

# INCREASING MEDICAL DEVICE SECURITY WITH MAINSTREAM IT PLATFORMS AND TECHNOLOGIES

A Layered Security Approach Improves Protection and  
Eases the Burden on Health-Care IT

## TABLE OF CONTENTS

Executive Summary . . . . .	2
Device Security Challenges Today . . . . .	2
Securing a Platform . . . . .	3
Layered Security Model . . . . .	3
Seven Safeguards for Protecting Medical Devices . . . . .	3
1. Stop Unauthorized Data Copying . . . . .	4
2. Prevent Untrusted Code Execution . . . . .	4
3. Interrogate Incoming Packets . . . . .	5
4. Protect Data and Communications . . . . .	5
5. Prevent Unintended Interactions Between Applications . . . . .	6
6. Prevent Device Performance Degradation During an Attack . . . . .	7
7. Reduce Attack Surface . . . . .	7
Intel Processor-based Platforms Mapped to Medical Devices . . . . .	8
Conclusion . . . . .	9
Notes . . . . .	9

---

## EXECUTIVE SUMMARY

Medical devices, such as diagnostic tablet computers, heart-rate monitors, and MRI scanners, are just as susceptible to malware as standard laptop computers. Keeping them secure in any networked environment is certainly challenging, and the stakes are particularly high in the health-care industry.

Proving this point, computer security firm McAfee and a medical equipment manufacturer recently raised awareness of security holes with potentially life or death consequences. They identified a networked insulin pump with a security flaw that allows the device to be hacked and subsequently administer a potentially lethal amount of insulin to diabetes patients. Although not currently typical targets of cyber-attacks, medical equipment can become “collateral damage” in a malware outbreak, or even be the weak link that opens the door to a cyber-attack.

As the complexity of securing devices increases, so does the risk of vulnerabilities slipping past equipment manufacturers and hospital IT organizations. However, this complexity is reduced significantly when medical devices are designed for security using platforms similar to typical networked clients, such as laptops and workstations. This synergy enables hospital IT personnel to apply consistent security strategies across the network, making it easier to administer and monitor equipment. Moreover, as new technologies and methods roll out to thwart attacks, they can be implemented in a similar fashion across the network.

There isn’t a single security solution capable of addressing all existing and future risks; instead, most would agree it’s necessary to implement a series of different defenses across the system. This can be done using a layered security approach that enforces security policy from the CPU to the application software, as outlined in this paper and demonstrated by the Intel Medical Security Reference Platform. In the best case, devices will be fully protected; and in the worst case, malware is detected faster, allowing counteractive action to be taken before any harm is done.

---

## DEVICE SECURITY CHALLENGES TODAY

One of the challenges facing hospital IT organizations is the large variety of hardware and software systems they must manage and secure. Further complicating matters, some equipment manufacturers come up with unique security solutions, often the result of designing purpose-built solutions based on nonstandard or proprietary components. Consequently, it can be difficult to determine whether they comply with the security policies of the purchasing hospital.

Devices based on nonstandard platforms present other drawbacks, including the need to send them to the manufacturer for upgrades, security or otherwise, making them unavailable for a period of time. Additionally, it may be more difficult to capitalize on the latest security advancements developed to secure IT infrastructure built with standards-based computing technology. For instance, nonstandard platforms may not be able to use hardware-assisted virtualization—available on mainstream server and client processors—that can offer security benefits by providing an additional isolation boundary that can aid in security protection that complements software-only solutions.

It can also be challenging for organizations to reach consensus on security policy due to conflicting viewpoints and goals of key stakeholders. As an example, security officers tend to advocate locking down systems to better protect the network, while IT managers gravitate toward opening up the network to deliver the best end-user experience. Some common ground may be found with a layered security model implemented on standards-based platforms, which improves device security and lowers hospital IT support requirements.

### SECURING A PLATFORM

Like other devices on the network, once compromised, medical devices could be the vehicle for launching all sorts of attacks. They can be used to harm patients, access patient records, initiate network attacks—denial of service (DoS)—or spread malware to other systems on the network, among other things. To stop such actions, it is necessary to prevent hackers and malware from breaching the platform. While the basic principle behind securing a platform is conceptually easy to understand, it is far more difficult to realize in practice:

- **Principle:** Protect the system by ensuring any malware that infiltrates a system cannot execute; if malware is present on the system, it cannot be allowed to embed itself in system memory.

- **Reality:** The most problematic malware finds a way to load itself into memory and obscure its presence; consequently, the platform's security mechanisms are unable to discover it and take appropriate action.

### LAYERED SECURITY MODEL

Although there are no ironclad solutions, a proper layered security approach, with safeguards deployed throughout the platform, goes a long way to providing robust protection against the vast majority of attacks. The basic premise is that by creating multiple barriers, a device has more opportunities to discover the malware before it causes harm, which forces hackers to write more sophisticated malware to circumvent all the lines of defense. Additionally, a well designed layered defense helps contain malware, thus increasing the possibility a device can continue to perform safety-critical tasks even when attacked.

### SEVEN SAFEGUARDS FOR PROTECTING MEDICAL DEVICES

Using the basis for the layered security approach, Intel, Wind River, and McAfee have developed a secure platform for medical devices, demonstrated by the Intel Medical Security Reference Platform. This proof of concept incorporates eight security safeguards spanning multiple layers: hardware, virtualization, operating system, and services software, as shown in Figure 1. The platform is designed with off-the-shelf components, and it applies security policy consistent with standard IT practices.

In health care, networked medical devices can fall victim to all types of perpetrators using a wide variety of methods. These eight safeguards for potential vulnerabilities, implemented across the platform, can either prevent attacks or minimize their impact until corrective action is taken.

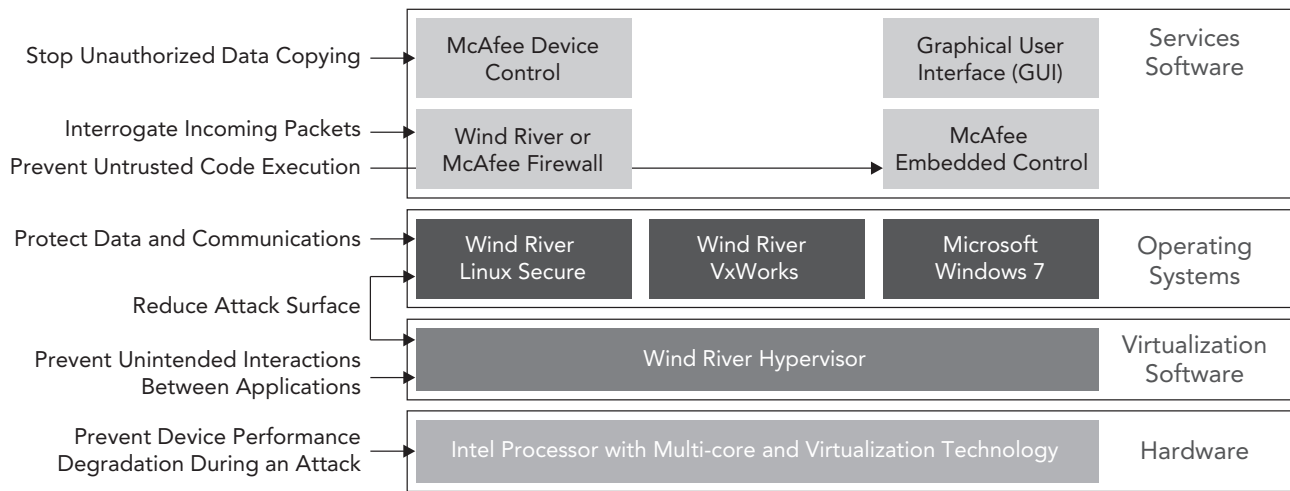


Figure 1: Device platform with layered security

## 1. Stop Unauthorized Data Copying

Data is the life blood of the connected hospital, and it has to be accessible to add value. But how accessible can sensitive data be? Protecting it in a world of outsourcing, portable storage devices, and Facebook and Twitter is the challenge:

1. **Attack:** Confidential patient records fall into the wrong hands when an unauthorized person downloads the data onto removable storage devices and media, such as USB drives, MP3 players, CDs, and DVDs.
2. **Action:** Implement a security strategy that safeguards users and data while providing hospital IT organizations granular control over data privileges, such as specifying what data can be copied to external devices.
3. **Safeguard:** McAfee Device Control, depicted in Figure 2, enables hospitals to implement data security regulation without suppressing the flow of vital information.

## 2. Prevent Untrusted Code Execution

Medical devices, unlike tablets and laptops used by hospital staff, typically run a predetermined set of applications that are carefully controlled by the manufacturer. Two approaches for ensuring that

only the trusted applications can execute are called blacklisting and whitelisting. PC users are familiar with blacklisting, from running antivirus software that searches for bad software and neutralizes it. Whitelisting is a complementary approach, to ensure that

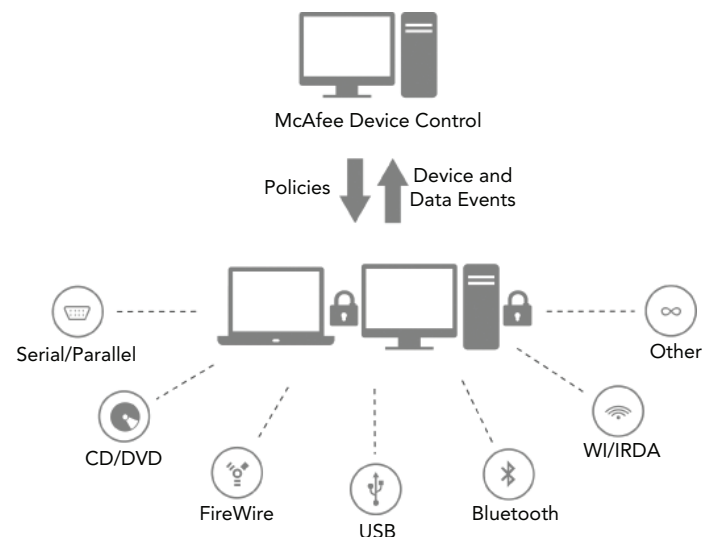


Figure 2: McAfee Device Control specifies which devices can be used and what data can be copied

only known, trusted applications run on the system. Whitelisting is well-suited for embedded devices because it employs a list of permitted applications that can execute; any application not on the list is prevented from executing:

1. **Attack:** Untrusted code, such as worms, viruses, spyware, and other malware installed on a medical device, begins to execute and compromise the device.
2. **Action:** Implement a security measure that stops untrusted code from launching and unauthorized changes from being made.
3. **Safeguard:** Lock down the system with McAfee Embedded Control, a whitelisting application that ensures only trusted applications are permitted to execute while all others are prohibited from launching.

### 3. Interrogate Incoming Packets

Viruses often gain access to medical devices through the network. This common method of attack can be curtailed by locking down access so only legitimate communications are received and transmitted by the device:

1. **Attack:** A hacker conceals a virus in spurious packets, or a mis-configured host system sends unintended packets to the device.

2. **Action:** Implement a firewall on the device that discards unwanted packets and logs packets, which can be used to identify potential malicious actions at a later time.
3. **Safeguard:** Use either a Wind River or McAfee firewall to protect the protocol stack from security breaches and attacks by hackers.

### 4. Protect Data and Communications

Once compromised, a medical device can become a base from which a hacker launches attacks on other devices and systems on the hospital network:

1. **Attack:** After breaking into a medical device, a hacker attempts to communicate with other devices and systems on the network to access confidential data.
2. **Action:** Enforce password-based authentication using an identification mechanism incorporated in a security-enhanced Linux distribution.
3. **Safeguard:** Use Wind River Linux Secure, with enhancements shown in Figure 3, which is certified to Common Criteria Evaluation Assurance Level 4+ (EAL4+) and Federal Information Processing Standard (FIPS) 140-2.

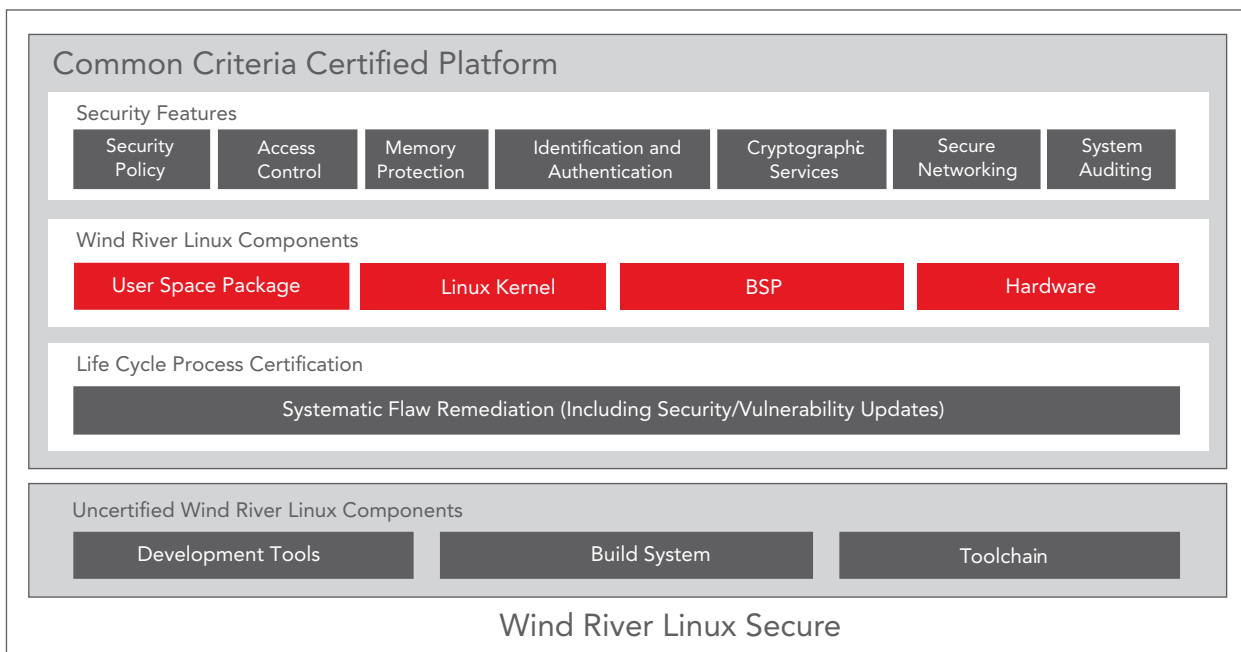


Figure 3: Wind River Linux Secure, certified to Common Criteria EAL4+ and FIPS 140-2

## VIRTUALIZATION BASICS

Virtualization provides the ability to run multiple operating systems and their associated applications on the same physical board. This is achieved by executing software in individual partitions, called virtual machines (VMs), which are separated from the underlying hardware resources. As a result, applications run on their native operating systems (called guest OSes), allowing them to easily migrate to a new system, often with only minor or no changes.

At the heart of virtualization is the virtual machine monitor (VMM, or “hypervisor”), which is a software layer that abstracts the hardware and manages guest OSes in much the same way that a standard OS manages the execution of its applications. For example, the VMM in a medical device may create and manage separate VMs for communication ports, safety-critical applications, and a human machine interface, as illustrated in Figure 4.

Developers can implement virtualization using Wind River Hypervisor, which takes advantage of the hardware-assisted virtualization features of Intel VT. A Type 1 embedded hypervisor with a very small memory footprint, it is less susceptible to attack than using a general purpose operating system. Furthermore, this thin hypervisor has minimal impact on system performance and device access latency and incorporates deterministic capabilities and optimizations for maximum performance.

## 5. Prevent Unintended Interactions Between Applications

A hacker can infiltrate one application with the intention of using it to gain access to another application’s data. After malware embeds itself in system memory, it will look for software applications and files to exploit by accessing their memory space. To greatly reduce the harm malware can cause, restrict the number of software elements it has access to, thus limiting a virus’s ability to move around. This can be achieved using virtualization technology to run applications in their own secured partitions (see sidebar):

1. **Attack:** A virus exploits a security hole in the graphical user interface (GUI) software of an MRI scanner and then hooks onto the application administering the radiation dosage.
2. **Action:** Run safety-critical applications in virtual machines (VMs), so a virus resident in one VM cannot infiltrate the memory space of an application in another VM.
3. **Safeguard:** Applications requiring a higher level of security can be isolated in secure virtual machines, whose memory space is protected by hardware features in Intel processors and Intel Virtualization Technology (VT).<sup>1</sup> This means software running in a VM only has access to its own code and data regions and is unable to access outside its memory boundaries. With Intel VT, memory address tables are safer because they are managed by the hardware, not the software, making it far more difficult for a virus to manipulate them.

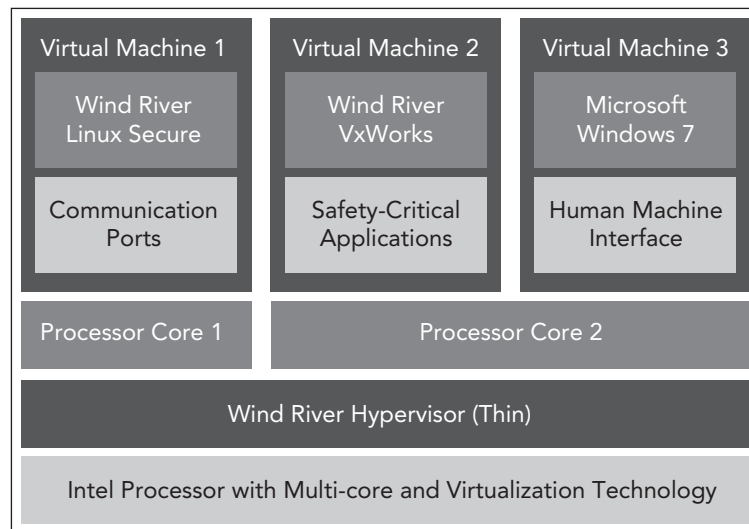


Figure 4: Example of virtualization

## 6. Prevent Device Performance Degradation During an Attack

Any virus executing on a device consumes computing resources, but in some cases this is its primary intention: to consume as many device resources as possible, rendering the device useless for its intended function. This is known as a denial of service (DoS) attack. Such viruses can degrade the device performance to the point of putting a patient at risk:

1. **Attack:** A virus executes on a medical device and launches a large number of routines, prompting the operating system to divert a large portion of computing resources away from its medical applications, thus negatively impacting performance.
2. **Action:** Run the safety-critical application on a dedicated core of a multi-core processor, which can provide it a fixed level of computing resources despite a virus running on another core.
3. **Safeguard:** With Intel multi-core processors, it's possible to designate that applications run on specific processor cores using a feature called processor affinity. For medical applications, this feature allows a safety-critical application to run relatively unencumbered by a virus running on another core, or at least until the hazardous situation is identified and corrective action is taken.

Processor affinity can also simplify software integration. Each development team can be assigned its own processor core, guaranteeing a certain level of performance even when other software is running on the platform.

## 7. Reduce Attack Surface

Viruses frequently enter devices via network ports, so controlling this exposure can minimize security vulnerabilities:

1. **Attack:** After embedding and launching itself in device memory, a virus accesses the device's network ports to look for other programs it can manipulate.
2. **Action:** Minimize malware entry points into the system (using VM separation), by using gatekeeper VM to protect direct access to the network ports, thereby making the other VMs less vulnerable. If the gatekeeper is attacked, another VM acting as a monitor could initiate a recovery sequence.
3. **Safeguard:** Use Wind River Linux Secure as a gatekeeper through which all communications with the device must pass, as shown in Figure 5. The Wind River Linux Secure operating system passes messages to the applications in the other VMs through a virtual network port. As a result, the other operating systems and associated applications do not have direct contact with the network ports, making it more difficult for malware to exploit their potential security vulnerabilities.

If the Wind River Linux Secure gatekeeper is attacked, a watchdog function implemented in a Wind River VxWorks VM will quickly discover this through a heartbeat mechanism that continuously monitors the baseline performance of the Wind River Linux Secure-based gatekeeper. When performance degrades as the result of an attack, the VxWorks VM tells the hypervisor to do one

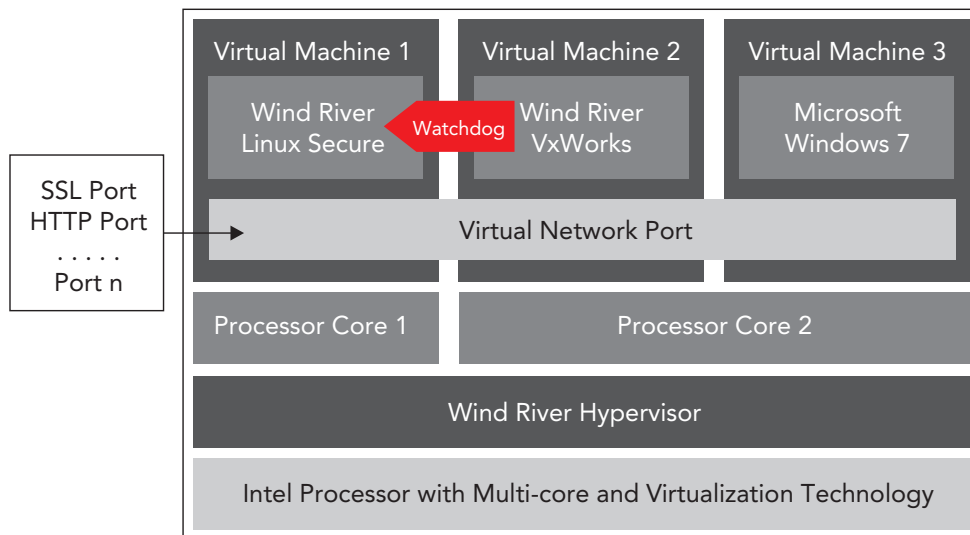


Figure 5: Device with gatekeeper and watchdog

## ABOUT CONTINUA HEALTH ALLIANCE

Continua Health Alliance is a non-profit, open industry coalition of the finest health-care and technology companies joining together in collaboration to improve the quality of personal health care. With more than 200 member companies around the world, Continua is dedicated to establishing a system of interoperable personal health solutions with the knowledge that extending those solutions into the home fosters independence, empowers individuals, and provides the opportunity for truly personalized health and wellness management.

To build trust and ensure customer peace of mind, Continua Health Alliance has created a product certification program with a recognizable logo signifying interoperability with other certified products. This program provides a high level of assurance that a device displaying the Continua Certified logo has met the Continua interoperability requirements. Continua Certified products and services undergo extensive testing through a neutral third party to verify compatibility to the Continua guidelines. Continua also hosts “plugfest” events to give member companies the opportunity to test their products with others in an informal yet secure environment. Intel Evaluation Kit for medical applications ships with Continua Certified software, which automates the process of connecting to multiple laboratory, fitness, and medical devices.

of the following: Reboot the Wind River Linux Secure VM; reload the VM software; or failover to a backup copy.

## INTEL PROCESSOR-BASED PLATFORMS MAPPED TO MEDICAL DEVICES

Code-compatible Intel architecture processors enable equipment manufacturers to cost-effectively develop a family of devices designed with the right processor to reach specific price performance targets. Intel processor-based platforms allow standard networking and communication stacks to be implemented, which greatly simplifies the task of integrating the latest networking, communications, wireless, and security technologies. Whether developing high-end portable ultrasound devices or a low-cost bedside terminal, there is an Intel processor ideal for the job.

With respect to security, performance headroom is critical because devices have to cope with security updates, as well as improved software, given they are likely to be deployed for seven to 15 years or longer. Since a hospital’s security policies are likely to change over time, medical devices need the computing headroom to be able to adapt accordingly.

A major benefit of designing with Intel processors is the ability to use the same application code base across different devices. This attribute also facilitates the consolidation of modalities using Intel VT, further protecting software development investment. Moreover, Intel platforms make medical devices look like standard IT systems, so they are easier to administer (i.e., support, monitor, and update). For instance, hospital IT personnel can update device security in the field instead of sending devices back to the manufacturer. To help decrease development time, Intel offers Continua Certified software that runs on Intel processors (see sidebar).

## CONCLUSION

No single security solution can offer complete protection. Living this reality everyday, hospital IT organizations must sort through countless solutions and support a large number of them. The complexity is multiplied by purpose-built medical devices incorporating unique and sometimes obscure solutions, which increases the support effort.

Security cannot be “bolted on” as an afterthought at the end of the development cycle. Addressing security concerns must be part of the design process, from an analysis of all attack vectors that might be used by a hacker, through the selection of secure building blocks, to thorough security-focused testing, which is made an integral part of the medical device release checklist.

Moving forward, medical devices using standards-based platforms based on IT infrastructure can greatly simplify security management while offering state-of-the-art security protection.

For more information about Intel solutions for the health-care industry, visit [www.intel.com/go/medical](http://www.intel.com/go/medical).

For more information about Wind River software solutions, visit [www.windriver.com](http://www.windriver.com).

For more information about McAfee security solutions, visit [www.mcafee.com](http://www.mcafee.com).



## NOTES

1. Intel Virtualization Technology (Intel VT) requires a computer system with an enabled Intel processor, BIOS, virtual machine monitor (VMM), and for some uses, certain platform software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Check with your application vendor.

**WIND RIVER**