



Webapps

The Secure Modern Interface for Remote Working

ACCESS FROM ANYWHERE

For many people, years ago there was a clear distinction between work and home life. Corporate offices were the locations for work to occur and little thought was given to work when outside those offices. Contrast that with today's mobile workforces utilising connected devices in the field or air, as well as the flexible working from home arrangements now common for many organisations.

Virtual private networks, or VPN's, allow for an encrypted connection between a remote device and a corporate network across a public connection such as the internet. They have been the traditional way of granting access to a remote user but have suffered from performance and security issues.

Modern webapps provide a more direct connection that is also encrypted which are generally regarded as a better solution.

Types of Applications

Historically, one of the first types of applications, or apps, was the desktop app. This was "installed" on a computer and therefore required administrative access to the device. In addition, if another computer was used, it needed to be installed again.

As apps became more complicated, some centralised storage or data and processing was required, and client/server apps were born. This started before the internet was generally available.

The general availability of the internet provided the first opportunity for web apps. These applications were unique, in that they ran inside a web browser, negating the need for the app to be installed on the device.

However, limitations in browsers meant that user interfaces within these web apps were often clunky and limited in what features were available. So even when webapps were available, they were often supported by desktop apps for the power users.

We still see this today with Microsoft Word being available in a browser, but most users prefer to use the desktop version of the application. Of course, these webapps continue to improve and approach the same functionality of the desktop versions of the same apps.

The second iteration of the internet, known as Web 2.0, provided for "responsive" apps which resized and adjusted themselves dynamically to suit the screen size and resolution of the device being used.

Today's modern webapps, thanks to evolutions in the features of modern browsers, are virtually indistinguishable from the installed desktop apps from a user experience perspective. Yet so many apps today are still offered only as desktop apps.

Benefits of Webapps

Modern webapps provide some significant advantages over desktop and client/server apps of the past.



Access from remote devices – webapps utilise encrypted connections through the internet to enable remote access in exactly the same way as using the application within a corporate network. There is fundamentally no difference to how a device in a corporate office accesses the system when compared with working from home, a coffee shop, airport lounge or any other internet-connected location. This means that no special VPN hardware or software is required to be implemented, and no software installation is required on remote devices.

Access from non-Windows Computers – Because only a modern browser is required to be able to run a webapp, Apple Mac computers, and mobile devices such as tablets and smartphones with non-Intel processors can also run these applications. In the past, different types of devices required separate specially designed apps to be able to be used.

Access from any browser – any modern, up-to-date internet browser is generally supported by modern webapps, including Microsoft Edge, Internet Explorer, Google Chrome, Apple Safari and Mozilla Firefox, provided that they are reasonably up-to-date.

Of course, ensuring all browsers are running the very latest version is an incredibly important thing to do from a cybersecurity perspective. Browsers are often targeted by cybercriminals searching for vulnerabilities in the software which are patched regularly by developers. Out-of-date browsers represent a significant security risk for all organisations.

Limiting Access from Anywhere

Although the technology now allows for access from anywhere, sometimes limiting this access is desired from a cybersecurity point-of-view.

Security systems have responded with the available of specific technologies to address this need. This is particularly important as in the old days of corporate office networks and client/server apps, firewalls provided a security perimeter around the computer networks used within offices.

The modern security perimeter now extends to connected devices outside the network, accessing cloud systems directly through the internet.

It isn't possible to put a firewall around the whole internet, so other solutions are required.

These address the competing goals of empowering users to be productive whenever and wherever, and protecting the organisation's data assets.

Conditional Access is a solution that grants access to a system or app when there is a valid username and password, *plus* some additional conditions. These additional conditions can include signals about the user and location, the device being used, the application being accessed and real-time risk data.

Examples of how conditional access policies can be deployed include:

- Limiting access to a specific application to certain IP addresses
- Enforcing a requirement for a device to have up-to-date anti-virus software
- Identification of risk-based sign-in behaviour such as impossible travel (a user logging in from Europe and then from Australia an hour later)

Remote Access with Business Central

ERP and accounting systems have evolved to provide easy access to information for team members outside the finance team.

Traditionally, any data within the finance system that was required by another team, would generate a request for information. Finance team members would then access the ERP system, generate a report and send the information to the person requesting it.

Modern finance systems such as Microsoft Dynamics Business Central provide for relatively inexpensive "team member" licences for all users to be able to access information, transactions and reports from the finance system directly, without having to interrupt Finance team members and wait for responses.

Of course, Business Central provides a strong security and permissions feature to be able to restrict what data is available to which users and groups of users. This security model allows for more than just access to a particular report or module within the ERP system. It can also provide access to certain data within that module, such as "only customers in my region", or "only specific general ledger accounts".

Business Central uses a webapp as its main user interface for all users. It isn't an add-on, limited functionality, app that supplements a desktop app. This also provides for an additional benefit of users being able to customise their own user interface.

If you prefer to enter transactions with a particular order for the information entered, or you prefer a more streamlined, simple set of fields to process a transaction, then you can set up the data entry screens to suit yourself.

As a webapp, these modifications to data entry screens will be available from any device, without having to copy or synchronise these changes across devices.

Business Central is built for remote access by design. It is built into the very fabric of the system, not tacked on as an afterthought.

Any device, anywhere, anytime access is available, supported by a strong security model with configurable audit trails to ensure your data is safe and accessible for all.

