T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Infrastructure

Assignment 1 - Workbook - Distinction

Guide standard exemplification materials

v1.1: Specimen assessment materials
January 2023
603/6901/2

Internal reference: DSS-GSEM-22

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Infrastructure

Guide standard exemplification materials

Assignment 1

Workbook – Distinction

Contents

About this assignment

Introduction

All evidence should be placed in this workbook.

Save your document regularly as you work through the assignment. It is recommended you save after inserting each piece of evidence.

You can use multiple copies of the floor plan as required - copy a blank version from the appendix and paste where required. It is recommended that you use a new copy of each floor plan for task 1 and task 3.

Submit this workbook in .pdf format at the end of the assignment using the file naming convention. Surname_Initial_student number_Workbook1

For example Smith_J_123456789_Workbook1.pdf

Evidence

Print screens of websites should be captioned with the following information:

- article title
- website address
- date accessed
- publisher

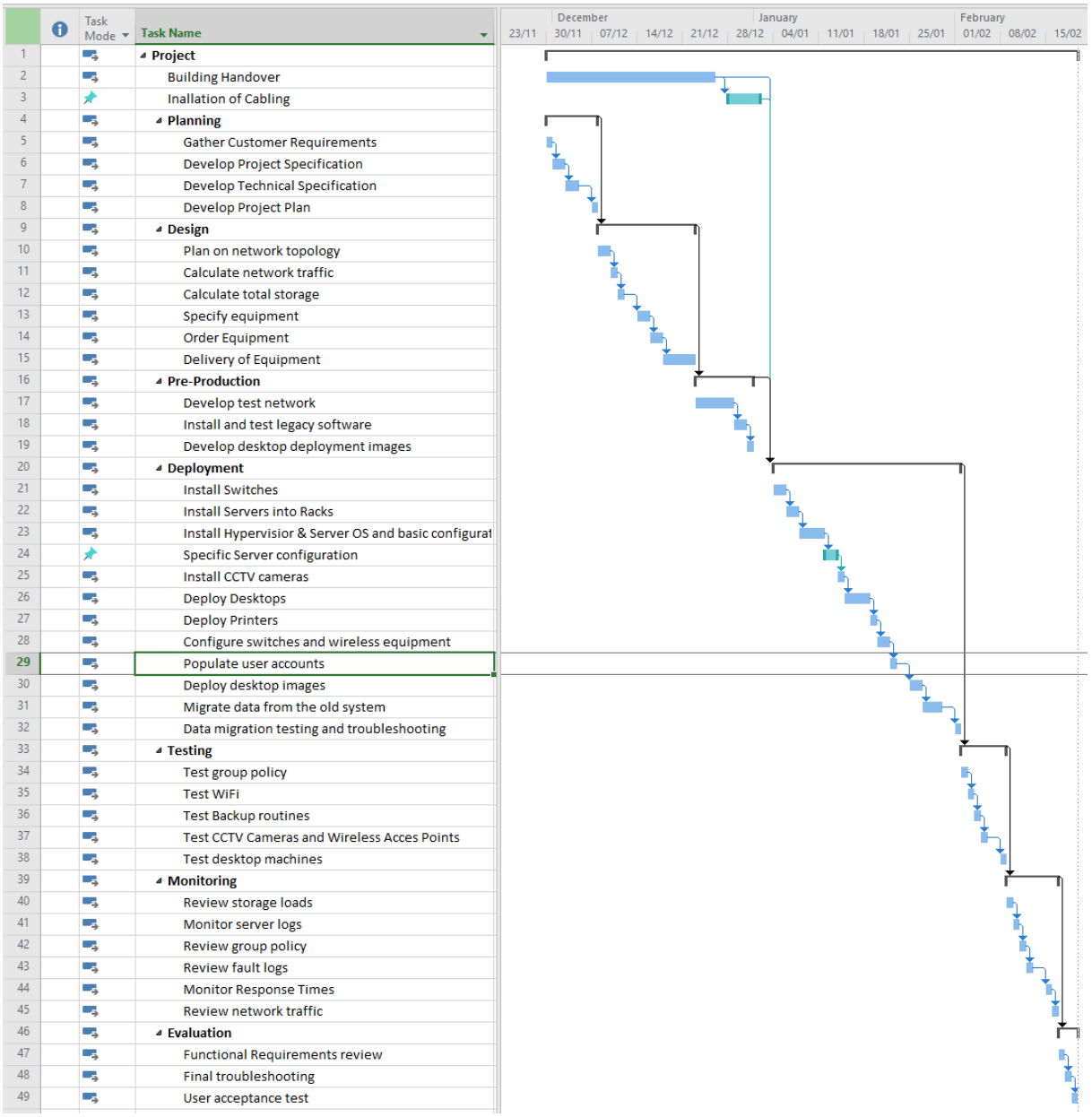
All print screens should be numbered and linked to the task. For example, task 1, evidence 2 would be shortened to 1.2.

Ensure each print screen is labelled with a brief description of what is being shown.

Task 1: planning

Project plan and Gantt chart

	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1		**Project**	**60 days**	**Mon 30/11/2**	**Fri 19/02/21**	
2		Building Handover	20 days	Mon 30/11/2	Fri 25/12/20	
3		Inallation of Cabling	5 days	Mon 28/12/2	Fri 01/01/21	2
4		**Planning**	**6 days**	**Mon 30/11/2**	**Mon 07/12/2**	
5		Gather Customer Requirements	1 day	Mon 30/11/2	Mon 30/11/2	
6		Develop Project Specification	2 days	Tue 01/12/20	Wed 02/12/2	5
7		Develop Technical Specification	2 days	Thu 03/12/20	Fri 04/12/20	6
8		Develop Project Plan	1 day	Mon 07/12/2	Mon 07/12/2	7
9		**Design**	**11 days**	**Tue 08/12/20**	**Tue 22/12/20**	**4**
10		Plan on network topology	2 days	Tue 08/12/20	Wed 09/12/2	
11		Calculate network traffic	1 day	Thu 10/12/20	Thu 10/12/20	10
12		Calculate total storage	1 day	Fri 11/12/20	Fri 11/12/20	11
13		Specify equipment	2 days	Mon 14/12/2	Tue 15/12/20	12
14		Order Equipment	2 days	Wed 16/12/2	Thu 17/12/20	13
15		Delivery of Equipment	3 days	Fri 18/12/20	Tue 22/12/20	14
16		**Pre-Production**	**7 days**	**Wed 23/12/2**	**Thu 31/12/20**	**9**
17		Develop test network	4 days	Wed 23/12/2	Mon 28/12/2	
18		Install and test legacy software	2 days	Tue 29/12/20	Wed 30/12/2	17
19		Develop desktop deployment images	1 day	Thu 31/12/20	Thu 31/12/20	18
20		**Deployment**	**21 days**	**Mon 04/01/2**	**Mon 01/02/2**	**16,2,3**
21		Install Switches	2 days	Mon 04/01/2	Tue 05/01/2:	
22		Install Servers into Racks	2 days	Wed 06/01/2	Thu 07/01/2:	21
23		Install Hypervisior & Server OS and basic configurat	2 days	Fri 08/01/21	Mon 11/01/2	22
24		Specific Server configuration	2 days	Tue 12/01/2:	Wed 13/01/2	23
25		Install CCTV cameras	1 day	Thu 14/01/2:	Thu 14/01/2:	24
26		Deploy Desktops	2 days	Fri 15/01/21	Mon 18/01/2	25
27		Deploy Printers	1 day	Tue 19/01/2:	Tue 19/01/2:	26
28		Configure switches and wireless equipment	2 days	Wed 20/01/2	Thu 21/01/2:	27
29		Populate user accounts	1 day	Fri 22/01/21	Fri 22/01/21	28
30		Deploy desktop images	2 days	Mon 25/01/2	Tue 26/01/2:	29
31		Migrate data from the old system	3 days	Wed 27/01/2	Fri 29/01/21	30
32		Data migration testing and troubleshooting	1 day	Mon 01/02/2	Mon 01/02/2	31
33		**Testing**	**5 days**	**Tue 02/02/2:**	**Mon 08/02/2**	**20**
34		Test group policy	1 day	Tue 02/02/2:	Tue 02/02/2:	
35		Test WiFi	1 day	Wed 03/02/2	Wed 03/02/2	34
36		Test Backup routines	1 day	Thu 04/02/2:	Thu 04/02/2:	35
37		Test CCTV Cameras and Wireless Acces Points	1 day	Fri 05/02/21	Fri 05/02/21	36
38		Test desktop machines	1 day	Mon 08/02/2	Mon 08/02/2	37
39		**Monitoring**	**6 days**	**Tue 09/02/2:**	**Tue 16/02/2:**	**33**
40		Review storage loads	1 day	Tue 09/02/2:	Tue 09/02/2:	
41		Monitor server logs	1 day	Wed 10/02/2	Wed 10/02/2	40
42		Review group policy	1 day	Thu 11/02/2:	Thu 11/02/2:	41
43		Review fault logs	1 day	Fri 12/02/21	Fri 12/02/21	42
44		Monitor Response Times	1 day	Mon 15/02/2	Mon 15/02/2	43
45		Review network traffic	1 day	Tue 16/02/2:	Tue 16/02/2:	44
46		**Evaluation**	**3 days**	**Wed 17/02/2**	**Fri 19/02/21**	**39**
47		Functional Requirements review	1 day	Wed 17/02/2	Wed 17/02/2	
48		Final troubleshooting	1 day	Thu 18/02/2:	Thu 18/02/2:	47
49		User acceptance test	1 day	Fri 19/02/21	Fri 19/02/21	48



	Task Mode	Task Name
1		**Project**
2		Building Handover
3		Inallation of Cabling
4		**Planning**
5		Gather Customer Requirements
6		Develop Project Specification
7		Develop Technical Specification
8		Develop Project Plan
9		**Design**
10		Plan on network topology
11		Calculate network traffic
12		Calculate total storage
13		Specify equipment
14		Order Equipment
15		Delivery of Equipment
16		**Pre-Production**
17		Develop test network
18		Install and test legacy software
19		Develop desktop deployment images
20		**Deployment**
21		Install Switches
22		Install Servers into Racks
23		Install Hypervisior & Server OS and basic configurat
24		Specific Server configuration
25		Install CCTV cameras
26		Deploy Desktops
27		Deploy Printers
28		Configure switches and wireless equipment
29		Populate user accounts
30		Deploy desktop images
31		Migrate data from the old system
32		Data migration testing and troubleshooting
33		**Testing**
34		Test group policy
35		Test WiFi
36		Test Backup routines
37		Test CCTV Cameras and Wireless Acces Points
38		Test desktop machines
39		**Monitoring**
40		Review storage loads
41		Monitor server logs
42		Review group policy
43		Review fault logs
44		Monitor Response Times
45		Review network traffic
46		**Evaluation**
47		Functional Requirements review
48		Final troubleshooting
49		User acceptance test

Legal requirements

Health & safety – Good health and safety covers a wide range of areas from PPE to display screen equipment. It is about making sure that you are adequately trained and supported in doing your job reducing stress and risks. It establishes the legal requirements for employers to protect the health, safety, and welfare of all employees.

Manual handling – When working with the various items of equipment that will require installation. Good manual handling is required to ensure you do not cause damage to yourself or the equipment. Being fully trained in manual handling and good manual handling technique is essential to help mitigate the risks. Servers are very large, heavy, and awkward devices and combined with the cost of the equipment it is essential that good technique is adopted.

COSHH – When moving equipment, it might be required to use either compressed air or anti-static foam as part of housekeeping routines. COSHH, exists to protect you from hazardous chemicals whilst ensuring you use suitable procedures when using them.

Display screen equipment – as an infrastructure technician you will be required to work for long hours with a computer. To prevent back pain, aching limbs, eye strain or fatigue it is important that the computer workstation is setup correctly. Regular breaks should be taken alongside a varied workload as to prevent strains.

Data Security

Data Protection (2018)/GDPR – As the companies' data, which could include sensitive personal data that will need to be migrated from the old site to the new one. It is crucial that data is handled in a way that ensures appropriate security. This would cover data migrated to the cloud or physically during the moving of physical equipment.

Backing-up – A company's data is its lifeblood, it is trends, sales, customer records and other digital assets. It is imperative that data is backed up before any migration of data and/or equipment. Data will need to be moved physically or digitally from the old site to the new one. Regular backups should be taken daily if not live for the business as so much digital content will be created based on being a web and multimedia business. Also, the systems need to be backed up so that if migration fails or some upgrade fails, the system can be rolled back to a previous good state.

Antistatic precautions – Even though new equipment is being purchased and installed, components might still need to be handed that could be considered static sensitive. It is important that when handing these components suitable anti-static precautions are taken to prevent damage. These include the use of wrist straps, antistatic mats and using anti-static bags when handling and moving components. A good example of this is when installing hard disks into the new servers to increase the capacity.

Remote access – Staff and sometimes customers might require remote log in capability. Some of this could be achieve by using cloud based authenticated storage with multi factor authentication. A confirmation code could be sent one the user has entered account details that match those stored in active directory.

Physical Threats and Security Countermeasures:

Fire

The first risk to the building is fire, this can cause major disruption to the business whilst the building is repaired, and equipment replaced. With such a large amount of electrical equipment and important data all located in one space it is essential that the server room is protected as far as is reasonable. The first step in the addition of a gas suppression system (for example, CO2) this will prevent the fire developing. This has been shown on the floor plan with annotation. Throughout the building, a sprinkler system and extinguishers will be placed to help reduce any fire from spreading. Staff should also be fully versed with what to do in the unlikely event of a fire.

Theft

Theft of equipment will not only cost the business money to replace the hardware, but it is the loss of the data stored on them. All equipment should be tagged with asset numbers and for fixed installations, the use of Kensington locks or other devices to lock the physical equipment. All data should be stored to the main servers, that way if any computers are stolen, the amount of information on the device will be reduced.

All laptops or other portable devices should be managed using a form of MDM software and remote wiped if lost or stolen.

The building should also implement CCTV cameras throughout, as shown on the plan a combination of external IP cameras and internal ones will provide a suitable deterrent in the high traffic areas. The CCTV feed could be stored on prem, or stored to cloud service, so that it would be secure if something happened to the building. The CCTV infrastructure would run over a separate physical network to isolate it from the wireless and wired network.

Electrical and Heating

The server room is where the main countermeasures would be placed and these mainly comprise of UPS and air conditioning units. The UPS will help reduce the risk of electrical damage to equipment by providing a constant quality of electricity free of surges and drops. Also, in the case of a failure the UPS could provide enough power to backup and or power down the network without damaging the equipment or data.

The air conditioning units will be used to help cool the operating temperature in the server room. This will ensure that the equipment does not overheat and should extend the life of the equipment as excess temperature requires the devices cooling system to work harder.

Flood & Extreme Weather

The risk of flood damage and extreme weather have been considered even though the risk of it occurring is very slight. A failover plan would be in place to switch to a cloud-based environment with staff working remotely or switching to another site. The combination of cloud backup and the other countermeasures would help mitigate the risk of downtime.

Digital Threats and Security Countermeasures

Equipment Failure

The plan is not to worry about the desktop infrastructure as this can be easily swapped out in times of device failure. The focus should be on the switching, data storage and server failure. These typically are where a single point of failure can have dramatic repercussions for the business. Servers will be VM based with a mirror server available on prem to fail over to. The switches will have two core switches that connect to multiple edge switches around the building. This way if a core switch fails a level of redundancy exists with traffic being re-routed.

Malware

A number of approaches will be adopted to help reduce the threats from malware, firstly all desktop and server computers will have update software patching and anti-security in place. The virus checkers will be set to live scan all files and constantly monitor the devices. Users will not be able to install software or use portable storage as this will be locked down with group policy.

The network will also include a Network Security Appliance with firewall to monitor all incoming data preventing the typical day-to-day incursions that could bring down a network.

Hacking

To reduce the risk of hacking, all desktop and server storage will be encrypted to ensure that if anything is accessed the data is safe. Unused network ports around the building will be disconnected at the patch panel to ensure they cannot be used to break into the network. The wireless network will be run over a separate VLAN, isolating it from the physical network traffic. Wireless access will require authentication with active directory to ensure that all users have valid accounts.

Remote access

Remote access into the business will required a two-factor authentication system using a RSA security token to create the VPN connection into the business. This functionality will only be made available to users who require this and cannot work in any other way. Other alternative approaches include cloud based storage of non-sensitive documents, reduce the need for remote access into the physical network.

Proposed changes to the workplace

Security Cameras: I propose we install security cameras in strategic locations around the site. These include 2 external IP cameras capable of seeing down 2 sides of the building each. This will act as a first line deterrent and provide exterior coverage to prevent any forced access into the building.

I will also install Fisheye (360 degree) cameras in 4 strategic locations so that we can see movement in key internal rooms. In case of an intruder, we will then be able to see where they have been and track what they are doing.

Server Room upgrades:

Air conditioning - For the server room environment to be protected, the room should be fitted with high quality air conditioning to maintain a constant temperature. I propose we install three server room air conditioning units will be installed. These will run on a two on and one-off rotation to extend the life of the air conditioning units and provide spare capacity if one of the units fail. These are designed to keep the room running at a suitable temperature to ensure the servers do not overheat. Maintaining data security and preventing downtime in relation to heat based failure.

UPS Battery Backup - The UPS battery units will provide a double function, firstly they will maintain a constant current of electricity into the server room preventing any spikes or surges from damaging the electrical infrastructure. Secondly, in the event of a power loss they would be able to sustain the servers until the power resumed or provide enough time to graciously power down the servers.

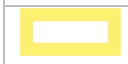
Reinforced walls - The server room will have reinforced walls rather than the standard plasterboard internal walls. This will ensure the room is more secure and act as a stronger barrier against fire and theft.

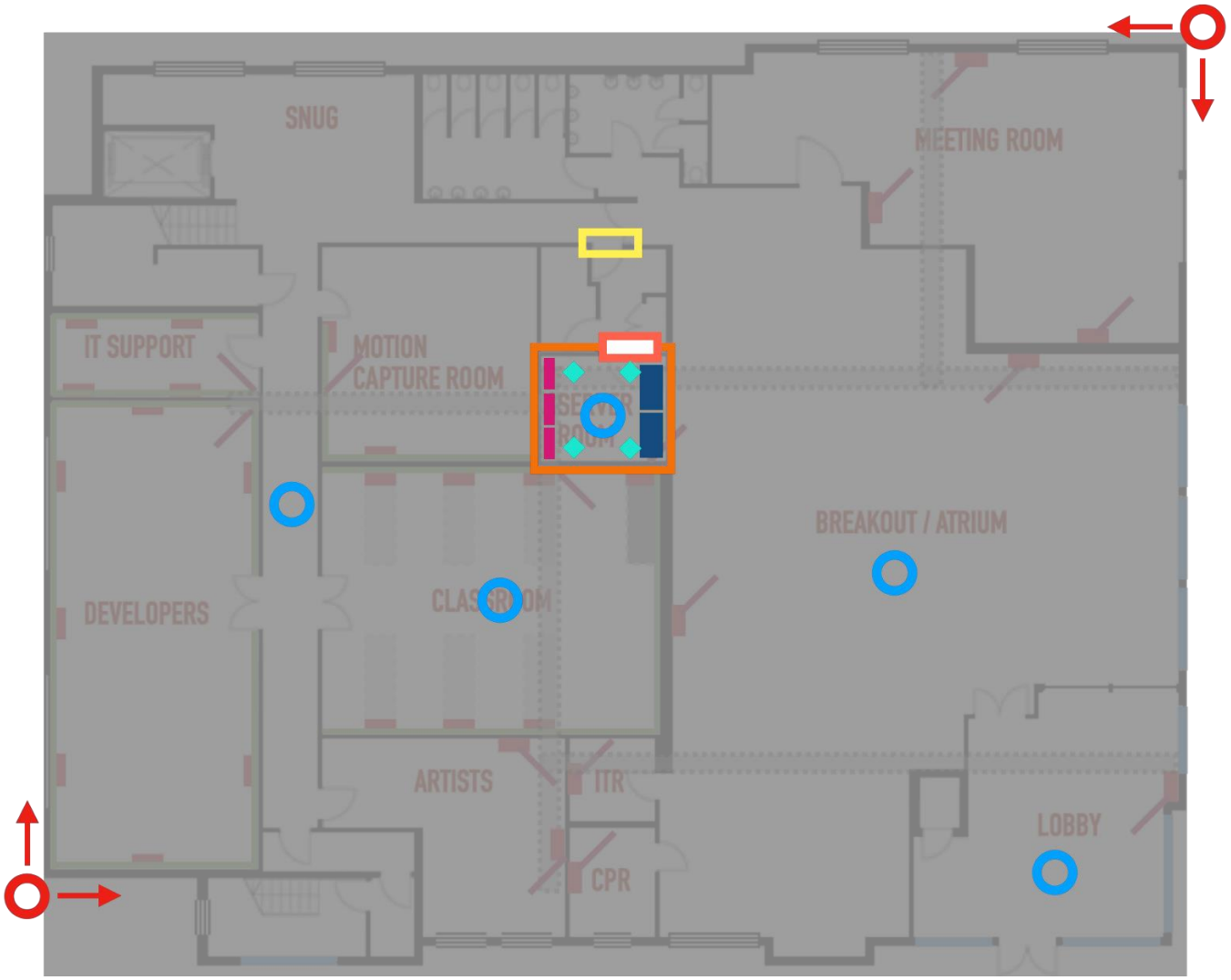
Gas Suppression - The server room will be fitted with a gas suppression system that will deploy in the event of a fire, preventing the fire from developing whilst not damaging the equipment.

Door Locks: we need to install locks. I recommend a physical mortice lock for access to the general server area to keep intruders out. For the physical server room itself I would install a swipe card entry system. This will again prevent unauthorised access to the server room but will also create a log of whoever's swipe cards are used to get access to the server room.

Annotated floor plans

	External Fixed IP Cameras	Two fixed IP external cameras with night vision, will be installed to vide down the two exterior walls of the building (as shown by the direction of the arrows). This will act as a first line deterrent and provide exterior coverage to prevent any forced access into the building.
	Fisheye Internal IP Camera	The internal fisheye cameras will provide 360º coverage in selected spaces. It was felt that the placement of the cameras in the breakout, lobby, classroom, server room, long downstairs corridor, dining room and long upstairs corridor by the stairs represented good coverage of the high risk/high value equipment whilst not being too invasive. These will be used to guard against any theft of equipment or other malicious activity.

	Server Room Air Conditioner	To ensure the servers work as efficiently as possible, three server room air conditioning units will be installed. These will run on a two on and one-off rotation to extend the life of the air conditioning units and provide spare capacity if one of the units fail. These are designed to keep the room running at a suitable temperature to ensure the servers do not overheat. Maintaining data security and preventing downtime in relation to heat based failure.
	UPS Battery Backup	The UPS battery units will provide a double function, firstly they will maintain a constant current of electricity into the server room preventing any spikes or surges from damaging the electrical infrastructure. Secondly, in the event of a power loss they would be able to sustain the servers until the power resumed or provide enough time to graciously power down the servers.
	Reinforced walls	The server room will have reinforced walls rather than the standard plasterboard internal walls. This will ensure the room is more secure and act as a stronger barrier against fire and theft.
	Gas suppression	The server room will be fitted with a gas suppression system that will deploy in the event of a fire, preventing the fire from developing whilst not damaging the equipment.
	Swipe card door entry	The external door will have a swipe card access, this will be authenticated to ensure that only the relevant members of staff have access to the room outside the server room. This will help add an extra layer of complexity and challenge to help reduce the risk of unauthorised access to the server room.
	Physical mortice lock door	The server room will have a heavy-duty locked door that will act as a final layer of security against unauthorised access to the server room. Only people with the correct key will be able to gain access to the physical server room.


SNUG
MEETING ROOM
IT SUPPORT
MOTION
CAPTURE ROOM
BREAKOUT / ATRIUM
DEVELOPERS
ARTISTS
ITR
LOBBY
CPR


KITCHEN
THE CINEMA
TECHNICAL
DINING ROOM / LARGE MEETING SPACE
LEAD CREATIVE OFFICE

Task 2: design - servers and storage

Server approach

Willow Technology is a company that specialises in the creative industries developing websites, computer animation, video and some motion capture work. At a very high level this means they will require large fast storage, web server capability and a database to support both the business but also the websites created.

It has been decided that a virtualised approach will be adopted for the business, focusing on fewer physical devices and providing greater cost saving and efficiencies. Physical servers with single roles will be consolidated into virtualised servers and stored on a single physical server. This reduces the cost of buying multiple devices, software licenses, maintenance agreements and even reduces the cost disposal at the end of life. The ability to consolidate servers means that hardware has better utilisation (for example, CPU and Memory can be run at higher usage levels rather than on separate machines running at low percentages). Reductions in the costs involved in running the servers (for example, reduced power and cooling demands over the life of the machine will be achieved).

In the long term this will help pave the way to transition to a cloud-based environment.

The following table shows the various roles that will need to be installed as part of the initial build of the network.

Virtualisation	Server Roles	Application Roles	Support
Hypervisor (ESXi)	DNS DHC P Directory Service (Active Directory)	IIS SQL Server File and Storage Services Exchange (Not Implemented)	Windows Deployment Server Backup Load Balancer (Not Implemented) Volume Activation Services Bitlocker Windows Server Update Service Group Policy

Virtualisation

VMWare ESXi has been selected as the hypervisor for Willow for a number of reasons. Firstly, it acts as a bare metal hypervisor installed on a USB or SD media directly on top of the hardware layer. This provides a consistent layer on which to build out the virtual machines. VMWare ESXi can also be used in conjunction with the other products from VMWare that provide a central point of control and management of the VMs, also the ability to move VMs from one server to another without any downtime during the migration.

VMWare ESXi supports a wider range of operating systems unlike Hyper-V and when developing for customers, it might be required for other platforms to be used and supported. VMware are the specialists in this field and the products are used by a large range of enterprises due to the excellent stability and compatibility of the platform.

Server Roles

DNS – Domain Name Service will be required on the network to allow the mapping of device names to IP addresses. This means that when we talk about Server01, then we know that this is 192.168.10.1. This makes management, organisation and control that much easier on **the** network.

DHCP – Dynamic Host Control Protocol, this will ensure that both wired and wireless devices are allocated an IP address that will allow them to connect to the network. It will save time, reduce complexity of manually allocating IP addresses to computers.

Directory Service (Active Directory) – The directory service will provide the address book of all the resources available on the network. It will provide the mechanism to authenticate computers and users on the network, allocate permissions, group objects for management (for example, users, computers) and even provide distribution groups.

Application Roles

IIS – This is Microsoft's webserver. Internet Information Server, is a webserver that will respond to server requests from browsers and web clients. This is where websites will be deployed for customers to test and review as they are developed.

SQL Server – This will provide a relational, multi-instance database that can be used for multiple purposes from supporting and storing website data, corporate information and integrates well within a Windows environment. When Windows Update Service is installed, SQL can provide the backend database to support the storage and management of update records. This will require a high level of CPU, Memory and storage demands when allocated to a VM. The actual database storage files can be stored on a local disk, shared storage, SMB file store or a Storage Spaces Direct and will need to be considered when selection a server.

File and Storage Services - This extends the default file management process and provides the require functionality to manage multiple file services, centralised storage, centralised backup and employ a quota service to manage file storage amounts. It will also provide efficiency in storage by reducing duplication of data using data deduplication. It also provides storage spaces to deploy high availability storage that is both resilient and scalable by using cost effective disks.

Exchange – This could be viewed as an optional application; it might be the requirement of the business to use a local email and communication service. Exchange will integrate with the Microsoft environment and provide email communication. Though not required for this project, it might be useful to consider moving this to Office 365 and utilise a SASS solution for productivity.

Support

Windows Deployment – As the network solution is new a mechanism for deploying desktop and server images out to the various new devices would be essential. WDS, provides the ability to do lite touch deployments of Windows images over the network. This will reduce the challenge of installing operating systems on all the new computers.

Server Backup – This will allow the scheduling of backups to occur on the network, allowing for quite precise control over what is backed up and where the backup is stored. More powerful backup tools exist, but this will provide enough features to support the new network.

Load Balancer – A load balancer will provide the functionality to spread processing between to servers forming a cluster. This provides a high availability solution, if one machine fails then the other machine(s) in the cluster will carry on process.

Volume Activation Services – Keeping the company compliant with the demands of software licensing will be made far easier with this service. It will allow machines to activate against the volume activation service and avoid going into any form of reduced functionality mode.

Bitlocker – This will allow all files stored on a disk to be encrypted, this is essential to keep the business compliant and secure. Without the key, any disks will be unreadable, and the data kept secure.

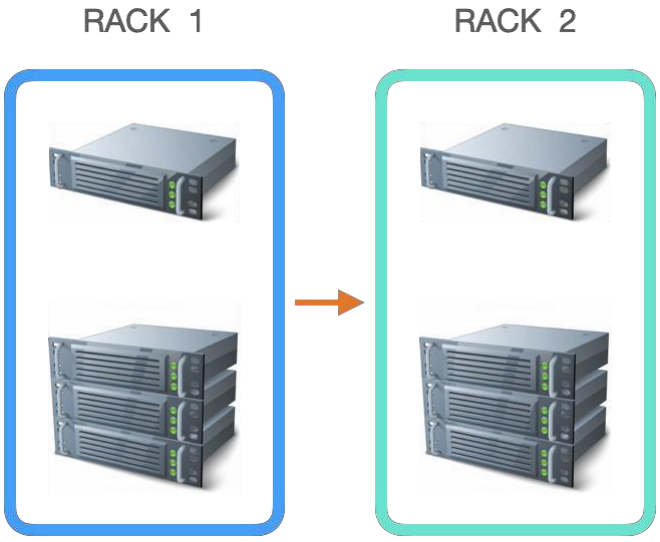
Windows Server Update Service – This role will allow updates from Microsoft to be managed locally and deployed out over the network. Rather than each machine making a call to Microsoft and downloading updates placing a significant load on the internet connection. One download of an update can be made from Microsoft and deployed out over the network to all the targeted machines.

Group Policy – Though a default role, it will still need to be configured on the server to put in place security rules that can secure machines. It could be used to remove the control panel, block removeable devices or even place am image on a desktop.

Technical documentation

General Approach

The approach to the servers and storage was to utilise virtualisation and condense down the number of physical machines and also build in redundancy in the network to reduce downtime due to a single point failure. The main concept is the mirrored approach using vSphere replication. The idea is that the server and the file server will replicate on premise to the mirror system. This means that when a file is saved, the same operation occurs on the sister machine. This has been shown as Rack 1 and Rack 2 in the diagram below, with only the 2 physical servers existing in each rack.



Main Server

	PowerEdge R740XD 2x Intel® Xeon® Gold 6252N, 2.3G, 24C/48T, 10.4GT/s, 35.75M Cache, Turbo, HT (150W) 6x 32GB RDIMM, 3200MT/s, Dual Rank Dell Recommended Emulex LPe31000-M6-D Single Port 16Gb Fibre Channel HBA 4x 960GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug Dell Price £11,731.62

The main server has been selected based on a number of reasons, not only the reputation of Dell but the years of experience, support available and the product range. The PowerEdge R740XD server offers 2x Intel Xeon Gold CPUs with 24 physical cores and an extra 24 virtual cores providing a logical 48 core CPU clocked at 2.3GHz and turboboosting to 3.6GHz. This means this is a very powerful CPU and affords this server a significant processing potential to be shared between the various virtual machines.

The memory has been set at 6 x 32Gb (192Gb) to be shared between the various virtual machines and the server can still be expanded further with scope to increase up to 24 slots of memory.

The main storage will reside on the file server, but 4x 960GB SSD drives have been added to the base specification. The platform is very flexible and the storage can be increased with up to 24 NVMe drives and a total of 32 x 2.5” or 18 x 3.5”drives in a 2U dual-socket platform.

Using the VMWare ESXi hypervisor and VSphere suite of applications, 6 virtual machines (virtual servers) will be created that will adopt the following roles.


SV1 - PDC
SV2 - Resources
SV3 - Database
SV4 - Web Server
FS1 - Customer
FS2 - Staff

The following table breaks down how the various roles and applications will be split over the various VMs.

SV1	PDC (Primary Domain Controller)	DNS DHC P Directory Service (Active Directory) Group Policy
SV2	Resources	Windows Deployment Server Backup Volume Activation Services Windows Server Update Service
SV3	Database	SQL Server
SV4	Web Server	IIS, File and Storage Services
FS1	Customer	File and Storage Services
FS2	Staff	File and Storage Services

File Server

	SC7020F array (4) 8-core Intel processors per array (30) 2.5” drive slots, 3U chassis 606 drive max expansion 6 PCIe slots (3 per controller) 16Gb FC 16,000 snapshots 29,000MB/sec front-end bandwidth Supports intermixed SSD formats All premium software features included 12 x 960GB (11.52 terabytes) SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug

The file server has a good level of processing capability, but it is 30 2.5” drives that can be added to the storage server that makes this a very powerful choice. The storage on the array will be split into blocks / segments as shown in the table below:

Block 1	SV3 Database Storage
Block 2	FS1 - Customer Project Storage
Block 3	FS2 – Staff User Profiles
Block 4	Media – Central repository for all media, graphics etc created

The direct fibre connection to the core switch will provide very fast data read and write from the array supporting the demands of the business. Rich media files can be very large, so it is important that the server and storage infrastructure are robust, reliable and fast enough to cope with these demands.

One of the most important features of the drive is that is has the ability to support up to 30 drives, whilst only planning on starting with 12 drive bays filled giving a total storage of 11.52 terabytes or storage, the array can be extended further. The balance of capacity, rich features and flexibility of storage media makes this a very wise choice for Willow.

Operating System

Each of the virtual servers will be Windows Server 2019, this powerful and well used operating system is used extensively in industry and aligns with the desktop operating systems. The OS is the latest server release from Microsoft and will receive the latest security updates and patches from Microsoft.

The new OS has a real focus on hybrid cloud, security, application planform and hyper-converged infrastructure. The last point HCI, is at the core of the approach taken for the business. Consolidating 6 separate servers down into one physical box will align with this approach.

Another benefit of the OS is that it has a rich and successful history and numerous sources of product support and certifications exist to ensure all infrastructure technicians have the relevant skills to administer the environment.

Print screens of online sources used and written evaluation of sources

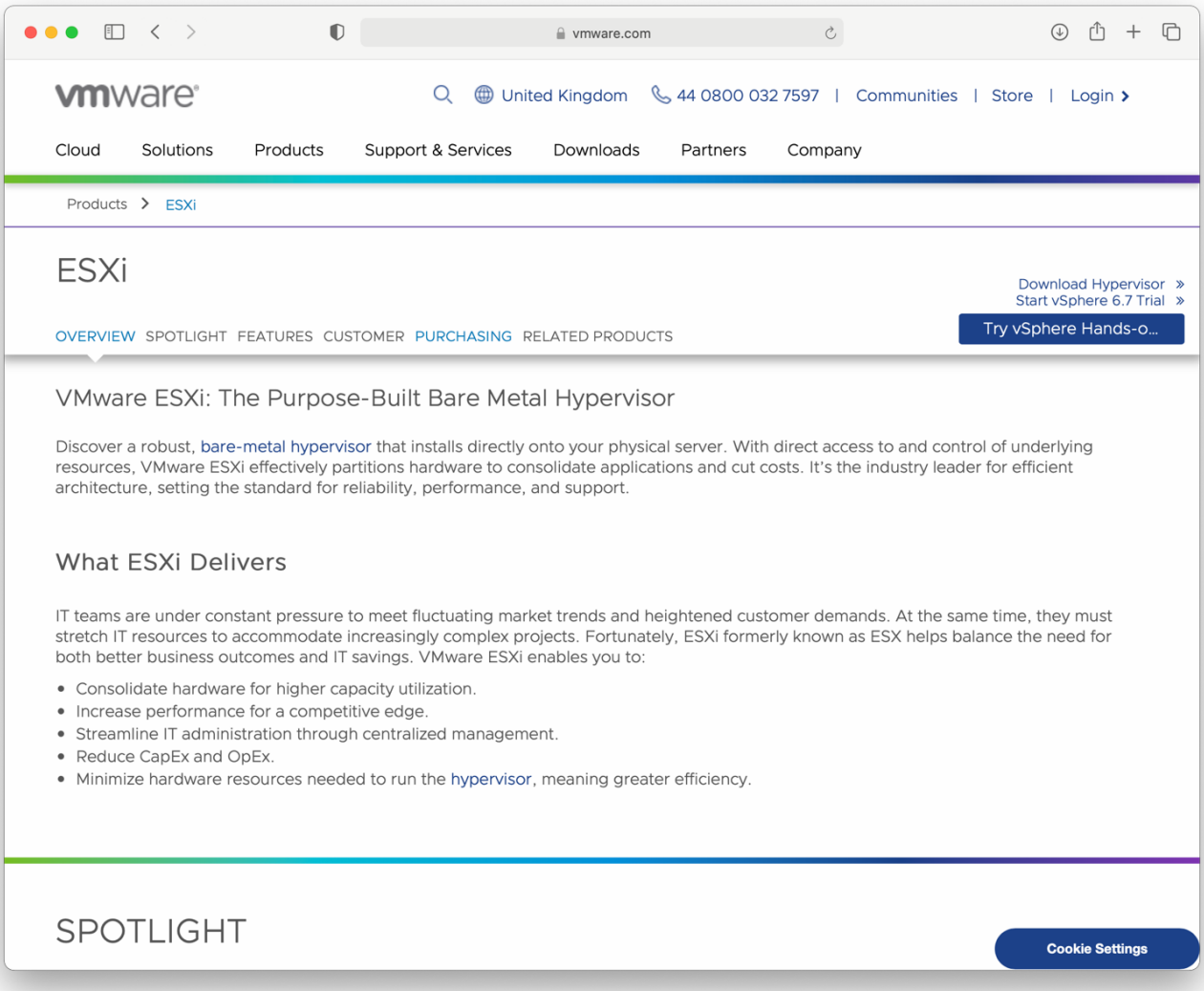


Figure 1 - https://www.vmware.com/uk/products/esxi-and-esx.html

A source was required that would justify the selection of ESXi as the virtualisation layer on the servers. The product overview page was very useful in explaining the benefits and capabilities of the product. It related how it would integrate with VSphere and the other VMWare products that will support a hyper-converged environment.

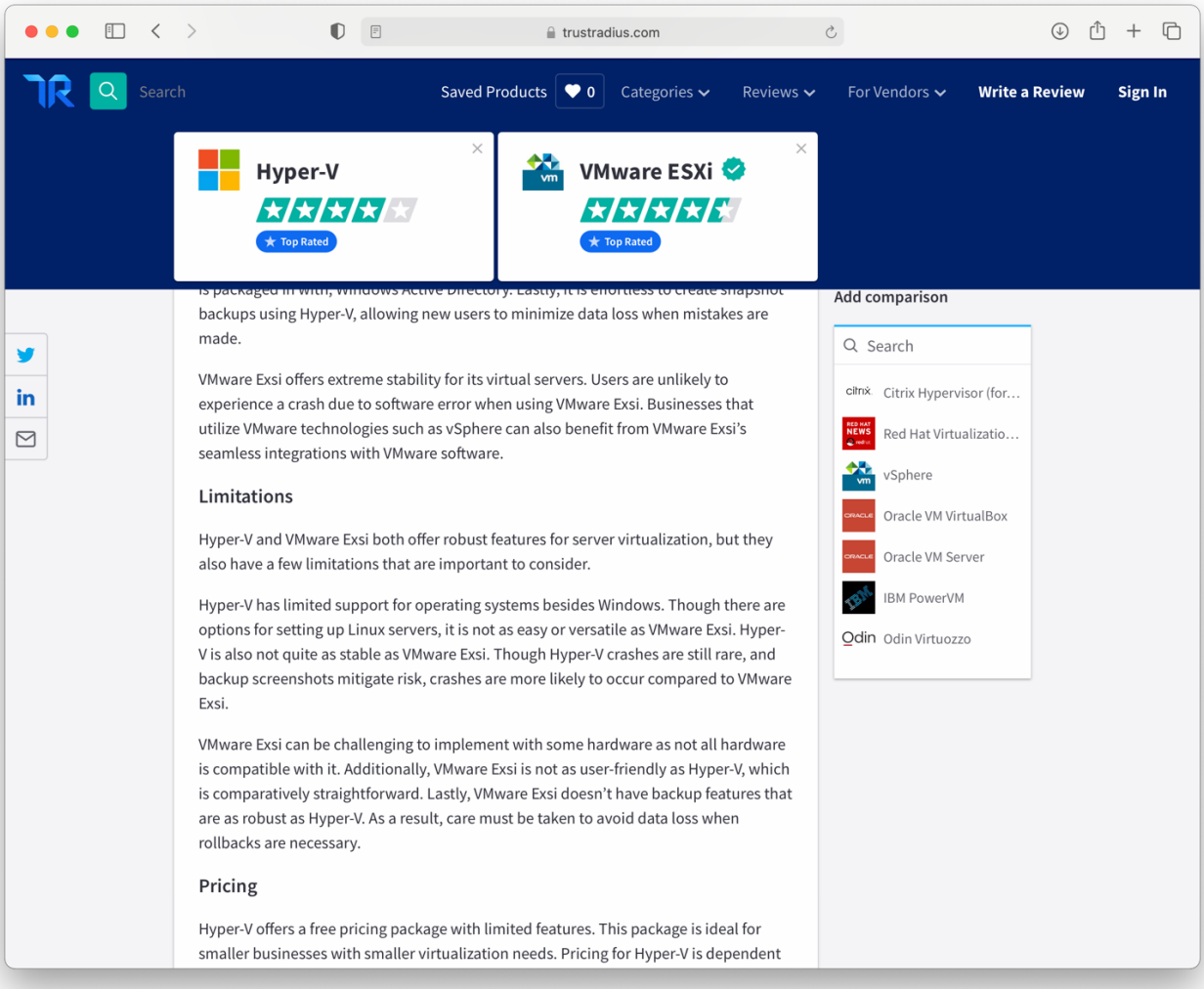


Figure 2 - https://www.trustradius.com/compare-products/hyper-v-vs-vmware-esxi

With the information taken from the manufacturers' website, it seemed appropriate to get a second opinion on virtualisation software. TrustRadius seemed to be a reliable website with some editorial control over the quality of the review. They do not seem to be biased to any one manufacture and the review was found to be honest, detailed and neutral. The information regarding Hyper-V and EXSi, covered advantages and limitations along with information about pricing. With budget not being an issue for this project, cost was considered but the quality of the product and features would be most important. After reading the review, I feel it has justified the approach taken in my approach.

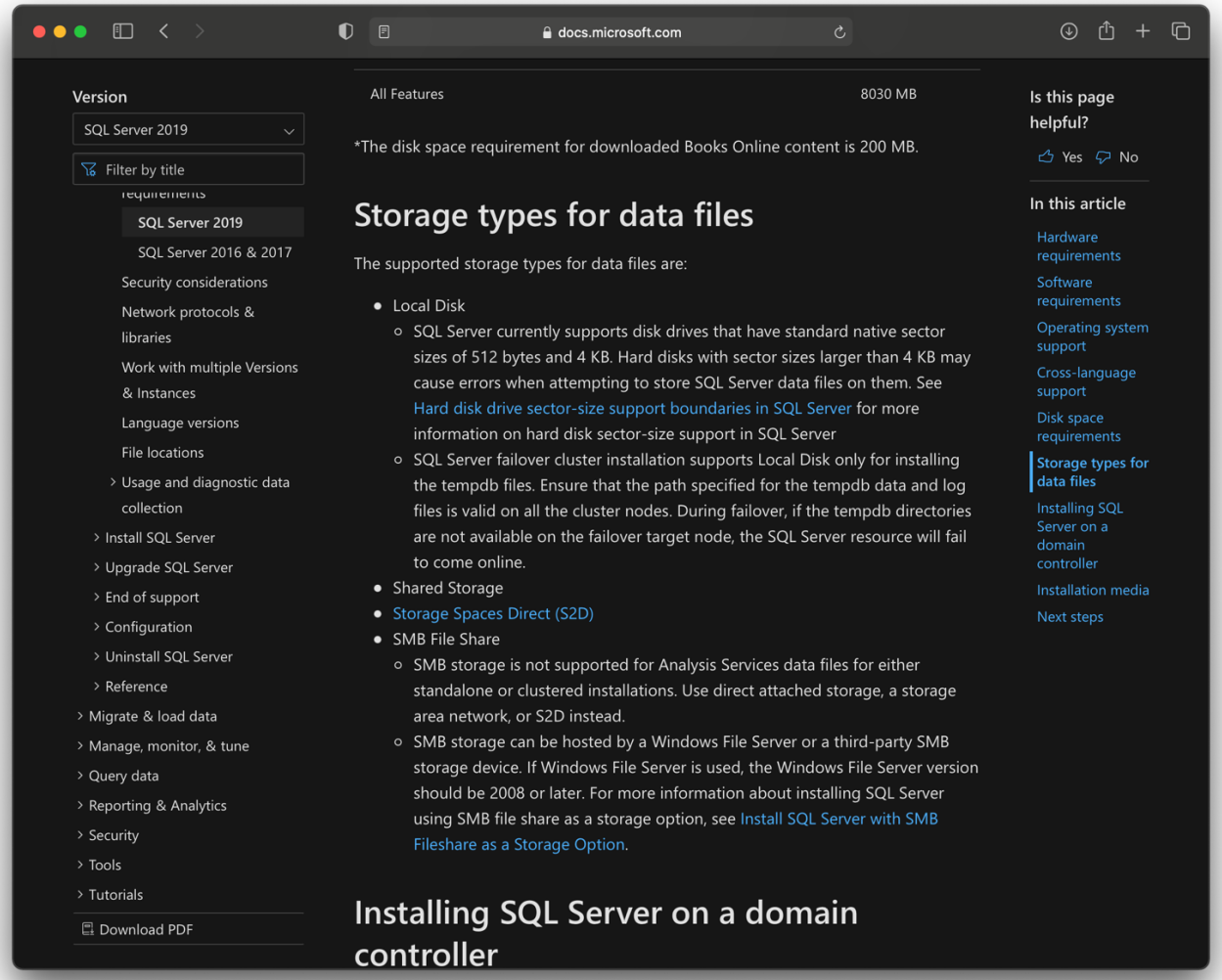


Figure 3 - https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-ver15?view=sql-server-ver15

Microsoft is a trusted source and I needed to confirm information about the latest version of Server 2019 and the different storage options when it comes to working with the disk array. The ability for the OS to support the addressing of S2D storage spaces on the drive.

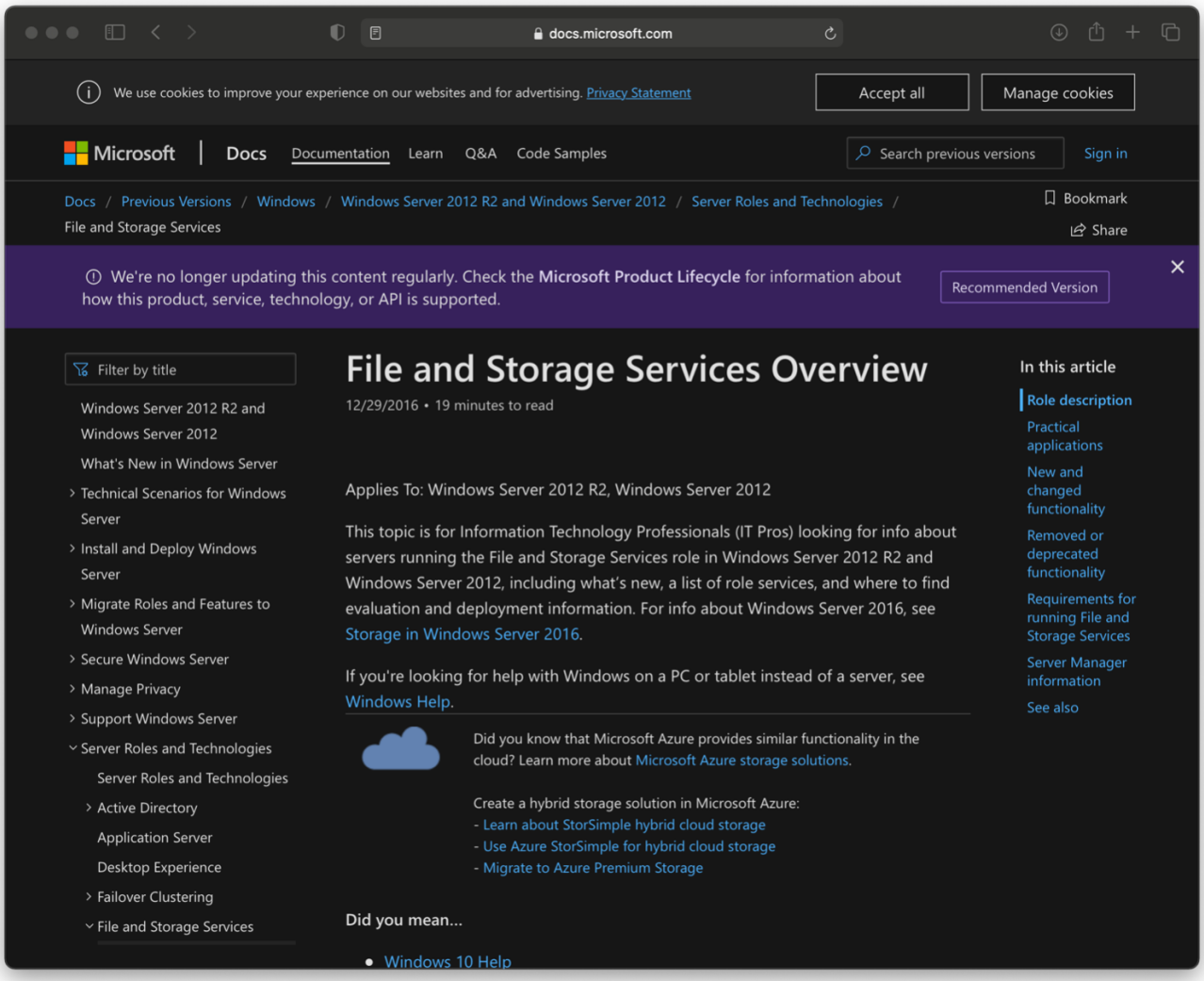


Figure 4 - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831487(v=ws.11)

The following source just added a little more detail about file and storage options and helps provide some clarity of the judgements made.

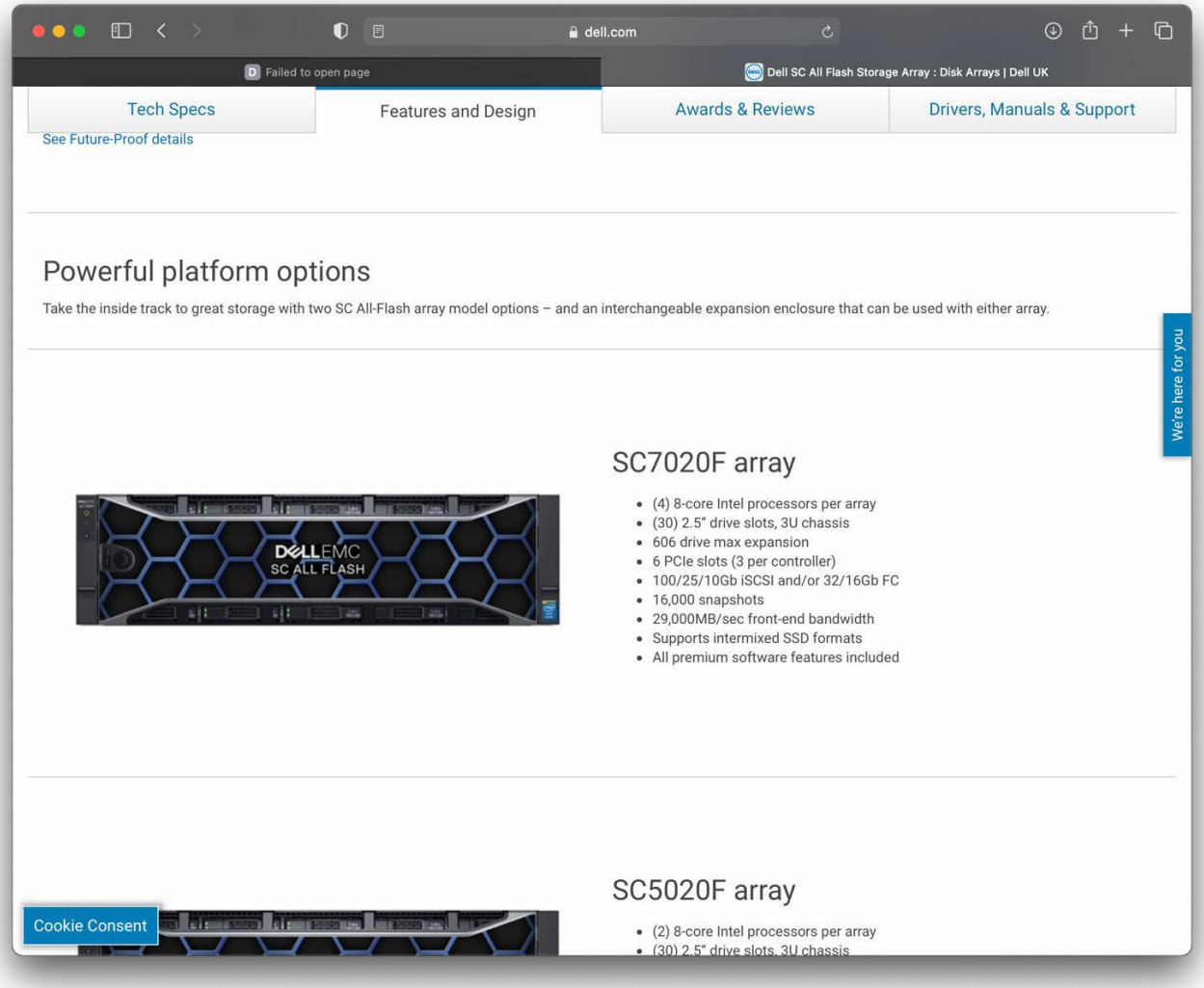


Figure 5 - https://www.dell.com/en-uk/work/shop/povw/storage-sc-all-flash

As part of the selection of servers for storage an all flash based device would be required to ensure the quality of service. Staying with Dell, for the common management layer, the build quality and range of options the SC7020F storage array proved to be a very viable product. The Dell site provided plenty of details regarding the configuration and technical specification.

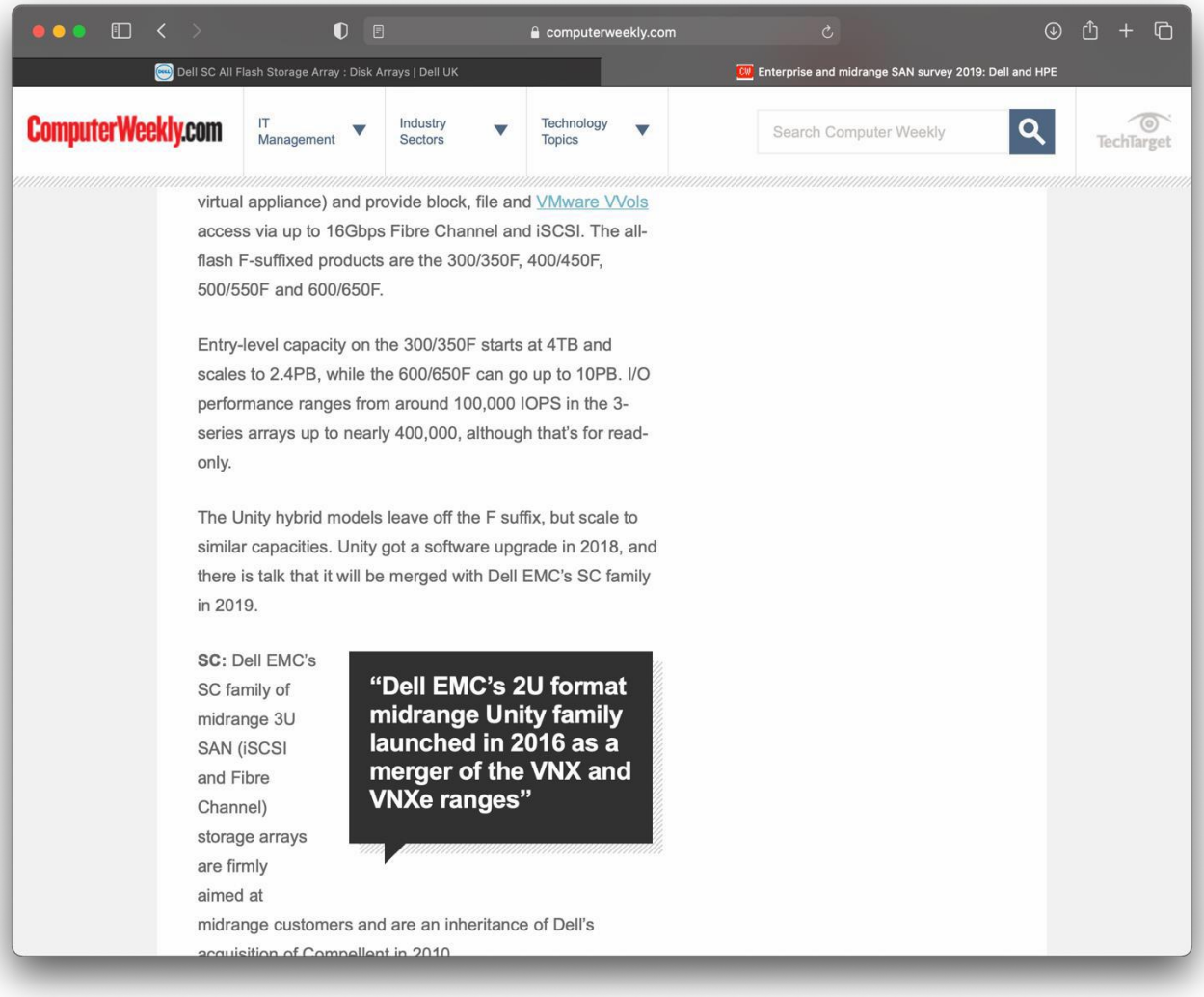


Figure 6 – https://www.computerweekly.com/feature/Enterprise-and-midrange-SAN-survey-2019-Dell-and-HPE

As an extra check a review of the product was found on Computerweekly.com comparing the Dell and HPE SAN devices. It was useful to get a consolidated review of similar products and how the Dell compared. The article had a high degree of technical focus and didn't include any real product reviews. I was able to compare several products at the same time which was useful. The article was very trustworthy and focused on technical detail derived from manufacturer information.

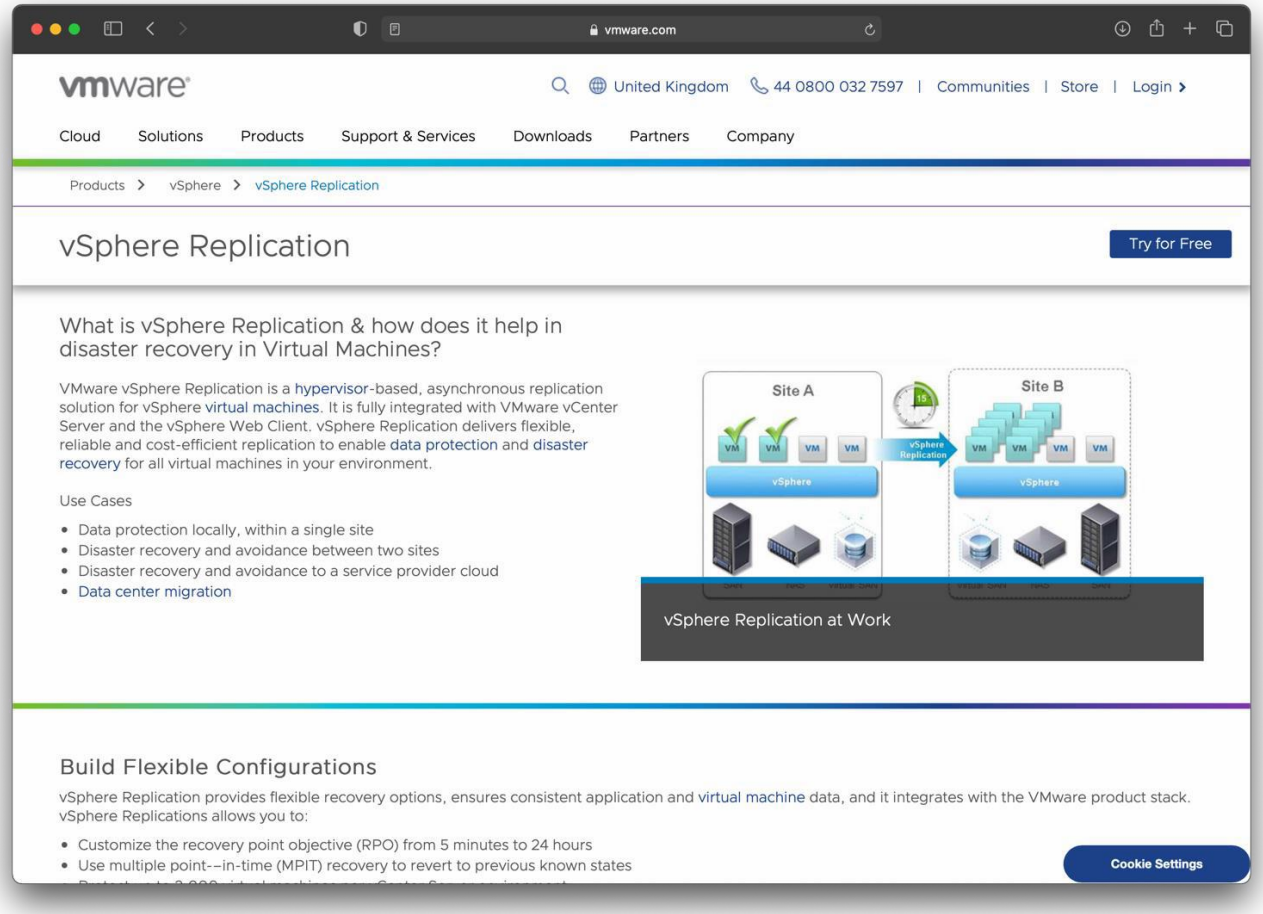


Figure 7 - https://www.vmware.com/uk/products/vsphere/replication.html

This article provided just a reference piece, it provided details of how using ESXi would allow hypervisor-based replication between the two racks of servers. This provides the backup/failover option for the network in case of failure. A good article, written for the technically minded and from a trusted source.

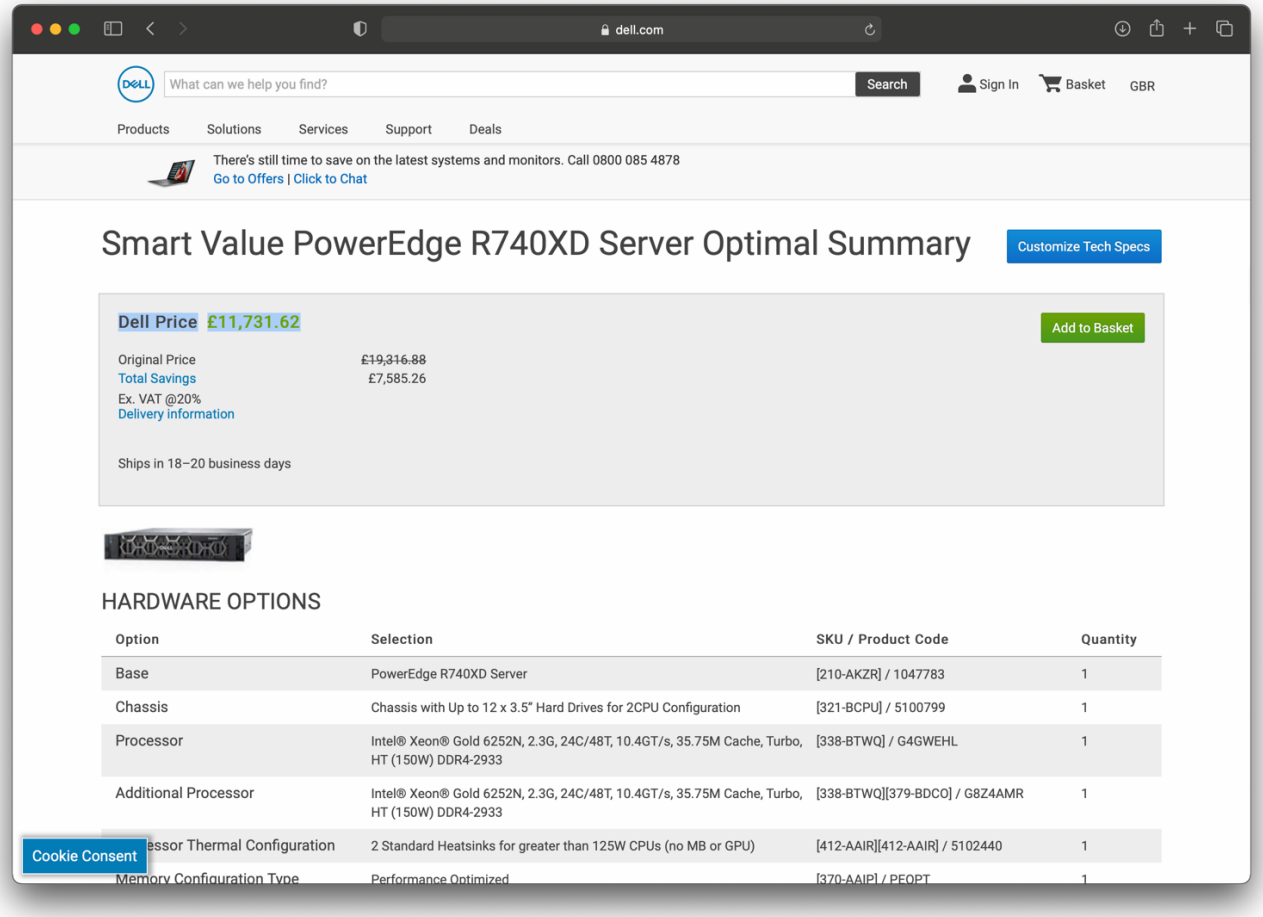


Figure 8 - https://www.dell.com/en-uk/work/shop/pdr/poweredge-r740xd/per740xd01m?selectionState=eyJPQyI6InBlcjc0MHhkMDFtIiwiTW9kcyI6W3siSWQiOjE1MTYsIk9wdHMiOlt7IklkIjoiRU1MMDAifV19LHsiSWQiOjE1NTAsIk9wdHMiOlt7IklkIjoiRzRHV0VITCJ9XX0seyJJZCI6MTU1MSwiT3B0cyI6W3siSWQiOiJHOFo0QU1SIn1dfSx7IklkIjoxNTYwLCJPcHRzIjpbeyJJZCI6IkdRSjFXTEsiLCJRdHkiOjZ9XX0seyJJZCI6MTU3MCwiT3B0cyI6W3siSWQiOiJHQUY1WFFPIiwiUXR5Ijo0fV19LHsiSWQiOjE2OTcsIk9wdHMiOlt7IklkIjoiNTEwMjQ0MCJ9XX1dLCJUaSI6IiIsIkRpIjoiIn0%3D&cartItemId=

This source only provided the option to configure the server before purchasing, but it helped build a system that would be fit for purpose.

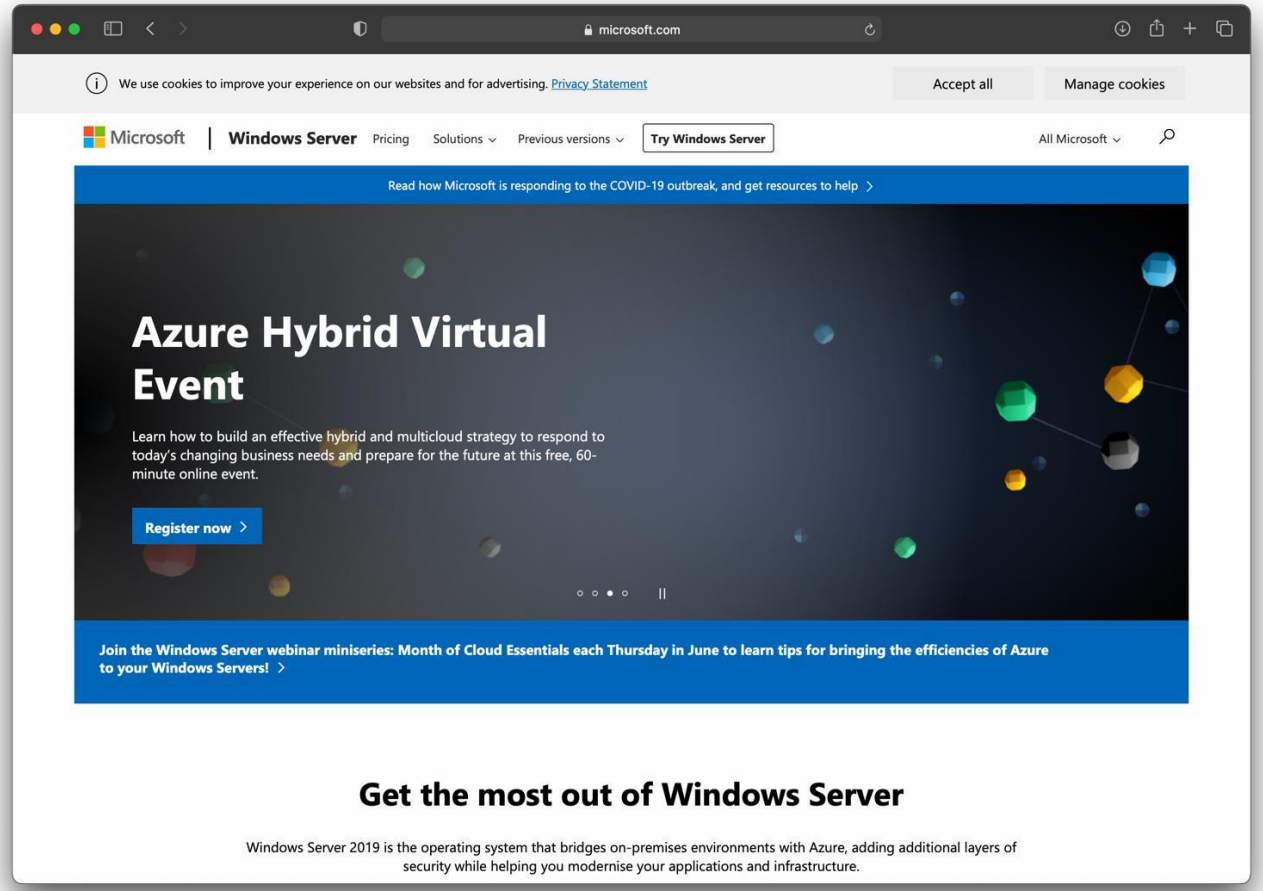


Figure 9 - https://www.microsoft.com/en-gb/windows-server

The official Microsoft Server 2019 web page provided many details about the new features but lacked information about all of the functions and features. It was used in conjunction with the other 2 sites to help get a review of how it is actually used, benefits and shortcomings. This information would help provide a “sanity” check and justify the selection.

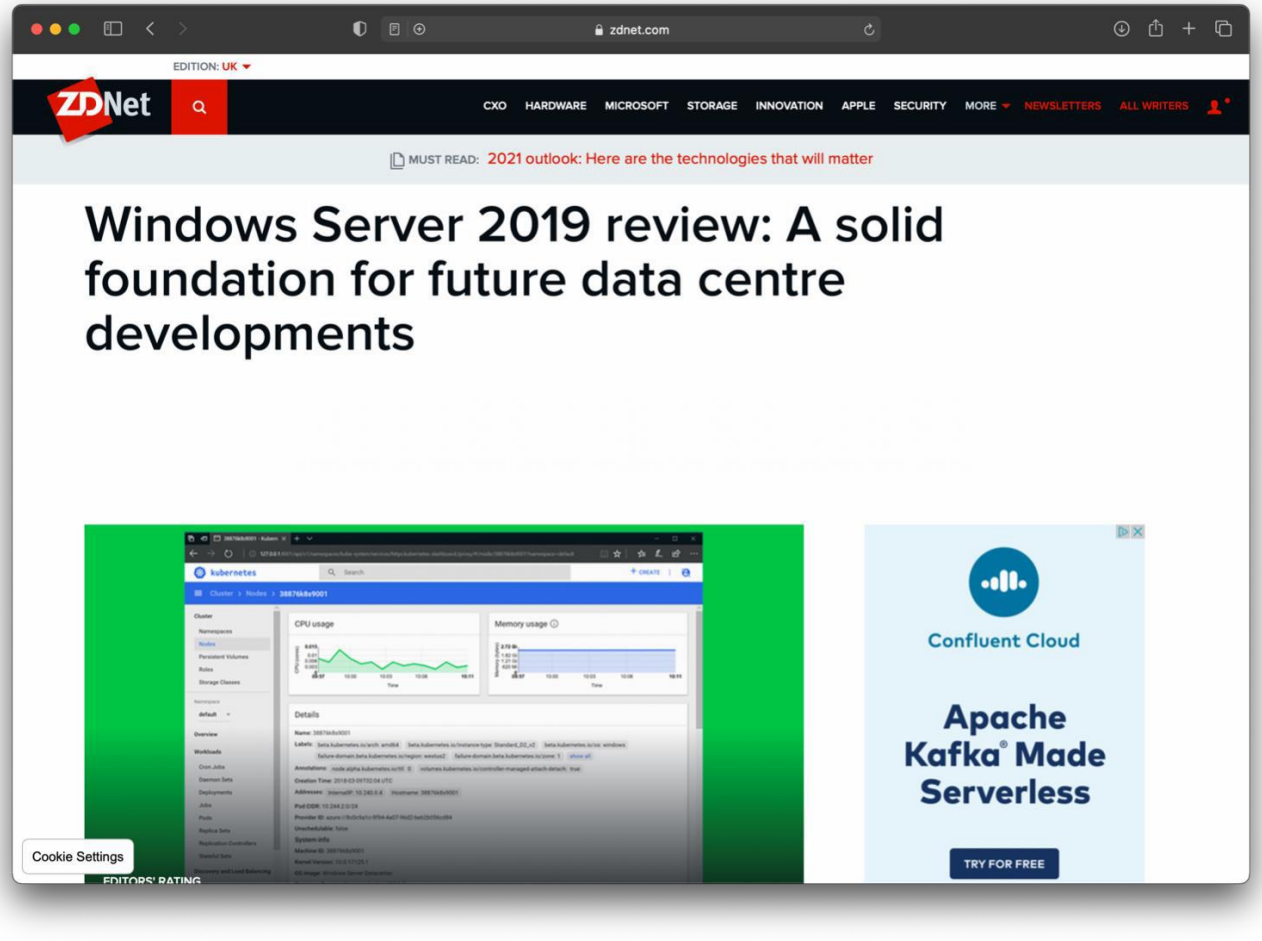


Figure 10 - https://www.zdnet.com/product/windows-server-2019/

The ZDNet site has been reviewing products, both hardware and software for a number of years. Professionals find the site to be balanced, independent and have a real-world focus on product reviews. The comments for Windows Server were used in the justification commenting on it being a route to the cloud. The article was well written and had real quality journalism at its core, making the information very credible.

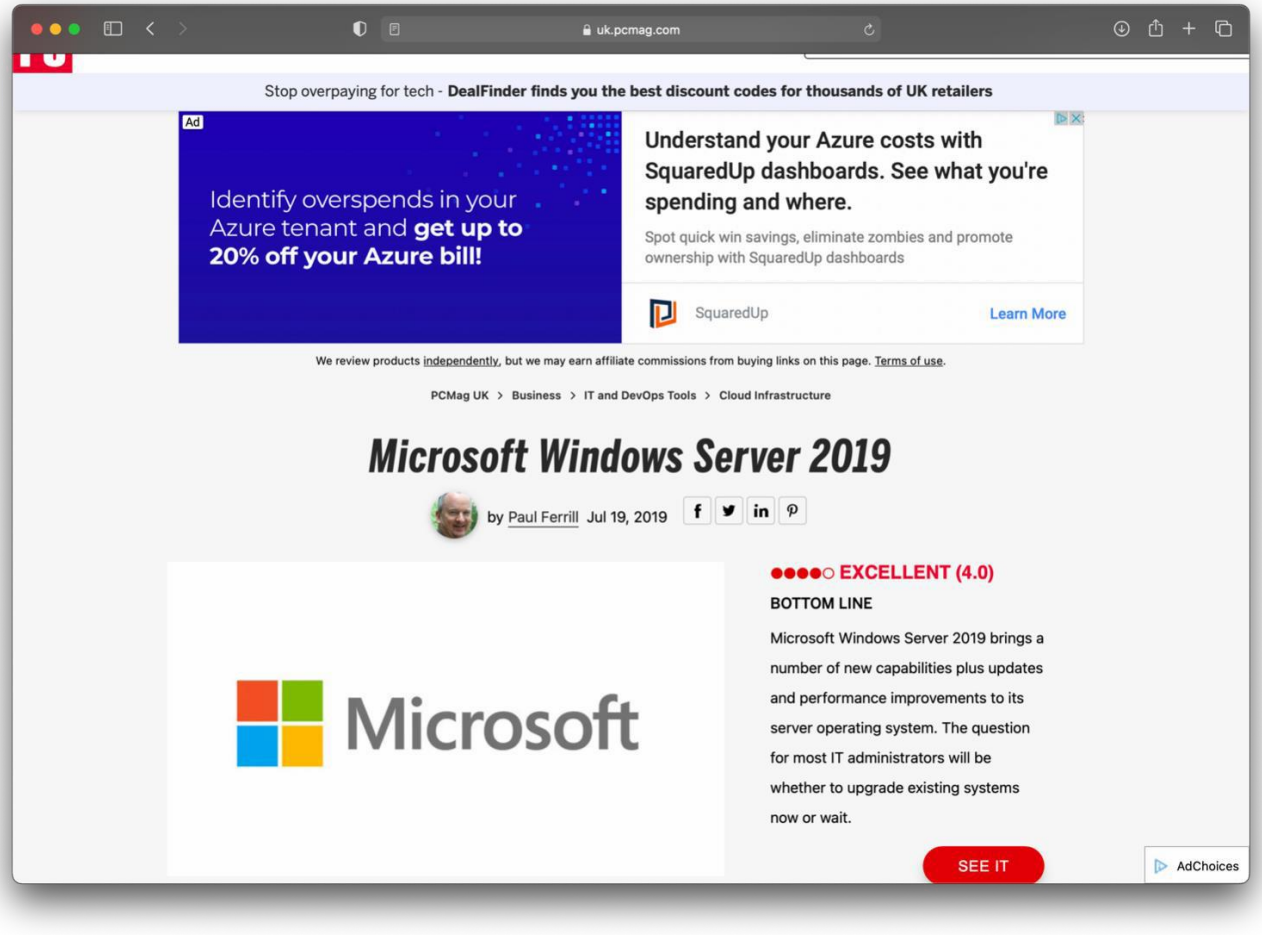


Figure 11 - https://uk.pcmag.com/software/121736/microsoft-windows-server-2019

Another source, UK PC Mag provide balanced opinion on the products. Even if you just take the overview of the article, it helps provide assurance in the selection of the OS. The article was unbiased and provided insightful comment that reflected the technical capabilities of the OS.

Task 3: design - communication equipment

Technical documentation

Switches

The approach taken is to implement four switches in the building to deliver the solution for Willow. A core switch with direct connection to the servers and the other switches and then three edge switches that will connect to the various network ports around the building. The edge switches will come in 2 different forms due to the nature of where they are placed.

The switches will be broken down into three VLANS (Virtual LANs), this is to ensure that traffic is isolated from each other keeping the illusion of three separate networks albeit running over the same physical infrastructure.

- VLAN1 will carry all the desktop and server traffic, serving all the printers and desktops dotted around the business
- VLAN2 will carry Wireless traffic, reducing the potential risk of a hacker compromising the integrity of the network
- VLAN3 will be used exclusively for the CCTV network, providing POE and connectivity back to the dedicated NAS solution

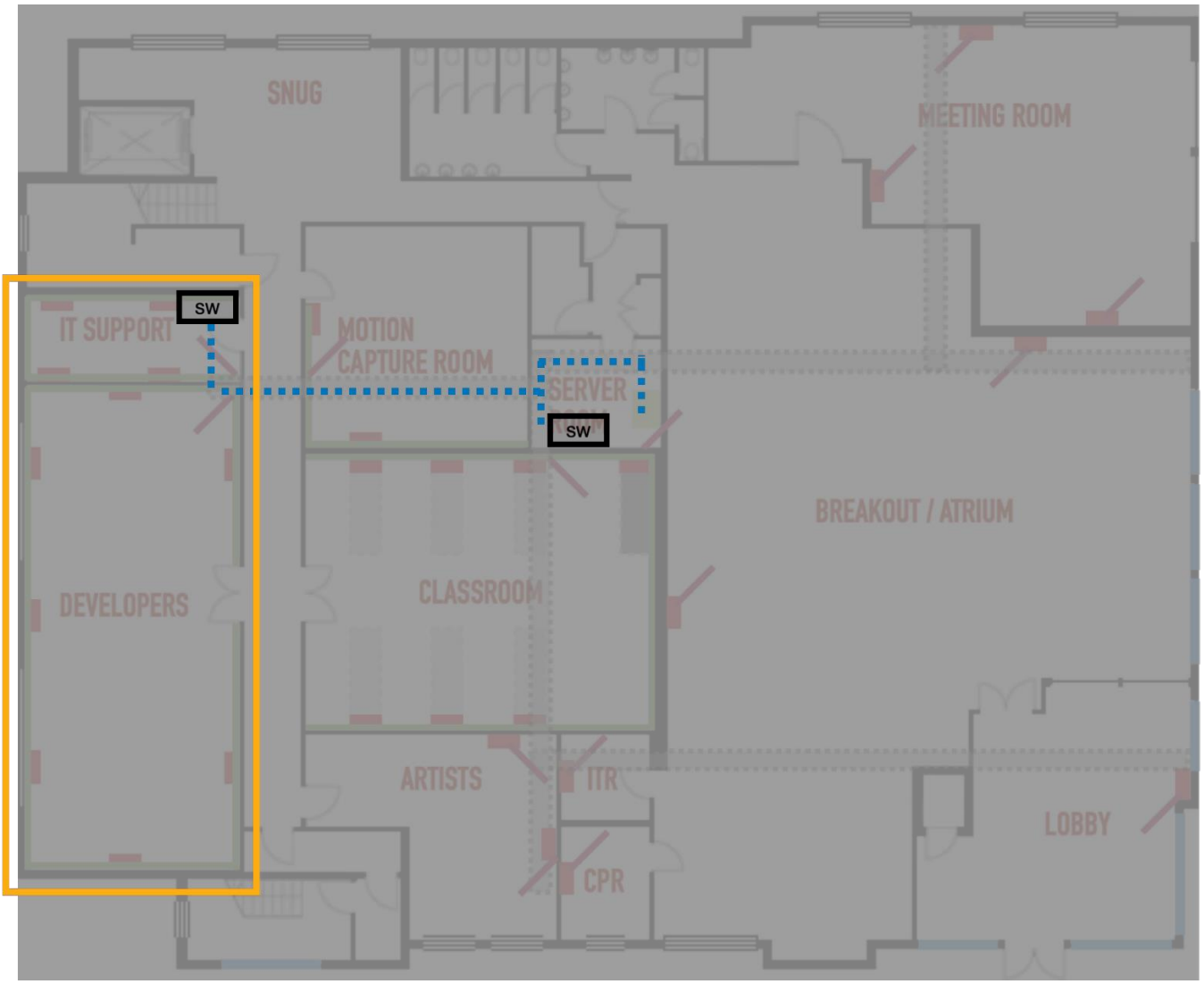
Switch	Location	Coverage	Summary
Core Switch	Server Room	Server 01a (4) + 1 Fibre Server 01b (4) + 1 Fibre File Server 01a (4) + 2 Fibre File Server 01b (4) + 2 Fibre Network Appliance Firewall 1 Port SW01 – 1 Fibre SW02 – 1 Fibre SW03 – 1 Fibre Wireless Controller 3504 – 1 Fibre 11 Fibre Ports	Central core switch will provide fast fibre connectivity from the servers to the 3 edge servers placed around the buildings using the Dell EMC PowerSwitch N3224F-ON.
SW01	Server Room	Lobby (2), Breakout (4), Meeting Room (6), Motion Capture (4), Classroom (14), Artists (4), ITR (2), CPR (2) 4 POE Ports for Access Points 3 POE Ports for IP Cameras 45 Ports	The first edge switch will be stored in the server room and will have 48 network ports and 4 high speed fibre connections. This switch also provides PoE support to power the IP Cameras and Access points around the building that will all directly connect to the Dell EMC PowerSwitch N2248PX-ON switch.
SW02	IT Support	IT Support (8), Developers (14) – 22 Ports	The two other servers will be placed in the left-hand zone of the building covering the developers and IT support area. Whilst the other switch will be upstairs and cater for all the first-floor ports. Both of these switches will be the Dell EMC PowerSwitch N2224PX-ON 24 port switch.
SW03	The Cinema	Cinema (4), Dining Room (4), Lead Creative (2), Technical (8) – 18 Ports	

	Dell EMC PowerSwitch N2224PX-ON N2224PX-ON - 1RU, 24x1/2.5GbE RJ-45 with 802.3bt Type-3 (60W) PoE on 12 ports and 802.3at (30W) PoE on 12 ports 160Gbps Stacking with up to 12 members 25GbE Uplinks to aggregation Powers and backhauls data from 802.11ac Wave 2, 802.11ax WLAN deployments and 802.3bt Type-3 high power PoE applications requiring up to 60W per port Ideal for Mid to Large Enterprise Campus networks, Retail deployments requiring support for a range of PoE devices
	Dell EMC PowerSwitch N2248PX-ON Latest generation 2.5GbE Campus Access Switches with full scale 2.5GbE MultiGig on all ports and 802.3bt Type-3 (60W) PoE on subset of ports N2248PX-ON - 1RU, 48x1/2.5GbE RJ-45 with 802.3bt Type-3 (60W) PoE on 24 ports and 802.3at (30W) PoE on 24 ports x86 platform based on Broadcom Hurricane 3 MG chipset 160Gbps Stacking with up to 12 members 25GbE Uplinks to aggregation 802.11ac Wave 2 WLAN deployments and 802.3bt Type-3 high power PoE applications requiring up to 60W per port. Ideal for Mid to Large Enterprise Campus networks, Retail deployments requiring support for a range of PoE devices

	Dell EMC PowerSwitch N3224F-ON Latest generation 1G Fibre Campus Access Switch N3224F-ON - 24x 1G SFP, 4x 10G SFP+ ports 400G Stacking with up to 12 members 10G Uplinks to aggregation Ideal for Mid to Large Enterprise Campus networks, Retail deployments

As you can see on the floorplan below, the server room will have the 2 switches installed in the rack as outlined earlier. The core with will have a fibre connection run through the overhead trays to the switch in the IT support office. Here the edge switch will connect to all the network ports located within the orange box. This reduces the amount of cable running back to the centralised switch. It also facilitates the easy expansion of the network if additional ports are to be installed in this area.

Having the 2 switches in the server room add an extra element of security to the installation as they will be being double locked doors. It should be noted that a significant amount of cable will need to be installed to connect from the remaining rooms back to the server room. This option seems logical as it reduced the need for other expensive switches for such a few network ports scattered through a number of locations.



Just the single switch will be installed on the first floor, despite the location being so close to the server room, it was felt that having a single upstairs switch would be a better option. The switch will be connected back via a fibre cable to the core switch in the server room.

Despite the size of the upstairs, only 18 network ports have been positioned on the floor plan. The ceiling already has the cable tray installed so the challenge of running the cable back to the single switch is relatively simple to overcome. If a considerable number of additional ports were to be added to the upstairs then it might be useful to add in an extra switch, but as it stands this is considered overkill.

Wireless Infrastructure

The wireless element to the network will comprise two products, a Cisco wireless LAN controller and 4 Cisco Aironet wireless access points. The Lan controller will be located in the main server room and will plug directly into Switch1. The purpose of the controller is to provide a wireless management device that will allow the deployment of rules, security setting and configurations to the four access points around the business. It will also integrate with the active directory to provide authentication against valid user accounts and passwords.

The four access points have been placed in high traffic areas with the majority of the customers will gather. This is why the dining room, the main walkway to the dining room, the classroom and the atrium have been covered.

The placement of the AP in the atrium has been moved into the building as far as possible to reduce the strength of

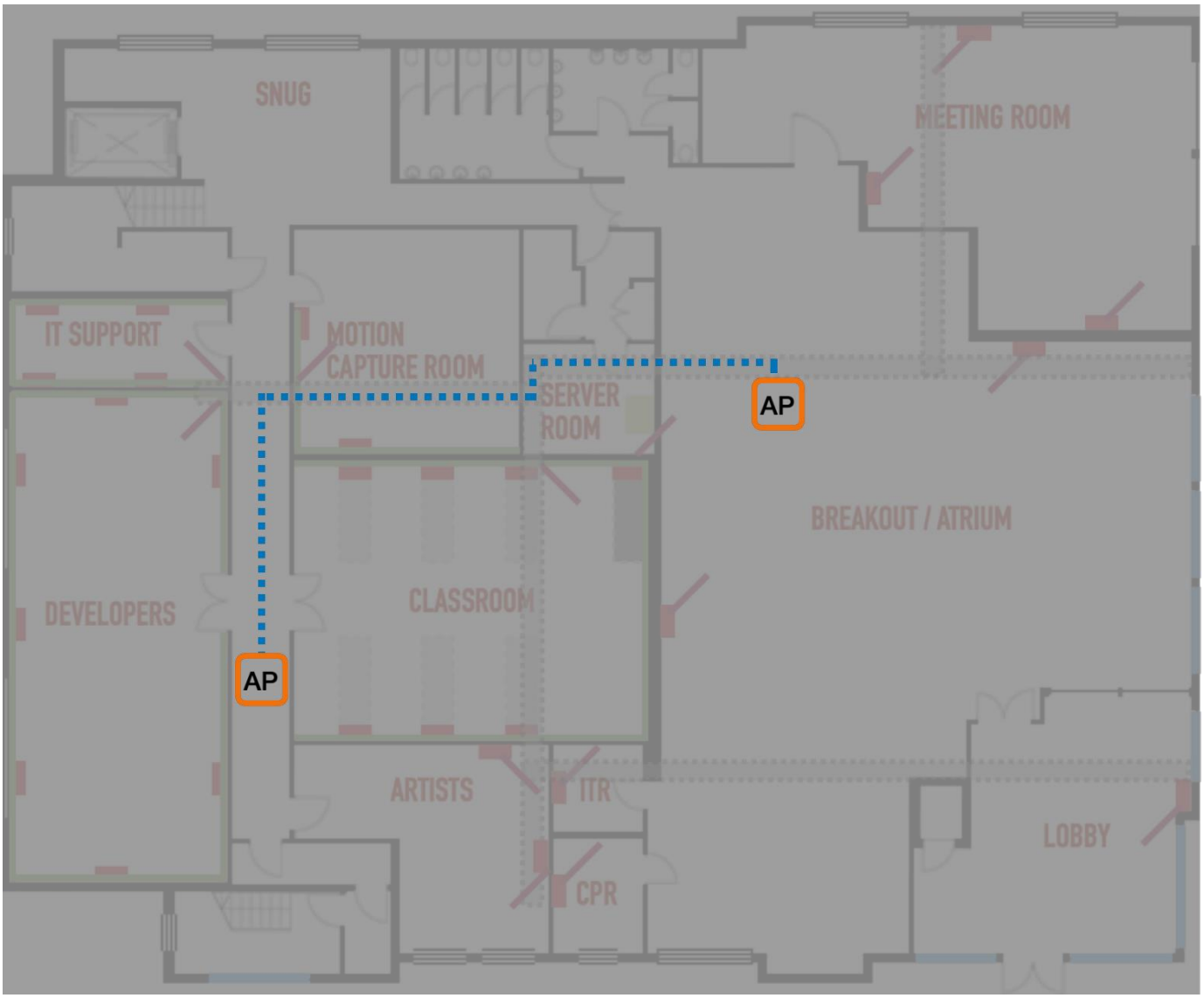
the signal as it passes through the external windows. This will hopefully make it harder for hackers to try and access the system via the wireless from outside the premises.

This is a departure from the Dell switches used on the network as Dell do not offer any WiFi infrastructure. Cisco equipment tends to cost a little more than similar equipment from other vendors, but they do manufacture quality products with a wealth of features that interact with each other.

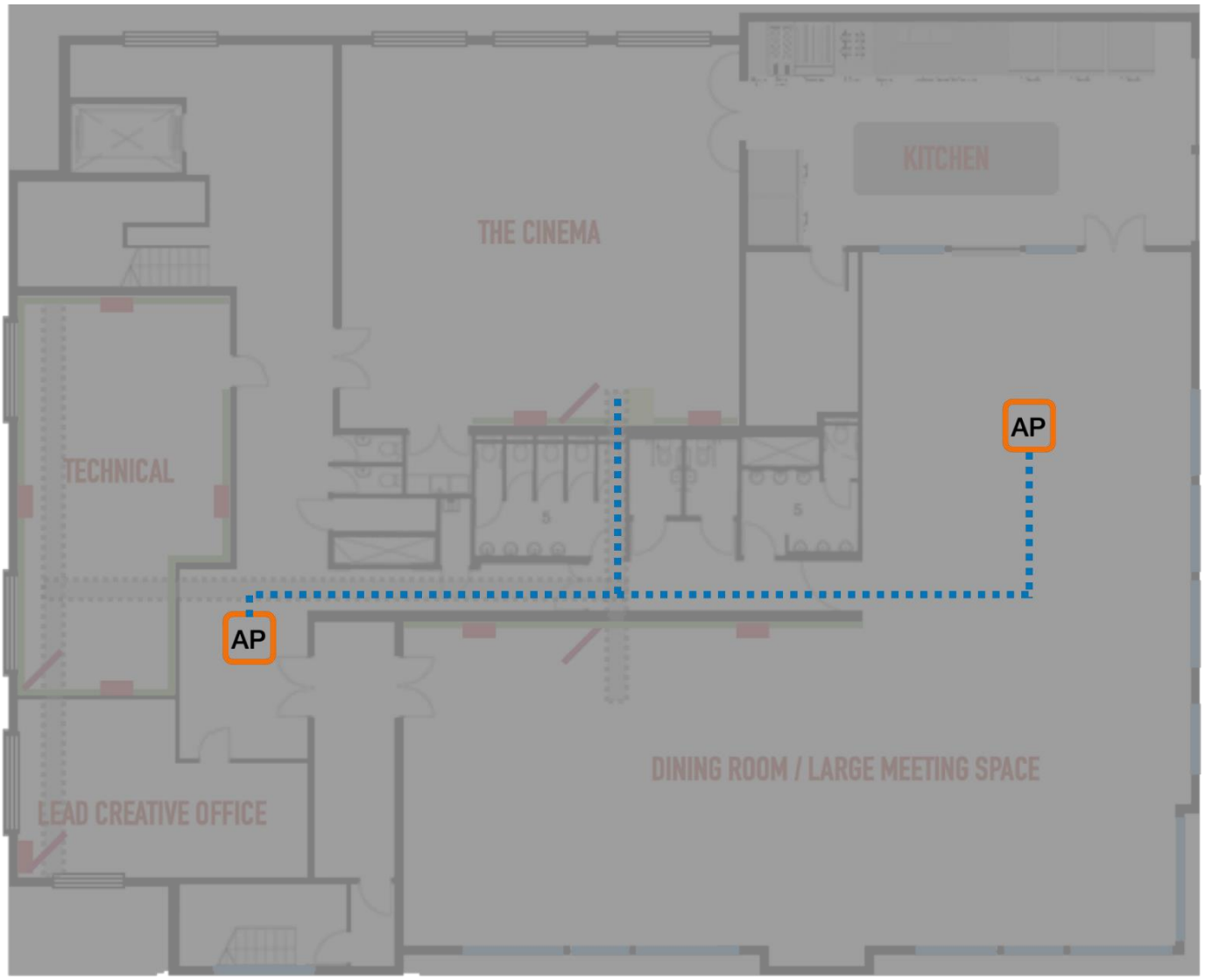
	Cisco Wireless LAN Controller 3504 Ideal for small and medium-sized businesses Optimized for 802.11ac Wave 2 with 4Gbps throughput Supports 150 access points and 3,000 clients
	Cisco Aironet 1830 3x3 MU-MIMO and 2 spatial streams 802.11ac Wave 2 supported Transmit beamforming Mobility Express for flexible deployment

The Cisco Aironet AP supports the latest mainstream speed of 802.11ac and also wave 2 supported for future development of the network. The beamforming capability will strengthen the signal and target the receiving device to improve the quality of service by maintaining a strong connection. The Aironet connects to the wireless Lan controller where the rules and authentication will happen to secure the wireless network.

The diagram shows where the AP's have been placed, only two APs have been installed in the breakout space, this is viewed as a public space for working so there is a demand for wireless connectivity. Another AP has been placed outside the classroom and should provide limited coverage to the developers and artists room. Both of these APs both connect back to switch 1 using standard ethernet and POE to provide power.



In the upstairs spaces an AP has been installed in the dining room, again this is another public space and an AP also provides limited coverage to the technical and creative office. All of these connect back via the same ethernet and POE combination.



CCTV Solution

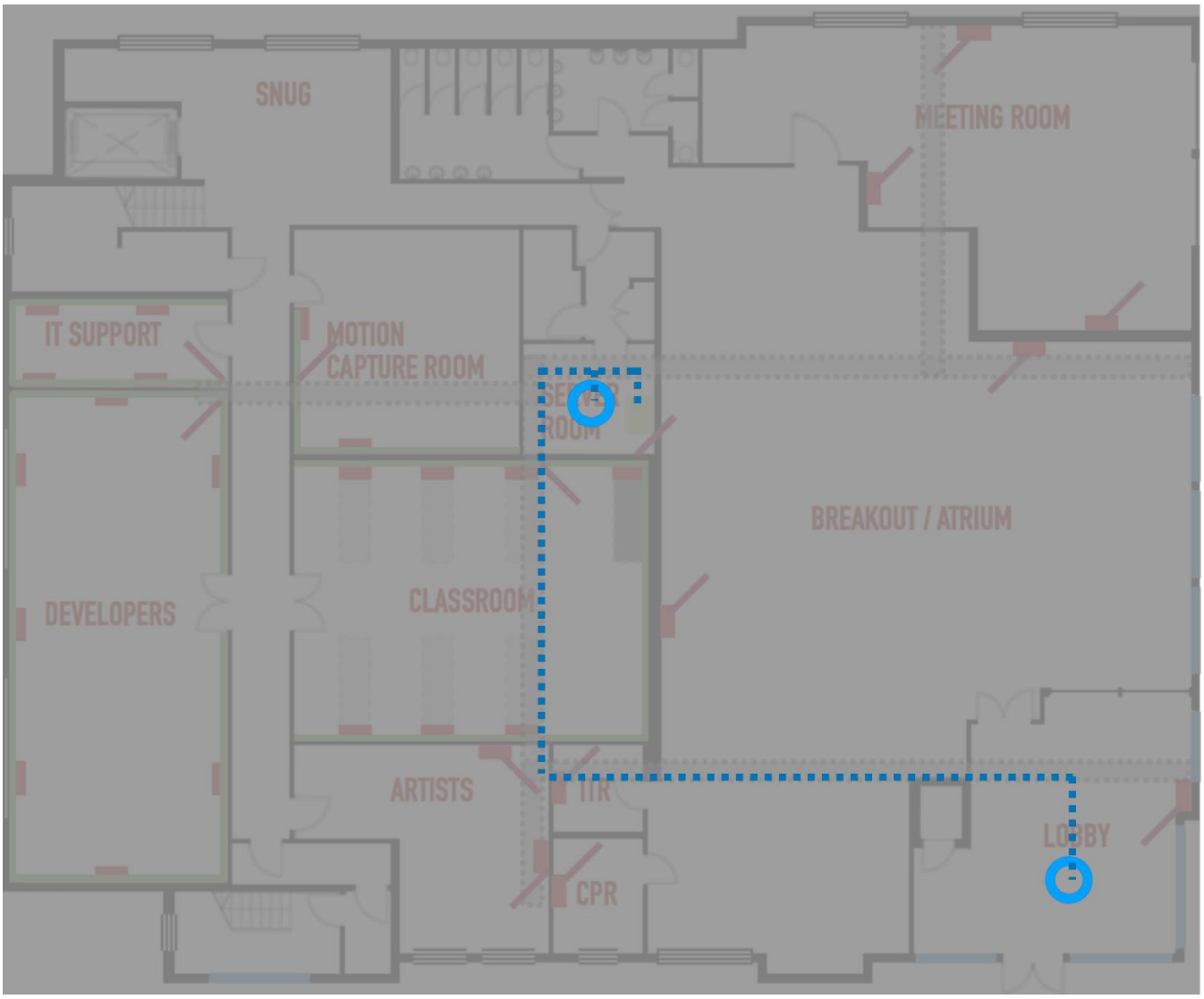
The placement of the CCTV equipment has been identified in the brief from the customer, they required a camera in the dining room, covering the server room and in the main entrance. It also stressed in the customers' requirements that they required a 360º degree camera. The Vigilance camera has been selected for a number of reasons including the full HD recording capability, the fisheye lens and the PoE connection that will reduce the complexity of providing power to the cameras.

The NAS solution will be rack mounted and stored in the server room, this has the capacity to scale out to 16 drives and will easily provide the option to store video recording for longer, and/or support the addition of extra IP cameras if they are required.

	RackStation RS1619xs+ CPU: Quad-core up to 2.7GHz RAM options: 8GB DDR4 UDIMM, up to 64GB High Performance: 1,523 MB/s sequential reading, 162,097 iSCSI random read IOPS Scalability: Up to 16 drives with one RX1217/RX1217RP1
	Vigilance 360° Full HD PoE Network Camera DCS-4622 1/3.2” 3 megapixel CMOS progressive sensor Fixed fisheye lens: 1.1 mm F2.0 High resolution video and snapshots up to 1920 x 1536 Distortion correction H.264 and Motion JPEG compression ePTZ viewing Simultaneous multi-stream support Built-in Samba client for saving to a NAS 10/100 Fast Ethernet port with PoE support

Only 3 cameras and the locations have been specified by the customer as shown on the 2 floorplans. Each of the cameras will connect directly back to SW1 and will be powered using POE. They will connect using standard ethernet cable and reside on a separate VLAN isolated from network traffic and internet access. Only relevant users will have the ability to connect to the NAS drive and review the captured footage.

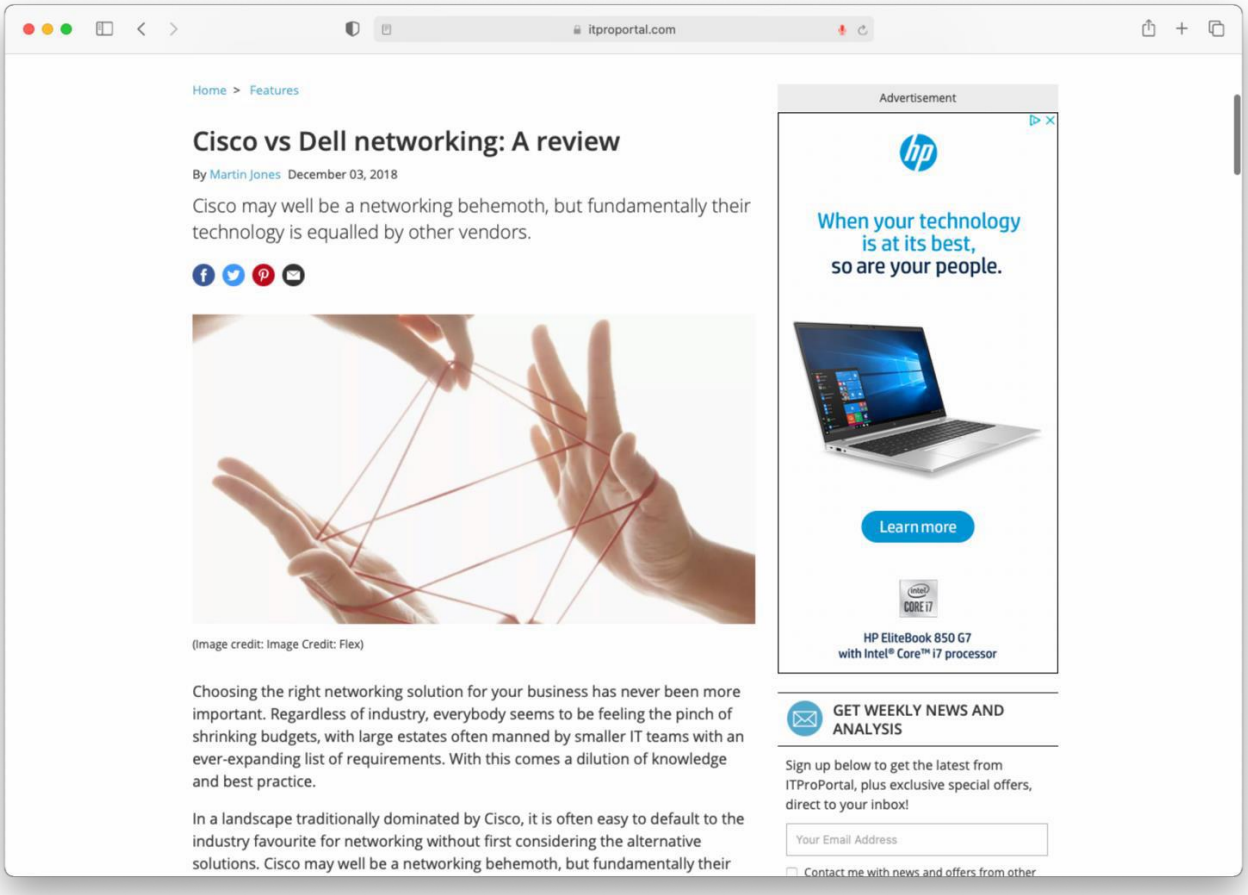
The NAS drive also features a complete operating system that would work independently of internet access, it is also very flexible and allows for other rich additional applications to be added to the NAS drive to add functionality. It is noted on the manufacturers website that additional CCTV licenses will be required to be purchased to support every camera.


SNUG
MEETING ROOM
IT SUPPORT
MOTION
CAPTURE ROOM
BREAKOUT / ATRIUM
DEVELOPERS
CLASSROOM
ARTISTS
TTR
CPR
LOBBY


KITCHEN
THE CINEMA
TECHNICAL
LEAD CREATIVE OFFICE

Print screens of online sources used and written evaluation of sources

The following site provided useful information about Cisco vs Dell networking, the price for the Cisco equipment would be an issue and based on the demands and requirements of the business the Dell switches would be viewed as suitable for the customer. I had never heard of the review site but the review was clear and informative and provided a valid view of the network capabilities from both vendors.



The following Dell website provided technical information about the range of switches available and the capabilities. It is useful that Dell adds in details about where the switch would be most suitable (for example, ideal for mid to large enterprise campus networks). This helped in the guidance when creating the technical specification and helped justify the selection further.

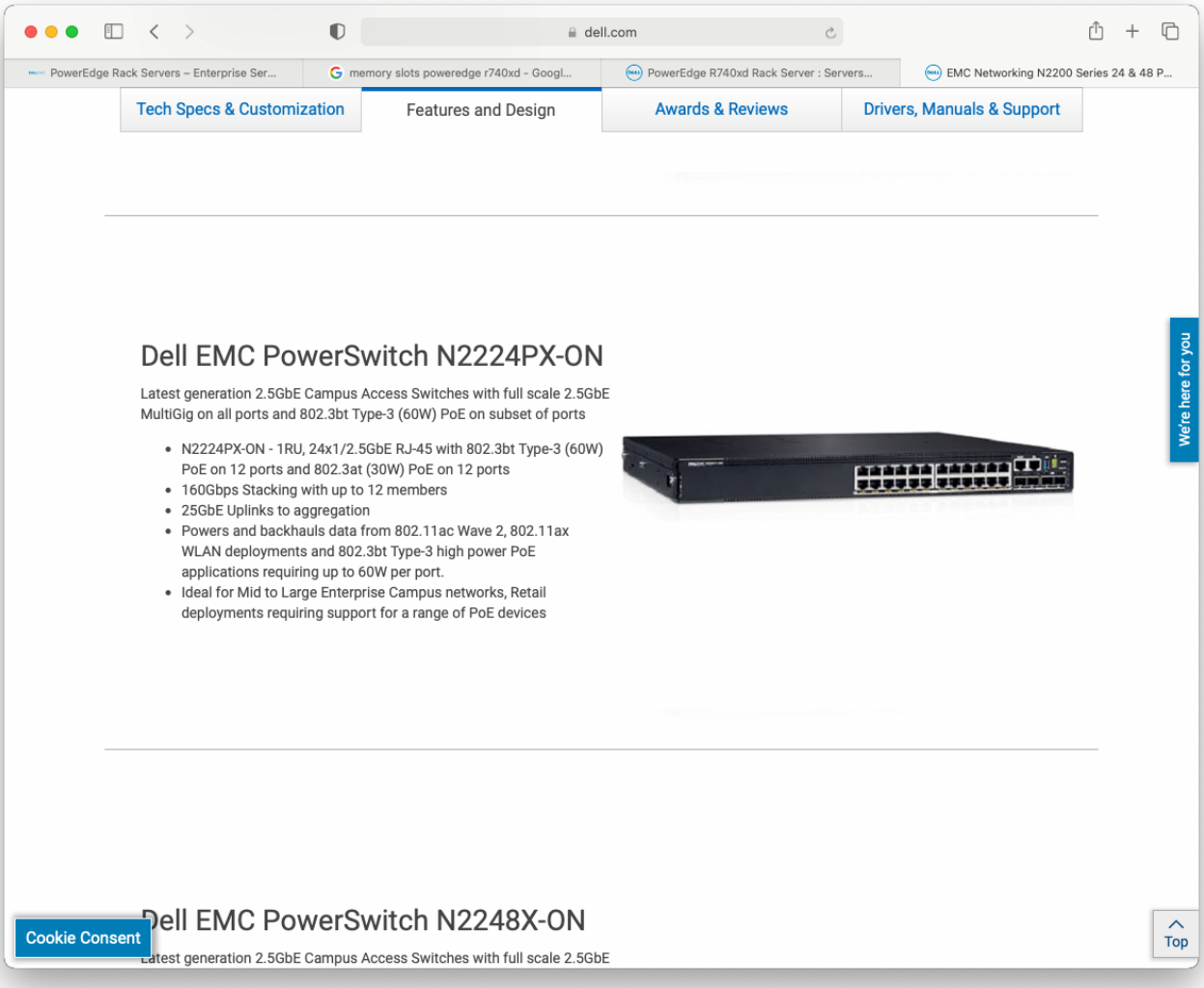


Figure 12 – https://www.dell.com/en-us/work/shop/servers-storage-and-networking/dell-emc-powerswitch-n2248px-on/spd/networking-n2200-series/dn_n2248px-on_13623

The following page and subsequent pages just showed the features and other technical information regarding the N3000 range of switches. The information was technically accurate as it came directly from the manufacturer also provided the option to specify additional features in the price.

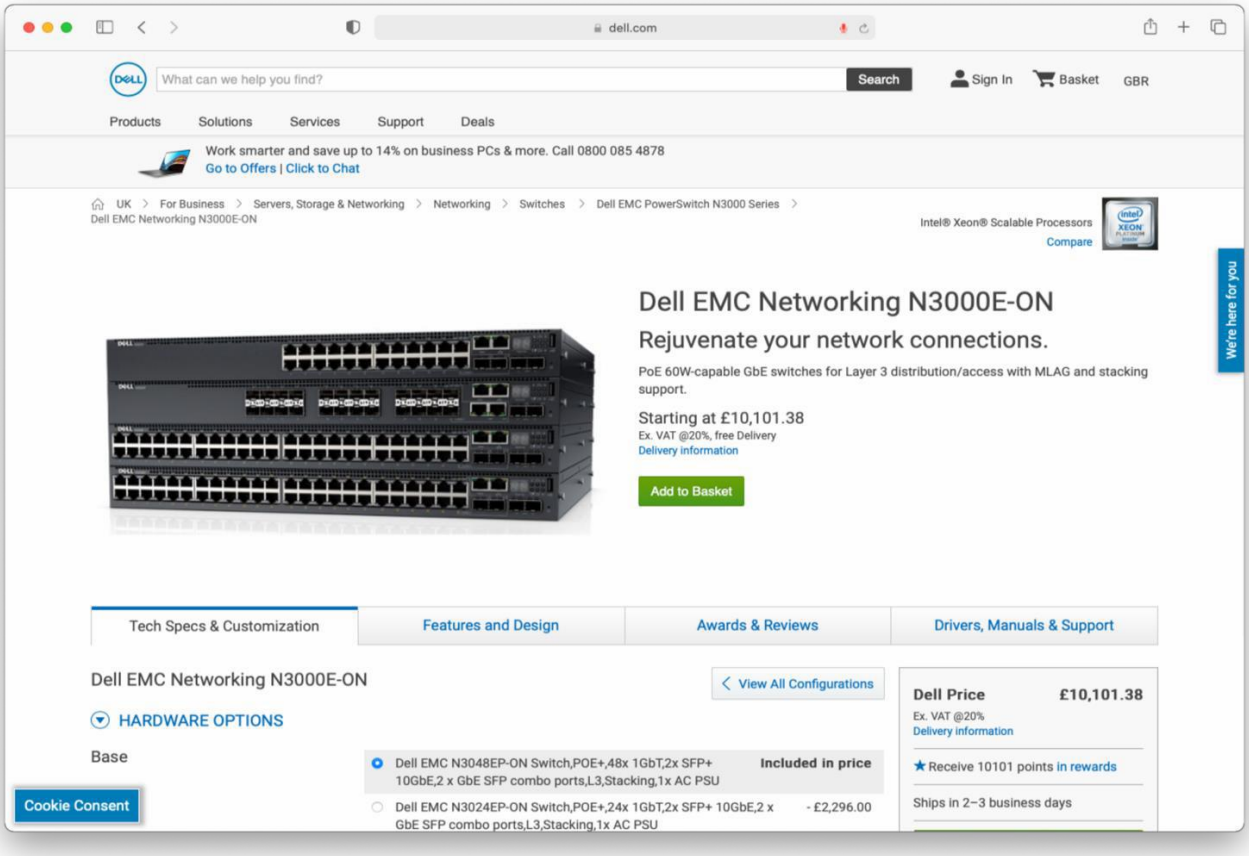
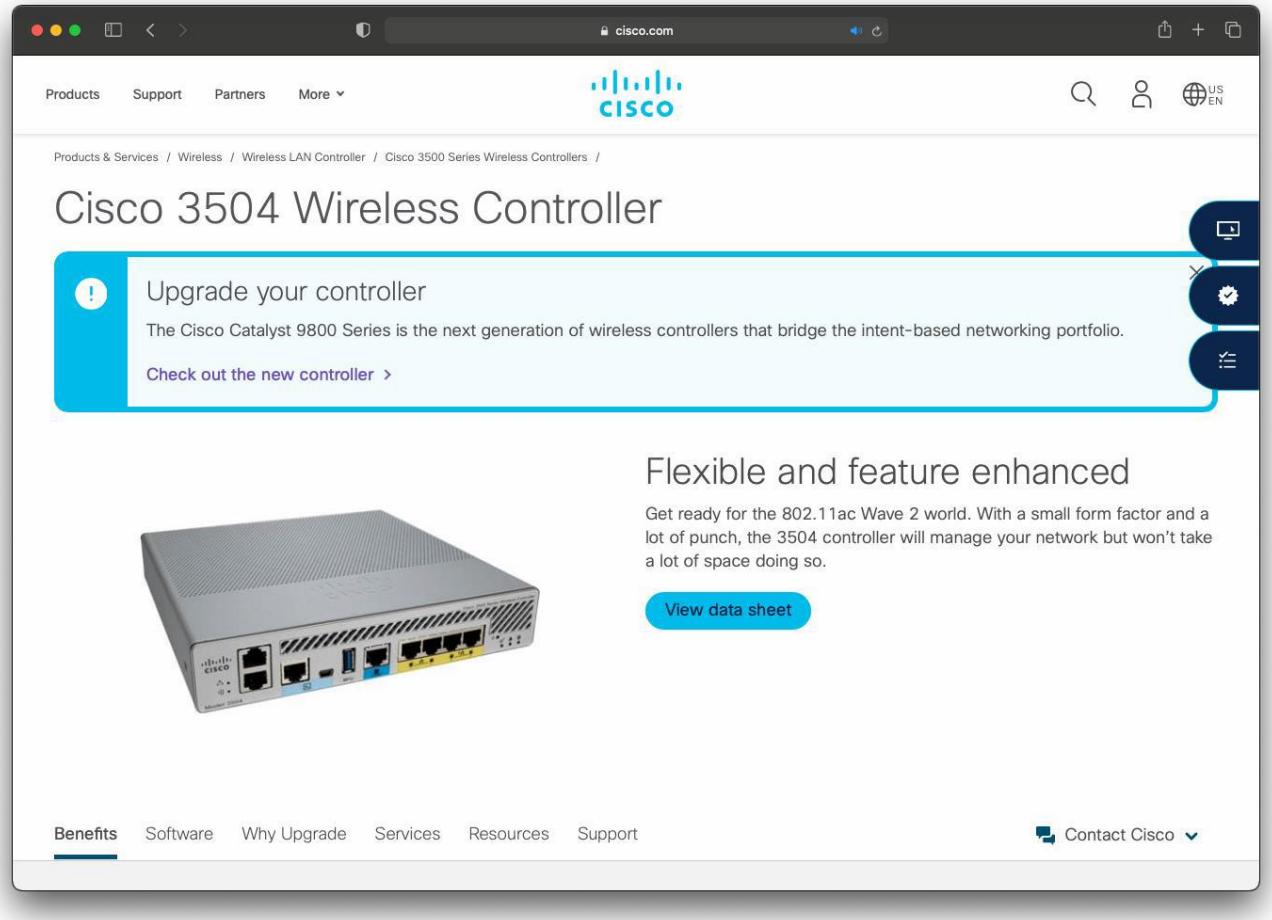


Figure 13 https://www.dell.com/en-uk/work/shop/povw/networking-n3000-series

The Cisco 3504 wireless controller is a smaller device used for managing all the WiFi infrastructure throughout the business. Technically it provided a lot of information about the features and capabilities when aligned with the access points. The information was clear and provided the data required to make an informed judgement on the product.



I felt it was useful to get a review of the product, TrustRadius, a respected review site included sever reviews regarding the controller. Knowing that the reviews are from industry experts provided additional reassurance on the quality of the device. Having a number of reviews about the product also helped to get a wider range of views and how it has been integrated into existing environments.

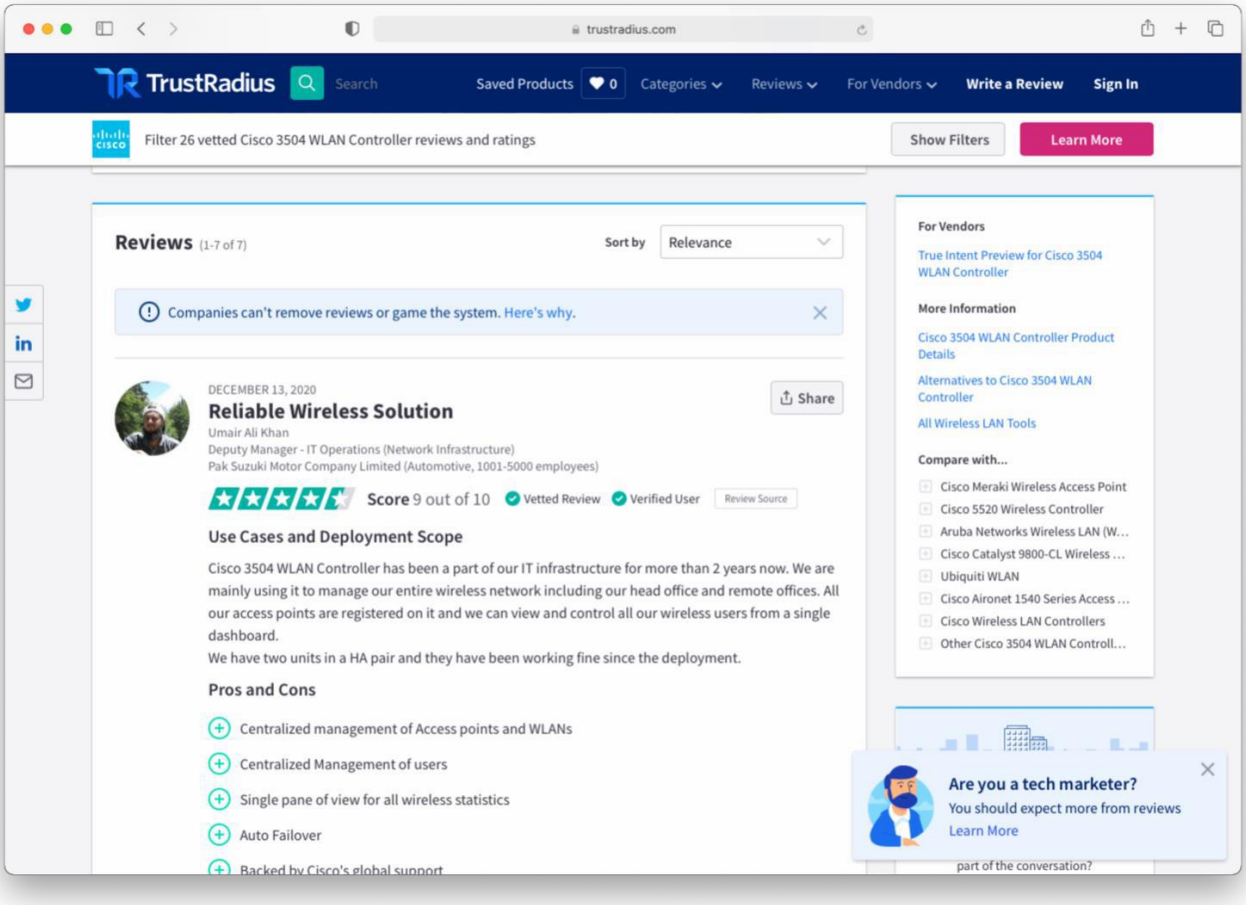


Figure 14 -https://www.trustradius.com/products/cisco-3504-wlan-controller/reviews

The Cisco site was used again to find information about the Cisco Aironet access point, it provided a wealth of technical information that helped make selecting the product easier. It was already decided that the wireless infrastructure would be Cisco. The webpage provided details over all the licensing, product specifications and features. Simply, a trusted source that provided information required information to aid the selection of a device.

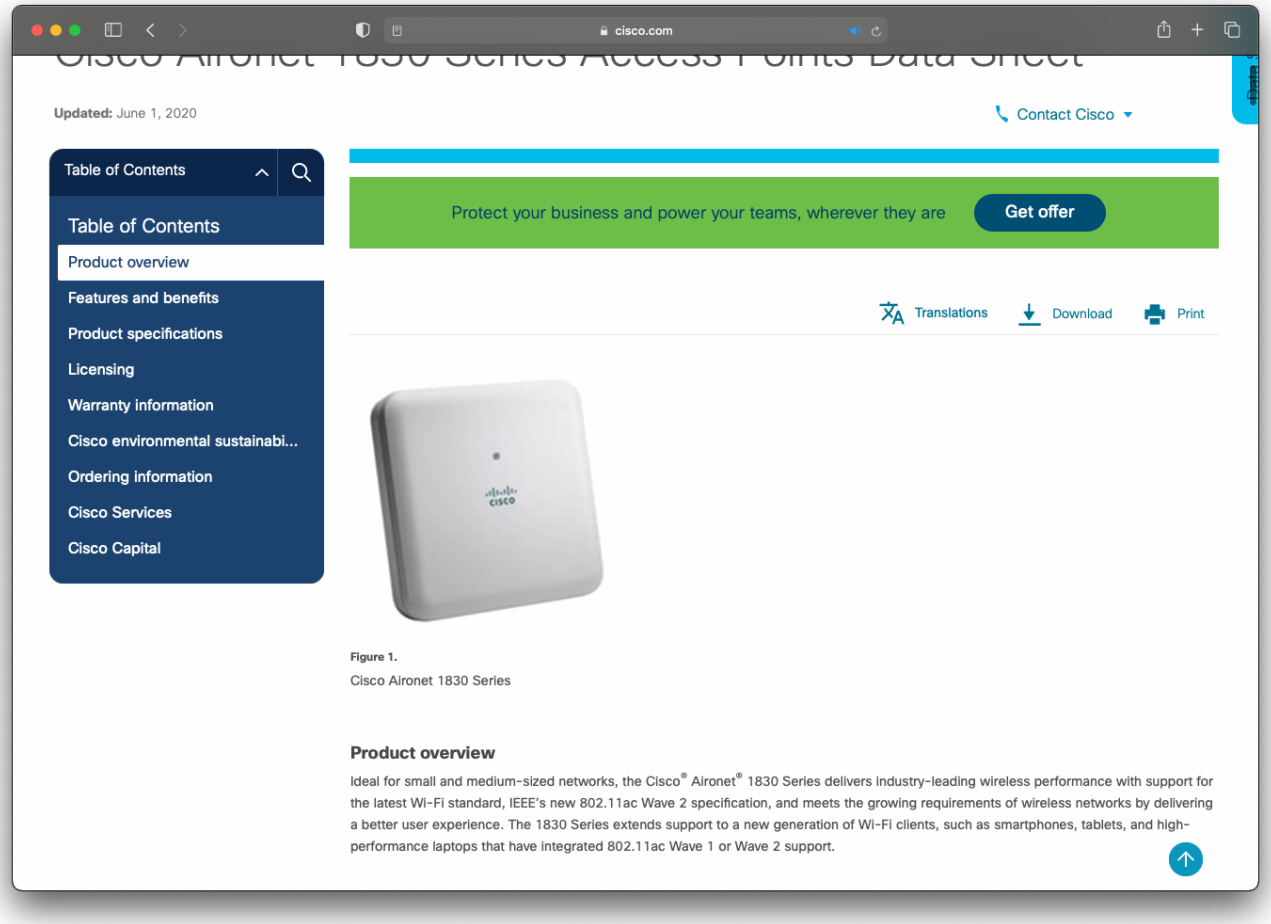


Figure 15 - https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1830-series-access-points/datasheet-c78-735582.html

The article from NetworkWorld site was used briefly just to clarify how the beamforming function was used in conjunction with the access points. This only reafirmed my knowledge in justifying the selection of the equipment.

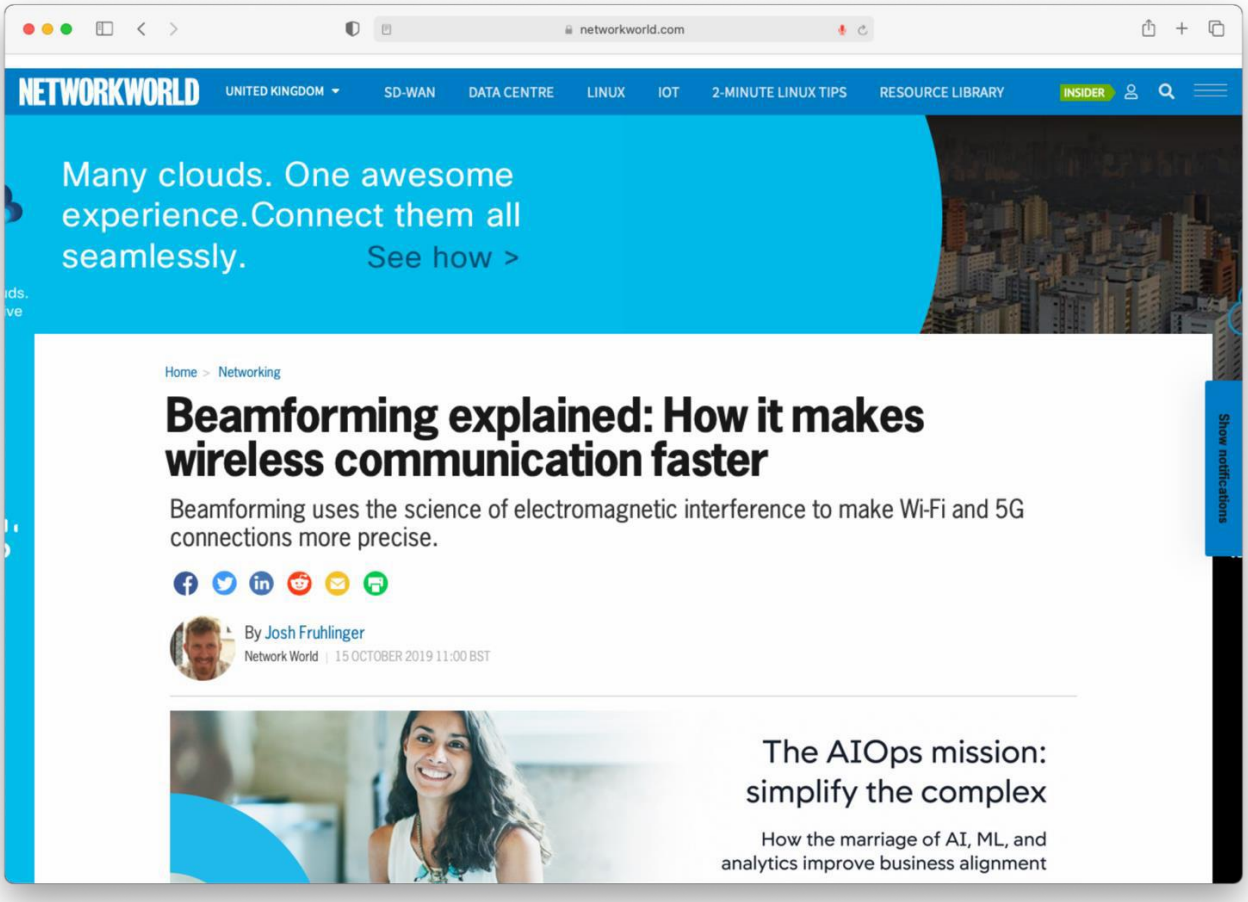
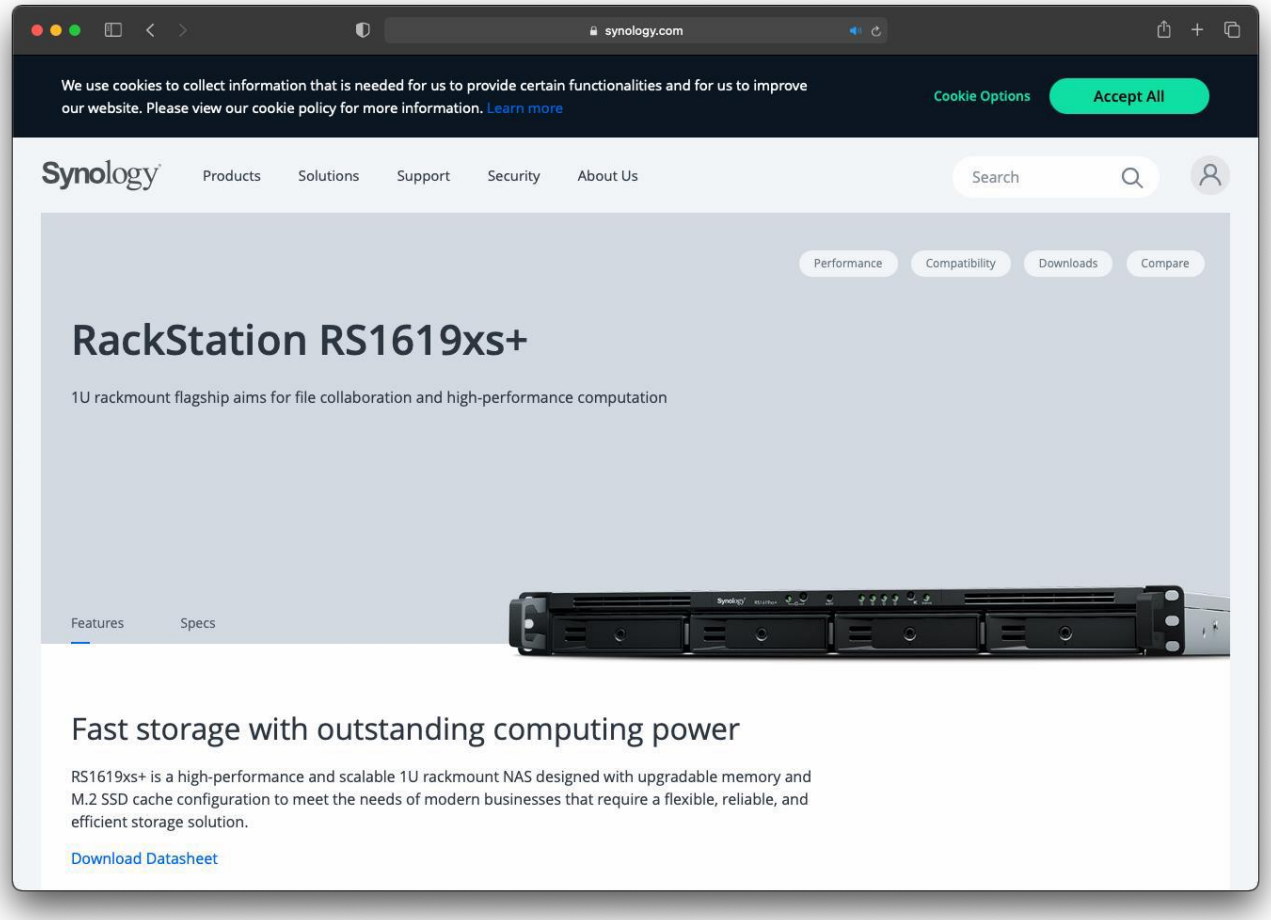


Figure 16 - https://www.networkworld.com/article/3445039/beamforming-explained-how-it-makes-wireless-communication-faster.html

The rackstation has been selected based on previous experience with Synology and the range of features available. When looking for which model, a number of prerequisites were in place (for example, closed system, upgradeability and a rack mounted solution). The information on the site was written and provided technical information and the functions. The site lacked any reviews, it was just about manufacturer-based content only.



The ITPro review of the Synology RS1619xs+ had a very positive verdict on the features and functions of the device and provided a good review in the context of the corporate environment. Though the verdict was very positive, the article did address some weaker areas of the review. ITPro has a very wide range of news and reviews on the industry and found the information very useful us justifying the selection.

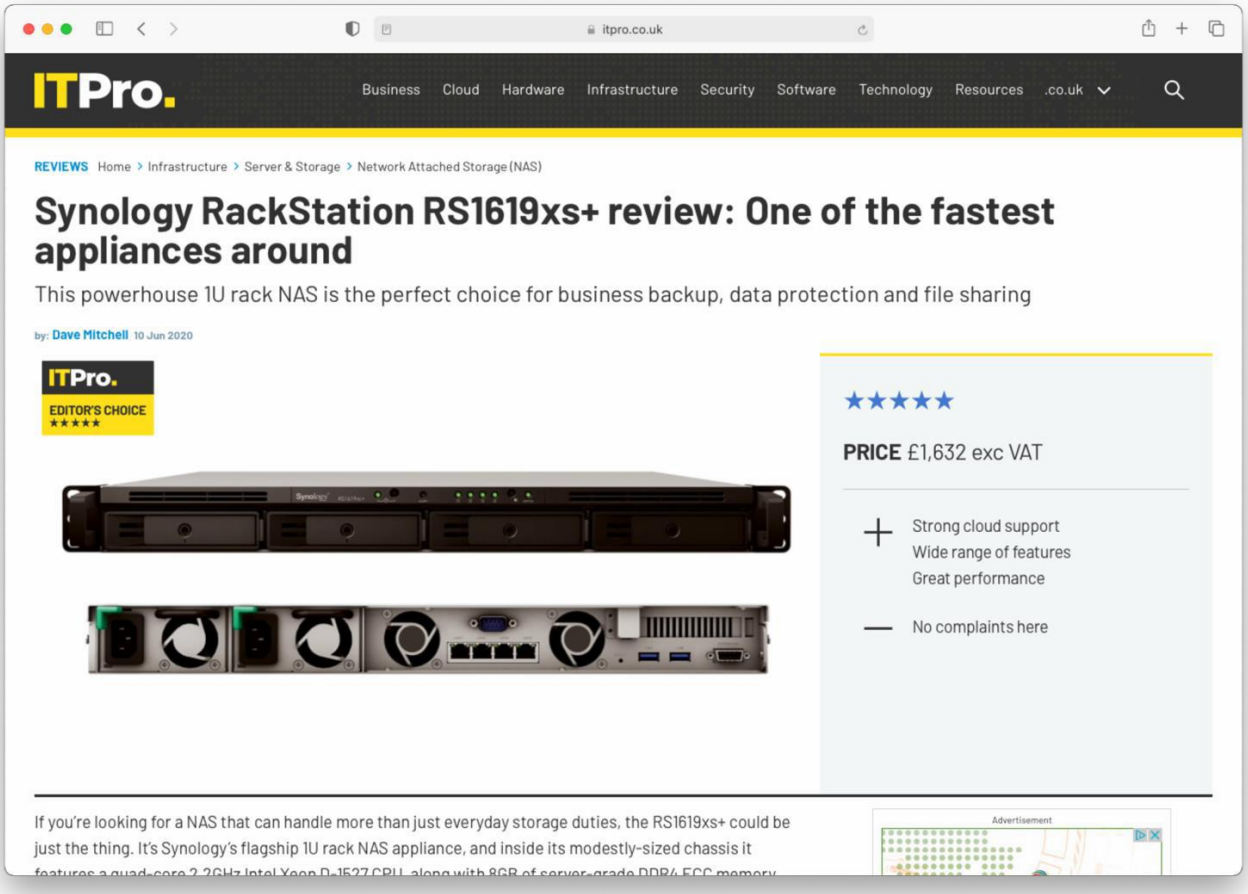
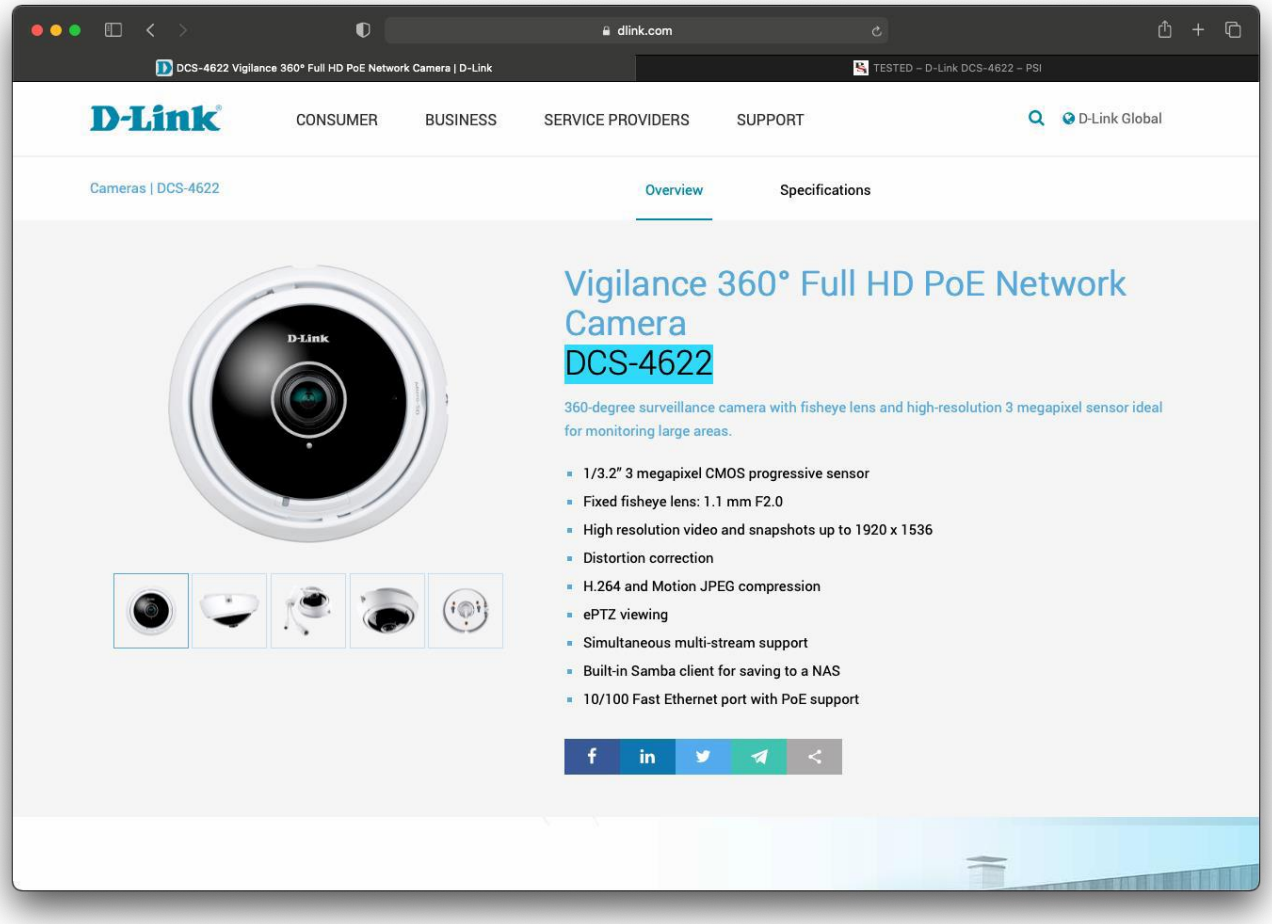


Figure 17 - https://www.itpro.co.uk/server-storage/network-attached-storage-nas/356016/synology-rackstation-rs1619xs-review-one-of-the

The D-Link website was very functional compared to those of the other products researched during this assignment. The description was limited to one line and only provided the feature set for the device. The quality of the information seemed accurate enough as this was direct from the manufacturer but didn't provide recommended implementation information like the Dell or Cisco sites.



As a result of the limited information on website the only useful review I could find came from the PSI website. The quality of the review was a little limited. The addition of the podcasts added a little more weight to the review but it lacked some of detail of a professional reviewing site (for example, ZDNet). However, the information was useful and provided some valuable insight into the device and how it fares in the real world.

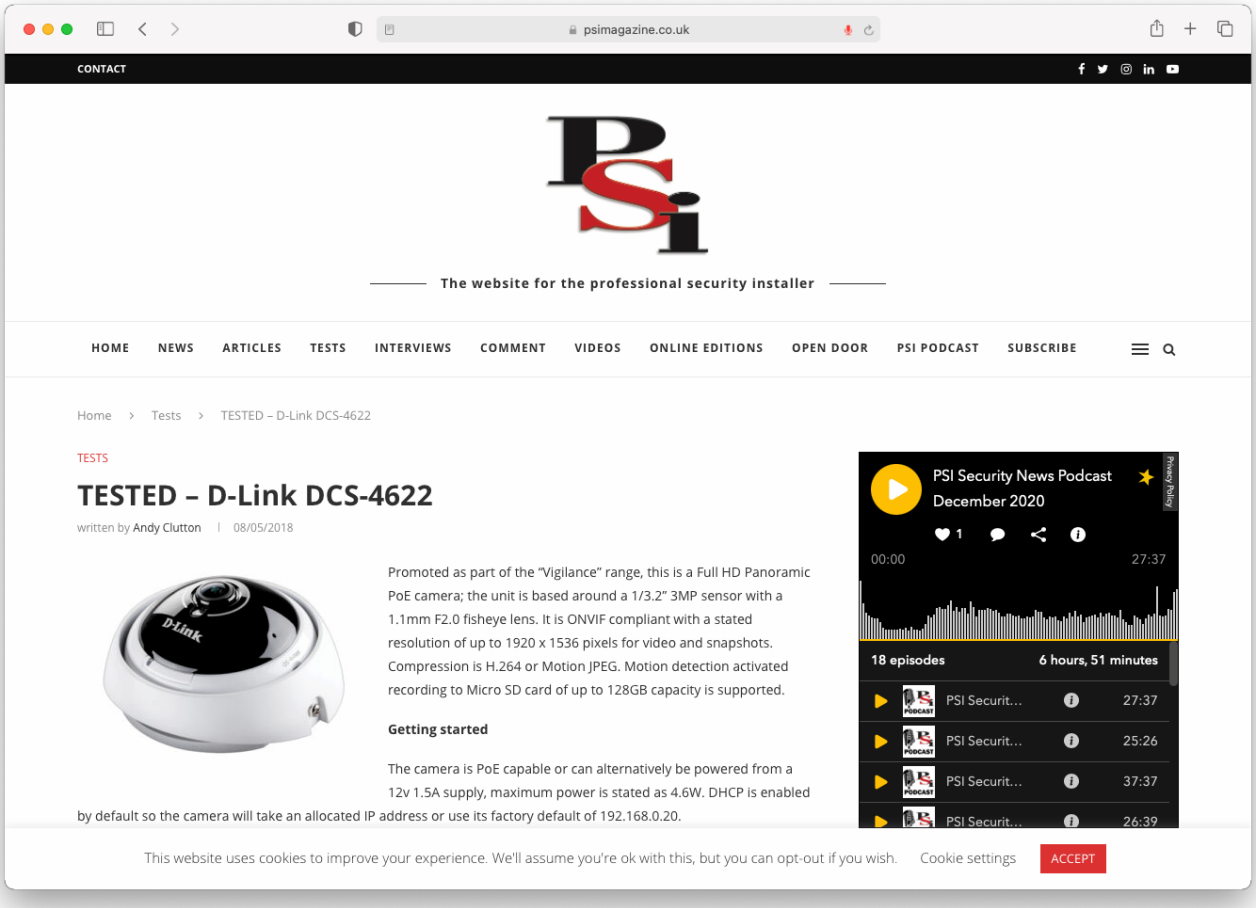


Figure 18 - https://psimagazine.co.uk/tested-d-link-dcs-4622/

Review and submit

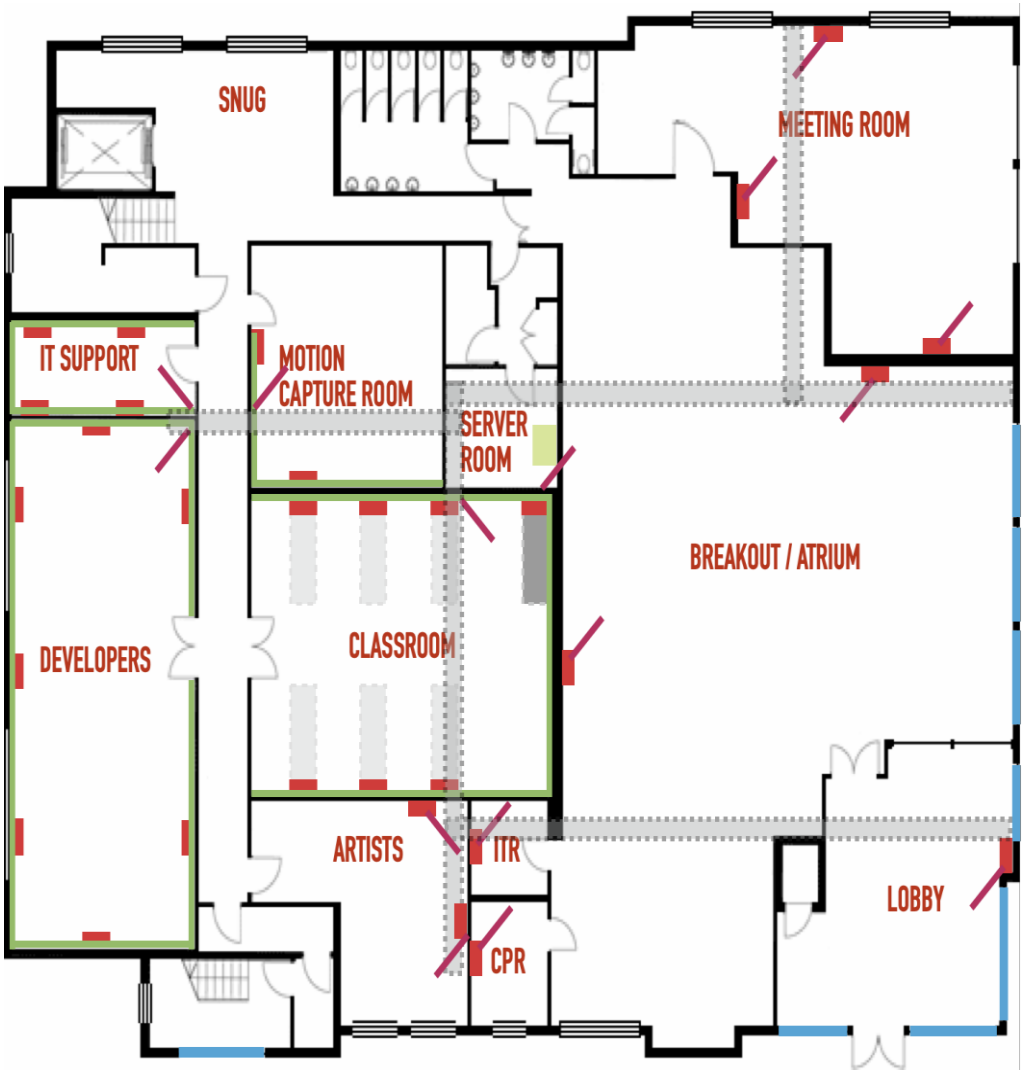
You have now reached the end of the assignment. It is recommended that you review all the evidence required for the assignment to ensure all print screens and annotations have been provided.

Save this document and convert into a .pdf for submission using the file naming convention.
Surname_Initial_student number_Workbook1

For example: Smith_J_123456789_Workbook1.pdf

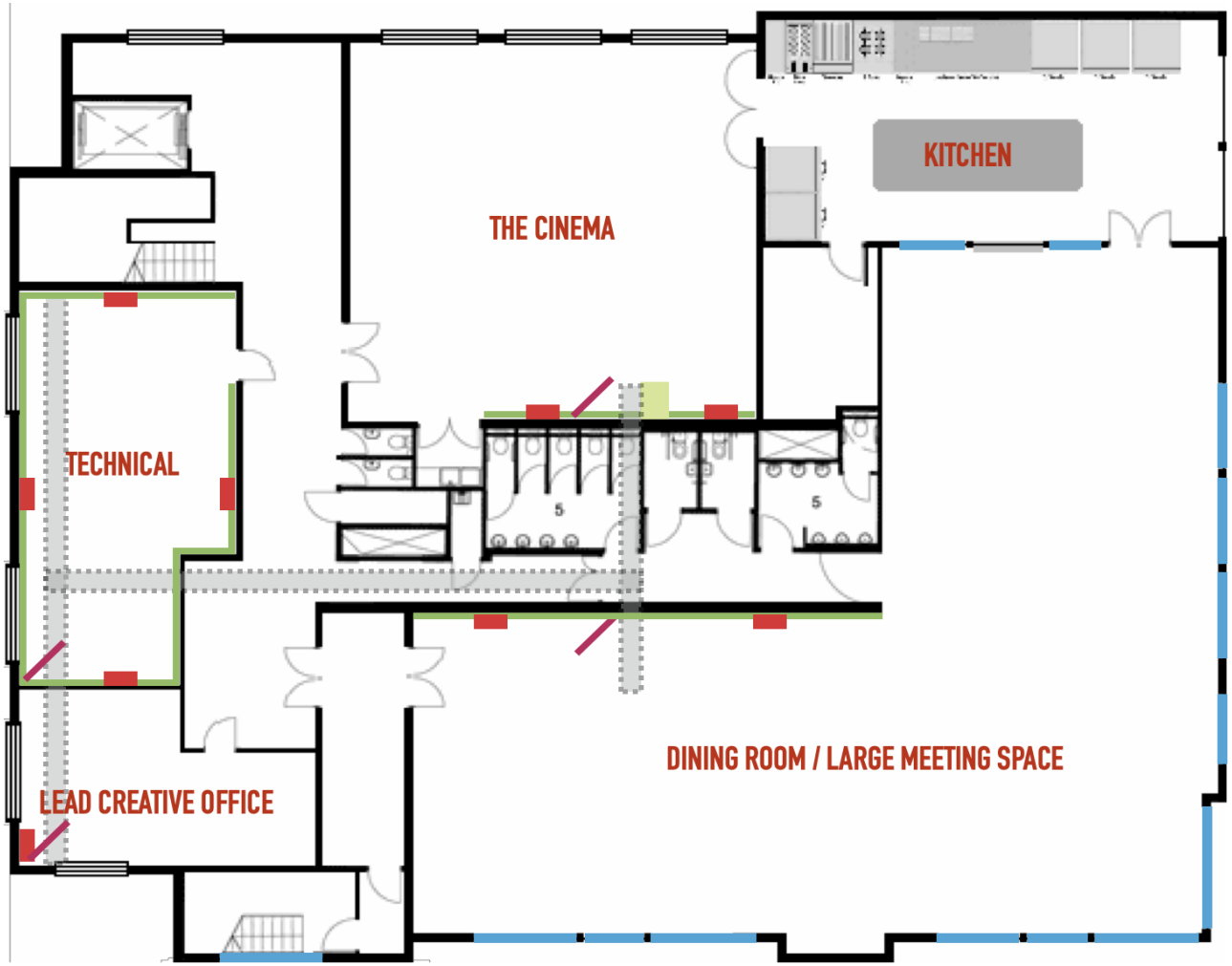
Floor plan: ground floor

To be copied as required.



Floor plan: first floor

To be copied as required.



Document information

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Published final version		May 2021
v1.1	NCFE rebrand.		January 2023