Changes to NetWitness Appliances by Customers for STIG or Vulnerability Management Purposes.

This document provides information and guidance for those occasions when an organization's policy dictates the addition or modification of software on a NetWitness Appliance.

Examples:
An organizational policy stipulates that a security checklist (i.e. a "STIG") must be run on a NetWitness appliance and discovered issues must be exempted or corrected to meet security requirements.

- An organizational policy stipulates that anti-virus software must be installed on a NetWitness Appliance
- An organizational policy stipulates that a host-based firewall must be installed on a NetWitness Appliance
- An organizational policy stipulates that regular, approved operating system patches must be installed on a NetWitness Appliance
- An organizational policy stipulates that a NetWitness appliance must be joined to an Active Directory domain.

Windows Appliances:

The NetWitness appliances running Windows Server run a hardened install of Windows. This install includes the minimum required number of optional components and services required for operation of the appliance. This is done for two reasons:

- Performance: a lightweight system runs faster
- Security: a limited number of services reduces the attack surface

For this reason it is recommended no 3rd-party software be installed on a NetWitness Windows appliance as it can make the appliance unstable, reduce performance or even make the appliance unusable. Such failures are usually rectified with a complete software rebuild of the appliance. It is recommended that no changes to the operating system or installed packages be made unless specifically directed to do so by NetWitness Support.

NetWitness Windows appliances have already been hardened but if you must run a security checklist against a NetWitness Windows appliance, backup the device first and carefully document and test each change as you make it so that you can easily back out the setting in the event it causes the appliance to malfunction or cease to operate.

Security policy may dictate the usage of Anti-Virus software. This software is by nature very I/O intensive. For this reason anti-virus software may need to be "tuned" with such changes as turning off any real-time scanning or at a minimum exempting NetWitness program and data folders which may contain hundreds of thousands of files. Failure to properly tune or adjust anti-virus software may degrade performance to the point where the device is effectively unusable.

Security policy may dictate the usage of HIDS or host-based firewall software. This software can interoperate with NetWitness software provided it is configured properly. It is important to note that any additional layer of network filtering will impact network performance. Failure to exempt processes and

operations from an active HIDS or open the appropriate ports and services on a host-based firewall can render the Windows appliance unusable or at a minimum impact performance.

Security policy may dictate that the Windows appliance be patched according to a regular schedule. It is important to note that any optional packages should not be applied unless they are intended to address a specific failure. It is also important to note that any major patches like service packs should not be installed without guidance from NetWitness Support. Windows provides you with the ability to "back out" a patch as well as recording what patches were installed on what dates. If a Windows appliance fails following a patch and reboot, the first troubleshooting step should be to roll back any changes made by patching the appliance.

Security policy may dictate that any Windows devices are joined to the organization's Active Directory domain. Generally speaking, the act of simply joining the Windows appliance to a domain should not impact the functionality, stability or performance of the system. However, in most organizations, domain membership brings with it various centrally managed policies, which can have wide-ranging impacts on the functionality of core Windows and also 3rd party components. It is strongly recommended that if a Windows appliance must be joined to a domain, it should be placed in a dedicated OU and carefully tested to make sure that any policy settings enforced by the domain do not adversely affect the system. If issues are encountered, enabled policies should be disabled one-by-one until the offending policy is identified and removed from the policy set applied to the OU containing the Windows appliance.

GNU/Linux Appliances:

The NetWitness appliances running GNU/Linux run a very limited subset of the full GNU/Linux set of offerings. This subset includes the minimum required number of packages required for operation of the appliance. This is done for two reasons:

- Performance: a lightweight system runs faster
- Security: a limited number of services reduces the attack surface

For this reason, any changes to packages or the kernel will be released as part of a NetWitness software update. Updating a Linux appliance outside of the normal NetWitness service release schedule can render an NetWitness appliance unstable, reduce performance or even make the appliance unusable. Such failures are usually rectified with a complete software rebuild of the appliance. It is recommended that no changes to the operating system or installed packages be made unless specifically directed to do so by NetWitness support.

NetWitness GNU/Linux appliances have already been hardened but if you must run a security checklist against a NetWitness GNU/Linux appliance, backup the device first and carefully document and test each change as you make it so that you can easily back out the setting in the event it causes the appliance to malfunction or cease to operate.