Facing the challenges of Desktop Virtualisation in Air Gapped Systems

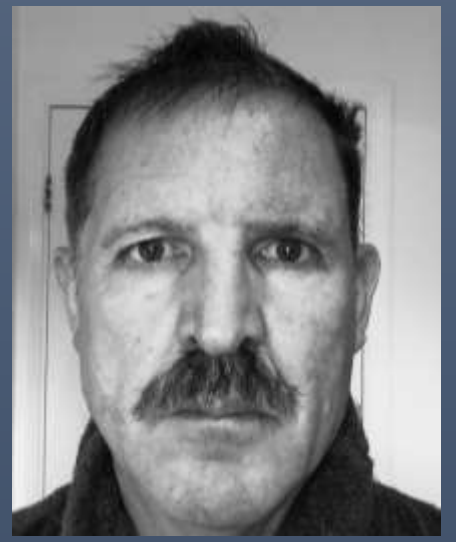
Jonathan Culver – Senior Enterprise PreSales Engineer – IGEL

EUC Forum – Winter Meeting

21st November 2023

Who is this bloke?

- Workshop Engineer
- Field Service Engineer
- Technical Support Engineer
- Microsoft IT Instructor
- PreSales Engineer



- EMEA region – Moscow to Cape Town & Dublin to Dubai
- FS&I, Government & Defence, Oil & Gas (E&P), Automotive/F1, M&E

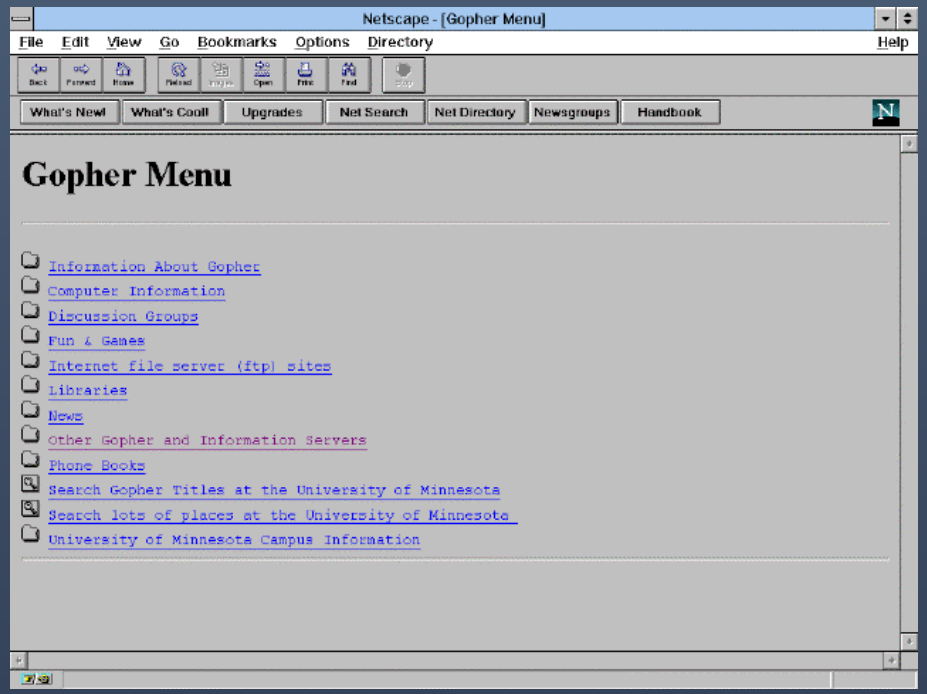
Preface

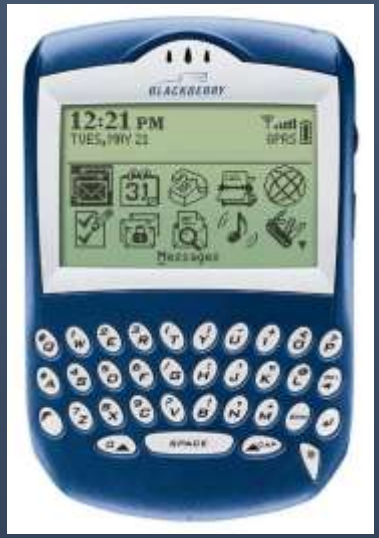
This session will provide field notes and practical experiences when working on customer sites; from planning, installing, managing and maintaining desktop virtualisation within an air gapped system.

This will not be a deep dive technical session, more so observation, preparation and reflection.

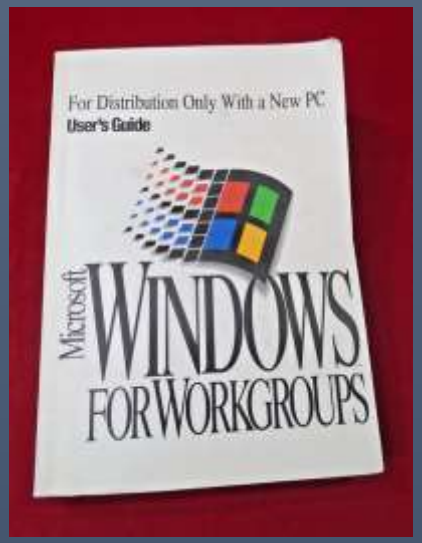
1984 - 1994

- The first 10 years of my career were air gapped
- Emergence of World Wide Web – 1993
- Blackberry 5810 – 2002
- Apple iPhone – 2007



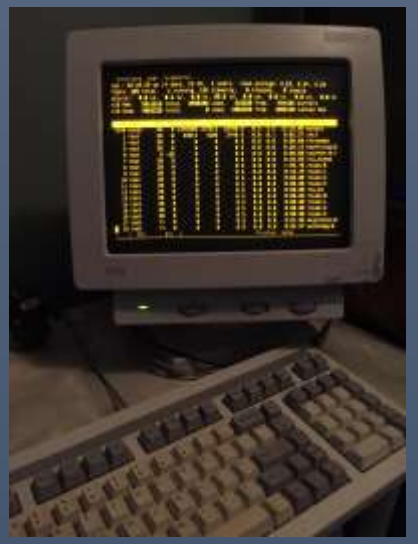


How did we work before the Internet?



Microsoft TechNet

From Mainframe Terminals to Thin Clients



1970s – 1990s

- IBM 3270, DEC VT100, Wyse WY-50 Terminals

- PCs with Terminal Emulator cards & software

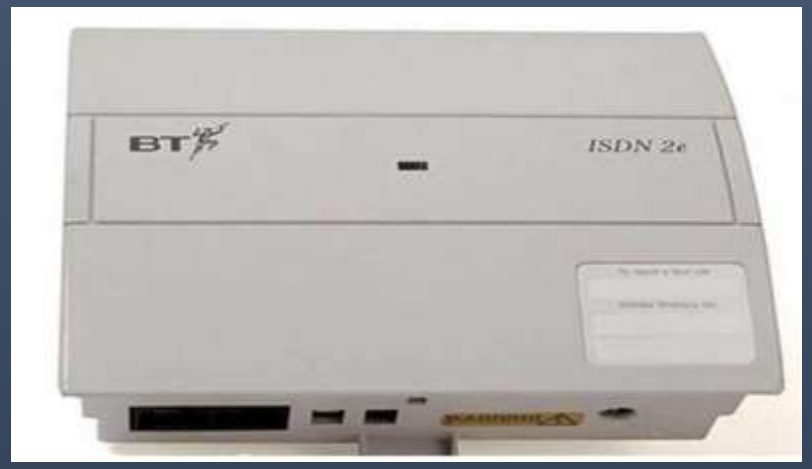
2000s – 2020s

- Wyse Winterm 2000
- Dell Optiplex 3000, HP t755, Lenovo M75Q

https://www.itpro.com/hardware/can-thin-clients-be-an-antidote-to-the-sprawling-attack-surface

Evolution of Networked Systems

- Physically Disconnected – Token Ring / Ethernet
- Bulletin Boards – Wildcat, modems
- CompuServe, modems
- Full Internet Connection



WHY AIR GAPPED SYSTEMS?

The Need For Air Gapped Systems

- Physical Air Gap
- Logical Air Gap

- Improved Security & Privacy
- Increased control – concentrated on-site, no remote access
- Enhanced regulatory compliance, due to lower inherent risks
- Improved Performance & Reliability – less malware, unscheduled updates
- Cost Reduction – less equipment to buy & manage

Organisation Types

Organisations that require high levels of IT system security typically limit or block Internet connections to Users, Endpoints, Desktops and Systems. Some examples:-

- Government & Defence
- Financial Services & Insurance
- Pharmaceutical
- Automotive
- Oil and Gas (E&P)
- Media & Entertainment

Examples

- Critical infrastructure
  - Power generation plants, Pharma labs
- Anything military
  - Buildings, vehicles, ships & ‘planes, temporary deployments
- Industrial
  - Just cables & patch panels, no switches or routers
- Testing networks
  - Developers are dangerous, they do things no one else will
- Video Editing & SFX – IP cannot escape until theatrical release

Preparation Processes

- Mindset Preparedness
- Product and Project documentation
- Timescales
- Travel and Customer site access
- Prerequisites
- Hardware
- Software
- Network
- Communications options

Mindset Preparedness

- Are you prepared for “The Bunker”?
  - Resilience
    - There will be lots of challenges
  - Pragmatism
    - You will need to find workarounds
    - Some issues cannot be solved
  - Negotiation
    - You may need to ask for security change management
  - Patience
    - You will be there for longer than anticipated
    - You may not complete the work you had planned

Be prepared to be underprepared, but not unprepared !

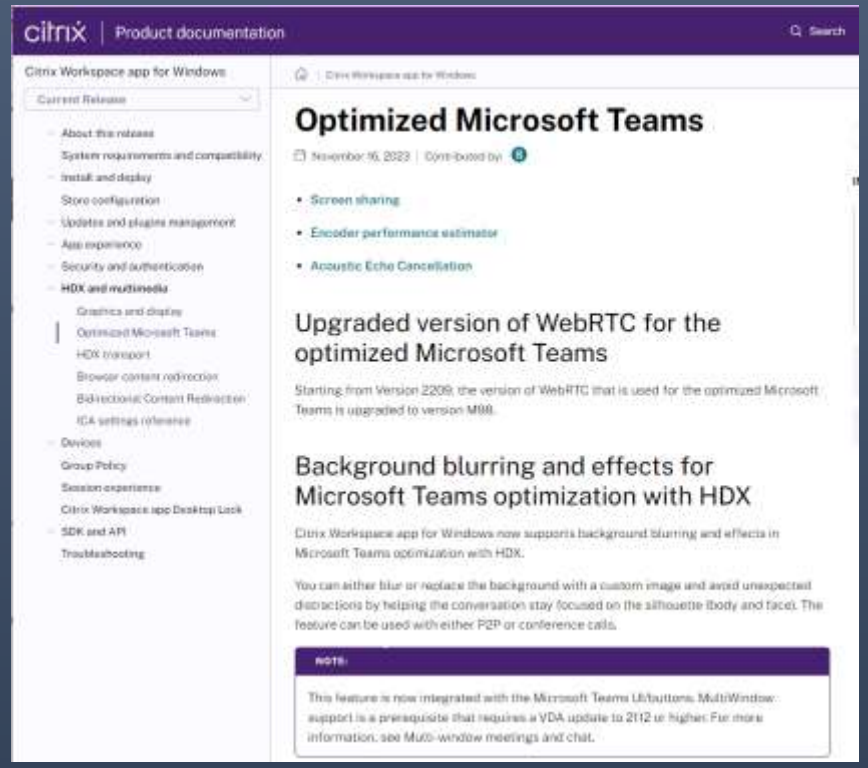
Project and Product documentation

- Does your Project Plan adhere to regulatory requirements
- Who signs off the plan, are they authorised and SC cleared
- Does the Change Control process differ in an Air Gapped system
- Project timescales must factor in the challenges of Air Gapped Systems
  - Has this been defined? This will add cost and resources

Project and Product documentation cont.

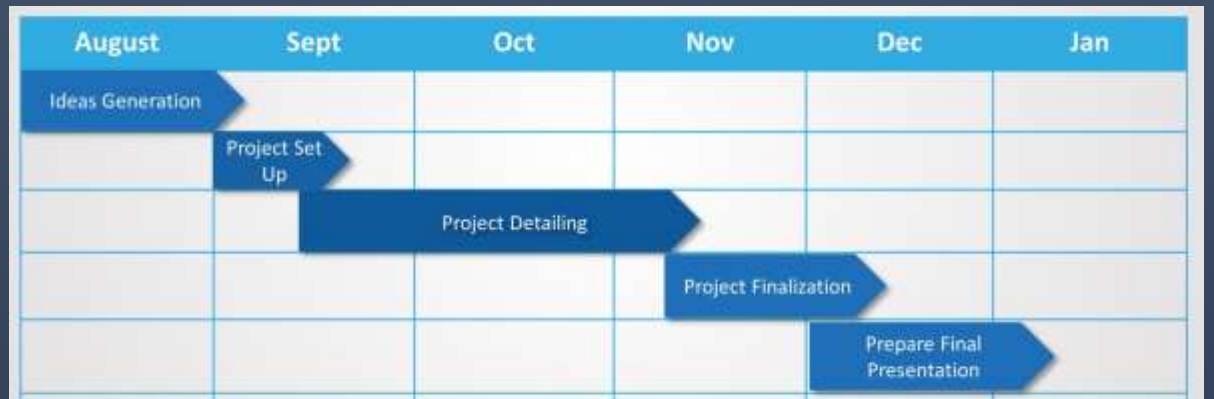
- Offline access to manuals, KB articles, community channels
  - Does the customer have these on site?
  - Can you call your colleagues / vendors / partners?

- Unlikely you can “search it up” on Google



Timescales

- Customer agreement on timescales to build, test and deploy
- Site access hours and working hours
- Hardware delivery, setup and testing
- Software delivery, setup and testing
- Arrange for Customer resources aligned to the project
- UAT and DEX timescales – when are Users available for test and review



Travel and Customer site access

- Passport & Visas / Security Clearance / Business Invitation / Languages
- Arrival time – security checks, car, ID, bags, equipment
- Does your airline allow computer equipment in the hold
- Do you have a colleague who is SC cleared, just in case
- Agreed site access times, HSE briefing

Prerequisite checklist before site visit

- Access to server room, network equipment & Users workplace
- Arrange assistance from:-
  - IT Management
  - Server & Storage engineers
  - Virtualisation and Desktop administrators
  - AD administrators
  - DB administrators
  - Network engineers
  - Security Architects
- Access for bio-breaks, refreshments etc

Hardware requirements

- On premises deployment only
  - DaaS / Virtual Private Cloud; Citrix, VMware, AWS, AVD
- Servers
- Storage
- Networking equipment
- Thin client endpoints, management workstations
- Monitors, audio peripherals, keyboard, mice, smartcard readers/cards
- Power & cooling
- Does the hardware meet security in manufacturing & supply chain
  - Country of origin

Software requirements

- Hypervisor & Hypervisor Managers
- VDI Broker, Agents & Clients
- Virtual Desktop golden image creation and management, OS & Apps
- Endpoint OS, VDI Client & security agents (AV, DLP, EDR, NAC)
- Licensing – offline/trust, Per server, desktop, endpoint (MAC based),

Software requirements cont.

SOFTWARE BILL OF MATERIALS
https://www.cisa.gov/sbom

- Cross compatibility table of software versions
  - Hypervisor, VDI broker/management, agents, clients, UC, AV)
- Obtaining and Applying Updates and Hotfixes
  - Frequency & Schedule
- Software security requirements, in development & supply chain
  - Provide File Hashes for corruption and tampering checks
- Penetration Testing – by the vendors & customers, remediation plans

Network requirements

- Physical network access
  - Copper / Fibre
  - Bandwidth, ports 1494, 4172, 3389, 8443
- Network Access Control
  - 802.1x & certificates
  - Operating Software ID
  - Forescout, Cisco ISE, Aruba ClearPass, Fortinet
- Temporary Security Exceptions
  - Whitelist devices
  - Negotiate the timescales and alternative workarounds

Communications Options

- What external connections are possible?
- Internet – Wi-Fi, Ethernet, mobile ‘phone tether
- Mobile networks – O2, EE, Three, Vodafone
- Proxy Servers & PAC files
- USB Sneakernet
- Notepad & pen

- RFC 1149

Working Practices

- Physical access to keyboard and mouse, or “over the shoulder mode”
- Remote shadowing of systems for troubleshooting
- Collection and extraction/redaction of logs and supporting info

In Conclusion

- Perform thoroughly detailed discovery and qualification
- Agree plans and contingencies with the customer
- Be aware of how much extra thinking you must do
- Have patience, it can be enjoyable!

THANK YOU

Jonathan Culver

https://www.linkedin.com/in/jonathan-culver-a152619/