vivitek
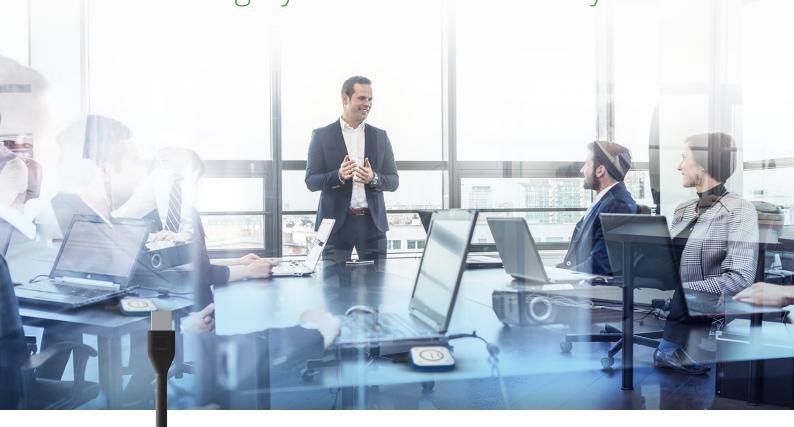# **Novo**Connect

Wireless Collaboration

Enabling meeting connectivity and collaboration while maintaining full data integrity and network security.

As an IT manager, security is at the top of your agenda, especially if your company is in a heavily regulated industry like banking, legal, insurance, education, or government agencies like the police, healthcare, customs and social services. Ensuring your company's security remains robust at all times, is a challenge made even tougher in the era of Bring Your Own Device - where collaboration is encouraged - and guests and visitors are invited to join your network, in order to share content from their devices in meetings or in training sessions.

A brand of **DELTA**

Of course, no IT manager wants viruses or trojans to be spread intentionally or accidentally by external visitors. Nor do you want to suffer data losses either, especially following the recent GDPR mandate which has made companies responsible for the safety of the data they collect. But forbidding devices from joining the network or locking USB slots isn't helping to facilitate BYOD and collaboration in the meeting room. Even in security sensitive organizations, wireless collaboration and team sharing need to be facilitated. The answer to this challenge comes from the NovoConnect wireless collaboration solution in combination with the Vivitek LauncherOne!

With the LauncherOne, any laptop can connect wirelessly directly to the NovoConnect solution, you no longer have to worry about network-based devices, or unlocking the USB slots. Combined with a NovoPro, NovoEnterprise or NovoTouch, the LauncherOne does not require any network integration as it uses the NovoConnect solution wireless ad hoc network.

A worry-free collaboration solution, LauncherOne comprehensively addresses your security concerns:

LauncherOne is Data Loss Prevention compliant
Compatible with Data Loss Prevention (DLP) compliance policies, LauncherOne has been designed to keep data secure. As it is a USB storage free device, it prevents unauthorized data transfer, keeping your company's information protected. Furthermore, your data benefits from robust AES-256 encryption, to ensure safe wireless communication at all times.

LauncherOne - designed for locked USB slots
LauncherOne is an effortless and secure way to collaborate and share information. With no USB storage functionality, it is not detected as a storage device meaning that there is no need to white-list it or to change the security settings of your company.

LauncherOne has zero impact on existing network traffic
Network performance must never be compromised. Thanks to the dedicated and direct wireless connection between the LauncherOne and the NovoConnect main unit, existing network traffic is not affected by it, meaning critical business applications continue to run as they should.

LauncherOne offers hassle-free deployment and updates
Your main deployment server can push the LauncherOne application file easily to all client devices. Additionally, the LauncherOne application file doesn't need very high privileges to install, as it falls into the lower category of privileges required to deploy it. Therefore, large-scale deployments are very easy to do, as is rolling out any updates – an important consideration for IT managers under pressure to resolve more important day-to-day technology issues.

Model number	WQL-340EUV
Connector	USB-A
Cross platform operation system support - Windows 7 above & mac 10.7 above	●
Built-in WiFi 802.11 b/g/n	●
Direct wireless mirroring to the main unit	●
Usage without administrator privilege	●
Wireless interactivity and multitouch support	●
Compatible with locked USB slots	●
Data security with AES-256 encryption	●
Zero network traffic impact	●
Warranty 2 years	●
4 screens (sharing at once) buttons feature	●
LauncherBase optional accessory	●

Compatible main unit		
	NovoCast	NA
	NovoPro	●
	NovoEnterprise	●
	NovoTouch LK6530i	●
	NovoTouch LK7530i	●
	NovoTouch LK8630i	●
	NovoTouch LK9810i*	●

LK9810i* is bundled with NE3000

A brand of ⟁ΠELTΛ