EVERYTHING CONNECTED, EVERYTHING PROTECTED

COLIN WILLIAMS
CTO, SECURITY

What is Secure Connected Enterprise?

It's hard to imagine the world we live in today without technology. Of course, technology will never supplant the human existence, but it plays a very valuable role, augmenting and enhancing everything we do at work, at play and in broader society. Technology is such a key part of our lives that it is "invisible" whilst highly "visible".

We may view IT systems or personal computers as technology but do we really think the same thing about televisions, smart phones, home assistants and many other technology based offerings that are so embedded in our day-to-day lives based on the value they deliver that how they function as technical systems is no longer important.

But there is a core element of many of the modern systems we use that has transformed the value we realise from IT enabled systems and that is Secure Network Connectivity. Standalone, non-connected systems perform functions in isolation, but networked or secure connected systems can communicate and share information with users and other systems offering near limitless potential.

The term **Secure Connected Enterprise** describes this new landscape of technology enablement with a user or business expectation of secure access to a potentially endless mass of IT systems that are always on, resistant to failure, accessible by users and other IT systems regardless of location to deliver value and experiences. The secure connected enterprise is not a product, it positions the concept and the benefits realised by users and business enabled by secure networking to deliver the outcomes of a secure connected enterprise. Secure connectivity facilitates user and system access to other systems and is a principle enabler of applications, processes and services working in harmony with networks binding every digital action or transaction together by ensuring data packets flow effectively and reliably.

Cyber Defence & Security

The secure connected enterprise is underpinned by security by design, built in and always on. The network 'sees all' - therefore Cyber Defence and Security is positioned as the gatekeeper of every user, system or IOT "thing" action performed via applications or data that flow across the available and accessible network.

Inherent security is a mandatory element of the secure connected enterprise to reduce the negative impact of 'bolt-on' security which can open the door to cyber-attacks or compromises where security coverage gaps are apparent. Ransomware is an example of a type of cyber threat so damaging that the destruction caused creates headlines on mainstream news challenges. By embracing a 'shift left' approach to security and imbedding controls at the earliest point of application or system creation, a proactive and preventative posture can be adopted. When security is designed in and becomes 'the system' it simplifies the user experience and delivers consistent, secure application and business outcomes due to acting in an invisible, always on operational mode.

Dynamic Networking & Connectivity

The Secure Connected Enterprise is more than IT and networking platforms. It is underpinned by Dynamic Networking & Connectivity and includes the extensive network of networks that facilitate access using mobile (4G & 5G), wireless & Wi-Fi, local & wide area solutions to the connected global landscape of systems, services and applications. A positive experience is everything, increasing the importance of the type of connected devices used to access systems and resources, which may include user centric devices, smart phones, tablets, laptops and nonhuman systems that deliver value without or via minimal human intervention.

Digital Identity & Access

The increasingly popular culture of mobility and "work" everywhere has highlighted the importance of Digital Identity & Access as a critical enabler of the secure connected enterprise ensuring the dynamic network edge resides securely wherever users or 'connected things' access systems and resources. Work is an activity, therefore should be possible wherever relevant systems can be accessed. The ability to offer high speed connectivity via always available mobile networks across the globe with services and data processed on the edge devices, whether a connected car, intelligent building or other environments suggests there may be no limits to the scale of the future value of the secure connected enterprise.

Secure Connected Enterprise – What's next?

The Secure Connected Enterprise is here to stay but even with evidence so compelling of the value delivered it is still not be maximised by all. Many business processes and services remain anchored to a world of static access from fixed locations that delivers an IT enabled experience that is dictated to but the not requested by the user.

As the blur between office and home work continues the next wave of the secure connected enterprise will see the workplace become smart, with an increased level of "facilities intelligence" available by the use of sensors and IOT devices to enable automation and new functionality to buildings and workspaces.

User experience is key, and the use of smart office or city technologies connected securely via reliable networks to transform workforce or citizen engagement can only be beneficial to all.

Now is the time to challenge if the secure connected enterprise is being truly maximised within the enterprise. By leveraging the power and potential of always on, always available networking, the business value of the secure connected enterprise will enable new ways of engagement and beneficial user experiences that we have never dreamed of.