

LynxSecure

Secure client virtualization based on military-grade technology



In today's modern connected world, the security of either PC-like or embedded client devices is vital. These devices often hold sensitive company and personal information, and yet are connected to the open internet that is home to cyber-criminals and malicious attacks.

Securing the internet connection or adding security to a browser are traditional methods of protection, but a more secure approach is to isolate sensitive data and applications away from the point of potential attack.

The LynxSecure separation kernel and hypervisor from LynuxWorks™ gives a secure software platform that virtualizes and isolates operating systems, applications, devices and data from one another while running on the same hardware platform.

LynxSecure was designed from the ground up to operate in highly secure

defense environments where data and applications with different security levels need to co-reside on a single device without contamination.

LynxSecure's military-grade technology is now available for other markets such as medical, consumer, financial, industrial and communications. LynxSecure supports commonly available processor architectures, operating systems and applications, and offers the ultimate in protection, without interfering with the desired functionality of the device.

Virtualization can only provide real system security if the hypervisor has been built with security in mind (a hypervisor or its underlying operating system can be compromised).

The virtualization in LynxSecure is based on a type-1 (bare-metal) hypervisor that runs directly on the hardware, providing vastly improved performance over the more traditional type-2 (hosted) hypervisors that run on top of another operating system. LynxSecure also has the benefit of a built-in separation kernel that offers military-proven security for the OSes and applications running on it.

The LynxSecure separation kernel has been designed to securely isolate devices, memory and resources and contain them in their own partitions. The configuration of LynxSecure also allows for the definition of information flow between the different partitions, adding flexibility to the usage model while maintaining secure isolation where required. The hypervisor part of LynxSecure then allows different operating systems and applications to run in these secure partitions, and offers virtualized versions of the physical devices where appropriate.



Virtualization of guest operating systems

The built-in embedded hypervisor and virtualization technology allow guest operating systems (and their applications) to run on top of LynxSecure, in effect allowing multiple dissimilar operating systems to share a single physical hardware platform.

Virtualization technology allows for significant cost savings through hardware consolidation, while retaining the ability to leverage the ecosystem of applications that belong to different operating-system domains into a single system.

LynxSecure uses its hypervisor to create a virtualization layer that maps physical system resources to each guest operating system. Each guest operating system is assigned certain dedicated resources, such as memory, CPU time and I/O peripherals, which can be securely shared with other guest OSes if required and even includes a secure communications link between the different partitions.

Two types of virtualization are provided by LynxSecure. Para-virtualization, also known as "co-operative virtualization," provides superior performance for the guest operating systems—such as Linux® or LynxOS® family of real-time operating systems. Full virtualization allows unmodified operating systems

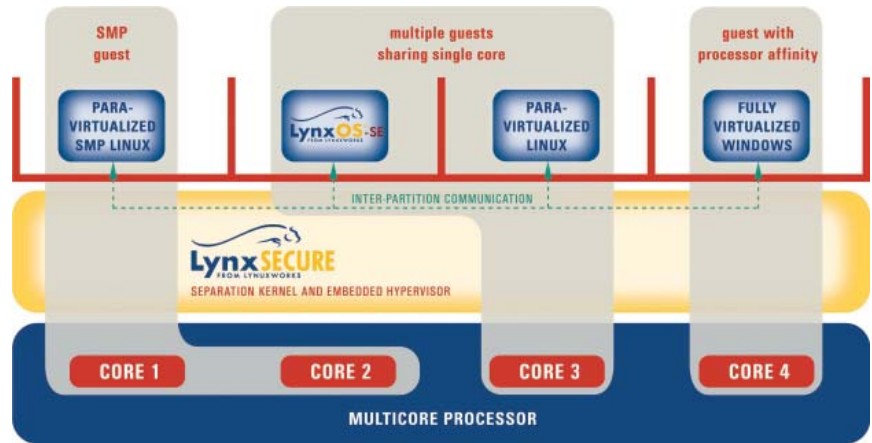
Advanced secure client virtualization

- Military-grade secure platform
 - More secure than traditional hypervisors
- Small footprint, non-intrusive, efficient technology
- Supports commercial multicore processors
- Virtualizes commercial OSes
 - Windows, Linux, Solaris, Chromium
- Protects devices against malicious attacks

like Windows® or Solaris™ to run next to para-virtualized ones. Both types of virtualization are supported concurrently by LynxSecure, and by utilizing hardware virtualization technologies, even fully virtualized guest OSes can run at near-native performance.

100% application binary-compatibility with the non-virtualized instance of the operating system is preserved. This allows legacy applications and operating systems to be reused on the new and secure hardware, offering cost-effective migration and reuse of existing systems. LynxSecure isolates each virtual instance by providing hardware protection to every partition with its own virtual addressing space.

In addition, it guarantees resource availability, such as memory and processor-execution resources, to each partition, so that no software can fully consume the scheduled memory or time resources of other partitions. LynxSecure supports simultaneous use of system interfaces, including multiple instances of



Advanced multicore support in LynxSecure

the same or different operating systems in different partitions.

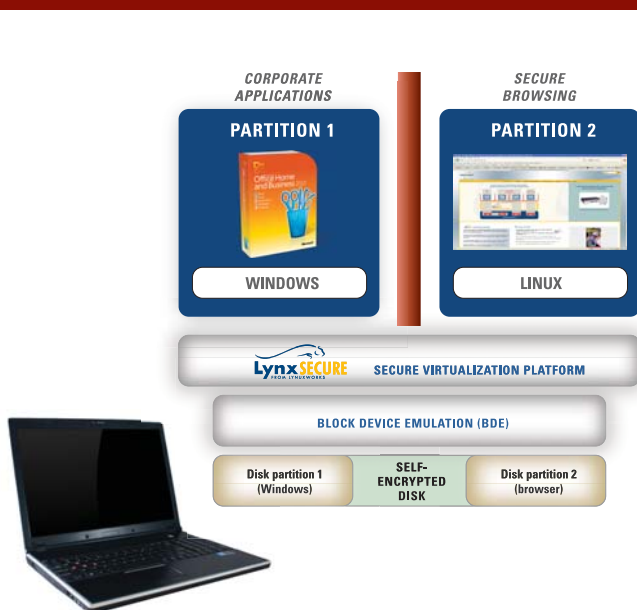
Superlative virtualization performance

A question that is often asked of virtualization solutions is around the performance of applications and operating systems when running virtualized versus the performance when executing directly on the hardware.

LynxSecure has answered this question by using a combination of hardware and software features designed to bring the virtualized performance extremely close to native.

The small and efficient separation kernel was designed to run in real-time environments, and has a fixed-cyclic scheduler that manages CPU time to prevent

Secure use case 1 - Protection of data at-rest and in-motion on laptops



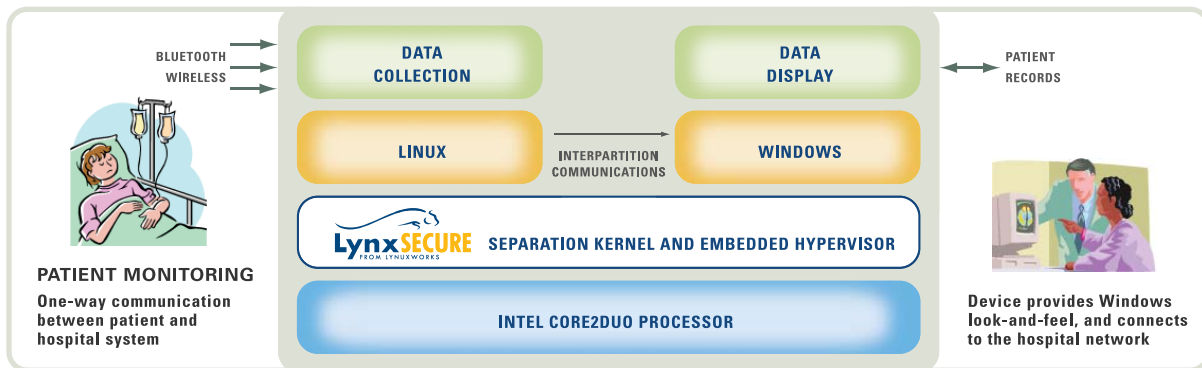
Equipping a standard laptop with LynxSecure and self-encrypting hard drive (SED) technology from Wave systems keeps corporate and personal data safe from physical theft or cyber attacks. If the laptop is stolen, the data on the self-encrypting hard drive is not accessible to the thief, providing data-at-rest security.

While the laptop is in use, LynxSecure protects the corporate data from attack from the open internet, offering data-in-motion security. This combination offers the most protection without compromising the functionality of the laptop.

Secure use case 2 – Medical device combines real-time and desktop functionality

A recent proof-of-concept put together by Intel, LynuxWorks and Portwell shows how the use of secure virtualization on a standard hardware platform can dramatically increase the functionality of a medical device without compromising functionality or security.

The device combines a real-time environment collecting live data wirelessly from a patient using Bluetooth technology, and then having a Windows-based environment on the same hardware platform that displays the information collected using a user interface familiar to the care-giver, and then communicates to the hospital network without compromising the security of the device.



starvation in any partition, providing a truly deterministic environment. LynxSecure also allows dynamic scheduling policies for maximum flexibility when developing secure applications using OS virtualization.

LynxSecure also takes full advantage of the hardware features of modern processors, such as the VPro technology from Intel® found in everything from PCs and laptops to embedded systems and mobile devices. Multicore processors can significantly boost the performance of virtualized systems, and LynxSecure provides very advanced schemes for using these devices, including a new dynamic scheduling policy for changing the amount of CPU time allocated

to a guest operating system while the system is running.

Only one instance of LynxSecure is required for building a system on a multicore device. Subsequently, different views of the processor can be shown to the virtualized operating systems running on top.

Multiple guest operating systems can share a single core, which is useful if the operating systems or the applications running on them do not require 100% of the core's processing power.

Alternatively, a guest operating system can be given a dedicated core, for near-native performance of fully virtualized

operating systems that do not know that they are running in a shared or virtualized system and assume that they have 100% of processors bandwidth.

For more computing performance than a single core can offer, LynxSecure also allows guest operating systems with symmetric multi-processing (SMP) functionality to be executed across multiple cores.

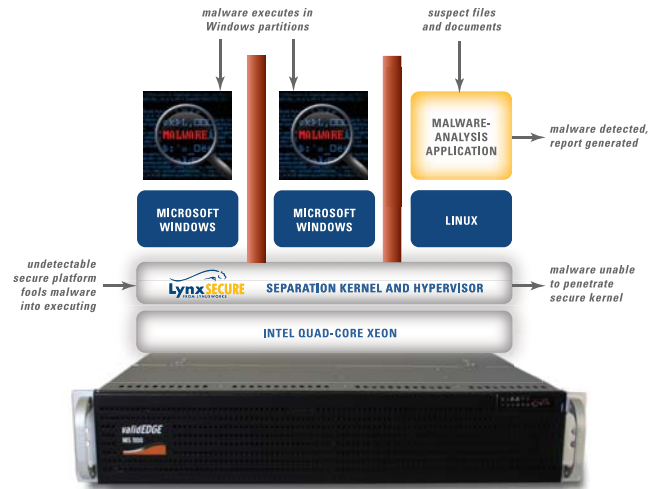
The wide use of virtualization in servers and data centers has resulted in increased availability of hardware for virtualized systems. LynxSecure takes

Secure use case 3 – ValidEdge MIS1100 appliance – using secure virtualization to safely detonate and analyze malicious code

The MIS1100 appliance from ValidEdge uses LynxSecure to provide a secure platform to execute potentially malicious code in a contained Windows environment.

The code is observed as it executes and a report is generated about its behavior.

ValidEdge takes advantage of LynxSecure's ability to run multiple operating systems concurrently on a multicore processor. Six separate malware samples can execute simultaneously, which speeds detection and provides solutions and warnings before an attack has become widespread.



advantage of the hardware virtualization features built into modern processors.

Processor extensions offering Virtualization Technology (VT) like vt-x and vt-d, found in most new Intel processors, increase the performance and security of both para-virtualized and fully virtualized systems.

By using Extended Page Table (EPT) and Page Attribute Table (PAT) in Intel's latest processors, the performance of fully virtualized systems comes very close to both native and para-virtualized figures.

Benchmarks run by both independent organizations and LynuxWorks engineers have shown that an overhead of between 2% and 5% over a native OS is typical. This allows for the migration of legacy OSES and applications to a secure virtualized environment with virtually no performance impact, and

often as new hardware is also involved, the performance of the legacy system can be improved.

Functionality and security

Adding extra security to a system can sometimes lead to an unwanted loss of functionality. With LynxSecure, the security is built into the underlying platform, so the virtualized guest operating systems and applications function exactly as they do when running natively.

For many applications, this ability to add security without compromising the functionality or performance of the legacy system is a key attribute helping to make the move to a virtualized solution.

For example, developers of medical devices can now add network connectivity without fear of compromising patient information, and IT organizations can

add security to their corporate PCs and laptops without removing users' ability to email, surf the web, or chat on instant-message and social-media applications (see secure use cases 1 and 2).

An entire family of secure real-time operating systems

LynxSecure is the latest addition to the LynxOS family of secure real-time operating systems.

Today—after 22 years—our LynxOS RTOS is a mature operating system in its fifth generation of reliability.

When it comes to specific security and certification requirements, we are known for our LynxOS-178 RTOS, for critical avionics systems requiring software certification, and our LynxOS-SE RTOS with time and space partitioning.



1.800.255.5969



LynuxWorks, Inc.
855 Embedded Way
San José, CA 95138-1018
408.979.3900
408.979.3920 fax
www.lynuxworks.com

LynuxWorks Europe
50 Broadway
London SW1H 0RG
United Kingdom
+44 208 906 9506
+44 208 906 2338 fax

©2011 LynuxWorks, Inc. LynuxWorks and the LynuxWorks logo are trademarks, and LynxOS is a registered trademark of LynuxWorks, Inc. Linux is a registered trademark of Linus Torvalds. All other trademarks are the trademarks and registered trademarks of their respective owners.

All rights reserved.