Securing Your Information When Migrating To The Cloud

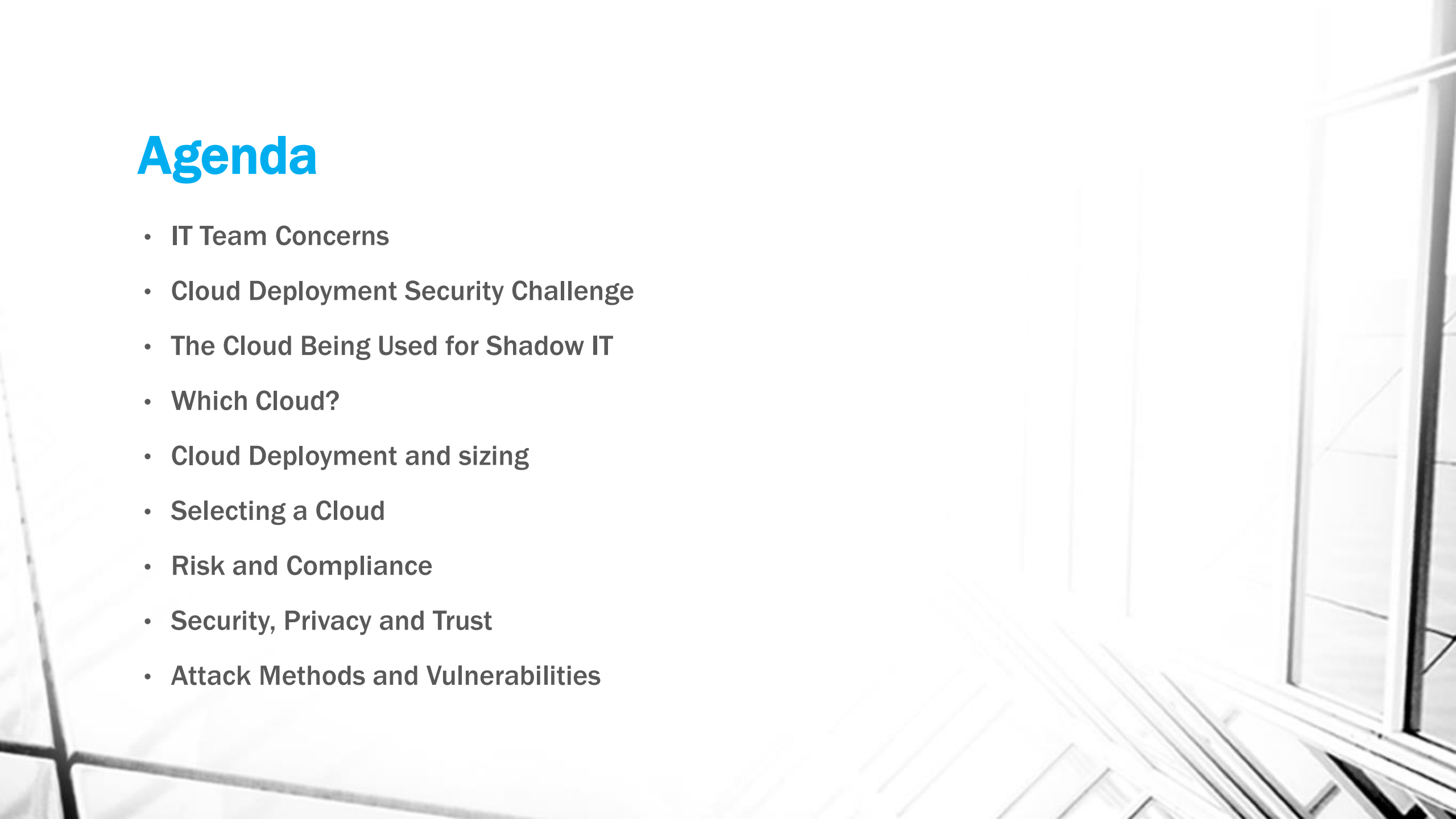
Em: Derek.Grocke@cyberops.com.au

Em: sales@cyberops.com.au

Ph: +614210566699

Agenda

- IT Team Concerns
- Cloud Deployment Security Challenge
- The Cloud Being Used for Shadow IT
- Which Cloud?
- Cloud Deployment and sizing
- Selecting a Cloud
- Risk and Compliance
- Security, Privacy and Trust
- Attack Methods and Vulnerabilities



IT Team Concerns

Security

"The world has gone mobile; not all traditional security measures apply"

Compliance

"Compliance is not optional. By using cloud applications operational visibility and control may be lost"

Shadow IT

"Unauthorised or unrestricted use of cloud applications can lead to data security incidents and compliance breaches"

BYOD

"Users are increasingly working in the office and on the move, but corporate security has to follow the user regardless of the device used"

Productivity

"Corporate and personally owned devices may increase productivity, but access to corporate data and the network needs to be protected at all times"

Cloud Deployment Security Challenge

Mission critical applications are being deployed to the cloud

- many information security professionals are unaware of what is required to make sure environments are secure

Classic security architecture and testing is not sufficient

- knowledge of cloud technologies, data security/confidentiality, identity/access controls, need for data sovereignty, layered security zoning, regulatory/industry requirements are required when testing and leveraging cloud architectures

The Cloud Being Used for Shadow IT

Use of Shadow IT is increasing to satisfy business needs, but at what cost?

- covert activities are undermining IT staff from running an efficient, safe, compliant and coordinated IT capability
- frustrated business leaders have finally found a way to bypass the constraints of IT departments

Shadow IT provides a great opportunity for IT departments to refresh business systems technology, assuming they are aware of the need, are supported by the business and are prepared to evolve/embrace the rapid need for the business change.

Which Cloud?

- If you have in-house or skilled vendors with cloud knowledge, you need granular infrastructure transparency/controls, Amazon Web Services is a great fit.
- If you need of Platform as a Service (PaaS), you want seamless hybrid cloud and you're already using a lot of Microsoft services, Azure is the way to go.
- If you're business relies on data analysis, Google's data storage and analytics tools are very feature rich.

Different Clouds
Different Uses
Different Security Needs

SaaS (Software as a Service)

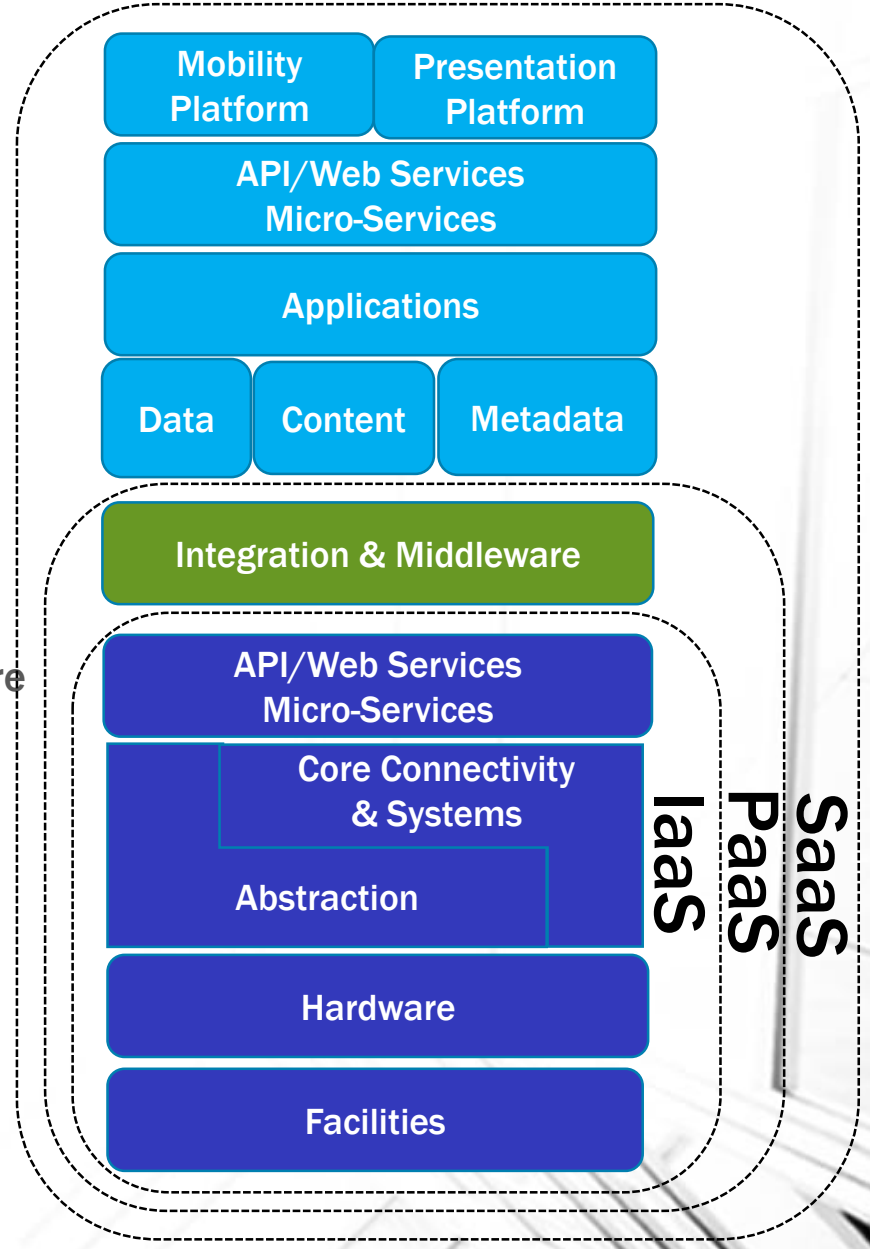
- available to multiple users over the web or private/VPN network
- is a complete application stack on top of PaaS
- security primarily provided by the provider

PaaS (Platform as a Service)

- used for rapid application development and adds middleware to IaaS
- no cost or complexity of buying and managing the infrastructure
- includes database, middleware, development tools & infrastructure software
- hybrid security responsibilities with the service provider

IaaS (Infrastructure as a Service)

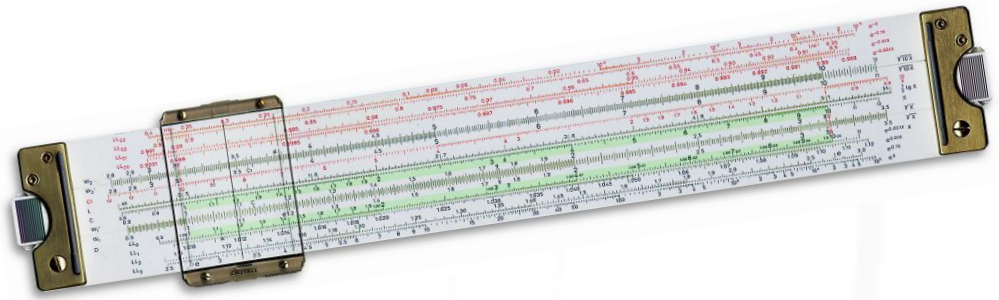
- provides compute & storage requirements
- is the foundation of the footprint
- delivery of hardware and software as a service
- does not require any long-term commitment
- can allow users to provision recourses on demand
- security primarily provided by your organisation



Typical Cloud Project Approach

1. Understand your business and business systems requirement.
2. Assess your assets compute, application, networks, data, transaction and security requirements.
3. Select your public, private (in-house and/or cloud) or hybrid deployment model.
4. Select your cloud service model and vendor; referencing vendor standard architectures.
5. Understand application, customer, network traffic data flows and program authentication/identity logic.
6. Establish, integrate and activate the service environment or platform.
7. Operate the service.
8. Maintain service, monitor business outcomes and security quality.

Cloud Sizing



- Cloud environments vary greatly based on business demand and existing IT resources.
- Cloud sizing doesn't have one correct answer, since every environment is truly unique in its demands.
- Differing business requirements vary the type and/or combination of cloud designs.

Overall Environment Sizing

Identify Initial & Phased Approach Against Business Needs

- it is critical to decide what physical and virtual components will be placed into the cloud
- architects and administrators must look at a variety of business drivers when building the deployment roadmap, standards, solutions, governance and user experience

Growth Considerations

- cloud architectures must be built with growth in mind
- as business demands evolve, business and IT must be able to respond
- good solution architecture will enable the capability to expand with minimal disruption to the existing running business systems environment
- establish initial capability and monitor ongoing resource requirements through peak processing periods and as business needs change

Risk and Compliance

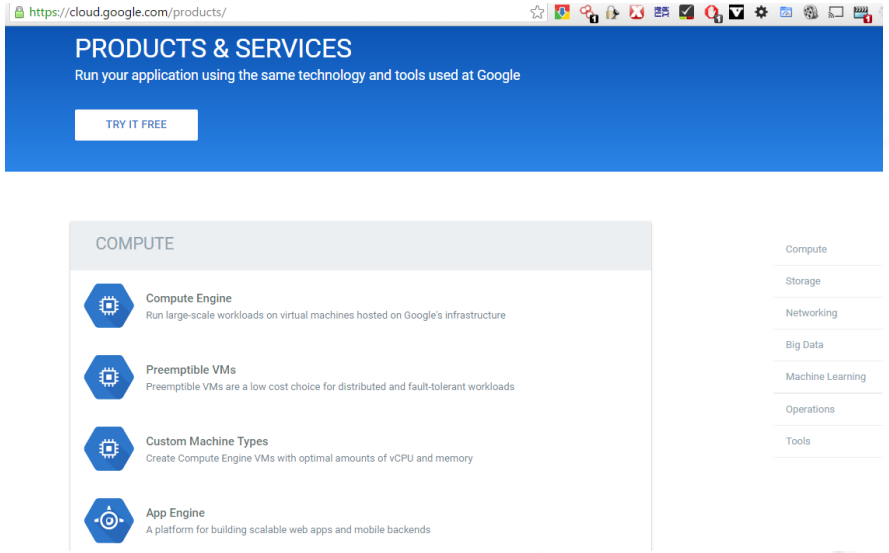
- Many organisations look to cloud providers to safeguard the privacy and security of personal data that they hold on behalf of organisations and users.
- Responsible management of personal/corporate data is a central part of creating the trust that underpins the adoption of cloud based services.
  - without trust, customers will be reluctant to use cloud-based services
- In cloud computing, effective risk management needs to follow a well-defined information security management processes.

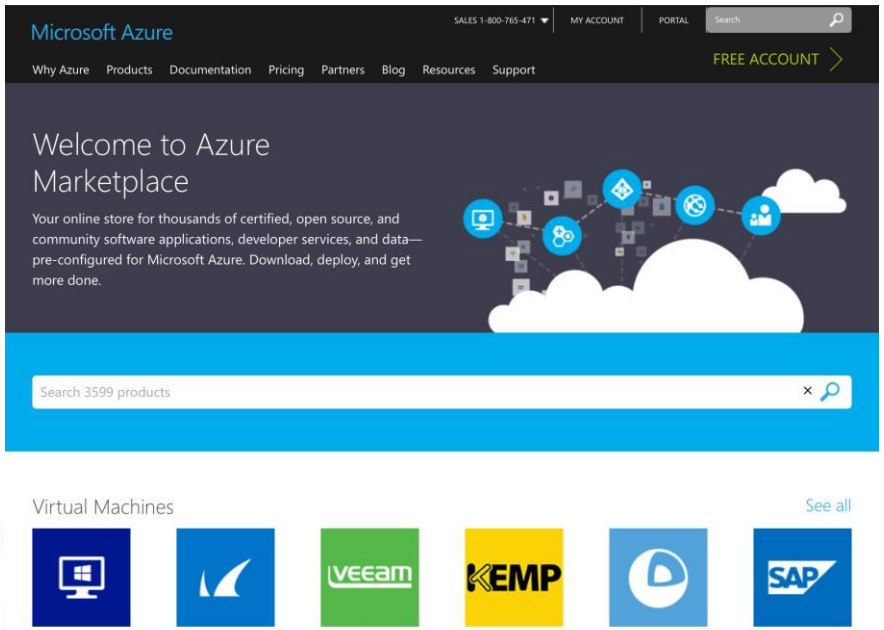
You cannot outsource risk !!!

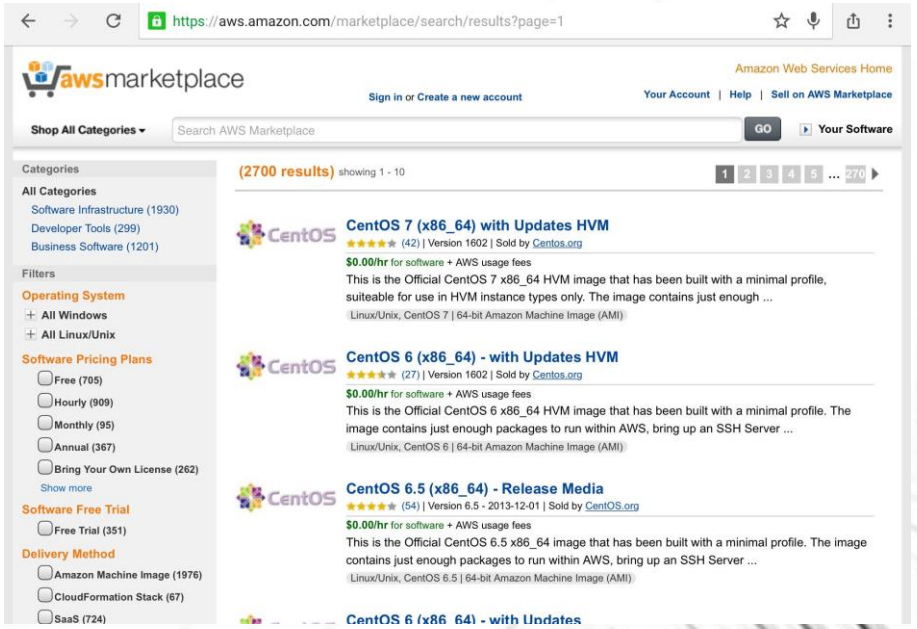
Cloud Marketplaces

Thousands of applications, services, infrastructure, security and data storage/analytics options are available in the cloud.

Not all are created equal

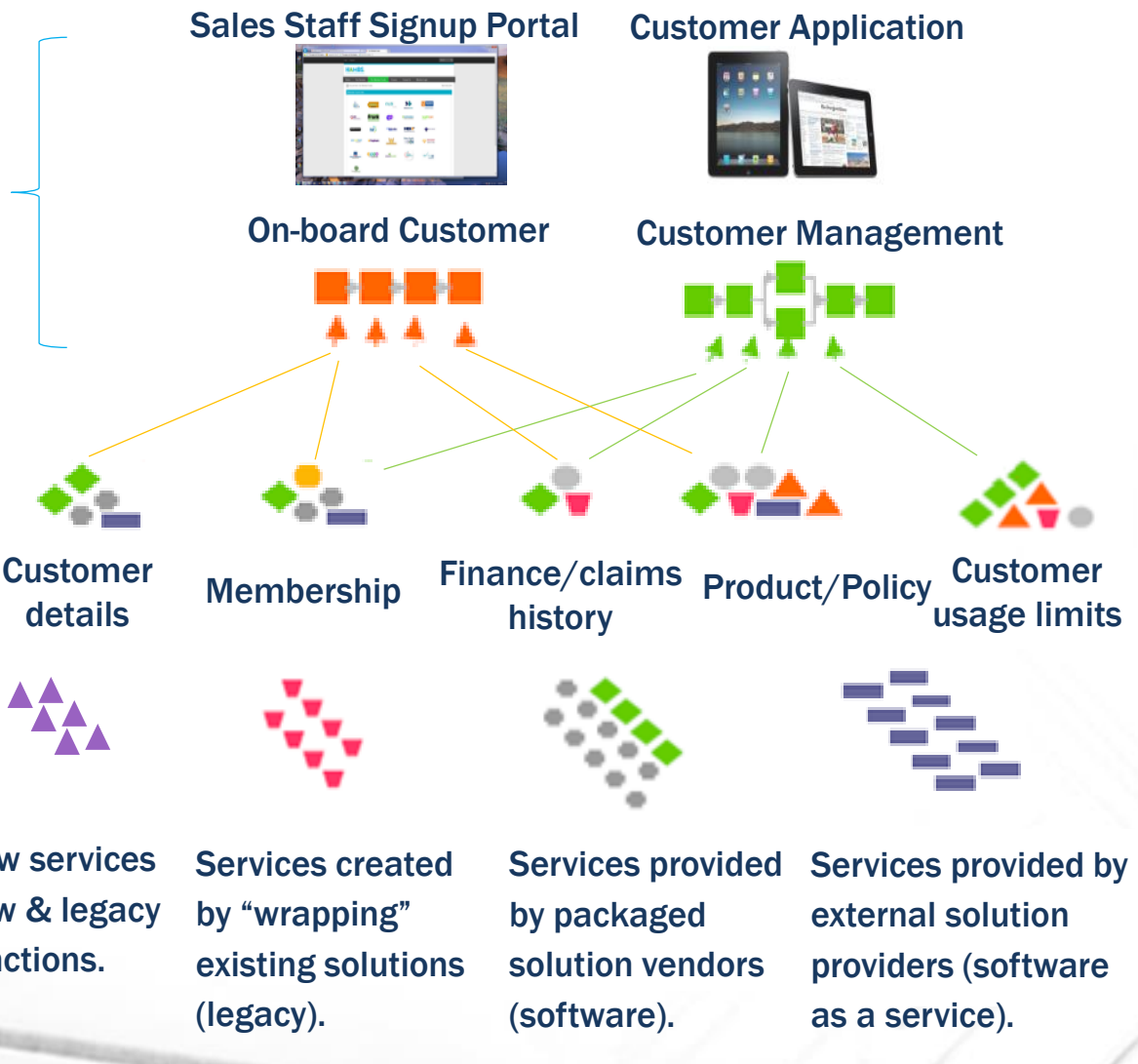






Applications are only limited by your imagination

Processes and applications created internally, by vendors and Industry supplied libraries.



Customer facing application

Business processes

Business services/ Core Processes

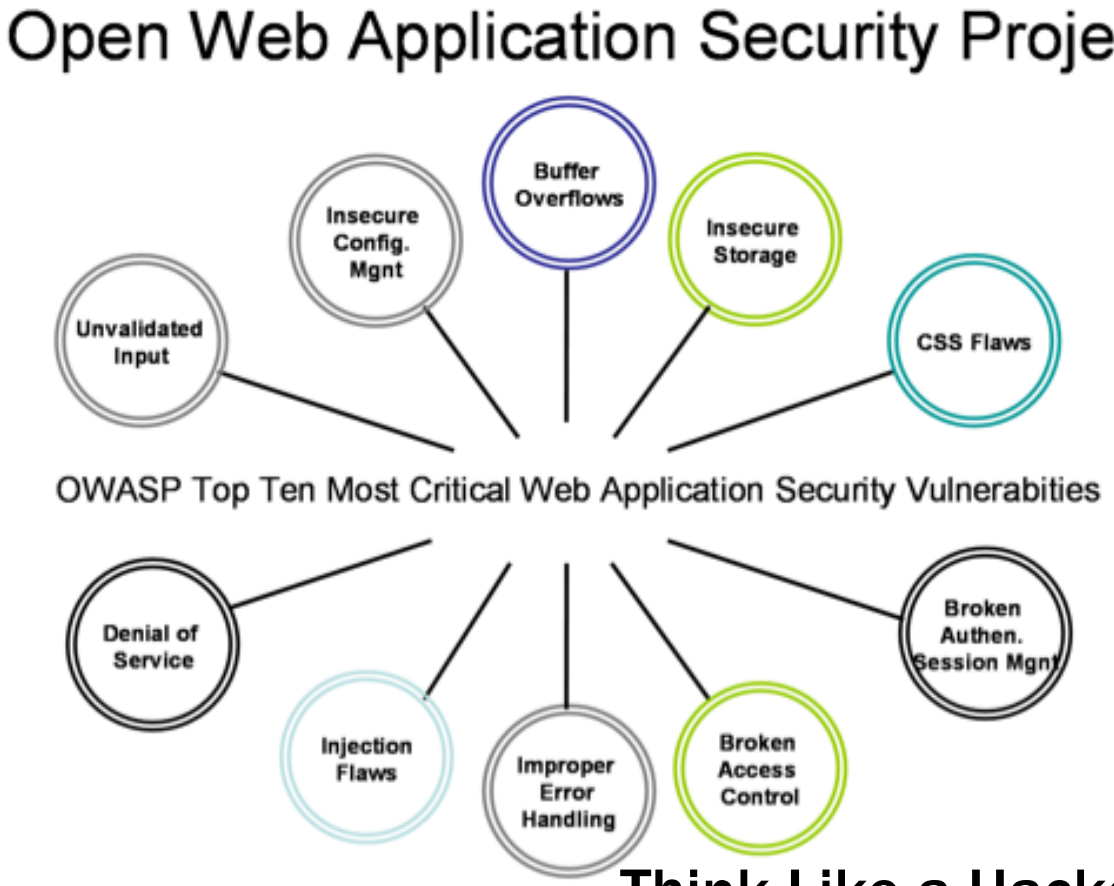
Raw services

Security, Privacy and Trust

Cloud Computing often invokes passionate security, privacy and trust debate

- Will I be considered compliant?
- Do I know where my data is?
- Will a lack of standards drive unexpected obsolescence?
- Is my provider really better at security than me?
- Are the hackers waiting for me in the cloud?
- How is my data safely stored and handled by cloud providers?
- Is my data privacy being managed adequately?
- Are the cloud providers standards/ certifications relevant to my business?
- Are Cloud providers adhering to laws and regulations relevant to my country and business?
- How are business disruption and outages kept to a minimum.
- Has the cloud provider secured their products and services to my required standards?
- Are all cloud providers equal?
- Globally incompatible legislation and policy govern cloud providers and services.
- Non-standard private & public cloud offerings.
- Lack of end-to-end risk management & compliance monitoring.
- Incomplete or incompatible integrated access/identity management (customer and management).
- Ad-hoc or non-contiguous availability and security incident response.
- Reliance on cloud provider for BCP/DRP capability.
- Will my cloud provider be transparent about governance and operational issues?

Attack Methods & Vulnerabilities



Other Vulnerabilities and Attack Vectors

- Lack of Secure Boundaries.
- Compromised Nodes, Systems and Services.
- Lack of Centralised Management/Standards.
- Scalability and Resource Exhaustion.
- User and Administrator Impersonation.
- Data Interception and Eavesdropping.
- Attacks Against Routing.
- Exploit poor cloud design and network zoning.

Think Like a Hacker and Hack Yourself

New Tools, Techniques and Exploits have been developed

Get Assistance From Cloud & Industry SME's

- Engage with experienced integrators.
  - Talk to proven industry experts.
  - Discuss with cloud provider.
- Utilise reference architecture, adhere to laws, regulations and desired business/policy needs.
  - Check with your chosen cloud supplier.
- Embrace flexible integration methods when establishing the required cloud capability.
- Construct a Cloud Controls Matrix to identify interdependencies with existing business/IT controls, policies and process.

Conclusion

- Cloud computing is a technology used for rapid development and use.
- Security is a key obstacle or opportunity which must be solved.
- Security is not just a technical problem it also involves standardisation, monitoring, alignment with laws, regulations and business ownership.
- Future cloud industry improvements are required to embrace and support holistic business risks.

Useful Links & Resources

Security

- Amazon
  - http://aws.amazon.com/security/
  - http://blog.trendmicro.com/category/aws/
- Azure
  - http://blog.trendmicro.com/category/azure/
  - http://www.microsoft.com/en-us/server-cloud/trusted-cloud/overview.aspx
- https://www.cisecurity.org/
- Cloud Security Alliance (CSA) https://cloudsecurityalliance.org/

Architecture and Sizing

- https://azure.microsoft.com/en-us/documentation/articles/architecture-overview/
- https://aws.amazon.com/blogs/aws/choosing-the-right-ec2-instance-type-for-your-application/
- https://support.rackspace.com/how-to/rackspace-cloud-essentials-choosing-the-right-size-cloud-server/

Shadow IT

- https://apps.google.com.au/learn-more/gartner_embracing_and_creating_value_from_shadow_it.html

- Em: Derek.Grocke@cyberops.com.au
- Em: sales@cyberops.com.au
- Ph: +61421056699