019.

**Figure 7: Worldwide spend on Managed Security (2013-2019)**

IWG has developed a suite of products which are in line with the current direction and motives of the security industry; given the separation of networks, choke points, and cloud infrastructure. IWG’s technology, thus, has the potential to replace numerous products currently in the market, such as old-style VPN products, and may be able to establish itself as preferred security technology and gain market share, in what is a massive market.

**CORPORATE**

As at 30 September 2015, IWG reported only $0.2m of cash on hand. On 16 October 2015, IWG completed a $2.0m share placement at $0.17/sh, and established a $1.0m senior debt facility (drawn) via a US-based investor. Thus we estimate IWG has a current cash balance of c$3.2m. Given a cash burn of c$1.5m per quarter, we expect IWG to return to market in 3 to 6 months.

The debt facility has been put in place by three parties representing an up-front amount of $1 million with an ability for this amount to be increased by another $1 million by mutual consent. The loan is repayable in three tranches with 25% of funds to be repaid within 3 months, 50% repaid within 6 months, with the balance repaid in 9 months. Interest of 10% per annum is payable quarterly. In the event of default, the loan is convertible at a conversion rate of 80% of VWAP over the 5 days immediately preceding conversion.

We note that due to IWG’s relatively low cost base and the current operations being in the latter stages of negotiations; in addition to the software being available on the Telstra marketplace, we believe that IWG could easily swing to cashflow break-even with the commercialisation of 1 or 2 of its current leads.

IWG has 2 tranches of options outstanding at exercise prices of $0.187 and $0.25, with the options expiring on 04 November 2020 and 31 October 2017 respectively. We note that all the options are currently out-the-money and thus do not represent unpaid capital or value to IWG currently.
RISKS & CATALYSTS

Risks

- **Technology**: IWG may be adversely affected by rapid macro changes in technology that renders its products obsolete. IWG is also exposed to issues specific to its software, such as security and downtime issues. However, we feel the technological risk should be able to be managed as IWG seems to have software, which is targeted at the next stage of development in the IT security industry and should be adjustable.

- **Competition**: Competition from an increased presence and establishment, of other, security solutions globally could negatively affect IWG’s impact and market share. However, we feel that IWG’s innovate and unique solution specifically customised for the market, has gone some way to address this concern.

- **Regulation**: The increase in cyber-attacks and internal data breaches, and the importance of information storage on networks and the internet and cloud; may see increased regulation being imposed on the IT security industry. It is not known what form such regulation may occur in and the effect of it may have on software such as IWG’s. However, IWG is said to be actively developing its software to cater to future changes in the IT market and has a goal to establish itself as the standard for virtual segregation which could place it as an industry standard in terms of regulation.

- **Security**: The rise of IT security has seen the rise of hacker hobbyists, who specifically target software and companies that are stated as security specialists. An attack on IWG itself, or an organisation which has implemented the IWG software, could be a serious risk for IWG which could undermine its entire security software proposition. However, as security experts, we expect IWG to be able to nullify such attempts and react proactively to potential threats.

Catalysts

- **Geographic Expansion**: IWG has a footprint in Australia, with its software and platform being marketed on the Telstra Marketplace to SMB’s, and has an established operation in the USA. We note that IWG is also focused on deploying its software and products in the European market. Success in either geography could have a positive proof-of-concept effect globally, which may see an increase in uptake in the other geographies. IT security is a global need and thus IWG has the potential to expand beyond its initial markets.

- **User Growth**: IWG is currently in advanced stages of talks and negotiations in the USA, in the proof-of-concept stage in Europe and has rolled out its product in Australia, via the Telstra Marketplace. The uptake of the software in Australia is a large near-term potential catalyst, with the products being actively marketed to thousands of SMBs. Success of the current negotiations in the US, could see a large initial uptake and deployment of the software, while European penetration is a medium-term catalyst. We note that each user of IWG’s software and platform has substantial value, given the subscription nature of the product which increases lifetime value per customer and the high margins associated with each user.

- **Mobile Growth**: IWG is currently developing its software and platform to operate within the Android and Windows mobile devices ecosystem. The growth of mobile devices globally, and the importance or mobile devices in both a personal and business environment, has seen consumer awareness increase as to the security risks associated with these always connected mobile devices. IWG’s currently has proof of concept in development, which could see it add and additional product and revenue stream to its suite.

- **Third Party Developers**: IWG’s software is built and developed on a platform basis, which enables the Company to open up its platform to third party developers which increases compliance to associated software and applications. IWG may be able to package its software with popular third party developers software, or may be able to share in the revenue stream of associated software built on or around IWG’s platform.
BOARD OF DIRECTORS

Adam Sierakowski – Chairman

Mr. Sierakowski is a lawyer and director of Price Sierakowski (legal firm) and Trident Capital (corporate advisory & strategic consulting). He has over 15 years experience in legal practice, much of which he has spent as a corporate lawyer, consulting and advising on a range of transactions to a variety of large private and listed public entities.

Mr. Sierakowski has also for years, advised a variety of public and private clients on structuring of their transactions and has been engaged in co-ordinating fundraising both domestically and overseas. Mr. Sierakowski has vast experience in restructuring and mergers and acquisitions and has played a key role in the recapitalization of many ASX listed companies

Tim Gooch – Chief Executive Officer

As Chief Executive Officer of iWebGate, Mr. Gooch plays a pivotal role in the overall strategic direction and operation of the company.

In addition to overseeing product research, design and development, he is also responsible for business planning and marketing and sales strategy, including: the management of corporate policies; commercial transactions; investor relations; and strategic partner alliances.

Prior to iWebGate, Mr. Gooch built successful health services and software development companies and earned a Bachelor of Science Degree from the University of Western Australia

Mark Harrell - Managing Director Asia Pacific Executive Director

Mr. Harrell has been with iWebGate since 2006 and is responsible for overseeing the company’s Asia Pacific operations and expansion. Before joining iWebGate , Mr Harrell had over 10 years’ experience as a Chief Information Officer for a global company Worldmark. Previous experience includes managing online education programs throughout Asia and developing sophisticated automated finance programs in both Australia and South Africa. Mr Harrell also has strong business intelligence and information systems experience along with operational and project management skills. He also has numerous qualifications including Microsoft Certified Systems Engineer, Microsoft Certified Professional and Oracle Certified Professional.

Kathryn Foster – Non-Executive Director

Ms Foster has a strong background in technology, sales and early stage start-up companies. She has over 20 years’ experience, including key global roles at Microsoft. Ms Foster was the Principal Group Program Manager of the Xbox Live Games Marketplace at Microsoft where she drove the strategy that enabled subscription and gaming revenues to triple from US$500m to US$2bn within two years. Most recently as Microsoft, she was senior Director of MS Store Online Category Sales and Merchandising, where she had responsibility for generating US$1.4bn in annual sales across 230 plus worldwide online store locations.

Currently, Ms Foster is Managing Director of Lifeplan Services, the founding Director of Foster Consulting Services and is a Non-Executive of Class Limited. Ms Foster completed a Bachelor of Science and Business Administration, International Marketing at the Oregon State University and attended the University of Washington. She is a member of the Australian Institute of Directors.

James Tsiolis - Non-Executive Director

Mr Tsiolis has over 25 years of experience in funds management and capital markets and is currently a founder and Chief Executive Officer of Strategic Capital Management Limited (SCML), an investment management and advisory firm. Mr Tsiolis was the investment adviser to several large superannuation funds, including Military Superannuation ($3.9bn), as well as the fund manager of SCM’s retail product ($1bn).

Mr Tsiolis has been a member of several investment and corporate advisory committees including Macquarie Global Infrastructure Funds, Rosemont Partners, Direct Investment Fund, Deutsche Private Equity, military Super, Citic China Mezzanine Investment Fund and Energy Investors Group. Mr Tsiolis has overseen a number of investments from start-up to IPO in the technology sector.
Disclosure: The preparation of this report was funded by ASX in accordance with the ASX Equity Research Scheme. This report was prepared solely by Patersons Securities Limited. ASX did not prepare any part of the report and has not contributed in any way to its content. The role of ASX in relation to the preparation of the research reports is limited to funding their preparation, by Patersons Securities Limited, in accordance with the ASX Equity Research Scheme.

ASX does not provide financial product advice. The views expressed in this research report may not necessarily reflect the views of ASX. To the maximum extent permitted by law, no representation, warranty or undertaking, express or implied, is made and no responsibility or liability is accepted by ASX as to the adequacy, accuracy, completeness or reasonableness of the research reports.

Important Notice: Copyright 2015. The contents contained in this report are owned by Patersons Securities Limited (‘Patersons’) and are protected by the Copyright Act 1968 and the copyright laws of other countries. The material contained in this report may not be copied, reproduced, republished, posted, transmitted or distributed in any way without prior written permission from Patersons. Modification of the materials or use of the materials for any other purpose is a violation of the copyrights and other proprietary rights of Patersons.

Disclaimer: Patersons believes that the information or advice (including any financial product advice) contained in this report has been obtained from sources that are accurate at the time of issue, but it has not independently checked or verified that information and as such does not warrant its accuracy or reliability. Except to the extent that liability cannot be excluded, Patersons accepts no liability or responsibility for any direct or indirect loss or damage caused by any error in or omission from this report. You should make and rely on your own independent inquiries. If not specifically disclosed otherwise, investors should assume that Patersons is seeking or will seek corporate finance business from the companies disclosed in this report.

Warning: This report is intended to provide general securities advice, and does not purport to make any recommendation that any securities transaction is appropriate to your particular investment objectives, financial situation or particular needs. Prior to making any investment decision, you should assess, or seek advice from your adviser, on whether any relevant part of this report is appropriate to your individual financial circumstances and investment objectives.

Disclosure: Patersons, its director and/or employees may earn brokerage, fees, commissions and other benefits as a result of a transaction arising from any advice mentioned in this report. Patersons as principal, its directors and/or employees and their associates may hold securities in the companies the subject of this report, as at the date of publication. These interests did not influence Patersons in giving the advice contained in this report. Details of any interests may be obtained from your adviser. Patersons as principal, its directors and/or employees and their associates may trade in these securities in a manner which may be contrary to recommendations given by an authorised representative of Patersons to clients. They may sell shares the subject of a general ‘Buy’ recommendation, or buy shares the subject of a general ‘Sell’ recommendation.

Stock recommendations: Investment ratings are a function of Patersons expectation of total return (forecast price appreciation plus dividend yield) within the next 12 months. The investment ratings are Buy (expected total return of 10% or more), Hold (–10% to + 10% total return) and Sell (–10% negative total return). In addition we have a Speculative Buy rating covering higher risk stocks that may not be of investment grade due to low market capitalisation, high debt levels, or significant risks in the business model. Investment ratings are determined at the time of initiation of coverage, or a change in target price. At other times the expected total return may fall outside of these ranges because of price movements and/or volatility. Such interim deviations from specified ranges will be permitted but will become subject to review by Research Management. This Document is not to be passed on to any third party without our prior written consent.