LYNX
SOFTWARE TECHNOLOGIES

Secure Endpoint Solution

Market Landscape

In just ten cyber incidents during 2021, over $600 million in cash was stolen or taken as ransom, tens of millions of citizen records were stolen, 40,000 businesses' IT operations put at risk, one billion airline passenger details compromised and at least one bank was effectively shut down for over a week.

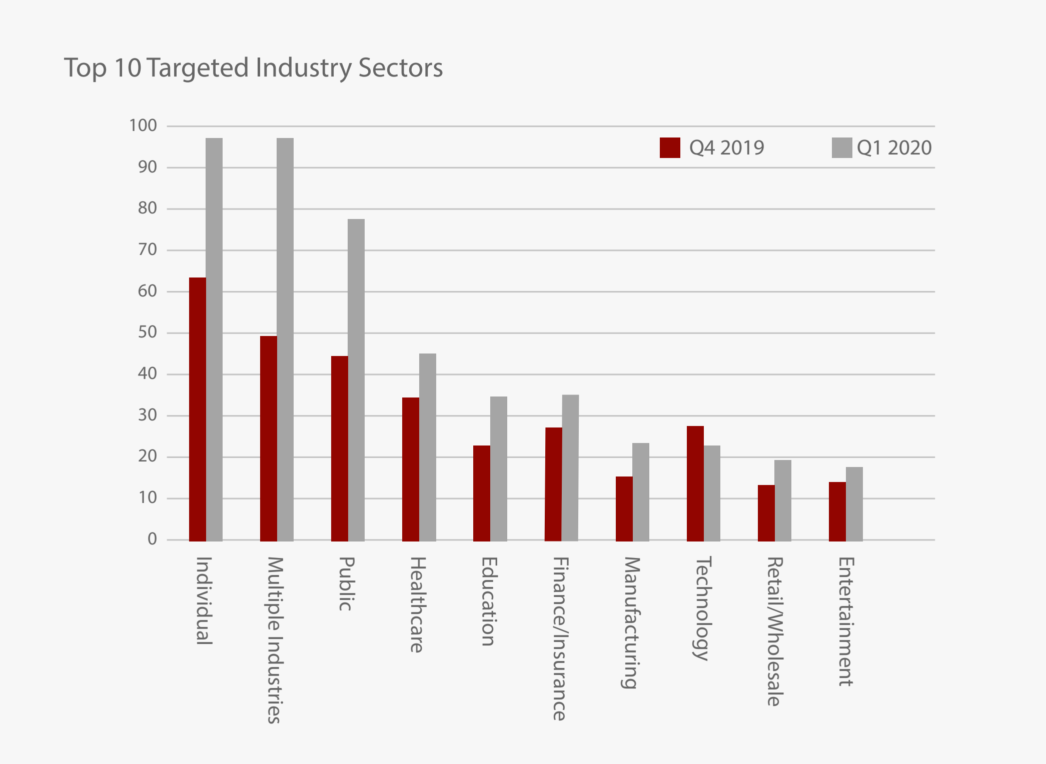
With a prolonged work from home period due to the COVID-19 crisis, companies like Twitter and Fujitsu are offering workers the opportunity to permanently work from home. While this is relatively easy to state, CIOs and CISOs have to adjust their IT networks to support this environment.

For users handling sensitive or classified information, a traditional endpoint system cannot be trusted when leaving the confines of the corporate/classified network.

Traditional operating systems (OS) such as Windows, macOS or Linux/Android running on endpoints and servers are vulnerable to cyber-attacks; security updates and anti-virus software cannot be relied on to protect the endpoint. Traditional IT endpoint security solutions rely on patching the endpoint OS or anti-virus applications running on the endpoint OS. In either case, a compromised OS allows the threats full access to the endpoint, the sensitive data residing on the endpoint and even the encryption keys that are used to protect the data. This threat limits the usefulness of portable endpoint solutions such as laptops or tablets, as the sensitive information could be compromised as soon as the endpoint is connected to the outside world, either via an IT network, or through peripherals such as USB memory sticks.

Additionally, the excitement and opportunity created by connecting businesses such as critical infrastructure and manufacturing businesses to public clouds has shown to generate an exposure point that can be attacked. In 2021, multiple critical infrastructure facilities such as, gas pipelines, water treatment plants and even food processing plants were compromised by an increased attack surface as these industries go through the software-defined transformation.

This chart, courtesy of McAfee Labs COVID-19 Threats Report, July 2020, shows the marked increase in disclosed incidents around the start of the COVID-19 outbreak. It also demonstrates how a wide set of industries have been targeted. In the two years that have followed, both the number of attacks and the impact of those from a financial perspective, has continued to grow. Overall, malware led disclosed attack vectors, followed by account hijacking and targeted attacks.



McAfee Labs COVID-19 Threats Report, July 2020, shows the marked increase in disclosed incidents around the start of the COVID-19 outbreak. It also demonstrates how a wide set of industries have been targeted. In the two years that have followed, both the number of attacks and the impact of those from a financial perspective, has continued to grow. Overall, malware led disclosed attack vecotrs, followed by account hijacking and targeted attacks.

Addressing the Challenge

Mobile knowledge workers dealing with sensitive and classified workers need access to data and applications without compromising security, however, their laptops are constantly subject to vulnerabilities such as zero day attack, unauthorized access via peripherals, malicious code, sniffing, and location tracing.

Virtualization has been used to provide an additional protection layer by separating the operating system from the hardware. However, traditional virtualization solutions built on enterprise hypervisors, are generally as vulnerable as the OSes they are hosting and provide little protection against cyber-threats or data exfiltration.

A new protection solution is needed that can provide the following characteristics:

- Isolate the user's sensitive work environment on a laptop preventing exposure to network threats.
- Protect the user's sensitive data so it is not compromised even if the laptop is lost.
- Allow sensitive corporate assets to be protected from insider threats.
- Facilitate monitoring of corporate assets and sensitive data that allow for remote backups, remote upgrades and remote disabling of sensitive data.
- Allow seamless operation of existing work environments on commodity laptops without significant loss of user experience.

The user experience needs to be identical to a normal user endpoint, but provide (invisible to the user) levels of protection to surround the sensitive data and the user applications that access it, isolating threats from these assets.

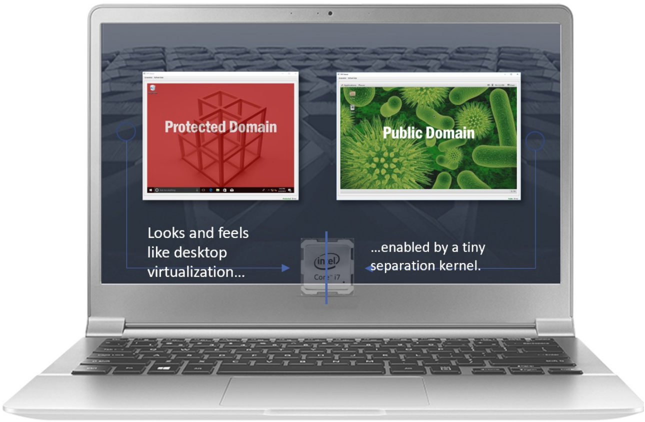
To achieve this, the OS and applications need to be housed in a secure virtual machine having no direct access to the internet. Any data that flows to and from this domain is encrypted before it leaves. Any data that is stored on the endpoint is also encrypted, and the encryption keys and algorithms are housed in their own secure domains. In some cases, the secure partition might be required to boot up only after the secure connection conditions have been met.

A simple key sequence should enable a user to move from the secure domain to the unsecure connected domain and vice versa, thus creating a productive work environment. At no time should any sensitive data be exposed in clear text form to the unsecure domain.

Commercial Solutions for Classified (CSfC) uses

The use of commercial products for classified use cases is being driven by the United States government through the Commercial Solutions for Classified (CSfC) applications program. This is run by the National Security Agency (NSA).

Commercial Solutions for Classified (CSfC) is an important part of NSA's commercial cybersecurity strategy to deliver secure cybersecurity solutions leveraging commercial technologies and products to deliver cybersecurity solutions quickly. It is founded on the principle that properly configured, layered solutions can provide adequate protection of classified data in a variety of different applications.


Protected Domain
Public Domain
Looks and feels like desktop virtualization...
...enabled by a tiny separation kernel.

NSA has developed, approved and published solution-level specifications called Capability Packages (CPs), and works with Technical Communities from across industry, governments, and academia to develop and publish product-level requirements in US Government Protection Profiles (PPs). CPs for Mobile Access, Multi-Site Connectivity, Campus Wireless LAN, and Data at Rest solutions are now published on this site.

The (CSfC) Program publishes Capability Packages (CPs) providing configurations that empower NSA customers to implement secure solutions using independent, layered Commercial Off-the-Shelf (COTS) products. The CPs are product-neutral and describe system-level solution frameworks documenting security and configuration requirements for customers and/or Integrators.

Of particular interest to the secure endpoint, is the Mobile Access (MA) Capability Package. Mobile communications are inherently risky and have to assume a zero trust environment. This CP describes a general MA solution to protect classified information as it travels across either an untrusted network, or a network consisting of multiple classification levels. The solution supports connecting end-user devices (EUDs) to a classified network via two layers of encryption terminated on the EUD provided that the EUD and the network operate at the same security level. The MA solution uses two nested, independent tunnels, to protect the confidentiality and integrity of data (including voice and video) as it transits the untrusted network. The MA solution uses Internet Protocol Security (IPsec) as the Outer Tunnel and, depending on the solution design, IPsec or Transport Layer Security (TLS) as the Inner layer of protection.

Lynx's Approach

Lynx's LynxSafe™ product is based on the separation kernel hypervisor technology, LynxSecure, adding additional security technologies to provide a unique endpoint solution for meeting security requirements for sensitive data such as the Commercial Solutions for Classified (CSfC) program and the Associated Capability packages.

The hardware-enforced separation and virtualization properties of LynxSecure allow for separate secure domains to exist. There are at least two domains:

a) A first unsecure domain that is not secure, and is connected to the outside world directly through the regular internet.

b) A second secure domain used for handling sensitive or classified data, without any possibility of connecting to a server through an unsecured connection. Any data transfer to and from this domain has additional security requirements beyond https/tls such as dual data in transit (VPNs) and dual encryption of the data at rest.

Such a solution would have multiple subjects running operating systems or bare-metal applications. The security functions such as VPNs and data encryption are hosted in their own separate operating systems, while the user facing operating systems have their own isolated partitions.

These operating systems are connected to each other via highly secure and minimal attack surface, FIFO-based, communication mechanisms. This scheme balances the ability of the operating systems to exchange messages and workloads while ensuring that the security posture is strengthened. As an example, a secure endpoint might have seven subjects as follows:

1. An inner Virtual Private Network (VPN) running on Linux
2. An outer VPN running on Linux
3. Secure domain operating system and VDI client
4. Non-secure domain Windows operating system for non-classified use cases
5. Network virtual machine that is able to select the internet connection interfaces
6. Domain master - Update manager for a domain that connects to a remote service for certificate or OS updates
7. Virtual device server – Internal small virtual machine that can emulate peripherals and perform management tasks

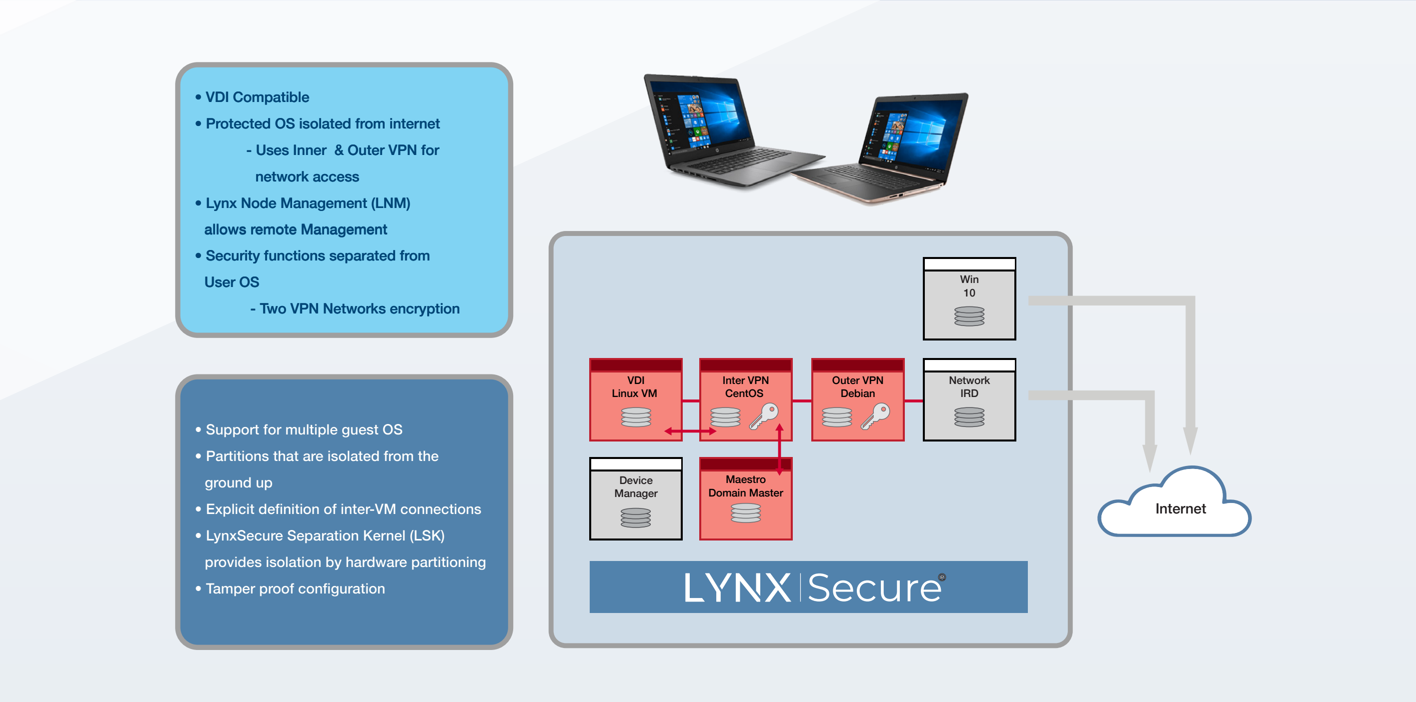
In this case, all seven subjects run on separate operating systems even though other solutions run one or two bare-metal applications in a separate partition. The value of this solution, shown below, lies in the unique approach to leveraging virtualization while meeting the security requirements for today's endpoint solutions that integrate into management platforms and IT networks.

Integrating into management platforms and IT Networks

Lynx offers management capabilities to perform updates and upgrades of operating systems and other software functionality executing in the isolated virtual machines, Lynx refers to these as "subjects". Responding to newly exposed vulnerabilities typically requires an update or certificate rotation to the operating systems running in the subjects. The LynxSafe platform is designed to integrate with current device management solutions since many of the solution providers and IT departments have an existing backend update platform. The product from Lynx supporting this capability on the device itself is referred to as LNM, Lynx Node Manager, which packages the APIs, messaging and integration required to be able to execute on security workflows without compromising security.

Lynx offers a set of APIs to integrate any third-party virtual machine management platform. The platform can instruct the Lynx platform to perform system functions via the low-level peripherals accessible by each subject. The management functionality is further secured by separating the virtual machine talking to the controller via a secure connection from the platform management agent instructing the subjects to perform tasks.

This solution allows one or more VPNs to be nested or sequenced. Each third-party VPN client, such as Aruba, Cisco, Palo Alto Networks, NordVPN, runs in its own isolated operating system and doesn't require any additional integration.



- VDI Compatible
- Protected OS isolated from internet
  - Uses Inner & Outer VPN for network access
- Lynx Node Management (LNM) allows remote Management
- Security functions separated from User OS
  - Two VPN Networks encryption

- Support for multiple guest OS
- Partitions that are isolated from the ground up
- Explicit definition of inter-VM connections
- LynxSecure Separation Kernel (LSK) provides isolation by hardware partitioning
- Tamper proof configuration

Solution Benefits

The Lynx solution-based secure laptops have fundamental advantages as compared to the systems that are built using enterprise hypervisors. More specifically, the key differences are:

- Least privilege architecture: This architecture does not include a privileged operating system that, can open up the system to vulnerabilities when compromised. This architecture does not have a hypervisor administrator login or an administrative user.
- Immutable hardware partitioning: The system's configuration, including the partitioning of hardware resources, interconnects between VMs and peripheral assignment and is done prior to boot time. A bad actor cannot do dynamic OS modification or try to execute code from the unsecure operating system into the secure operating system.
- No unprotected OS denial of service against secure OS: Since the unsecure OS is isolated and partitioned from the secure OS, a denial of service attack on the unsecured OS would not affect the secure OS.
- Strict isolation: The underlying software foundation preserves strict isolation between the different security functions and user-facing operating systems. Since the compute resources and peripherals are assigned at runtime, a guest does not have access to another guest's resources. LynxSecure by itself does not have access to the guest operating system.
- Full time system security enforcement: The security enforcement is always on or as defined by the security policy. With the configuration done before the boot, the data encryption is always on, the VPN can be configured to be always on and USB device insertion can be completely turned off.

Separation Kernel Technology

The concept of separation kernel was proposed by John Rushby where he noted "secure systems should be conceived as distributed systems in which security is achieved partly through the physical separation of their individual components and partly through the mediation of trusted functions performed within some of those components."

This introduced the separation kernel concept as a foundation for secure systems. Over the last 10 years, the notion of separation has matured and the processor architecture advances have resulted in capabilities within the separation kernel that were previously unavailable. With hardware offering support for virtualization through mechanisms like Intel's VT-d, a modern separation kernel is, in effect, an operating system that can run other operating systems as "subjects". A subject is defined as a collection of resources accompanying a piece of software (like an OS) that allow it to be executed and monitored by the separation kernel. It is important to note that a subject might not necessarily be an OS at all; in fact, it could be a dedicated program that runs without an OS within a separation kernel context.

Various parts of this system are protected by virtue of the separation kernel handling low-level communication with the outside world as well as providing protected interaction between the different subjects.

A separation kernel has the following unique characteristics:

- Creates an isolated context for each subject it runs
- Provides a means for different subjects to access hardware efficiently (I/O, mapped memory, DMA)
- Enforces security policies between different subjects as well as with the outside world
- Provides a subject-based scheduling policy
- Provides secure inter-subject communication
- Keeps overhead low with minimal abstraction during runtime

Summary

Lynx's secure laptop solution is built on a unique separation kernel technology providing benefits such as non-bypassable security, strict isolation and full-time system security enforcement. LYNX MOSA.ic adds management and integration capabilities with any third-party controller, allowing system integrators to rapidly build secure laptop solutions that meets or exceeds the most stringent security requirements.

1.800.255.5969

CERTIFIED ISO 9001:2015 COMPANY

Lynx Software Technologies, Inc.
855 Embedded Way
San Jose, CA 95138-1018
+1 (800) 255-5969
+1 (408) 979-3900
+1 (408) 9793-920 fax
inside@lynx.com
www.lynx.com

Lynx Software Technologies UK
400 Thames Valley Park Drive
Thames Valley Park
Reading, RG6 1PT
United Kingdom
+44 (0) 118 965 3827
+44 (0) 118 965 3840 fax

Lynx Software Technologies France
38 Avenue Pierre Curie
78210 Saint-Cyr-l'École
France
+33 (0) 1 30 85 06 00
+33 (0) 130 85 06 06 fax