

 Content archived on 2024-05-28



Multiplatform Usable Endpoint Security

Results in Brief

Working seamlessly and securely on multiple devices

EU-funded researchers have developed and tested a new corporate cyber security system – designed to fit with current trends of working on multiple devices – and identified a simple way of making corporate cyber space safer and more secure.



DIGITAL ECONOMY



© Shutterstock

Mobility and modern living mean that work begun on the office computer is often completed on the laptop on the train home, or sent via smartphone to the client the next morning. While convenient and efficient, this practice can in fact expose corporations to cyber security threats.


‘Company security protocols and practices have often failed to keep up with new technologies and how these are being used, both in the office and at home,’ explains project coordinator Sergio Zamarripa from S2 Grupo in Spain. ‘A key issue is the fact that the widespread adoption of mobile and portable devices has blurred the line between work and private life.’

Trends, such as the spread of social networks and policies like Bring Your Own Device (BYOD), pose new risks. ‘Imagine an employee with a BYOD profile using the same device at home while some hours ago he was downloading a confidential

document at work,' says Zamarripa. 'If the user is not aware that some actions could jeopardise confidentiality, a malicious attacker could obtain sensitive information.'

In addition, large organisations are increasingly adopting complex ICT mechanisms, which require users to complete a series of complicated tasks. This increases the likelihood of human error.

Adapted for the modern workplace

The [MUSES](#)  project has addressed this weak link in the security chain through the development of a device independent, user-centric corporate security system, which is able to cope with the concept of seamless working on multiple devices.

The system interacts with users by sending them real-time notifications containing information and recommendations that relate to current user actions. Some notifications might simply offer suggestions on how to complete an action securely, while others will actively block an unsafe action and provide guidance to ensure that the action is completed safely (e.g. by connecting to a secure wifi).

'Corporate security policies should govern the way in which employees, devices and IT systems interact,' explains Zamarripa. 'What we wanted to do was to raise employee awareness of risky situations, and assist them in dealing with those risks. This will allow employees to carry out their work as usual, and help corporations to actively enforce security policies without introducing any new hurdles.'

The MUSES consortium ran a number of field trials and found that the introduction of MUSES' usable corporate security led to a decrease in incidents due to improved user behaviour. 'The trials revealed a gradual decrease in the number of incidents over time, as users were able to learn how they should perform their tasks in a secure way, through automatic recommendations provided by the MUSES software,' explains Zamarripa.

Employer and employee benefits

The project has shown that engaging with users directly about cyber security can increase competitiveness and reduce direct and indirect costs associated with security incidents, such as down time and recovery costs, or indeed the cost of damage to reputation. 'We have identified SMEs as the most likely target, since they usually do not have a security department,' says Zamarripa. 'The MUSES concept provides a cost-effective way of ensuring their assets, and a next step for the consortium is to look into ways of commercialising MUSES.'

The successful trials also resulted in increased awareness of the importance of trustworthy ICT among employees, and a better understanding of the legal and

societal consequences of using both corporate and personal devices. Zamarripa also believes that the success of the project could open the door to future recommendations about standards, especially those related to BYOD.

Keywords

MUSES, cyber security, security protocols, mobile devices, smartphone, employees, corporations, competitiveness

Project Information



MUSES

Grant agreement ID: 318508

[Project website](#)

Project closed

Start date

1 October 2012

End date

30 September 2015

Funded under

Specific Programme "Cooperation": Information and communication technologies

Total cost

€ 4 673 614,00

EU contribution

€ 3 590 339,00

Coordinated by

S2 GRUPO SOLUCIONES DE SEGURIDAD SL



Spain

This project is featured in...



17 December 2018



Last update: 21 October 2016

Permalink: <https://cordis.europa.eu/article/id/188666-working-seamlessly-and-securely-on-multiple-devices>

European Union, 2025

