
iWebGate
Trusted Networks are Everything

Disclaimer

This presentation has been prepared for the consideration of potential investors by iWebGate Technology Limited ("the Company") and does not carry any right of publication or disclosure to any other party. This presentation is incomplete without reference to the Company and should be viewed solely in conjunction with an oral briefing provided by senior management of the Company. Neither this presentation nor its content may be used for any other purpose without prior written consent of iWebGate Technology Limited.

This presentation has been prepared by iWebGate Technology Limited. The information in this presentation is based upon information provided by the management of the Company as well as publicly available information and reflects prevailing conditions and our views as of this date, all of which are accordingly subject to change. In preparing this presentation, we have relied upon and assumed, without independent verification, the accuracy and completeness of any information made available from the management and public sources.

The information contained in this presentation is of general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

Whilst the information presented and views expressed in this presentation and the oral briefing have been prepared in good faith, iWebGate Technology Limited accepts no responsibility or liability to any party in connection with such information or views. This presentation is not an offer, invitation, solicitation or recommendation with respect to the subscription for, purchase or sale of any security, and neither this presentation nor anything in it shall form the basis for any contract or commitment whatsoever.

Introduction

I'm proud to be part of a company producing something great. A revolutionary product providing the Virtualization of Networks Services to the world. This is a massive leap forward for computer networking and cyber security. What's really exciting is no other security product empowers large-scale partners to deliver enterprise-ready solutions to their customers with the same business speed, efficiency and agility.

Companies and government agencies continue to make headline news when their computer networks are breached. More concerning is the news you don't hear or read.

For example, during our ASX listing process, we discovered crypto locking (ransomware) affected over 20% of the fund managers with whom we spoke. Their networks were compromised in the past 12 months along with a major healthcare provider. All focused on the immediate issue of getting their data decrypted. Some companies paid the ransom and others reverted to previous backups. In many cases unknown to the victim, the attacker(s) obtained copies of the data before executing a demand for ransom – and then received payment!

The IT security market is full of noise, with some companies claiming they have *the answer*. Data Breach Investigation Reports [1] outline the diverse nature of cyber threats. iWebGate's technology significantly enhances cyber security. The iWebGate team realizes the power of integrating many clever technologies to solve a really big problem. Our CEO, Tim Gooch, openly states "*we are not just making a computer networking product. We are combining the skills of diverse people to make something no one person or company can create alone*".

The purpose of this document is to provide an extended overview of iWebGate's product and current business activities. We look forward to sharing some exciting news in reference to meeting strategic objectives over coming months.

Adam Sierakowski
Chairman

Principle of Separation

Here's a thought…

Think of the street as the Internet. It's free to use and easily accessible 24 hours a day, 7 days a week. Now imagine some *cash* in your hands.

If you placed the cash on a café table for everyone to see from the street and walk away, how long do you think it would take to go missing? Minutes, hours, days? Would the window be smashed if left overnight?

Now take that same cash and place it on your office desk - located on level 15 of your corporate building. Reasonable to say the cash would stay on your desk longer than the café table.

The "**Principle of Separation**" has an immediate impact on protecting core assets.

The building provides the *layers of separation*. If the cash is taken from your desk, you can start to determine who took it and when – compared to the complete unknowns associated with the café.

Additional security including physical guards, smart card access, CCTV cameras, alarm sensor, floor safes and door locks can be applied to this *principle of separation*. You now have a secure environment to store and access core assets.

However, when it comes to cyber security, the principle of separation is rarely adopted or perfected. The following information provides deeper insights as to why.

After winning the Global Security Challenge (GSC), iWebGate was awarded a contract with a US Government agency called the Technical Support Working Group (www.tswg.gov). Without going into details for confidentiality reasons, the contract stated:

1. *Implementing a sub-network in a Demilitarized Zone (DMZ) to separate an enterprise's private / primary networks from all other networks including the Internet has been recognized as an industry "best practice".*

2. *The cost of server hardware, software and system administration has placed a proper DMZ sub-network beyond the reach of almost all SMEs and encouraged other enterprises with highly fragmented and widely distributed networks to cut corners.*

3. *The current VPN approaches circumvent the DMZ sub-network defensive layer.*

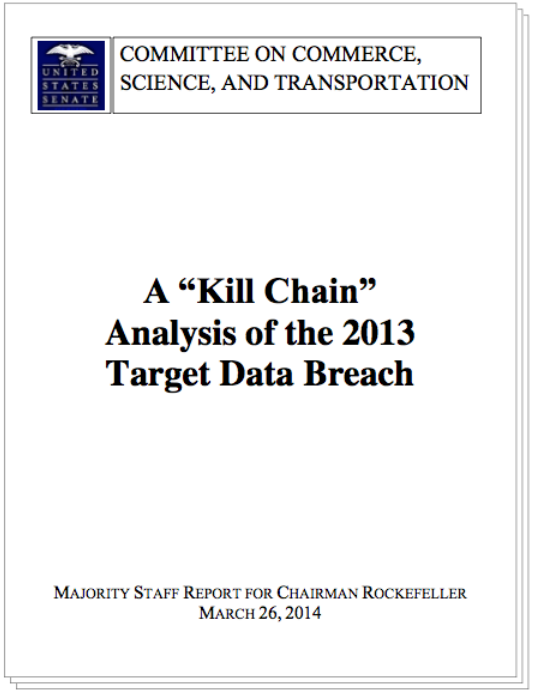
Summary of the Kill Chain Analysis[2] on the 2013 Target breach stated:

i) *Target gave network access to a third-party vendor, a small Pennsylvania HVAC company, which did not appear to follow broadly accepted information security practices. The vendor's* ***(SME) weak security*** *allowed the attackers to gain a foothold in Target's network.*

ii) *Target appears to have failed to respond to multiple automated warnings from the company's anti-intrusion software that the attackers were installing malware on Target's system.*

iii) *Attackers who infiltrated Target's network with a vendor credential appear to have successfully moved from less sensitive areas of Target's network to areas storing consumer data, suggesting that Target* ***failed to properly isolate its most sensitive network assets****.*

iv) *Target appears to have failed to respond to multiple warnings from the company's anti-intrusion software regarding the escape routes the attackers planned to use to exfiltrate data from Target's network.*


COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

A "Kill Chain" Analysis of the 2013 Target Data Breach

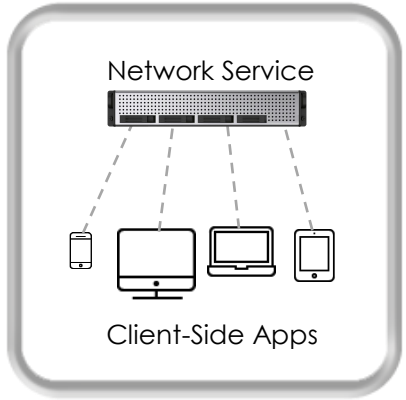
MAJORITY STAFF REPORT FOR CHAIRMAN ROCKEFELLER
MARCH 26, 2014

How Networks Work

A "network service" is a server-based application providing data storage, operation, presentation, communication or other capacity to client-side applications residing on a number of computer devices.

For example, web services are established to host website content, which is then accessed via client-software called web browsers. Web site content residing on one server can be accessed by millions of users (client side application – browser).

There are many forms of network services. Other examples include e-mail, file, voice over IP, messaging, remote desktop access etc.



Packets of data are exchanged between the client-server applications. Therefore, firewalls *must allow* packets of data to flow in *and* out of networks for client-server end point communications to occur.

Universal Problem

Firewalls and VPNs are the conventional security products used to try and separate private networks from all other networks.

It's important to note firewalls and VPNs are not computer end-points. They are susceptible to attack using a broad range of techniques. When an adversary gets through the firewall, network services and client-side applications are at risk.

Most security products and business applications are then deployed around this archaic network architecture, which doesn't include proper segregation.

Old Thinking - The Network Perimeter

A network perimeter is described as the boundary between a private and public network. As a result, the following traits occur for the vast majority of networks:

Internal Networks:

Many organisations believe their private networks are "*secure*" because they acquire and manage their own IT assets. As a result, it's common to find many devices (with client-side applications) **directly connecting** to the primary network services on the same IP network.

For example, a users' workstation, laptop and/or tablet computer connects to the same IP network as their organization's mail and file server. When a device is breached, adversaries can easily find and connect to other computers on the same network. Attacks like cryptolocking take advantage of this weakness.

External Networks:

A network service is an end-point. It must be able to send and receive packets of data with client-side applications. Externally, firewall ports are frequently opened and linked to primary services so client-side applications can communicate from other networks.

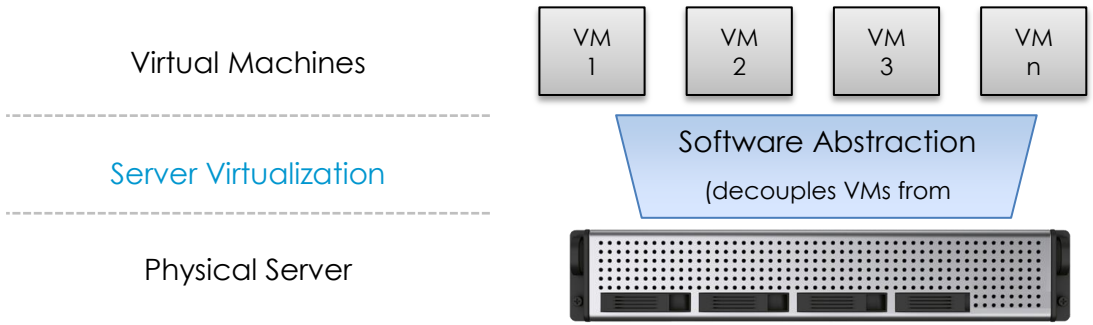
VPN tunnels attempt additional levels of security, however the VPN service becomes part of the networking connection by default. Adversaries can launch attacks against accessible firewall/router VPN services like IPsec and SSL to access encryption keys. Additionally, reports indicate PPTP-protected VPN communications pose little imposition to sophisticated attackers. Bit-flipping attacks can occur when adversaries modify PPTP (Point-to-Point Tunneling Protocol) packets without detection.

When any of these VPN service are breached due to misconfiguration or vulnerabilities, the consequences are devastating.

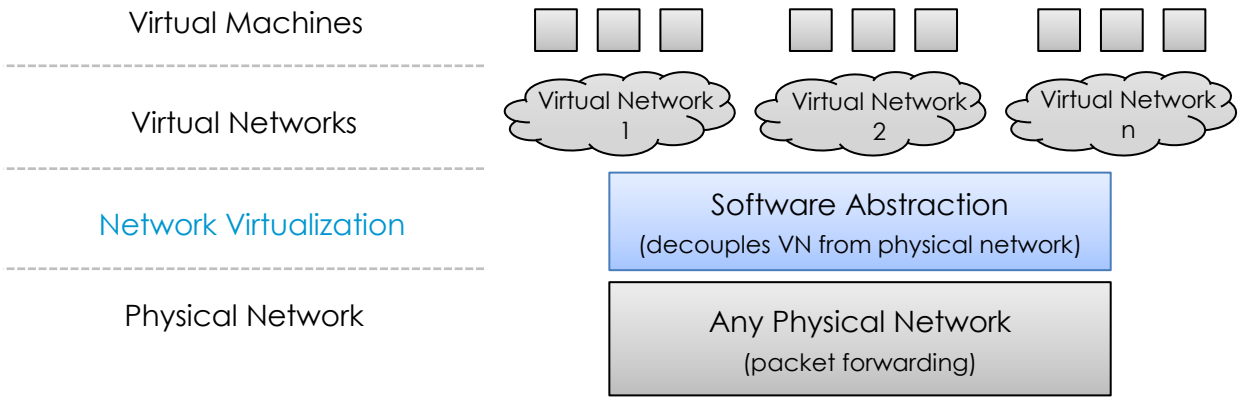
No public or private network can be trusted. Therefore, referring to a primary network's perimeter as the space between itself and public networks like the Internet is inadequate for today's IT.

Virtualization

The emergence of virtualization technologies has dramatically reduced IT complexity and cost. First came server virtualization – the ability to easily create a number of virtual servers in one physical server using software.



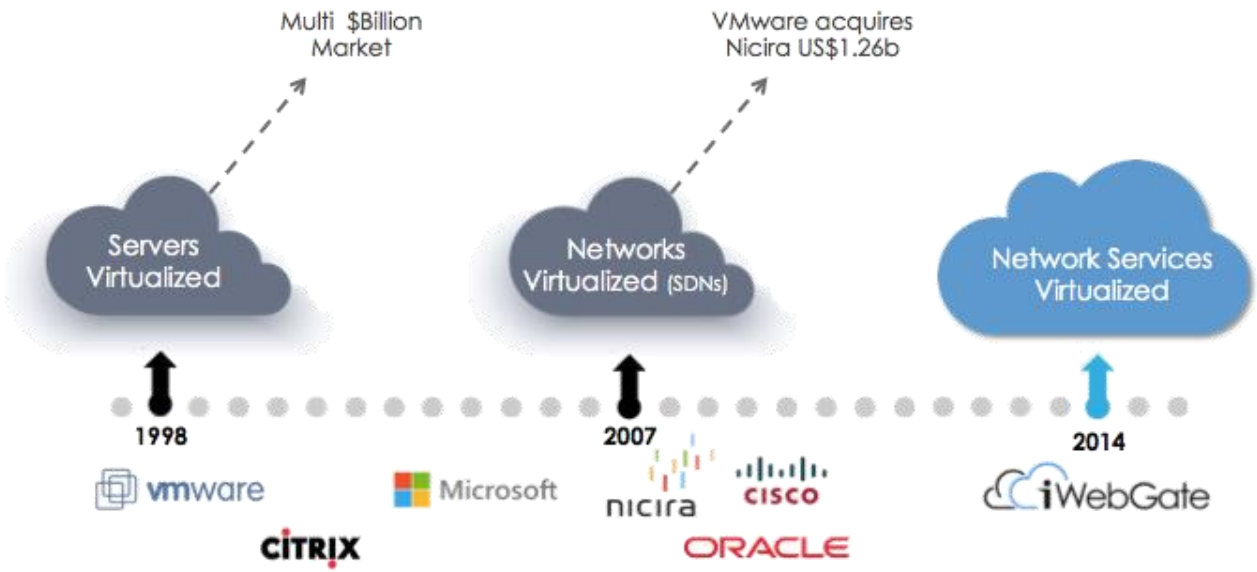
Network virtualization has started to emerge over recent years. Companies like Nicira (acquired by VMware in for approx. US$1.05b cash plus US$210m unvested equity awards [3]) empower data centres to easily create a number of virtual networks on top of one physical network using software.



So in both instances, **software is used to create a virtual representation of the physical**. Once established, server and network capacity can dynamically shift. Being able to set up servers and networking once in the physical, to then think and act upon them in the virtual has transformed IT.

The world has seen the impact of virtualized servers and networks with the rise of cloud technology. What's missing is the virtualization of network services. As a result, primary network services are missing a powerful abstraction layer for operational simplicity, new business capacity and significantly better security.

A New Market Segment - The Virtualization of "Network Services"



iWebGate has created a software product used to easily provision a wide range of "virtual network services" around an existing network.

This network transformation results in the emergence of a new and powerful layer, which re-defines the network perimeter forever.

Transformation of the Network Perimeter – New Thinking

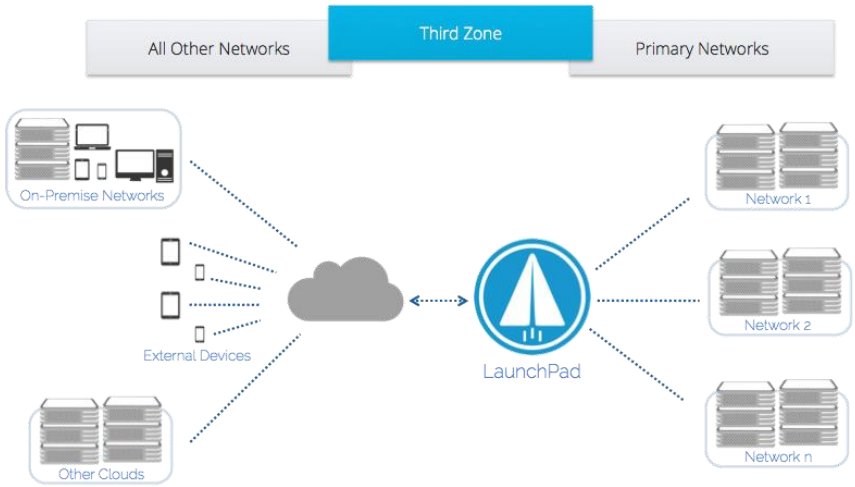
Until now, the cost of server hardware, software and system administration has placed proper network segregation beyond the reach of almost all SMEs. Inadequate levels of segregation are established using only firewalls and VPNs.

Large enterprises are at risk when connecting with these weak links and not implementing proper segregation between all networks due to the cost, complexity and resources involved.

Segregation does not start and stop between private and public networks – it needs to occur between **every internal and external network** … and the devices connecting to them.

iWebGate has created a Virtual Services Platform (VSP) called LaunchPad. Installed in minutes on a single physical or virtual server, LaunchPad segregates an existing network from all other internal and external networks with a broad range of emulated network services.

Emerging from this breakthrough is a new layer of abstraction we call the 3rd zone. This network segregation takes DMZ Security and Cyber Kill Chain Processes to new heights.



You still need firewalls and many other security products. However, these technologies are *re-purposed* around a new form of perimeter, which provides operational simplicity and new capabilities across many internal and external networks.

Properly segregating a network is extremely powerful. The operational simplicity and new capabilities is further enhanced when the principle of separation is extended to network connectivity and computing devices. Our team has been working very hard on the development of iWebGate's Virtual Segregation Suite (VSS).

iWebGate's VSS includes;

(previously called Virtual Services Platform)

Segregates Networks

LaunchPad is the cornerstone product of VSS. In addition to providing many VSS administration tools, LaunchPad segregates an existing network from all other internal and external networks with a broad range of emulated network services

The software includes a broad range of network services securely integrated into a single software platform. Installed in minutes on a single physical or virtual server, LaunchPad takes DMZ Security and Cyber Kill Chain Processes to new heights.

Segregates Connectivity

Linkup LP establishes a secure connection between LaunchPad and end-customer networks. Unlike traditional VPN, Linkup LP provisions a Virtual Local Area Network (VLAN) over a Peer-to-Peer connection.

Linkup LP empowers our partners to install LaunchPad in their cloud environments and 'link' it to on-premise and/or other cloud networks – without making firewall changes or weakening the security of existing networks.

In fact, end-customers can close their externally exposed firewall ports and redirect risk to a new and purpose-built virtual services network in the cloud.

Segregates Devices

The network perimeter has changed to the point it must remain *isolated* from all other internal and external networks – and their affiliated devices. Therefore, regardless of its location, any device connecting to a network needs to do so with network segregation in mind.

Device LP establishes a secure 'container' capable of running on all major operating systems including Windows PC, Windows Mobile, iOS, OSX, Android, Linux and Samsung Knox.

Once installed, the container ensures a device securely connects to a given network via LaunchPad and/or VPN LP (see below).

The container also includes a number of essential security features such as encryption at rest, multi factor authentication and inability to run or inject malicious code.

These security and product distribution features make life significantly easier for developers. Applications once classified "*enterprise friendly*" instantly become "*enterprise ready*" when seamlessly integrated with Device LP.

When iWebGate's VSS is deployed, a new abstraction layer transforms the network perimeter and properly segregates networks, connectivity and devices.

The platform is now set to launch a broad range of network security and collaborative applications to many organisations in an "*enterprise ready*" state.

By enterprise ready we mean really fast and easy to deploy, seamless integration with existing infrastructure, dynamic support for many networks and built with proper network segregation in mind.

iWebGate Connectivity Suite (CS)

Lets come back to our analogy on the principle of separation.

Once the construction of a building (segregation) is complete, fit-outs can be implemented to meet tenant requirements. Over time, tenants can change offices, floor plans and internal layouts. However, the principle of separation and other security features have not changed.

iWebGate's VSS can be viewed in the same manner. Organisations can upgrade or change their primary systems over time. However the Virtual Segregation Suite ensures security and collaborative processes are not compromised.

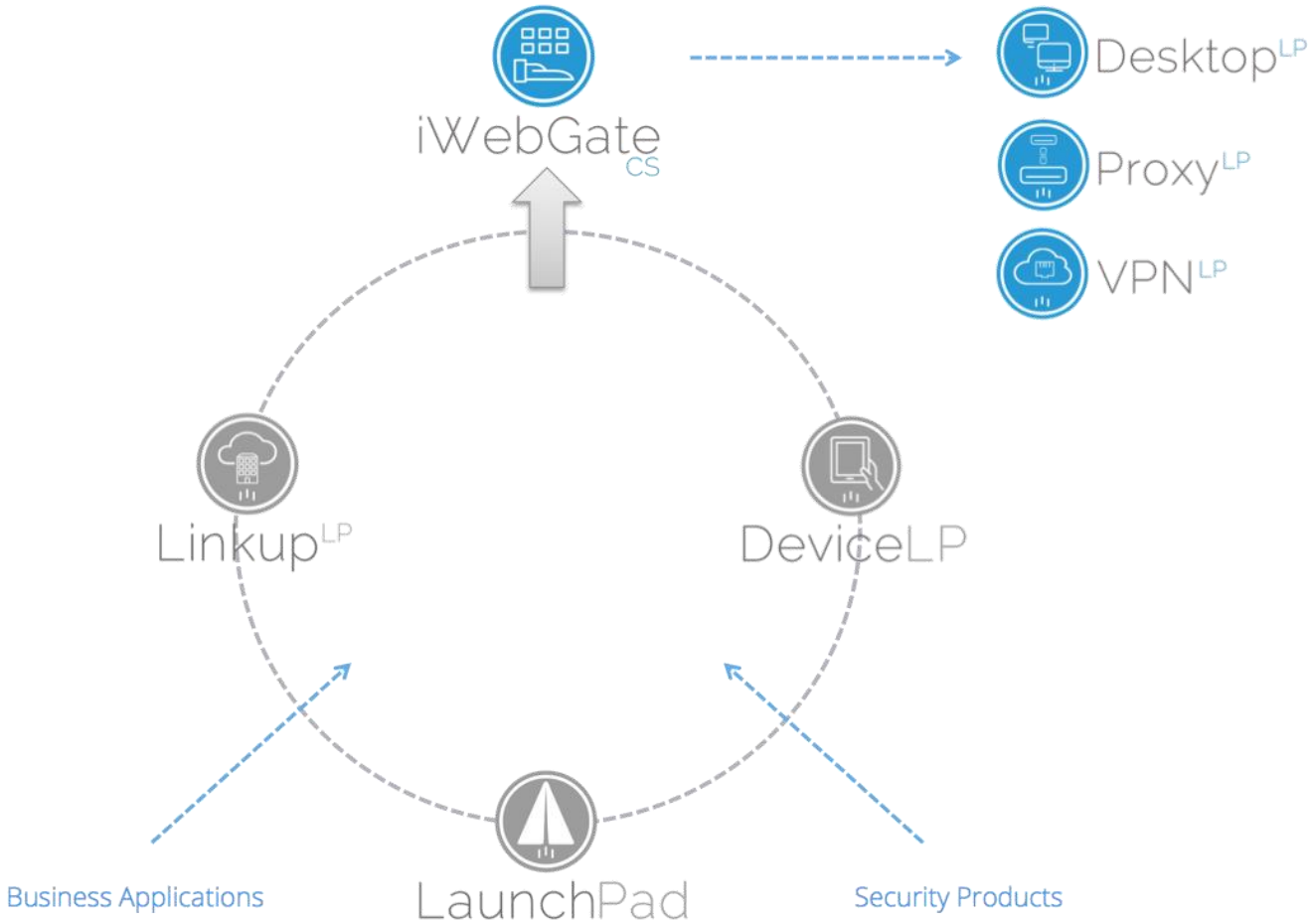
Now the foundation for segregation is set, a broad range of security and business applications can be rapidly integrated to meet channel partner and end-customer demands.

Previously these products functioned well. However, they were either difficult to install and/or weakened network security because they were not built with proper segregation in mind.

With iWebGate's VSS, theses enterprise "*friendly*" products are beautifully transformed into enterprise "ready" solutions - capable of being distributed to market via our channel partners.

There is no firewall, advanced persistent threat, end-point security or software defined networking technology offering this capability.

To demonstrate the power of this transformation, we've integrated a range of external security and business applications into VSS. The result is a product feature set we call the iWebGate Connectivity Suite.



Securely connect to computer desktops from within the organisational network and remote locations using all leading tablet, smartphone, laptop and PC devices.

Combination of several Proxy Services and host-based Network Intrusion Detection (NID) system in a CHroot jailed environment with multi-factor authentication for Microsoft based services (e.g. Exchange, SharePoint).

A new form of VPN technology that overcomes current security issues and easily provision VLANs over private AND public network infrastructure using software only.

Example

Based on 2013 preliminary analysis, the United States Internal Revenue Service (IRS) estimates paying $5.2 billion in fraudulent identity theft refunds [4]. Measureable information pertaining to fraudulent identity theft in the Australian and other markets is not available.

Multi Factor Authentication (MFA), a proven technology for protection against identity theft. To successfully gain computer access, MFA enforces users to pass at least two of the following authentication categories:

- Knowledge factors ("things only the user knows"), such as password
- Possession factors ("things only the user has"), such as smart phone or
- Inherence factors ("things only the user is"), such as biometrics

Requiring more than one independent factor significantly increases the difficulty of providing false credentials. Therefore, MFA is a *must* for any system with a user login.

Although the market is saturated with MFA solutions many SMEs, large enterprises, cloud applications and government portals do not implemented MFA across all of their networks and affiliated systems. This is primarily due to the cost and complexities involved.

MFA is included with iWebGate's Virtual Segregation Suite (VSS). With the click of a button, MFA can be applied across an organisation's networks and affiliated applications – from one platform. As an added bonus, these networks and applications would also be proxied by LanchPad.

Shifting the network perimeter to a new abstraction layer changes the speed and efficiency security features like MFA and Proxing can be implemented across all networks and their affiliated systems. Instead of taking days to months by qualified network administrators and/or software developers, iWebGate's technology empowers "average" computer users to implement powerful security solutions in minutes.

2015 Targets

Over the past 6 months, our team has been totally focused on gearing products and backend systems for mass distribution. As a result, we have transformed our technology by decoupling the interfaces from the underlying platform services – hence, the latest version of our Virtualized Network Services technology is called LaunchPad.

What this leads to is the ability for third parties to *easily* integrate in and around LaunchPad with the greatest speed and efficiency – whilst not compromising the integrity of our software platform or network architecture principles.

This is extremely important because we are entering the market using an indirect approach. Our target customers include those companies touching the networks, applications and devices.

Our channel partner targets for 2015 include:

- 3 Infrastructure as a Service (IaaS) Providers
- 3 Strategic Partners; and
- 6 Software Development Companies

1) Verizon Data Breach Investigations Report 2014.

2) A "Kill Chain" Analysis of the 2013 Target Data Breach.

3) VMware News Releases – Vmware to Acquire Nicira, July 2012

4) US Government Accountability Office: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud, Aug 2014.