

# **Business Strength Security for Mission critical Hosting**



10.12.2009

Copyright 2009 Macquarie Telecom

1 | 5

## Globalisation and Security

ICT is the driving force behind the next wave of globalisation. As we move into a post-carbon age, ICT and online technologies will increasingly supplement transport and aviation to make the world even more connected. Globalisation brings many advantages but one of the challenges is the difficulty in containing the breakout of negative contagions. Examples of this include: the speed and spread of the financial crisis of 2009 and the H1N1 pandemic. Security plays a crucial role to prevent the spread of online threats.

Some sobering security related statistics:

- > More than 7000 security vulnerabilities were catalogued in 2008 [1].
- > 83% of websites have had at least one serious vulnerability reported in 2009 [2].

Some of the effects of security breaches include Brand damage (through web site defacement), loss of revenue (through denial-of-service) and even involve legal ramifications (due to loss of private customer data or unknowingly taking part in a botnet to attack other online properties).

This whitepaper provides an overview of the implemented security processes which underpins the mission-critical hosting services enabled by Macquarie Hosting.

## Security Philosophy

Drawing on the principles of “defence-in-depth”, multiple layers of security are deployed in order to maximise protection from threats.

The “defence-in-depth” approach is a systematic end-to-end strategy which includes physical access controls, security measures for the network infrastructure layer (which we term Perimeter security) as well as security measures on the servers themselves (which we term Host-based security).

Finally, certifications to industry standards ensure integrated and consistent security management methodology; and assurance of the implemented security layers and controls.

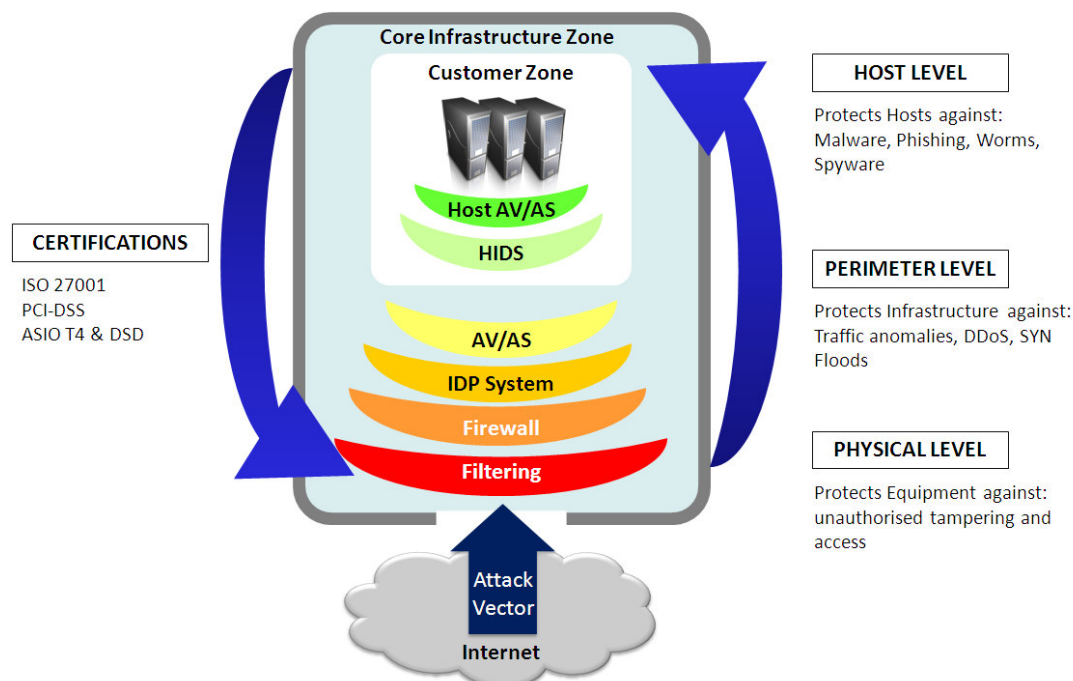


Figure 1 The Elements of our Security Philosophy

## Certifications

Our investments in certifications are testament of our pursuit of consistency and repeatable processes when it comes to security controls. Certifications also ensure that we are implementing the most up-to-date and best-of-breed security industry practices. Macquarie Hosting is the most highly certified hosting provider in Australia.

We have achieved the following certifications in relation to security standards:

- > ISO27001: a comprehensive Information Security Management System (ISMS) framework which is audited annually against a global ISO/IEC standard by an independent third party.
- > PCI-DSS: a standard which specifies 12 requirements that was created to help organizations that process card payments prevent credit card fraud. Compliance is assessed annually by an independent assessor known as a Qualified Security Assessor (QSA).
- > ASIO T4 & DSD: Certified by DSD (Defence Signals Directorate) to provide assurance of protection from external threats for the hosting of Federal Government systems & data classified up to “Highly Protected” & “Restricted” levels in accordance to ACSII33 & PSM – audited annually

This degree of certification provides customers with a secure hosting foundation so that they can confidently deploy their industry vertical applications on top. Having a certified and secure infrastructure foundation is particularly important for industries which are concerned with data confidentiality and privacy – such as Financial services, Online retailing & ticketing, Legal and Healthcare verticals.

## Physical Security Layer

Physical Security is the first stage of protection. Physical layer protection is provided through proper access control. Physical access is strictly controlled at entry/exit points around-the clock by security personnel, mantraps, access-card, biometric scanning and video surveillance.

Access to our Data Centre (“Intellicentre”) is only provided to specified employees and contractors. All customer equipment is located and racked on secure floors and locked cabinets to avoid any malicious or inadvertent tampering.

## Perimeter Security Layers

The perimeter security layer provides the second stage of protection. Different security components puts traffic through a “fine-toothed comb” by checking for threats at network level (i.e. IP addresses), aggregate traffic level and embedded threats. While the “Intellicentre” core provides a substantial level of protection on the network layer, the customer can further supplement with additional security measures themselves in their DMZ. The perimeter layer security measures can be divided into different sub-layers as follows.

### Core Routing and Switching

The Core switching and routing infrastructure on our platform is configured to filter out all un-necessary traffic in order to prevent the most common attacks such as DOS, DDOS, Bad IP Addresses, SYN flooding, Ping attacks (utilising abnormal sized TCP packets) and crafted TCP packets.

As a further level of segregation, all customers are configured in their own broadcast domain using VLANs. This means that individual customers who need to communicate with each other within our Data Centre needs to traverse an access-list, to prevent back-

door threats. This provides protection from arp-mac-table flooding/spoofing and broadcast storms.

### **Firewalls**

Firewalling provides the next layer of protection based on IP addresses. The default firewall settings for newly configured customers are to deny all. It is up to the individual customer to explicitly open each port depending on the applications they are supporting. e.g. in most cases, only port 80 (http) and port 443 (https) should be enabled in the inbound direction to reduce the security risks.

Further protection is provided by restricting access between zones at a protocol level. e.g. if the web server needs to write records to a database, only open a connection from the web server to the DB server for that specific protocol.

### **(Network level) Intrusion Detection and Prevention System**

The Intrusion Detection and Prevention (IDP) provides another layer of protection by picking up anomalies or abnormal traffic trends. This is different to deploying a firewall which looks at IP addresses. The IDP system is made up of two components - the IDS (Intrusion Detection System) monitors for abnormal traffic patterns and the IPS (Intrusion Detection and Protection) works to proactively stop the malicious attacks. As a conscious design principle, we deploy IDP components from different equipment vendors to provide further levels of security.

Together the components of the network IDP system provides zero-day protection against a wide range of attacks such as worms, trojans, spyware, keyloggers and other malware from penetrating the network or spreading from already infected users. The IDP achieves this by using industry-recognised stateful detection and prevention techniques. Whilst the inbuilt network IDP system is designed to stop most security threats, the customer can also deploy a dedicated IDP device in their DMZ as an additional line of defence conferring Application Protection, Performance Protection and Infrastructure Protection through total packet inspection.

- > Application Protection provides fast, accurate, reliable protection from internal and external cyber attacks.
- > Infrastructure Protection protects routers, switches, DNS and other critical infrastructure from targeted attacks.
- > Performance Protection capabilities enable customers to throttle non-mission critical applications that hijack valuable bandwidth and IT resources, thereby aligning network resources and business-critical application performance.

### **Anti-Virus and Anti-Spam**

The core infrastructure zone is designed with Anti-Virus and Anti-Spam (AV/AS) capabilities. This layer of security provides protection by scanning SMTP and web traffic for embedded security threats. This is available as an option on a per-user per-month fee basis.

## **Host Security Layer**

The third stage of protection involves adding security functionality onto individual dedicated hosts (or servers). Host-based security elements complement the network-based security measures installed on the core infrastructure zone. The following are optional services.

### **Host-based Intrusion Detection System (HIDS)**

A Host based IDS further protects individual critical servers within the customer network from malicious attacks. To combat these threats, the Server IPS combines several protection technologies into a single, multi-layered agent which offers broad operating system and platform support. Additionally, Host-based IDS also guards business critical

systems and data which may assist customers in meeting stringent audit and compliance standards.

#### **Host-based Anti-Virus/Anti-Spam**

Installing managed Anti-Virus (which covers spyware/malware detection) increases the protection profile on individual dedicated servers. Host-based AV/AS provides another layer of security to pick up embedded security threats which manage to evade previous security layers. Because it is a managed service auto-updates and event logging are included as part of the solution - ensuring you get the most up-to-date signatures for maximum protection.

## **Conclusion**

This whitepaper provides an overview of the end-to-end security processes which forms the cornerstone of our offerings and is “baked-into” the managed hosting services we deliver. As we move toward a more connected and integrated computing era, a secure hosting environment is a critical component of any online business. Online commerce would not exist if there was no trust (which is established through secure infrastructure) between the transacting parties.

Our customers from all industry verticals, depend on our certified security processes and infrastructure, day-in day-out; to deliver a secure and stable online business platform on which to underpin their business transactions. As we move forward, the focus on security and the complexity of maintaining a secure online environment will intensify as more and more transactions and data flows over the web.

## **References**

- [1] From <http://www.cert.org/stats>, Retrieved 03.12.2009
- [2] Whitehat security, Fall 2009 website security statistics report

## **About Macquarie Hosting**

A division of Macquarie Telecom; Macquarie Hosting is the Australian leader in mission-critical application hosting for companies who rely on their websites for their business. Macquarie Hosting owns and operates Australia’s most highly accredited Data Centre, the Intellicentre, and has the people and processes in place to provide the highest levels of security and uptime. Macquarie Hosting enables greater flexibility, agility and on-demand scalability for organisations to respond to spikes and increases in web-site performance. To find out more [www.macquariehosting.com](http://www.macquariehosting.com)

## **Disclaimer**

The content of this article is intended to provide a general guide on the subject matter. Specialist advice should be sought about your specific circumstances. No responsibility can be assumed for any loss or damage through the use of this content.