End to End Security for a Distributed Workforce

convergent

LEADERS IN THE IDENTIFCATION, ASSESSMENT & MITIGATION OF RISK

Dave Loveland, CISSP, OSCP, CRT, CPSA. Cloud Security Architect
Mathew Gilliat-Smith, EVP

convergent

How are working practices changing?

- Adjusting to new working practices
- Increased use of VPN
- Rapid upscaling of capability
- Temporary fixes need more permanent solutions
- The need to consider next generation tools in order to better enable a distributed workforce e.g. SaaS or PCoIP

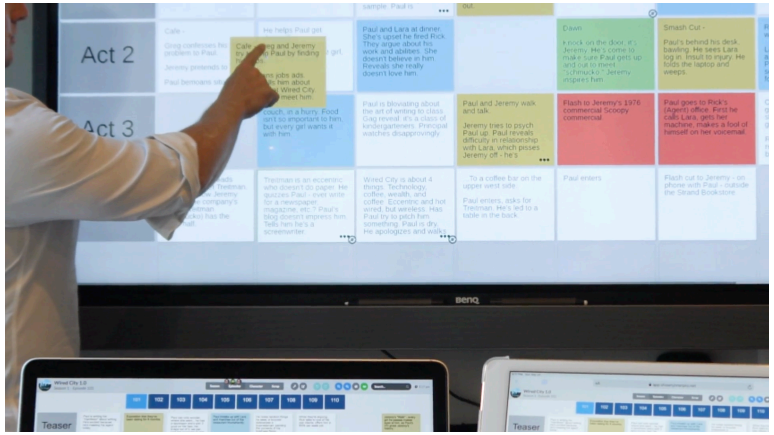
convergent

Collaborative Applications Transition to Distributed Workforce

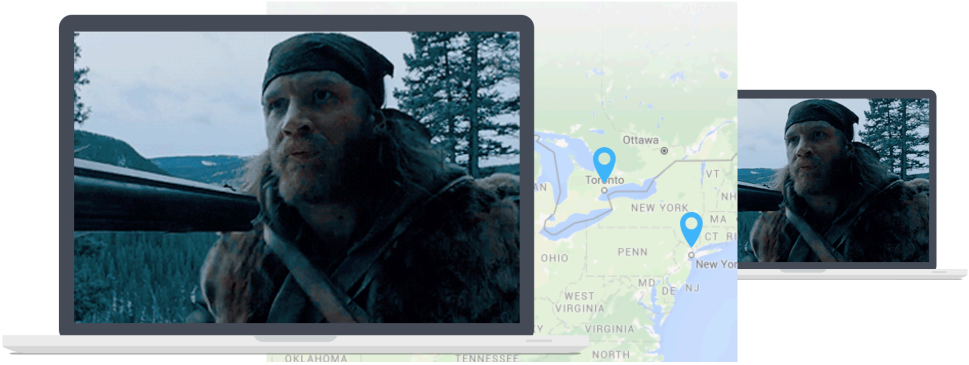
- Examples of New Applications
  - Collaborative scripting
  - Cloud based synchronisation
  - Dubbing Apps for remote editing

- So how do vendors take this step and do it securely?

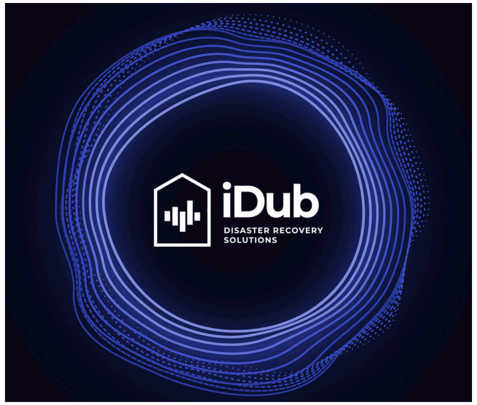
Script Collaboration



Synchronized Viewing



Dubbing Apps



Embracing SaaS Solutions Securely

	Security Measure	Reasons
	Continuous Security Monitoring & Alerting	Detect malicious activity and/or security misconfigurations
	Identity & Access Management	Secure access to the system and content
	Vulnerability Management	Provides effective management of vulnerabilities
	Independent Security Testing	Identify & remediate vulnerabilities within the platform.
	Security Incident Management	Customers informed if a compromise occurs. Provider able to manage incidents.
	Multitenant isolation	Prevent data leakage between customers
	Protection of content	Provider has no access to content. Content encrypted in transit & at rest
	Secure Use Guides	Customer is using the service securely

- Can I assume that the SaaS service is secure?

- What can I look for to establish if the service is secure?

- Other certifications already held may be relevant here

convergent

Remote Visualisation Solutions via On-Prem or Hybrid Cloud

- This type of tool is becoming more prevalent for the distributed workforce as it offers comparable levels of performance with a high-end workstation.
- Is the solution secure by default?
- In this scenario, security is the full responsibility of the user (vendor)
- Key security considerations are:

	Guidance	Reason
	Permit authorised devices only	Only authorised clients can connect to the service
	Secure the management console with a commercial certificate	Avoid MITM attacks
	Subscribe to the vendors security advisory service	Be aware of security vulnerabilities detected by the vendor
	Apply updates for clients and Management console	Mitigation against known vulnerabilities
	Change the default password for the management console. Use MFA for endpoints.	Avoid unauthorised access to the console or endpoints.
	Enable transport encryption	Avoid sending credentials and/or data in the clear
	Enable Security logging & alerting	Ability to detect malicious behaviour/connections
	Disable access to local devices such as USB.	Reduce the risk of content being extracted from the platform.
	Lock down client config options	Maintain a uniform security configuration across all endpoints.

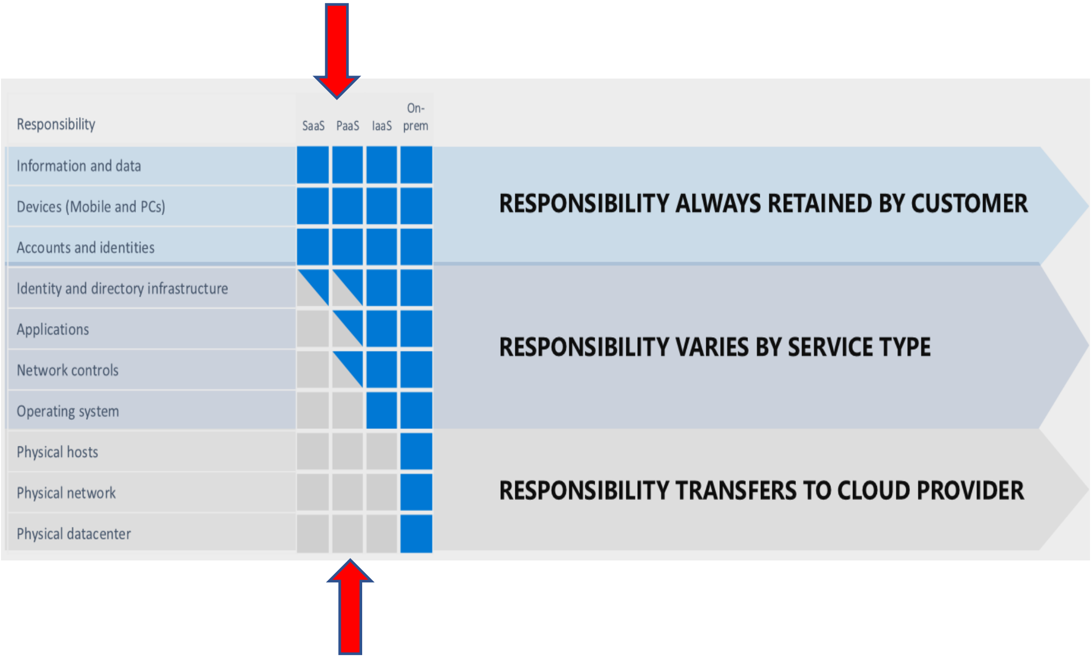
convergent

Remote Workstation Solutions Leveraging Cloud (PaaS)

Distributed working solutions leveraging cloud (PaaS)

amazon WorkSpaces   Microsoft Azure Windows Virtual Desktop   vmware Horizon

- Secure by default?
- Be aware of the PaaS shared responsibility model, you will be responsible for:
  - Security of the cloud environment
  - Security of the virtual workstation



Responsibility	SaaS	PaaS	IaaS	On-prem
Information and data	■	■	■	■
Devices (Mobile and PCs)	■	■	■	■
Accounts and identities	■	■	■	■
Identity and directory infrastructure	◪	◪	■	■
Applications	□	◪	■	■
Network controls	□	◪	■	■
Operating system	□	□	■	■
Physical hosts	□	□	□	■
Physical network	□	□	□	■
Physical datacenter	□	□	□	■

RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER

RESPONSIBILITY VARIES BY SERVICE TYPE

RESPONSIBILITY TRANSFERS TO CLOUD PROVIDER

convergent

Remote Workstation Solutions Leveraging Cloud (PaaS)

Suggested Guidance for the Cloud environment

	Guidance	Reason
	Cloud services configured as per the cloud vendor best practice	To avoid common security issues
	Perform independent security assessment of the cloud environment	Get assurance that adequate security controls are in place
	Include cloud security logs into your existing alerting solution	Detect malicious activity and/or security misconfigurations
	Implement MFA and integrate cloud admin console into Active Directory	Avoid unauthorised access to the cloud
	Block access to by BYOD devices to the virtual workstation environment	Reduce the attack surface

Suggested Guidance for the Virtual Workstation

	Guidance	Reason
	Install anti-malware	Detect viruses and malware
	Perform automated patching of apps and the OS	Remediate vulnerabilities
	Implement MFA and integrate workstation logon with Active Directory	Avoid unauthorised access to the workstations
	Implement a secure virtual networking connection to the content	Ensure that users can only get to the required network resources
	Perform independent security assessment of the workstation build	Get assurance that adequate security controls are in place
	Consider how the content will be protected in transit and at rest within the cloud	Ensure cloud provider has no access to content in transit or at rest

In Summary

End to End Security for a Distributed Workforce
convergent
experts in the identification, assessment and mitigation of risk

- Next generation of tools offer real benefits
- Security is not necessarily there by design
- Get some assurance that they have been configured or are being operated securely
- Remember to securely decommission any temporary solutions
- Make sure your team are aware of their obligations for distributed working

More Information & Discussion at our Virtual Booth

http://www.convergentrisks.com/

convergent

info@convergentrisks.com

‘Insights’ White Paper

‘Current and Future State of Production’

Cloud Security Reviews

Q&A Surgery