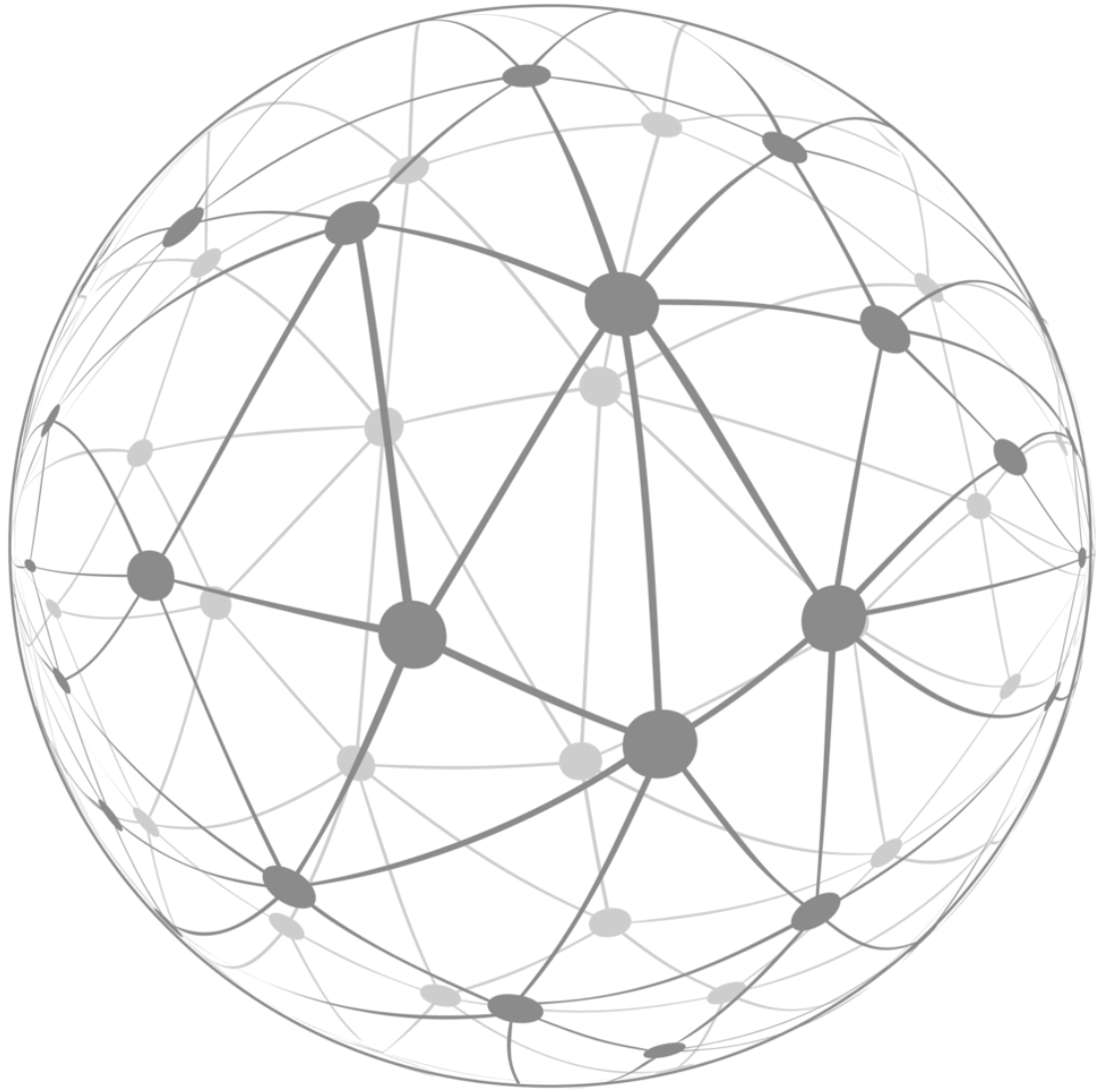
IT Reference Framework

Encouraging smarter discussions and connecting the dots !

By Richard Diver



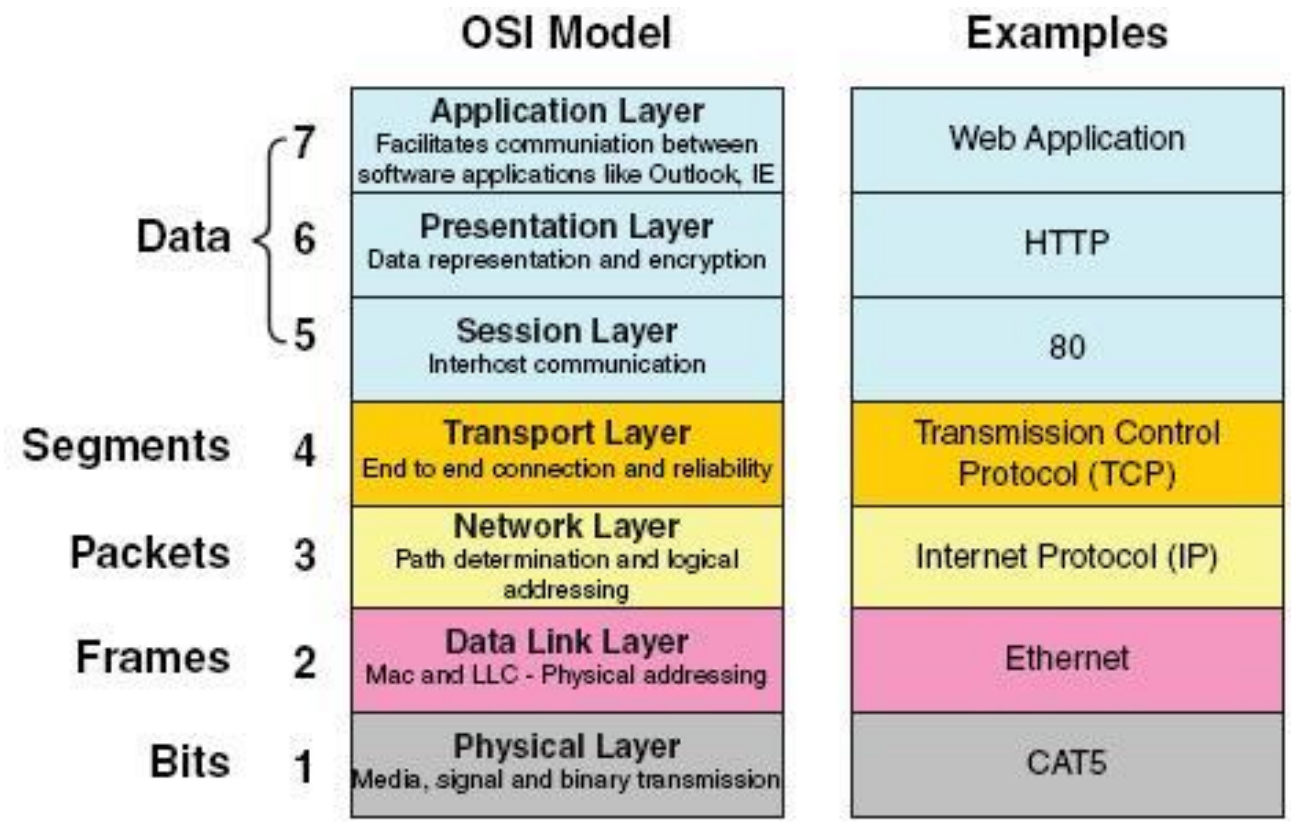
Richard Diver

- Solution Architect for security, cloud and infrastructure technologies
- 20 years experience across industries and geographies
- A visual communicator, thinker, innovator

Introduction

- There is a need for common language and reference points when discussing technology and building solutions
- We have to view a solution from end to end, with consideration of how each component connects to the next
- The proposed framework needs to be repeatable, extendable, and easy to understand
- It also needs to be visually appealing; the use of icons helps with visual recognition, and less wording
- The framework also needs to have some key principles to follow when using it to create a solution specific set of diagrams

Remember the OSI Layers?



- Simple and clear
- Common language
- Visual reference

*https://**en.wikipedia.org**/wiki/**OSI_model***

Key Principle 1:

The two most important elements in every solution that we need to control are:

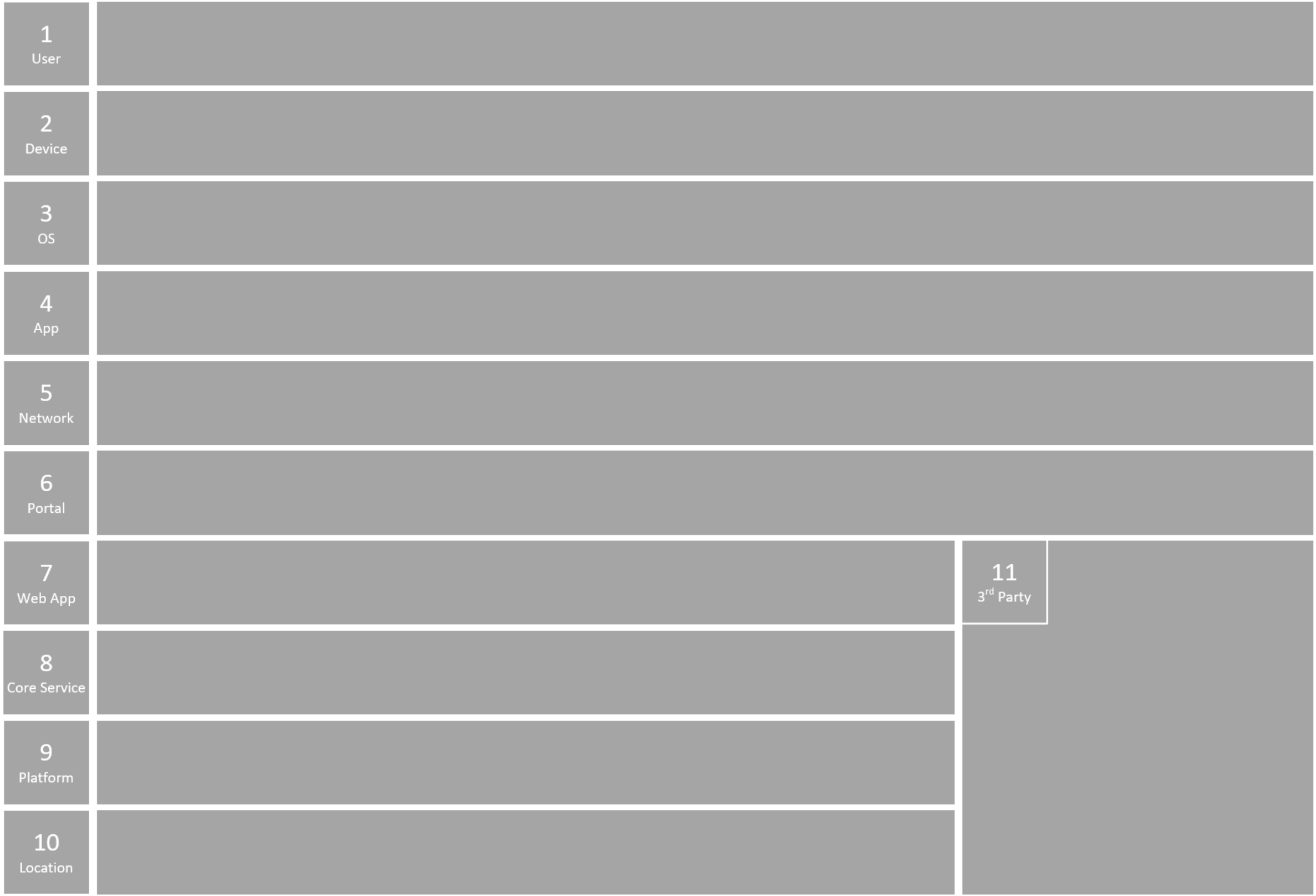
1. **Identity:** the end user trying to gain access to the system, the administrators building and maintaining it, and the security contexts that run the backend processes

2. **Information:** from raw data to highly sensitive information. Storing, analysing, and displaying accurate data in a timely fashion

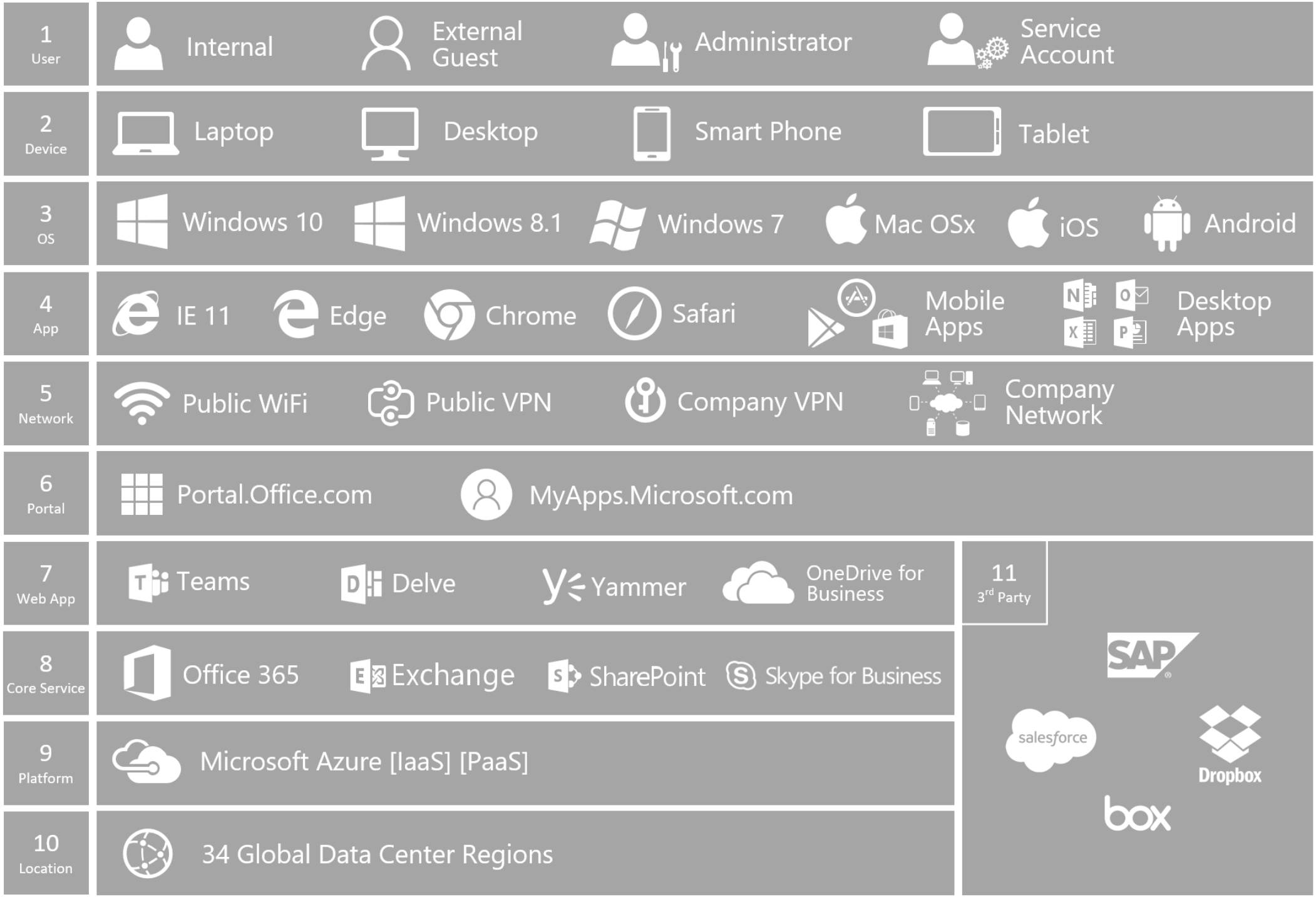
Everything else in a system should be designed to helping the user get to the information, and keeping the data secure from unauthorised access and distribution

Building a framework

- There are many ways of explaining how solutions work, and even more ways of drawing the solution in a basic or complex diagram.
- Because every solution contains common parts, a framework needs a standardised way of displaying solutions specific components, and how they integrate with other components.
- Using a number reference allows for ease of reference when explaining the solution in written text.
- The framework also needs to work for both cloud solutions, as well as existing on-premises solutions.
- This diagram shows the first stage of the framework - defining the component layers:

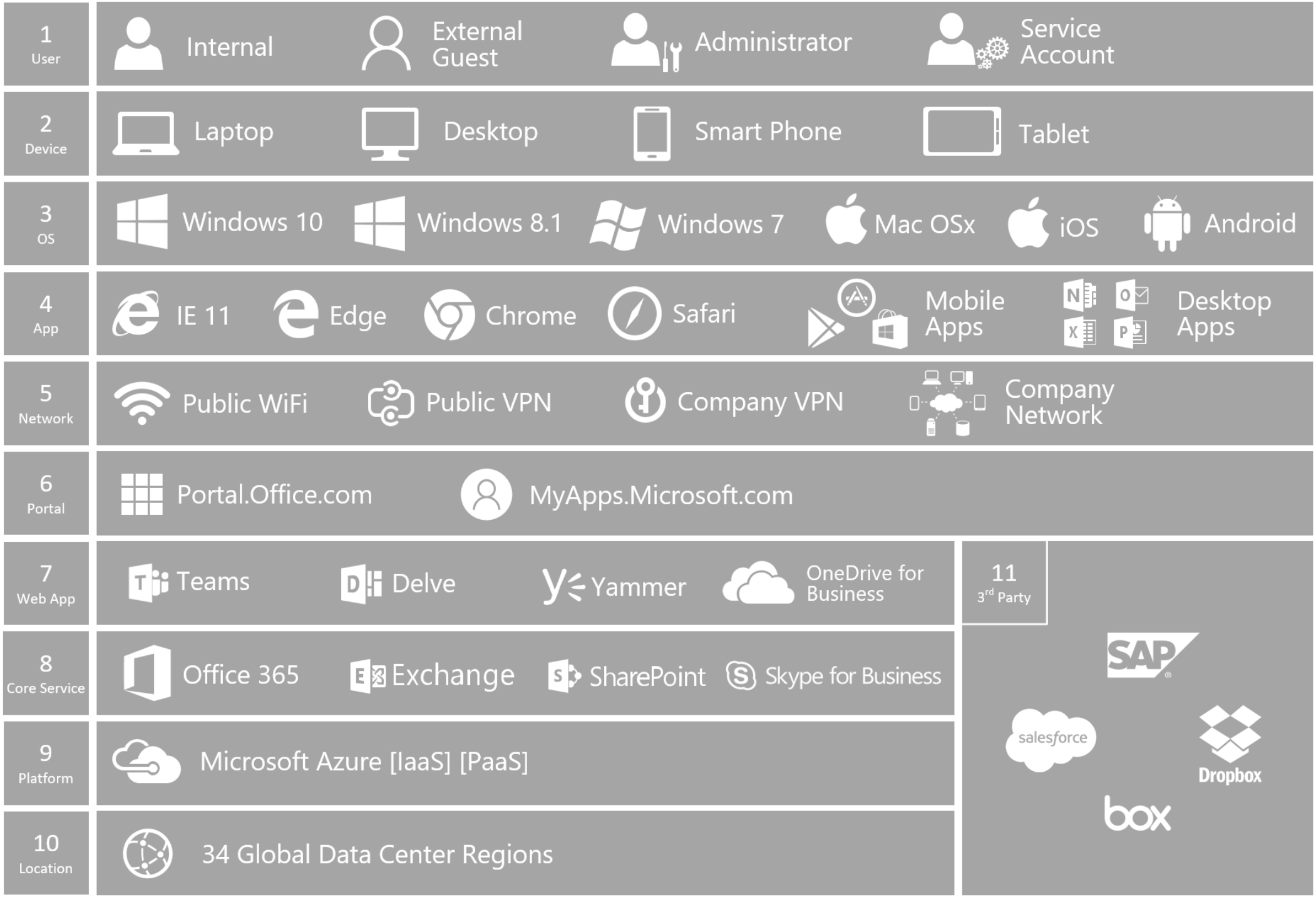

1
User
2
Device
3
OS
4
App
5
Network
6
Portal
7
Web App
8
Core Service
9
Platform
10
Location
11
3rd Party

1 User	This section identifies the type of user trying to access the system. There are 2 key types: **Internal** or **External**. They may also be a **Standard User**, or an **Administrator**
2 Device	Standardise the types of hardware that are used to access system, based on form factor, screen size, and functionality, such as a **Desktop**, **Laptop**, **Tablet**, or **Smart Phone**
3 OS	The **Operating System (OS)** is dependant on the hardware. This layer is critical when understanding the security, manageability, and user experience options available to the end user
4 App	The Apps layer can articulate the different ways a user can view and modify data. The 3 key types are: **Browser**, **Mobile Apps**, and full **Desktop Clients**, which can include Windows Explorer and PowerShell
5 Network	The type of network used to gain access to the system can vary; from a fast physical corporate network, to WiFi at home or 4G mobile network. The 2 key types are **Internal** (trusted), or **External**
6 Portal	The portal layer provides details about interface into the solution. It could be a **landing page**, **login screen**, a **portal** (such as portal.office.com, or portal.azure.com), or it could be an **API**
7 Web App	This layer is the key web-based user interface of any solution, access via a browser. The Web App may connect to one or multiple core services
8 Core Service	This layer is where most **PaaS** solutions would be presented: fully functioning solutions that provide specific functionality
9 Platform	The platform layer focuses on the Infrastructure Services (**IaaS**) components such as storage, compute, and networking
10 Location	Every cloud solution existing in one or more geographic, location. This layer can be used to explain the physical boundaries and data storage
11 3rd Party	This area is used to identify any connected services and 3rd party solutions that may reside outside of the core platform, and can also be used to explain on-premises solutions in a hybrid model

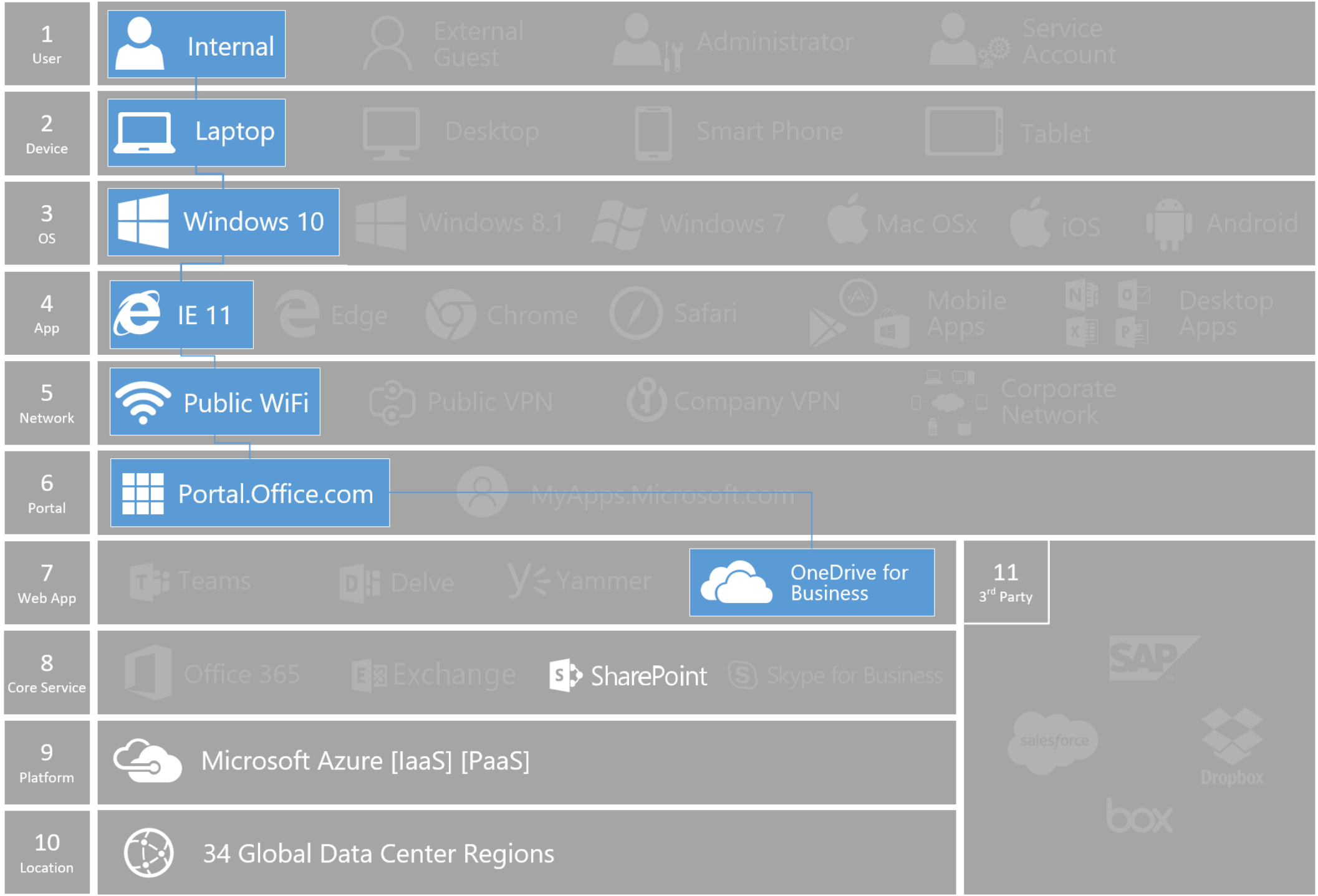

1
User
Internal
External Guest
Administrator
Service Account
2
Device
Laptop
Desktop
Smart Phone
Tablet
3
OS
Windows 10
Windows 8.1
Windows 7
Mac OSx
iOS
Android
4
App
IE 11
Edge
Chrome
Safari
Mobile Apps
Desktop Apps
5
Network
Public WiFi
Public VPN
Company VPN
Company Network
6
Portal
Portal.Office.com
MyApps.Microsoft.com
7
Web App
Teams
Delve
Yammer
OneDrive for Business
8
Core Service
Office 365
Exchange
SharePoint
Skype for Business
9
Platform
Microsoft Azure [IaaS] [PaaS]
10
Location
34 Global Data Center Regions
11
3rd Party
SAP
salesforce
Dropbox
box

Highlighting Options

- This model uses a greyscale theme to allow a simple view without distraction of colour themes. This can be tailored to meet the needs of the designer.
- One option is to grey out the items that are not applicable. You can also add colour to the icons, or the wording, for those items you want to specifically show.
- See the next slides for examples, the solution highlights the following scenario components:
- A corporate user on their Windows 10 Laptop connected using Public WiFi
- The user is browsing to their OneDrive for Business files, using IE 11
- OneDrive for business is built upon SharePoint Online, which is part of Office 365, hosted on Microsoft Azure in Australia


1
User
Internal
External Guest
Administrator
Service Account
2
Device
Laptop
Desktop
Smart Phone
Tablet
3
OS
Windows 10
Windows 8.1
Windows 7
Mac OSx
iOS
Android
4
App
IE 11
Edge
Chrome
Safari
Mobile Apps
Desktop Apps
5
Network
Public WiFi
Public VPN
Company VPN
Company Network
6
Portal
Portal.Office.com
MyApps.Microsoft.com
7
Web App
Teams
Delve
Yammer
OneDrive for Business
8
Core Service
Office 365
Exchange
SharePoint
Skype for Business
9
Platform
Microsoft Azure [IaaS] [PaaS]
10
Location
34 Global Data Center Regions
11
3rd Party
SAP
salesforce
Dropbox
box


1
User
Internal
External Guest
Administrator
Service Account
2
Device
Laptop
Desktop
Smart Phone
Tablet
3
OS
Windows 10
Windows 8.1
Windows 7
Mac OSx
iOS
Android
4
App
IE 11
Edge
Chrome
Safari
Mobile Apps
Desktop Apps
5
Network
Public WiFi
Public VPN
Company VPN
Corporate Network
6
Portal
Portal.Office.com
MyApps.Microsoft.com
7
Web App
Teams
Delve
Yammer
OneDrive for Business
8
Core Service
Office 365
Exchange
SharePoint
Skype for Business
9
Platform
Microsoft Azure [IaaS] [PaaS]
10
Location
34 Global Data Center Regions
11
3rd Party
SAP
salesforce
Dropbox
box


1
User
Internal
External Guest
Administrator
Service Account
2
Device
Laptop
Desktop
Smart Phone
Tablet
3
OS
Windows 10
Windows 8.1
Windows 7
Mac OSx
iOS
Android
4
App
IE 11
Edge
Chrome
Safari
Mobile Apps
Desktop Apps
5
Network
Public WiFi
Public VPN
Company VPN
Corporate Network
6
Portal
Portal.Office.com
MyApps.Microsoft.com
7
Web App
Teams
Delve
Yammer
OneDrive for Business
11
3rd Party
8
Core Service
Office 365
Exchange
SharePoint
Skype for Business
9
Platform
Microsoft Azure [IaaS] [PaaS]
10
Location
34 Global Data Center Regions
SAP
salesforce
Dropbox
box

Collapsed View

- Once the first stage is used to explain the possible options, and highlighting the chosen scenario, the next step is to use this information to present more details to the solution.

- Firstly we need to make more room on the screen…

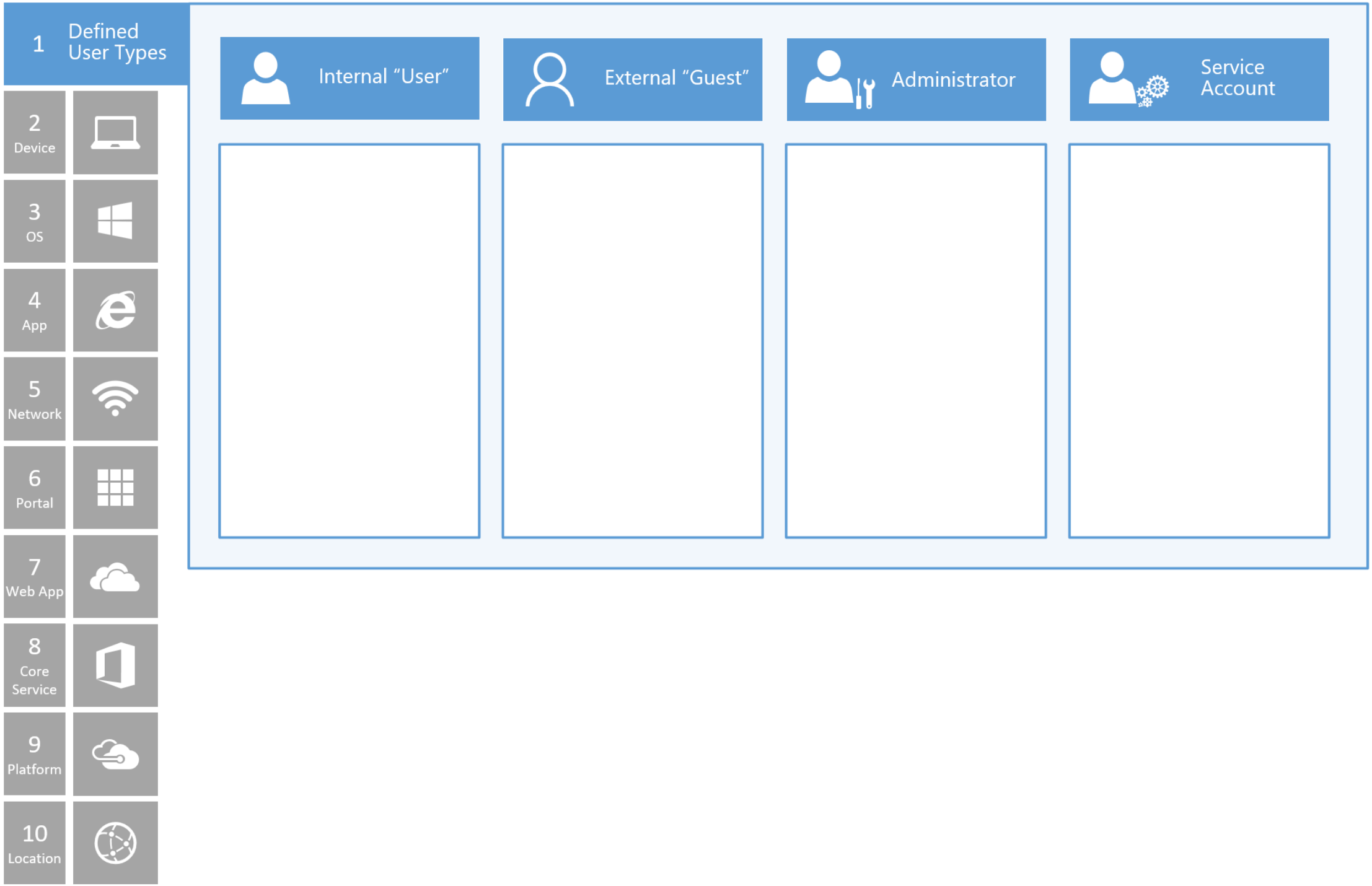

1
User
Internal
External Guest
Administrator
Service Account
2
Device
Laptop
Desktop
Smart Phone
Tablet
3
OS
Windows 10
Windows 8.1
Windows 7
Mac OSx
iOS
Android
4
App
IE 11
Edge
Chrome
Safari
Mobile Apps
Desktop Apps
5
Network
Public WiFi
Public VPN
Company VPN
Corporate Network
6
Portal
Portal.Office.com
MyApps.Microsoft.com
7
Web App
Teams
Delve
Yammer
OneDrive for Business
8
Core Service
Office 365
Exchange
SharePoint
Skype for Business
9
Platform
Microsoft Azure [IaaS] [PaaS]
10
Location
34 Global Data Center Regions
11
3rd Party
SAP
salesforce
Dropbox
box

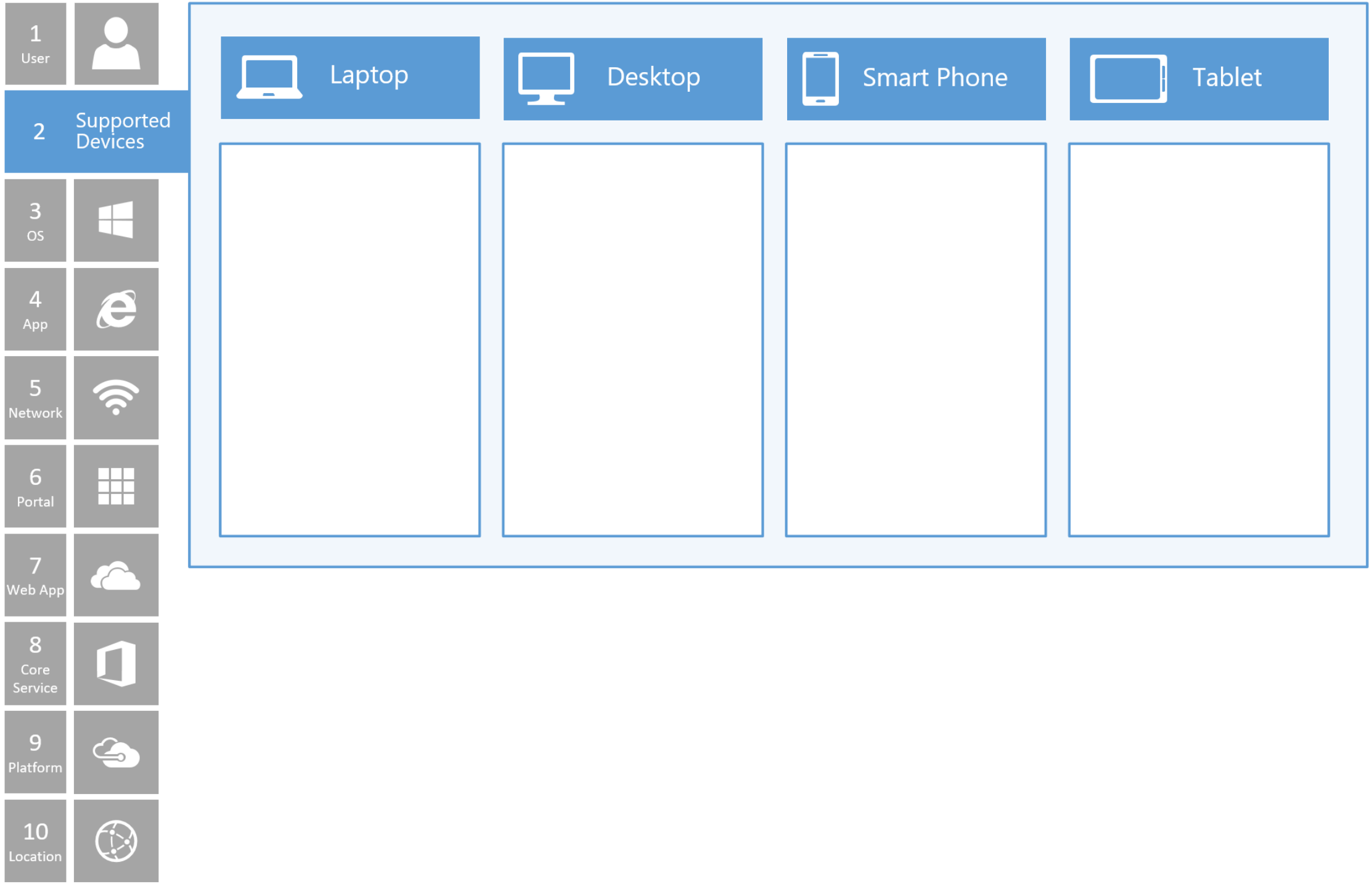

1
User
Internal
2
Device
Laptop
3
OS
Windows 10
4
App
IE 11
5
Network
Public WiFi
6
Portal
Office.com
7
Web App
OneDrive for Business
8
Core Service
SharePoint Online
9
Platform
Microsoft Azure
10
Location
Australia

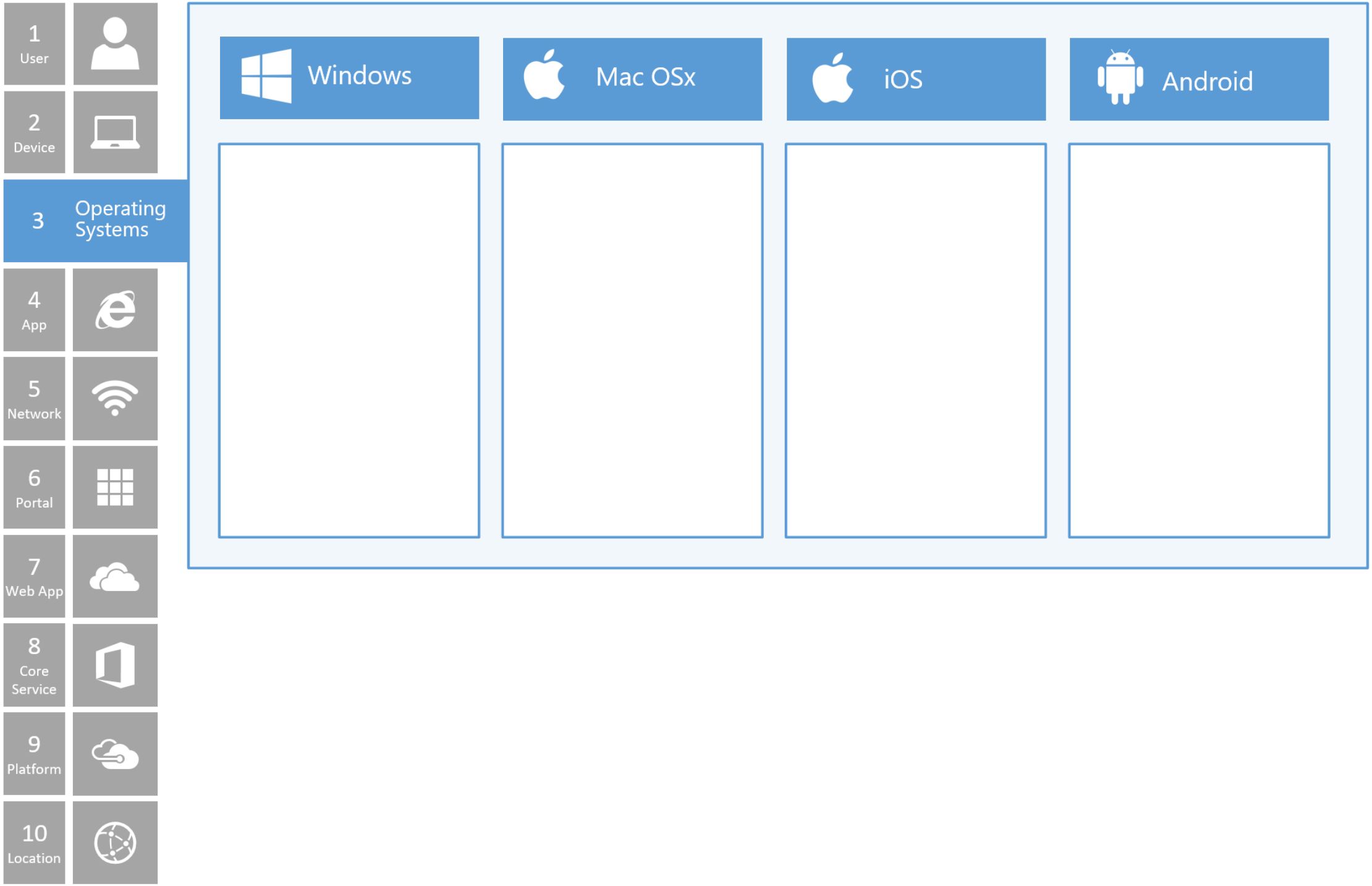
Detail Blades

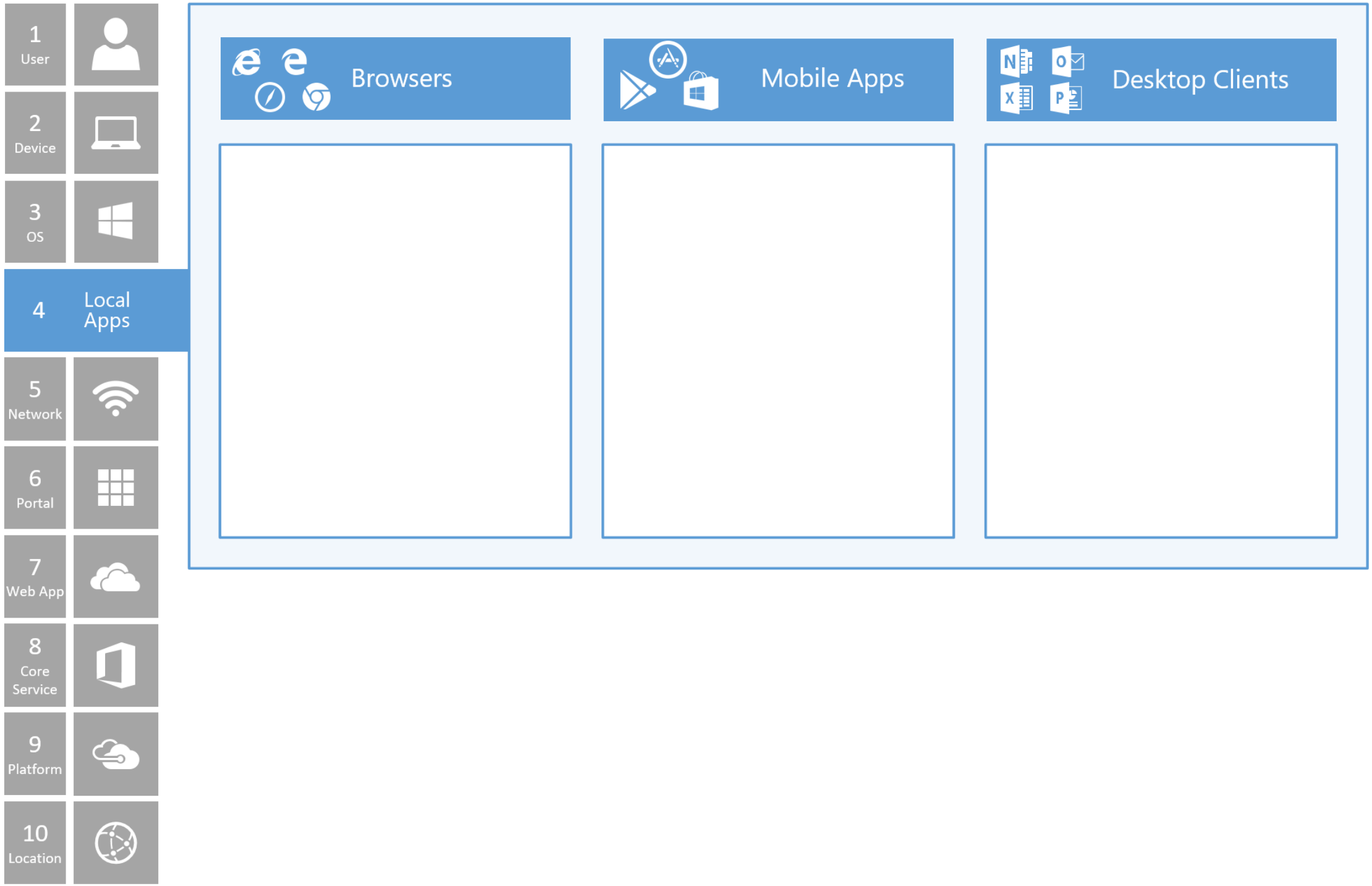
- This view can also be used with a default set of icons to represent the layers without specifically choosing any options.

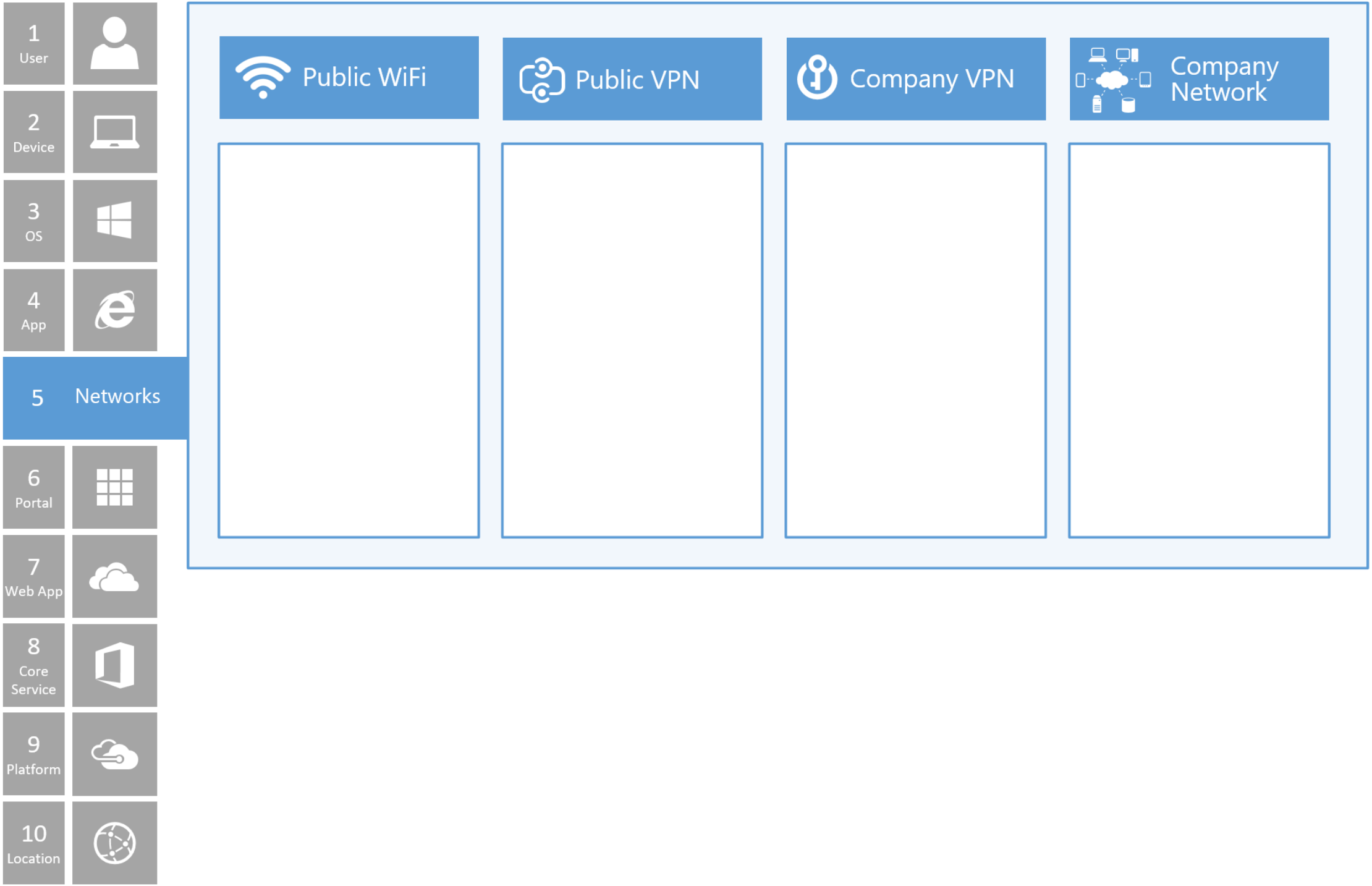
- With the navigation collapsed, we can show the details. These examples are based on my experience with Office 365 and Microsoft Azure.

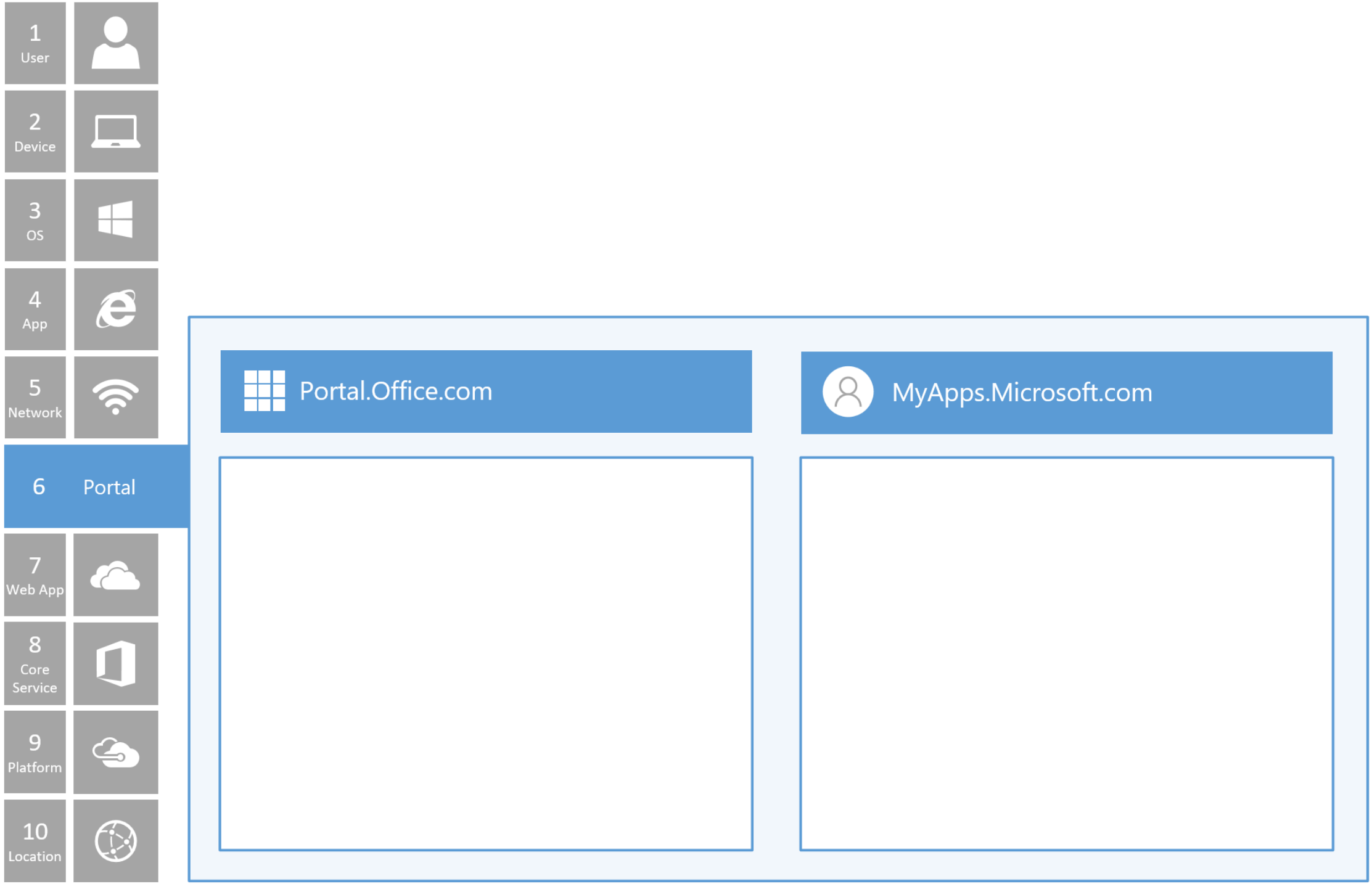

1
Defined User Types
Internal "User"
External "Guest"
Administrator
Service Account
2
Device
3
OS
4
App
5
Network
6
Portal
7
Web App
8
Core Service
9
Platform
10
Location

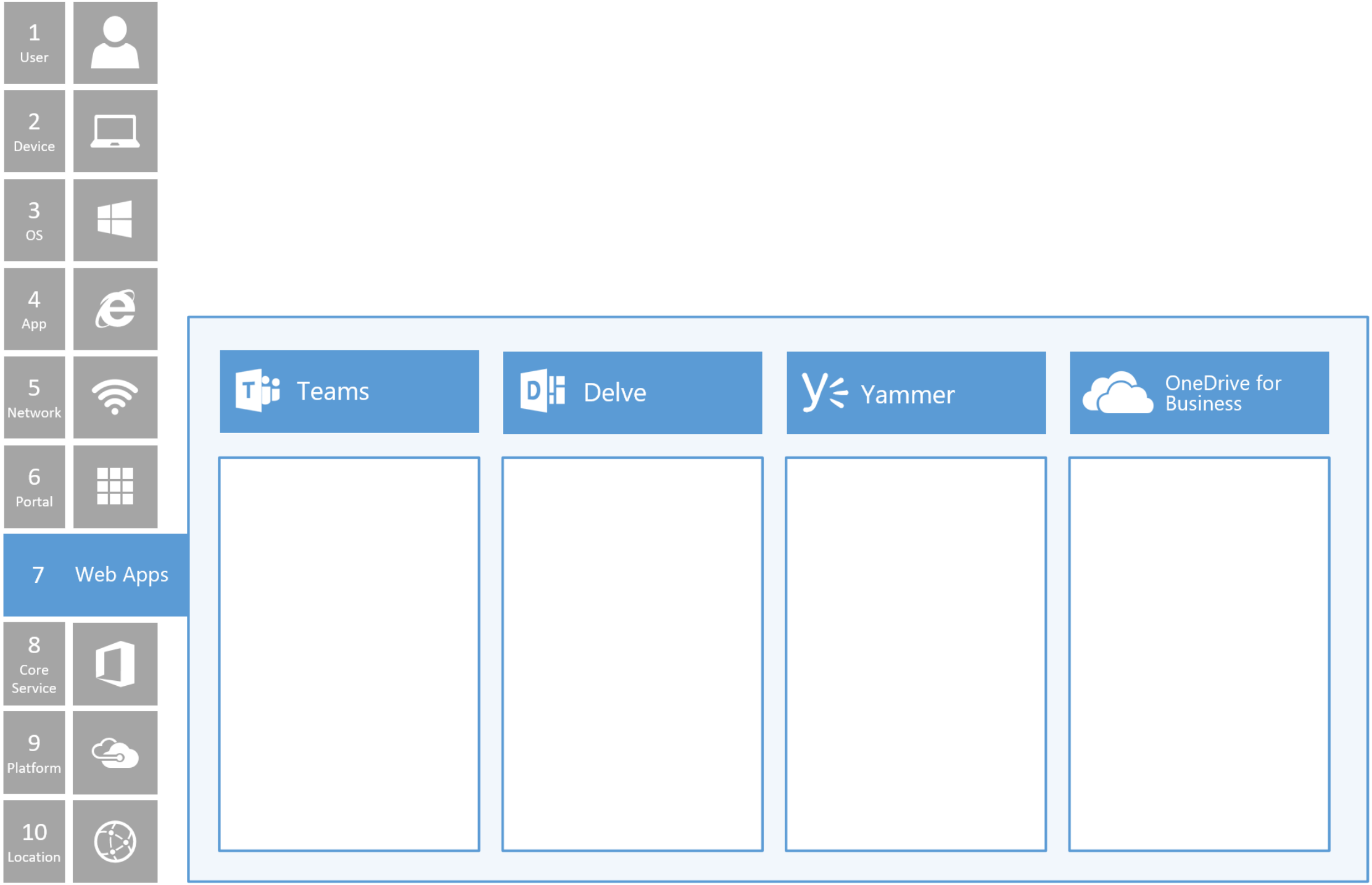

1
User
2
Supported Devices
3
OS
4
App
5
Network
6
Portal
7
Web App
8
Core Service
9
Platform
10
Location
Laptop
Desktop
Smart Phone
Tablet


1
User
2
Device
3
Operating Systems
4
App
5
Network
6
Portal
7
Web App
8
Core Service
9
Platform
10
Location
Windows
Mac OSx
iOS
Android


1
User
2
Device
3
OS
4
Local
Apps
5
Network
6
Portal
7
Web App
8
Core
Service
9
Platform
10
Location
Browsers
Mobile Apps
Desktop Clients


1
User
2
Device
3
OS
4
App
5
Networks
6
Portal
7
Web App
8
Core Service
9
Platform
10
Location
Public WiFi
Public VPN
Company VPN
Company Network


1
User
2
Device
3
OS
4
App
5
Network
6
Portal
7
Web App
8
Core Service
9
Platform
10
Location
Portal.Office.com
MyApps.Microsoft.com

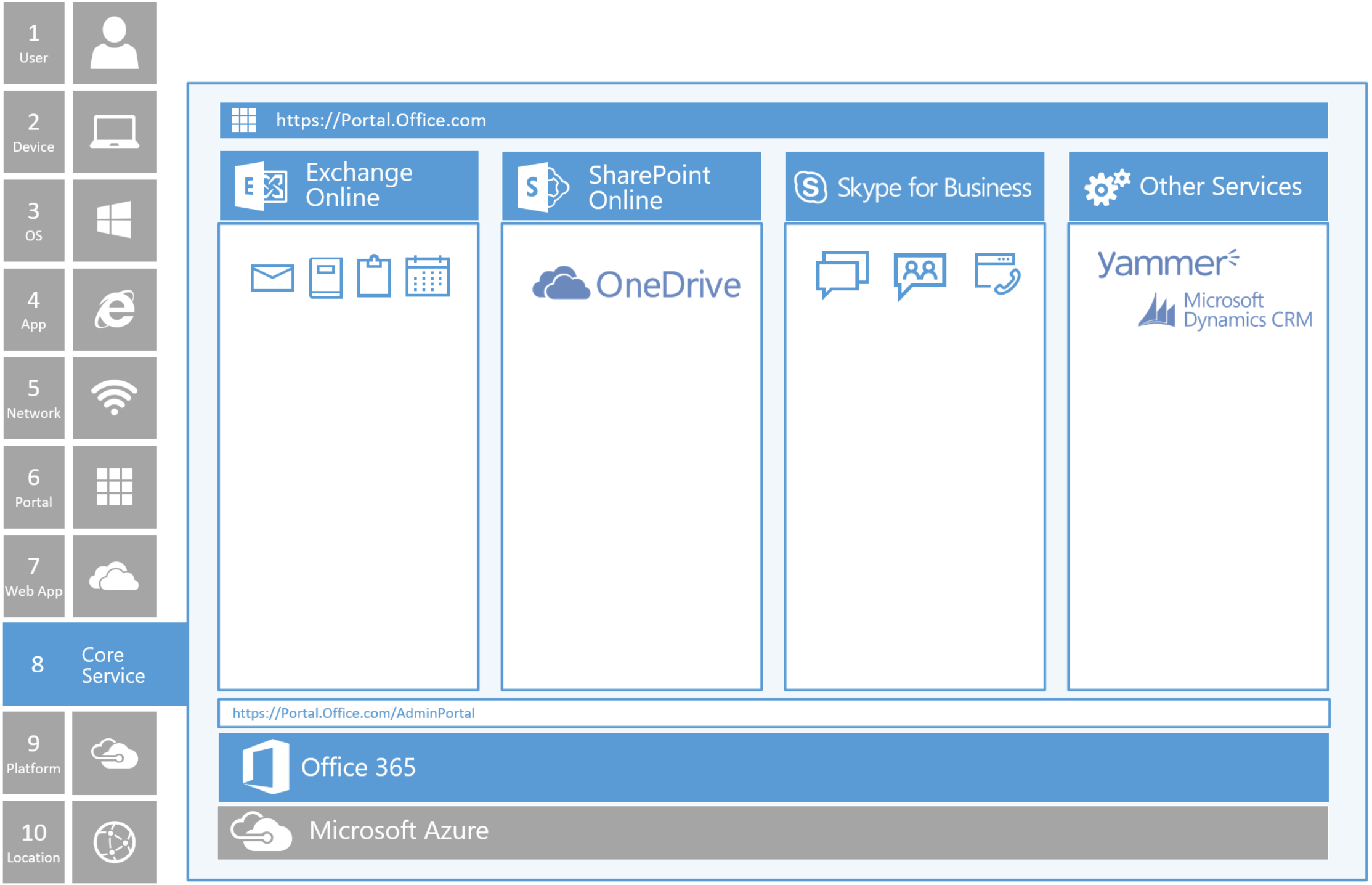

1
User
2
Device
3
OS
4
App
5
Network
6
Portal
7
Web Apps
8
Core Service
9
Platform
10
Location
Teams
Delve
Yammer
OneDrive for Business

Key Principle 2:

To encourage adoption and ease of use, a framework must be consistent but also customisable:

1. **Layout:** Be creative with content, there are specific elements that should remain the same, such as:
   - Naming conventions
   - Numbered layers
   - Navigation and transition

2. **Branding:** the creator of the solution design should be able to apply their own branding and colour schemes to enhance the appearance and be identifiable to the creator/owner


1
User
2
Device
3
OS
4
App
5
Network
6
Portal
7
Web App
8
Core
Service
9
Platform
10
Location
https://Portal.Office.com
Exchange
Online
SharePoint
Online
Skype for Business
Other Services
OneDrive
Yammer
Microsoft
Dynamics CRM
https://Portal.Office.com/AdminPortal
Office 365
Microsoft Azure

1 User

2 Device

3 OS

4 App

5 Network

6 Portal

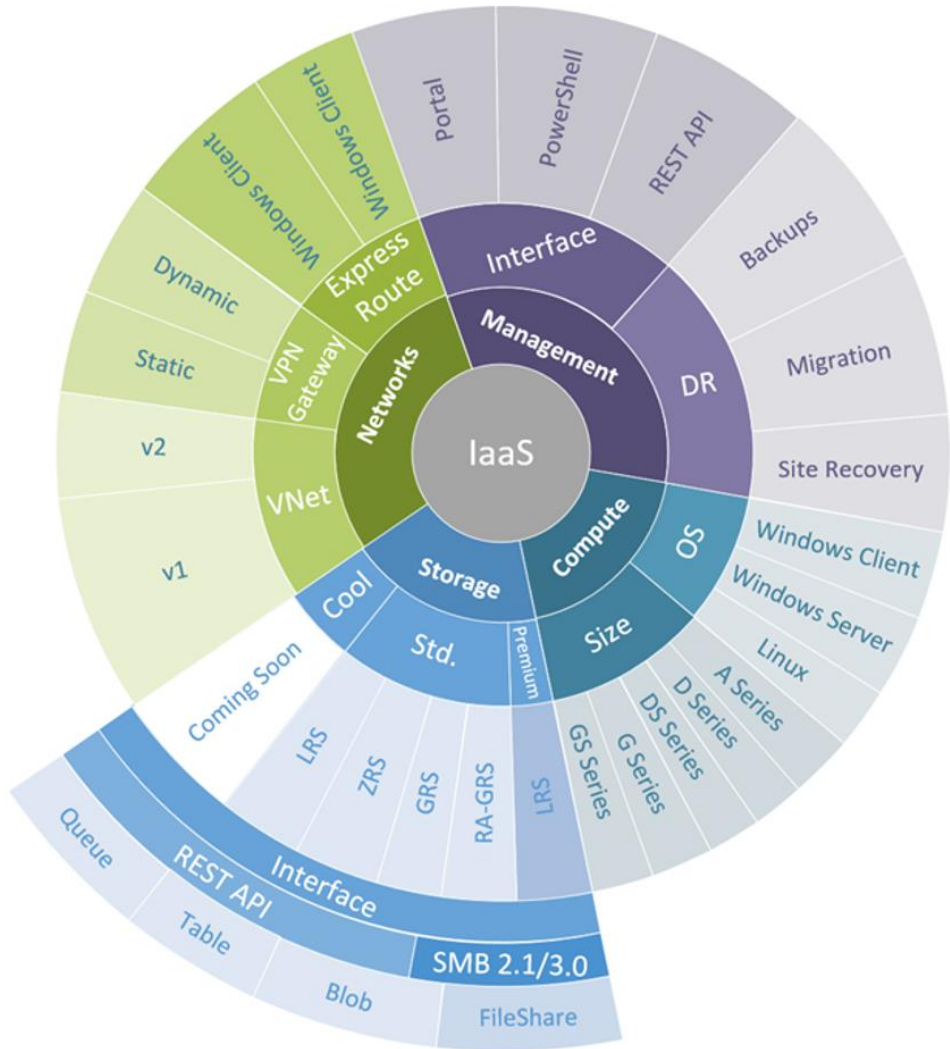
7 Web App

8 Core Service

9 Platform

10 Location

Microsoft Azure



1 User

2 Device

3 OS

4 App

5 Network

6 Portal

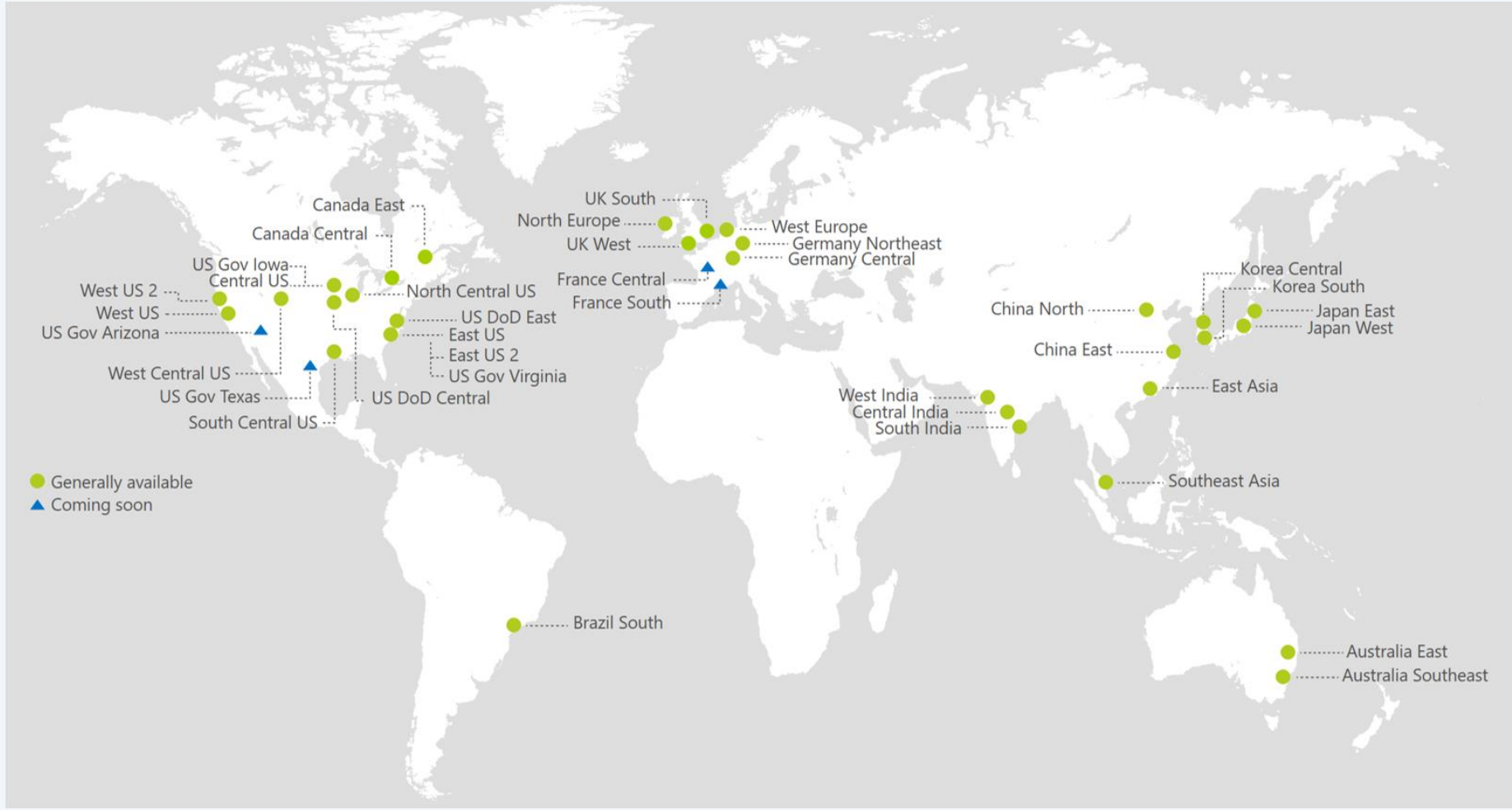
7 Web App

8 Core Service

9 Platform

10 Geographic Location

Australia



Solution Blades

Another view that would work well is to use the same method as the Azure Ibiza portal: Blades to open up and explain solution components in more detail, using navigation down the left hand side for the layers, and along the top for the various phases of deployment or approach to an issue:

- Example 1: **Information Security**: Identify, Protect, Detect, Respond, Recover. Use these headers to explore and explain the approach across all layers to ensure thorough analysis, design, and implementation.

The next examples focus on specific layers to show how the components interact to build a whole solution:

- Example 2: **Infrastructure as a Service (IaaS)**: show specific focus on a specific layer such as 9: Platform. Explaining components available like storage, compute, virtual networks, and Azure Active Directory (AAD)

- Example 3: **Office 365**: show the various platforms and products that are used to deliver vast array of productivity solutions

Information Security		Identify	Protect	Detect	Respond	Recover
1 User	 Internal					
2 Device	 Laptop					
3 OS	 Windows 10					
4 App	 IE 11					
5 Network	 Public WiFi					
6 Portal	 Office.com					
7 Web App	 OneDrive for Business					
8 Core Service	 SharePoint Online					
9 Platform	 Microsoft Azure					
10 Location	 Australia					

Information Security		Identify	Protect	Detect	Respond	Recover
1 User	 Administrator	The potential damage that could be caused by unauthorised use of privileged access, such as Domain Admin or Global Admin				
2 Device		If an administrator account is used on a compromised machine, their credentials could be used to carry out unauthorised changes				
3 OS		What are the potential risks associated with choice of operating system Is it managed, or unmanaged?				
4 App		Which applications and browsers should be used or blocked for administrators?				
5 Network		What are the risks of using various network connections when carrying out highly privileged systems administration tasks?				
6 Portal		What are the administrative portals that administrators are expected to use as part of their work? Can we monitor this to ensure admin accounts don't stray into unwanted territory?				
7 Web App		Are changes being made that will impact user interactions with the service?				
8 Core Service		Does the administrator have enough, or too many, privileges to the right systems?				
9 Platform		What is the underlying platform: Cloud, on-premises, hybrid?				
10 Location	 Australia	Are changes made locally or globally?				

Information Security		Identify	Protect	Detect	Respond	Recover
1 User	Administrator		All accounts should be dedicated for administrative purposes, access granted just in time (JIT), and enforce multi-factor authentication (MFA)			
2 Device			Privileged access is only carried out on dedicated machines. Follow the guidance for Privileged Access Workstations (PAW)			
3 OS			Only managed and compliance machines should be used by Administrator accounts, see PAW guidance above.			
4 App			Administrators must never use their account to browse the internet (select resources only) or check emails. Opening documents should only be from trusted sources that have been thoroughly scanned for malware			
5 Network			All resources must exist over secure channels and on trusted networks only. See PAW guidance above.			
6 Portal			Consider restricting internet access by URL to trusted sources only. Block attempts to any other resources			
7 Web App			Ensure all administrative changes are logged and carried out under change control. Audit administrator behaviours to look for anomalies.			
8 Core Service			Provide administrative access only when required and revoke immediately once the task is complete. Log and audit all changes to core services.			
9 Platform			Restrict potential impact by ensuring no single administrative account can make changes across all systems and solutions.			
10 Location	Australia		Enforce trusted IP's for administrative access across all systems			

Key Principle 3:

A common language is required to enable quick recognition and fair comparisons:

1. **Vendors:** there are numerous ways to present the same information – get their solution to match your understanding and environment specifics

2. **Experts:** Industry and solution experts should create and publish their work based on templates to make the work repeatable, standardised, and share the approach and learning with others

IaaS

1 User

2 Device

3 OS

4 App

5 Network

6 Portal

7 PaaS

8 IaaS

9 Platform

10 Location

https://portal.azure.com

Azure DNS

Traffic Manager

Azure Automation

Front End

Primary

Secondary

DR

Back End

Primary

Secondary

DR

Azure Portal

Web Services

Azure VMs

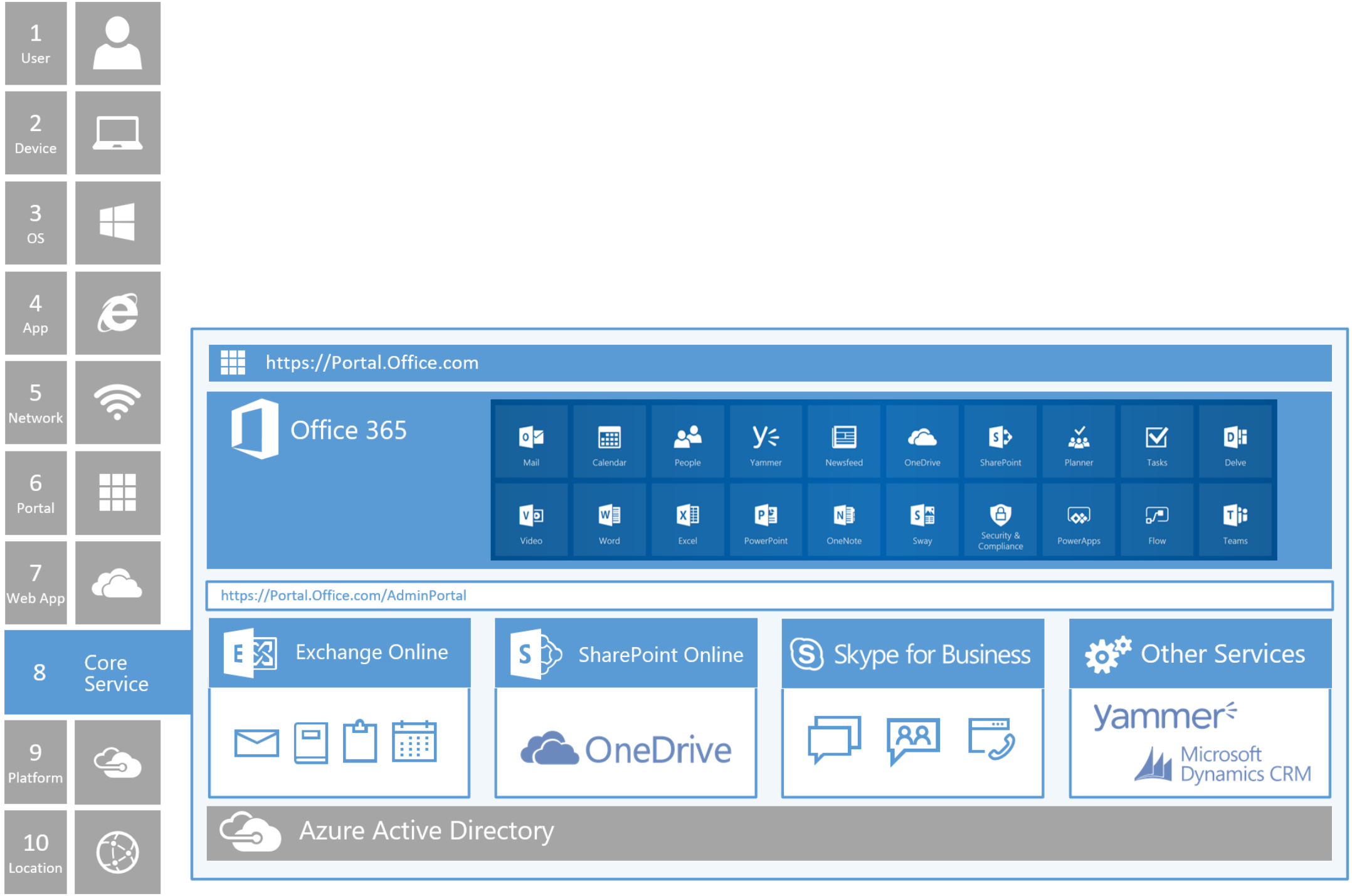
Microsoft Azure

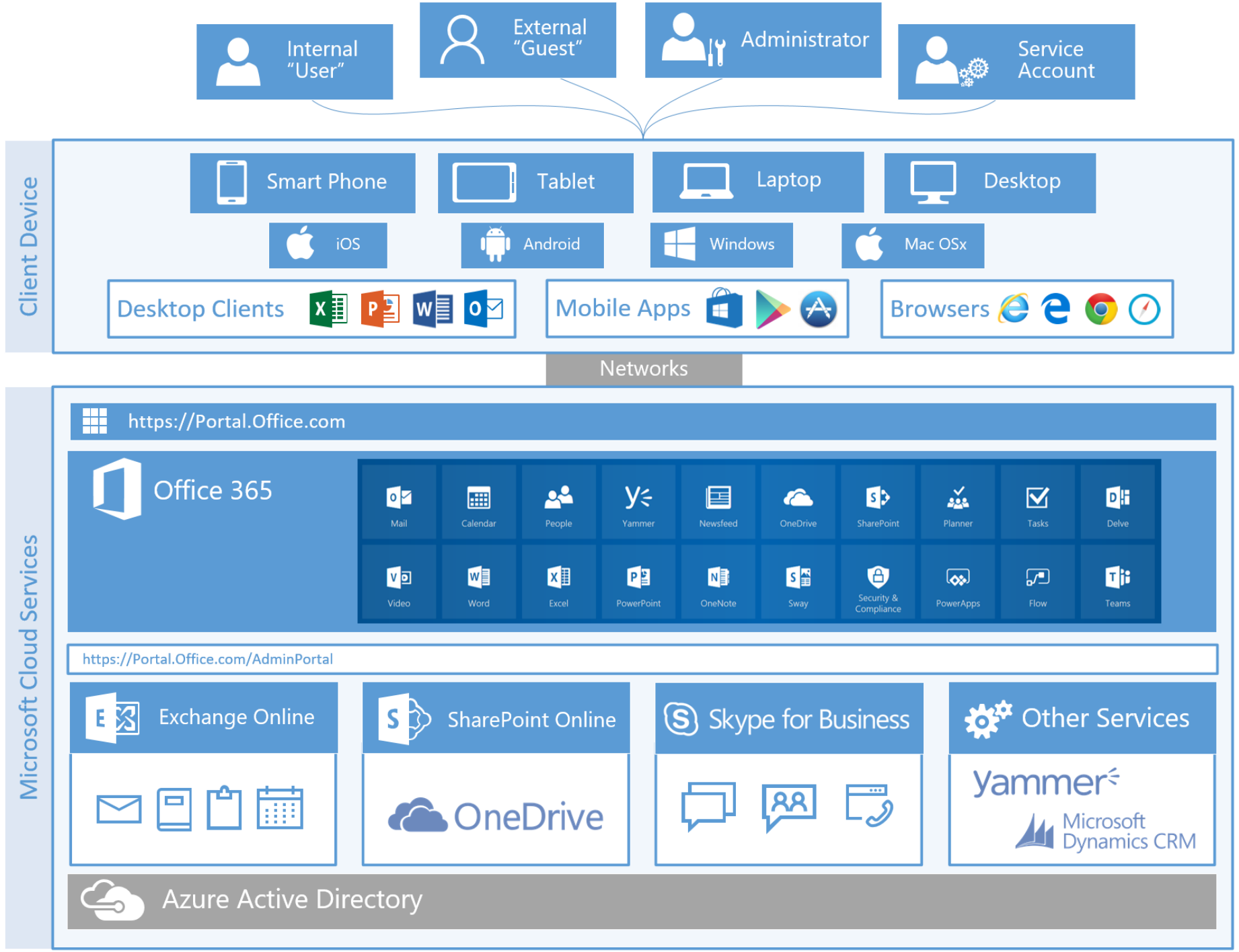
Azure Active Directory

Australia

Australia-SouthEast (Melbourne)

Australia-East (Sydney)


1 User
2 Device
3 OS
4 App
5 Network
6 Portal
7 Web App
8 Core Service
9 Platform
10 Location
https://Portal.Office.com
Office 365
Mail
Calendar
People
Yammer
Newsfeed
OneDrive
SharePoint
Planner
Tasks
Delve
Video
Word
Excel
PowerPoint
OneNote
Sway
Security & Compliance
PowerApps
Flow
Teams
https://Portal.Office.com/AdminPortal
Exchange Online
SharePoint Online
OneDrive
Skype for Business
Other Services
Yammer
Microsoft Dynamics CRM
Azure Active Directory


Internal "User"
External "Guest"
Administrator
Service Account
Client Device
Smart Phone
Tablet
Laptop
Desktop
iOS
Android
Windows
Mac OSx
Desktop Clients
Mobile Apps
Browsers
Networks
Microsoft Cloud Services
https://Portal.Office.com
Office 365
Mail
Calendar
People
Yammer
Newsfeed
OneDrive
SharePoint
Planner
Tasks
Delve
Video
Word
Excel
PowerPoint
OneNote
Sway
Security & Compliance
PowerApps
Flow
Teams
https://Portal.Office.com/AdminPortal
Exchange Online
SharePoint Online
OneDrive
Skype for Business
Other Services
yammer
Microsoft Dynamics CRM
Azure Active Directory

Questions & Answers

Richard Diver

www.rdiver365.com

@rdiver