



# Qubes OS & Xen Project

Qubes OS is a security-focused operating system based on Xen.

The goal of Qubes OS is to create a reasonably secure environment that is also practical and usable, capable of playing the role of a daily driver rather than a highly situational solution - and Xen is a major reason why we can confidently say that Qubes OS succeeds. The backbone of the system is the compartmentalization of various user and system functions and activities into separate domains, that is, Xen virtual machines; Qubes OS provides a user interface that turns what would otherwise be a usability nightmare into a friendly, modern operating system complete with support for template virtual machines and centralized VM updating. Key Xen features that we are using to make Qubes OS more secure are:

- **Stub domains** allow us to keep I/O emulation (QEMU) outside of the TCB (Trusted Computing Base), providing for improved separation and resilience; Qubes OS' implementation of Xen stub domains allows us to completely remove qemu from dom0.
- **Driver domains** allow us to keep drivers such as the network driver or USB drivers in a separate virtual machine, which in turn can provide network or device access to other VMs as required. This provides a level of security and fine-grained control difficult to achieve by any other means, isolates the TCB from potentially buggy or malicious hardware and hardware drivers, and allows the user to have complete control over access levels each of their VMs might have.
- **Xen's security disclosure process** is second to none – Xen security advisories, with their detailed descriptions of the impact and technical details of security issues, allow us to maintain security even when problems are discovered.
- As a **Type 1 hypervisor**, Xen is more resilient than Type 2 virtualisation solutions - any attacker would have to subvert not only the virtual machine but also Xen itself, which is vastly more difficult.
- Last, but certainly not least, the **Xen community** is supportive, friendly and security-conscious, and the cooperation with it has been and will continue to be a cornerstone of Qubes OS.

*“Xen and Qubes OS work together to create a unique security-focused solution - by leveraging the strengths of Xen and adding extensive usability features and hardening, we can provide users with a secure computing experience on personal computers without compromising their everyday needs.”*

- Marek Marczykowski-Górecki, CTO of Invisible Things Lab & Project Leader of Qubes OS