Manage and protect whiteboards and display panels is not an issue if you are not dependent to the form-factor.

CASE STUDY: TOUCHVIEW INTERACTIVE

About the customer

TouchView Interactive is an US whiteboards and display panels producers both for educational and business markets. Touchview Interactive mission is to provide its customers the latest in innovative interactive technology to accommodate the demands of the modern workplace of promoting and enhancing seamless collaboration. Whereas in the educational market, their leading-edge interactive displays transform classrooms, engage students, and empower learning institutions to enhance learning and teaching.

Situation

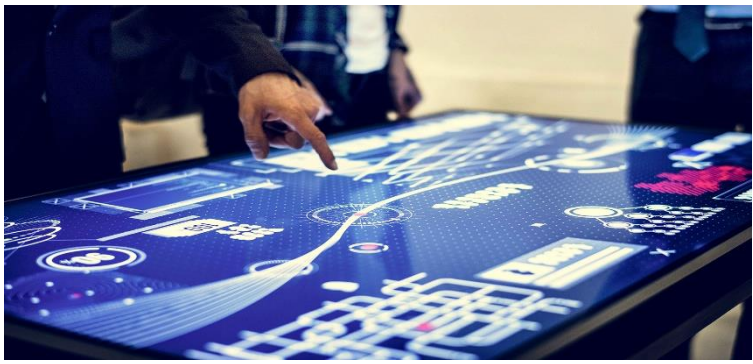
Whiteboards and display panels are static unmanaged systems by their nature, which are barely updated not only from an application standpoint but from the OS too. Furthermore, OS installed are not the latest versions available nor able to be updated to latter versions. On the other side such devices are subject to be used by a variety of users that could result in a potential threat because of misuse or unknown sw installation or external devices connection. At last, they are endpoints connected to internet and potentially exposed to the external threats.

The project

Touchview planned to increase their offering to the market by increasing services. Their will was to promote whiteboards and display panels which embed management and security tools provided as a service. All this in a view of an increase of the customer satisfaction but also of the customer loyalty to their network of partners/resellers.

The outcomes

A deep evaluation of Chimpa have been operated by Touchview to stress test the capabilities of the tool to protect and manage a great set of devices under different Android OS, some legacy too. The overall activities confirmed once more the non form-factor dependency of Chimpa, gaining the full control of different devices with different Android OS versions without any issue. At the same time Chimpa reached the expectations as far as the securitization of such devices. The final step has been an OEM agreement to let the Chimpa platform being promoted with their own brand name. The first PO was a bulk buy of 5000 licenses and a next regular recurring monthly purchase.



Chimpa is a Unified Endpoint Management (UEM) and Mobile Theart Defense (MTD) All-in-one platform designed to manage, monitor, and secure Android, iOS, and Windows devices. Chimpa's easy-to-use cloud-based console can provide to SME, Enterprise, and Large corporation the peace of mind of a full control of their company devices as well as all BYOD devices, providing a high-quality security protection through three lines of defense: User Restrictions (Attack surface reduction), Active Defence (AV, Anti phishing, Hash file, Firewall) and Proactive Defence (Threat Intelligence). Chimpa's software has been designed by a high skilled team of developers with security in mind.

android enterprise
EMM provider

Consultants
Network

Validated by
SAMSUNG Knox

Microsoft
Partner

Chimpa
With One Another