# NETSHIELD / Version 10.2 Patch 19 / July 13, 2020

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 19 includes the following:

- Asset Manual Update Fix

### Asset Manual Update Fix

Modifying an asset without a hostname (Unknown) will fail if a second DNS Server entry in Network Configuration is invalid or unavailable. Netshield tries to resolve the hostname and will generate an error if the second DNS server is invalid or unavailable.
This has been corrected.
Assets with hostnames are unaffected.

.

# NETSHIELD / Version 10.2 Patch 18 / June 3, 2020

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 18 includes the following:

- Quiet Port Scan Fix

### Quiet Port Scan Fix

The Netshield port scanner identifies the software configurations of hosts on the network by checking which ports respond to connection attempts and analyzing which services are active. This service can trigger other intrusion detection systems to alert on the port scans.

To prevent this issue, Netshield now includes a quiet port scan mode which only probes to see if the host is active.
Note that the host OS will not be discovered and will display as Unknown.
The mode is available from the Netshield console.

# NETSHIELD / Version 10.2 Patch 17 / January 30, 2020

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 17 includes the following:

- Midnight Crossing Audits Fix
- Remove from Asset Detection Fix
- NTP Should Stop Audits Fix
- Login Page Reload Fix

### Midnight Crossing Audits Fix

Daily audits not running if scheduled for midnight (00:00).

### Remove from Asset Detection Fix

An asset can be removed from asset detection but the setting is not being retained. The check has been made more robust.

### NTP Should Stop Audits Fix

Turning on NTP will stop all audits and reschedule them, as well as log the user out of the UI.

### Login Page Reload Fix

When the appliance restarts, but the UI is not reset, the login page can end up nested within the iframe used to display page content.

# NETSHIELD / Version 10.2 Patch 16 / November 18, 2019

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 16 includes the following:

- Malware Service Restart Fix

### Malware Service Restart Fix

There is an infrequent issue where the malware service can interfere with asset detection under heavy load. In these situations, the malware service will now restart itself to clear the interference.

# NETSHIELD / Version 10.2 Patch 15 / July 30, 2019

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 15 includes the following:

- Usage Statistics Collection Module
- Active Directory Authentication Enhanced Validation
- Manage Assets Fixes
- Database Check Utility
- Support Channel Fix

### Usage Statistics Collection Module

This patch adds a usage statistics collection module to the appliance to help Netshield understand how its customers are using the product. Unless otherwise stated, all information collected is anonymized and cannot be linked to the customer or partner. For its first release, the module collects the following information:

1. Which SmartSwitch plugins have been configured and whether they are in active use.
2. The hardware platform (e.g., Nano 25, Enterprise 100), which is linked to the customer appliance record. This information is collected to validate our appliance database.

Future releases may collect additional information. These changes will be added to the release notes.

### Active Directory Authentication Enhanced Validation

The Active Directory Authentication module now performs a more extensive validation of the user-specified configuration. If the configuration is incorrect, the Test Connection button will provide a more detailed reason for the failure.

**Note that the module now explicitly checks the TLS handshake and WILL FAIL if the domain controller does not have a certificate installed.** Installing a certificate is not difficult, see the information at this link: https://www.virtuallyboring.com/setup-microsoft-active-directory-certificate-services-ad-cs/

### Manage Assets Fixes

The issue with the IP Address column displaying out of sync with the rest of the grid has been fixed. The message boxes that display “This operation will take N minutes” after clicking a Trust, Untrust or Remove operation have been removed.

## Database Check Utility

A utility has been added to the appliance console to check the database consistency and repair any errors. Running option 17 will test each database table and provide a summary of actions taken. Though the check utility is safe to run on a production appliance, please use it only under the direction of  Netshield Support.

## Support Channel Fix

A bug that was causing the support channel to fail to tunnel non-standard SSL ports has been fixed.

# NETSHIELD / Version 10.2 Patch 14 / June 26, 2019

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 14 includes the following:

- TCP SACK Vulnerability Patch

### TCP SACK Vulnerability Patch

The appliance has been patched against exploits utilizing the TCP SACK vulnerability (CVE-2019-11477, CVE-2019-11478, and CVE-2019-11479). A full description of the vulnerability is available at https://access.redhat.com/security/vulnerabilities/tcpsack.

# NETSHIELD / Version 10.2 Patch 13 / June 4, 2019

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 13 includes the following:

- Asset Database Updates
- One-Click Support Channel
- Asset Replication Fixes
- Analyze Asset Fix
- Switch Integration Fix

### Asset Database Updates

The appliance's database of manufacturer's assigned MAC addresses has been updated, allowing the appliance to identify the manufacturer for all devices up to the current date.

### One-Click Support Channel

The support channel can now be opened without any intervention from the NetSHIELD support team. Click the "Open Support Channel" button under System | Utilities, or select option 13 in the console. The channel will remain open, even in the case of a reboot, until explicitly closed.

### Asset Replication Fixes

A bug in the asset detection system was preventing replicated assets from being marked as active if they were detected on the local network. This occasionally led to issues with assets becoming untrusted after a replication purge. This bug has been fixed.

A bug in the asset replication system was creating duplicate replicated assets on networks where the connection between the command center appliance and the managed appliance was intermittent. This bug has been fixed.

### Analyze Asset Fix

A bug in Analyze Asset was preventing information gathered during the analysis from being added to the asset record. This bug has been fixed.

### Switch Integration Fix

A non-functional entry blank marked "SmartSwitch Password" was erroneously added to some of the switch configuration forms under SmartSwitch Integration. This field has been removed.

### Miscellaneous Fixes

Internal Active Directory logging information has been enhanced for better debugging.

# NETSHIELD / Version 10.2 Patch 12 / April 1, 2019

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 12 includes the following:

- Command Center Trust Asset Feature
- IP Changes Untrusting Assets Fix

### Command Center Trust Asset Feature

Remote assets can now be trusted or untrusted on all managed appliances from the command center. In Manage Assets, go to the Replicated Assets view, find the remote asset, and change its trust state. This state will be replicated to all managed appliances on the next replication cycle.

To allow changes to be replicated immediately, a manual replication control has been added to the Asset Replication page under the Command Center menu.

For instructions, please see the Command Center Overview in the NETSHIELD Support FAQs.

### IP Changes Untrusting Assets Fix

Under some circumstances, assets changing their IP addresses could be misinterpreted as MAC spoofs and untrusted. This behavior has been corrected.

# NETSHIELD / Version 10.2 Patch 11 / February 11, 2019

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 11 includes the following:

- Database Check and Repair

### Database Check and Repair

Performs routine maintenance against the appliance database and repairs any issues.

# NETSHIELD / Version 10.2 Patch 10 / February 4, 2019

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 10 includes the following:

- Public Key Authentication for Remote Console
- Support for AdTran Switches
- Active Directory Event Record Overflow Fix
- Asset Detection Trusted Asset Logging Fix
- NTP Updates Fix
- Miscellaneous Fixes

### Public Key Authentication for Remote Console

The remote console can now be switched between password and public-key authentication. Use the revised System > Utilities page to install a new key and activate public-key authentication, or to switch back to password-based authentication.

### Support for AdTran Switches

Support for AdTran NetVanta switches has been added to SmartSwitch Integration.

### Active Directory Event Record Overflow Fix

A few customers experienced an issue in which Active Directory records were being logged, but the relevant user information was not being displayed in the AD User column in Manage Assets. This was due to the event record number from Windows overflowing a database field. The field size has been extended.

### Asset Detection Trusted Asset Logging Fix

The asset detection system periodically scans the network and adds a log entry for every asset it finds, whether the asset is trusted or untrusted. Trusted asset entries tend to accumulate in large numbers, sometimes slowing database operations, and provide little or no useful information. These entries have been removed from the database and the appliance will no longer log them. Untrusted asset detection will continue to be logged.

### NTP Updates Fix

A bug that was causing the appliance not to receive NTP time clock corrections has been fixed.

### Miscellaneous Fixes

The System > Utilities user interface has been improved and command descriptions added. On some versions of Chrome, the adapter list under Network Configurations was not sorted correctly; this bug has been fixed. Language regarding High vulnerabilities in the Risk Assessment wizard has been improved.

# NETSHIELD / Version 10.2 Patch 9 / January 14, 2019

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 9 includes the following:

- New Software Updates Module

### New Software Updates Module

The service pack installer has been replaced with a new software updates module intended to better display and manage appliance updates. The Service Packs and Service Pack Configuration menu items under Updates have been replaced with a single Software Updates menu item.

# NETSHIELD / Version 10.2 Patch 8 / November 12, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 8 includes the following:

- Changes to Cyber-Insurance Auditing Requirements
- Comments Field Added to Asset Record
- DNS Resolution Fix for Management Access
- Special Characters Allowed in Group Names
- Active Directory Configuration Test Fix

### Changes to Cyber-Insurance Auditing Requirements

The Risk Assessment Wizard now requires only Serious vulnerabilities to be mitigated to receive a Green status audit. Previous releases of the cyber-insurance component required the user to address both Serious and High vulnerabilities to qualify for insurance.

### Comments Field Added to Asset Record

User comments may now be applied to assets. The comments field is displayed in Manage Assets and can be edited in the Add/Edit Assets page by clicking the link in the asset row.

### DNS Resolution Fix for Management Access

A bug has been fixed in the management access module that was causing the appliance's own DNS requests to be blocked if the user restricted access to the appliance by IP or MAC address.

### Special Characters Allowed in Group Names

Users may now enter special characters (e.g. "<%) in group names in the Command Center.

### Active Directory Configuration Test Fix

A bug has been fixed in the Active Directory Configuration that was causing the Test Connection feature to return an internal error message if the configured Active Directory user did not have administrative privileges on the domain controller. The error prompt now returns the message from the controller.

# NETSHIELD / Version 10.2 Patch 7 / October 15, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 7 includes the following:

- Agentless Active Directory
- Remote Operations Configuration Changes
- Miscellaneous Fixes

### Agentless Active Directory

The NETSHIELD Active Directory (AD) Integration feature has been completely reworked. This feature no longer requires an agent to be installed on the domain controller. Instead, the appliance will periodically poll the domain controller for login events. This feature also allows events to be polled from multiple domain controllers.

You should uninstall the agent from the domain controller once you have verfied that the new configuration is working.

The AD Login feature, which allows the NETSHIELD appliance to use Active Directory domain accounts for login authentication, has been moved to a separate menu item in the Network Configuration menu.

Note that if you are currently running the AD agent or AD login features, the patch will attempt to port your existing configuration.

### Remote Operations Configuration Changes

The Remote Operations Configuration menu item in the Command Center menu has been renamed to Asset Replication. All settings on this page not related to asset replication have been removed as the default settings are sufficient for all command center configurations. The user interface on this page has been reworked with a focus on replication settings, and a warning to avoid duplicate replication masters has been added.

### Miscellaneous Fixes

A button has been added to the System Utilities page to display the support channel key in case email notifications are not configured. Backup and Restore now properly handle Active Directory settings. An issue with the Asset Trust/Untrust API has been fixed, and this API will now function correctly.

NETSHIELD

# NETSHIELD / Version 10.2 Patch 6 / September 17, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 6 includes the following:

- Performance Issues Fix
- Asset Removal Fix
- Improved Certificate Manager
- Switch Integration Fixes
- Miscellaneous Fixes

**Please note that the patch will reboot the appliance after it is successfully installed.**

### Performance Issues Fix

An issue with the asset detection queue that was causing some customers to experience sluggish UI behavior and delayed asset detection has been addressed.

### Asset Removal Fix

The asset removal feature has been fixed to address a bug that was causing stale assets to persist at some customer sites, and may have contributed to the performance issues problem.

### Improved Certificate Manager

The certificate manager has been replaced with a simpler design that performs the certificate signing automatically, and can generate root CAs for customers who don't have the facility to generate them.

### Switch Integration Fixes

The switch framework has been extended to handle a larger device count on individual switches (250-1000 unique MACs per switch). The Brocade plugin has been modified to correctly handle a switch that is configured to log into superuser mode.

### Miscellaneous Fixes

A bug in the asset replication service has been fixed to allow sites with longer VLAN names to replicate properly. An Active Directory category has been added to the Network log page, and client IPs will now log correctly.

# NETSHIELD / Version 10.2 Patch 5 / August 13, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 5 includes the following:

- Support for HP 1910 switches
- Backup and restore enhancements
- Juniper EX-2300 plugin bugfix
- Asset unblocking bugfix

### Support for HP 1910 switches

Support has been added for the HP 1910 switch.

### Backup and restore enhancements

The backup and restore process now restores:

- Network configuration
- Hostname
- Usernames and passwords
- VLAN details
- Company information details
- Notification, SNMP, Syslog, and UI settings
- Discovered assets and categories
- Command Center appliance details
- Malware Detection details
- Previously run audits and generated reports

To ensure proper functioning of the network , the appliance will reboot following the restore. Asset detection and blocking must be manually enabled following the reboot.

### Juniper EX-2300 plugin bugfix

On some networks, the Juniper EX-2300 plugin was not bringing the port back up following a quarantine. This issue has been corrected.

### Asset unblocking bugfix

Under heavy asset loads with many simultaneous blocks, the appliance would occasionally fail to unblock all blocking streams when asset detection was disabled. This issue has been corrected.

# NETSHIELD / Version 10.2 Patch 4 / July 23, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 4 includes the following:

- Support for Netgear M4100 and M4300 switches
- Manage Audit Issues enhancements
- OS detection enhancements
- Asset and Malware detection enhancements
- Asset and malware detection bugfixes
- User interface bugfixes
- Miscellaneous changes

### Support for Netgear M4100 and M4300 switches

Support has been added for the Netgear M4100 and M4300 switches. There is a known issue in which blocking assets simultaneously across multiple Netgear switches causes the appliance to temporarily lose connection to one of the switches and may not complete one of the blocks. This will be fixed in the next patch.

### Manage Audit Issues enhancements

Users can now see all open, fixed, and false positive issues for all audits or for a specific audit, as well as reopen fixed issues and false positives.

### OS detection enhancements

Turning on the “Enable NetBIOS Scans for Windows Host Names” option in the Asset Detection System advanced options will force asset detection to run a Windows-specific OS detection script against assets. This will allow the appliance to detect the exact Windows version, as long as the Windows firewall does not block SMB requests.
Asset detection will now use more aggressive and probablistic guessing of operating systems where appropriate.
NMAP signatures have been updated, improving accuracy of manufacturer and OS detection.

### Asset and malware detection enhancements

A “No VLAN” setting has been added to the Target VLAN option box in asset properties. Assets with this setting will become untrusted if they appear anywhere except the default VLAN.
Notifications that indicate an asset has been untrusted now provide the untrust reason.
An asset that has become untrusted by appearing on an unauthorized VLAN are now assigned an untrust reason of “Wrong VLAN”. This reason will appear in Manage Assets and in notifications.
A detection source column has been added to the malware log to indicate whether it originated from a phishing URL or a malware domain.

## Asset and malware detection bugfixes

Allowed VLAN name length in VLAN configuration has been extended to 256 characters, and long VLAN names will no longer interfere with the detection of assets on those VLANs.
The Malware untrust reason will no longer appear for infected assets if malware detection is set to alert only (i.e., untrust/block disabled).
A bug which was causing asset import to remove NETSHIELD placeholder assets (e.g. VLAN "assets") has been fixed.
A bug that was causing asset detection to fail under massive asset load has been fixed.

## User interface bugfixes

When adding a new asset manually via the Add Asset page, all fields are now being saved correctly. The obselete "Trust and Audit-exempt lists" and "Trust and Firewall/SmartSwitch safe lists" options have been removed from the "Add system to" setting, and replaced with a "Trust and Never-Block list" option.
Support for TLSv1.0 has been removed from the web interface as this protocol has been deprecated.
VLAN and Network Configuration utilities now correctly check VLAN names on entry for uniqueness.
The malware PDF report now reflects the headers used in the malware log.
Changing the syslog port now correctly updates the syslog configuration.

## Miscellaneous changes

Submission of a cyberinsurance risk assessment to the insurance company no longer requires asset replication to be turned on when running on a standalone Nano appliance.
Certificate signing requests are now correctly generated for all Subject Alt Name fields.
Regulatory compliance boilerplate has been removed from vulnerability audit reports.
The cyberinsurance risk assessment time limit has been moved to 30 days.
Executive and management sample reports have been updated to reflect changes.
The Asset Alert Only email address setting has been deprecated and removed from the Asset Detection System advanced options.

# NETSHIELD / Version 10.2 Patch 3 / June 25, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 3 includes the following:

- Management interface disconnection bug fixed
- Overlapping asset detection sweeps bug fixed
- Integration with Juniper EX2300 switches
- Switch integration save configuration bug fixed
- Active Directory record parser issue fixed
- Allow Multiple IPs duplicates bug fixed
- Malware events notification behavior changed

### Management interface disconnection bug fixed

Some customers have experienced an issue where adding a VLAN to the VLAN Configuration causes the browser to lose connection to the appliance. The internal routing tables have been fixed so that the eth0 interface is always available from any VLAN or subnet (as long as the customer's firewall is routing traffic between the two networks). To ensure uninterrupted operation, the GUI should always be accessed from its address on eth0.

### Overlapping asset detection sweeps bug fixed

Some customers have reported issues with asset detection on heavily loaded networks. This can be a result of asset sweeps running over their allotted period, causing them to overlap. This condition is no longer possible as the appliance will now defer a new sweep until the old one has finished.

### Integration with Juniper EX2300 switches

Support for Juniper EX2300 switches has been added to SmartSwitch integration.

### Switch integration save configuration bug fixed

An issue that was causing switch configuration saves to fail occasionally has been fixed.

### Active Directory record parser issue fixed

An issue that was causing the user interface to become unresponsive under high Active Directory traffic loads has been fixed.

### Allow Multiple IPs duplicates bug fixed

Assets with virtual IP addresses that migrate between multiple interfaces were causing duplicate asset records if the "Allow Multiple IPs" flag was set for any of those interfaces. This bug has been fixed.

## Malware events notification behavior changed

The “Asset Alert Frequency” setting was being used to control how often users receive alerts for malware connection events for each distinct asset. This was judged to be insufficient as the lowest frequency setting is 5 minutes. The alert frequency has been hard-coded to 1 minute.

# NETSHIELD / Version 10.2 Patch 2 / May 21, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 2 includes the following:

- Integration with Brocade switches
- Added new SNMP monitoring variables
- Malware monitoring port removed from ADS
- Cyberinsurance bug fixes
- VLAN Configuration bug fixes
- Manage Assets display bug fixes
- Switch management bug fixes
- Miscellaneous bug fixes

### Integration with Brocade switches

Support for Brocade IX72xx switches has been added to SmartSwitch integration. The switch must be in Layer 2/Switch mode to function with the appliance, not Layer 3/Router mode.

### Added new SNMP monitoring variables

Variables representing the number of blocked assets (1.3.6.1.4.1.51131.1.3) and untrusted assets (1.3.6.1.4.1.51131.1.4) have been added to the SNMP agent.

### Malware monitoring port removed from ADS

The malware monitoring port (eth1) has been removed from the sniff ranges and block ranges in the asset detection system configuration and the initial asset discovery page to avoid confusion because it is not used for Asset Detection.

### Cyberinsurance bug fixes

A timestamp has been added to the report filename to insure that multiple versions of the CI data can be uploaded. The customer ID has been added to the risk assessment data file.

### VLAN Configuration bug fixes

A bug in the VLAN configuration page was causing interfaces not bound to an address to be left out of the interface selection, and the bound interfaces to be specified incorrectly. Both bound and unbound interfaces are now displayed correctly on this page.

### Manage Assets bug fixes

The column alignment bug has been fixed. A bug causing deleted system assets to reappear with an “Unassigned” IP address has been fixed. A bug causing system categories with embedded spaces to break the Manage Assets display has been fixed. A bug causing subnet filtering to break the Manage Assets display has been fixed.

## Switch management bug fixes

The switch block will now work correctly even if one of the switches in the integration list is unreachable.

## Miscellaneous bug fixes

The simultaneous block limit default on the Asset Detection System page has been raised to 10. The wording on the Malware Detection System page has been changed to better reflect the functionality. A bug preventing pound signs from being used in passwords has been fixed. Calculated sniff ranges have been fixed for subnet masks /31-32, and single IPs are no longer allowed in sniff ranges. The delay on the System Statistics page has been greatly reduced. Generate Audit Reports no longer show “++” in titles.

# NETSHIELD / Version 10.2 Patch 1 / April 2, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 1 includes the following:

- Security Update

### Security Update

This patch updates the user interface service to its latest version.

# NETSHIELD / Version 10.2 Patch 0 / March 28, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.2 Patch 0 includes the following:

- CyberInsurance
- Simplified Auditing Workflow
- Untrust Reason
- Miscellaneous

### CyberInsurance

The Policy Request, Risk Assessment, and Claim Evidence wizards have been added to allow customers to apply for insurance against breaches on networks monitored by NETSHIELD appliances. Coverage is currently limited to customers in the United States.

### Simplified Auditing Workflow

The ticketing system under the Workflow menu has been removed and replaced with a single worksheet (Audit | Manage Audit Issues). The new system allows simple, one-click resolution of all vulnerabilities.

### Untrust Reason

The reason that an asset has become untrusted or blocked is now visible in the Manage Assets display. Current reasons are Manual, Malware, MAC Spoof, and New Asset.

### Miscellaneous

The MAL_ignore log event has been added to indicate when a malware detection event is ignored due to the domain or IP having been previously whitelisted.

# NETSHIELD / Version 10.1 Patch 27 / March 5, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 27 includes the following:

- Management Access Configuration
- Switch Connection Test
- Improved Network Configuration
- Asset Management Fixes
- User Interface Fixes
- Audit and Reporting Fixes
- Miscellaneous Fixes

### Management Access Configuration

A new utility has been added to the appliance to allow access to the management GUI to be restricted by VLAN, by interface, and by source IP. A console options has been added to clear all configuration to the default.

### Switch Connection Test

The SmartSwitch integration page now includes a button to test the connection to a configured switch. The appliance will attempt to log into the switch with the supplied credentials and report back whether it was able to do so.

### Improved Network Configuration

When changing the network and/or VLAN configuration, the time required for the appliance to make the configuration changes has been reduced significantly.

### Asset Management Fixes

A few bugs concerning how assets are managed have been fixed.

- Asset auto-remove will no longer remove assets marked as never-block.
- Attemping to manually remove assets marked as never-block requires confirmation.
- Replication of the untrusted state of an asset will not override the never-block state.

### User Interface Fixes

The Add Group and Add Appliance pages under Command Center now work correctly under FireFox.

## Audit and Reporting Fixes

Two bugs regarding audits and reporting have been fixed.

- Untrusted assets can now be added to audits.
- Sample reports have been updated.

## Miscellaneous Fixes

A number of other bug fixes and changes have been added in this patch.

- A new EULA has been added to the appliance initialization wizard.
- Command center change events have been added back into the event log.
- Factory reset correctly handles appliance name setting.
- Nomenclature has been changed from “quarantined” to “blocked” in notifications.
- The Cancel button under Restore Backup has been fixed.
- Gateway connection error reporting in the System Statistics has been fixed.
- The malware blocking test performance has been improved.
- The SmartSwitch blocking safelist has been removed as redundant.

# NETSHIELD / Version 10.1 Patch 26 / February 14, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 26 includes the following:

- Security Update

### Security Update

This patch updates the appliance kernel, device drivers, and utilities to their latest versions. Once the patch is installed, the appliance will automatically reboot.

# NETSHIELD / Version 10.1 Patch 25 / January 22, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 25 includes the following:

- SNMP Monitoring
- Asset Detection Fixes
- Switch Integration Fixes
- Auditing Fixes
- Command Center Fixes
- User Interface Fixes
- Miscellaneous Fixes

### SNMP Monitoring

The appliance can now be configured as an SNMP agent. Once configured, it can be queried for basic uptime and load variables, and will generate SNMP traps for network and system events.

### Asset Detection Fixes

- Asset Detection Improvements
- Audit on Detection has been removed from ADS configuration.

### Switch Integration Fixes

- The NetGear XS712T plugin now retrieves the entire MAC table regardless of number of entries.
- The NetGear XS712T plugin now properly sets the PVID for a port VLAN change.
- Adding a switch will no longer create a new asset if the switch is already present in the assets table.

### Auditing Fixes

- Changes to company information are now correctly reflected in generated reports.
- User can now recreate any audit report, instead of only the last generated report.
- Query Vulnerabilities now permits the report to be downloaded in CSV format.

### Command Center Fixes

- A verify button has been added to the Add/Edit Appliance page to allow the connection to the managed appliance to be tested. If successful, the appliance type will be retreived and set.

### User Interface Fixes

- The clock on the top bar now displays the correct times at midnight/noon crossings.

- Any punctuation mark or special character may now be used in passwords.

## Miscellaneous Fixes

- Manage Policies has been removed.
- Auto-removal of assets no longer removes system assets.

# NETSHIELD / Version 10.1 Patch 24 / January 16, 2018

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 24 includes the following:

- Kernel Configuration Update

### Security Patch

This patch updates the appliance kernel configuration in preparation for an upcoming security patch.

# NETSHIELD / Version 10.1 Patch 23 / December 18, 2017

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 23 includes the following:

- Support for Cisco, Meraki, Netgear, and Huawei switches added, plus fixes
- Replication filter and flush utility added
- Manage Appliances and Manage Groups simplified
- Asset Detection System sniff range validation fixed
- Asset Tracker removed
- New malware test page available
- National Vulnerability Database search fixed
- Rebranding

### Support for Cisco, Meraki, Netgear, and Huawei switches added, plus fixes

- Plugins have been added to support the Meraki MS225, NetGear XS712T, and Huawei S5720.
- The existing Cisco Catalyst plugin has been verified against the Cisco 3850.
- Improvements have been made to simultaneous blocking and unblocking of multiple assets.
- Attempts to quarantine an uplink port no longer result in invalid blocking rules being added.
- Switch names containing special characters (e.g., !@#$%) no longer cause blocking issues on Cisco or Dell switches.
- To avoid mistakes, user can no longer change switch model when editing switch configuration.

### Replication filter and flush utility added

Replication of assets between appliances will no longer include system assets representing the appliance itself or its interfaces. There is also a new utility under Command Center | Remote Operations Configuration that allows the replication list to be purged from all connected appliances. This can be used if the asset list has grown unmanageable or contains unwanted assets. Once purged, the list will be rebuilt on the next replication cycle.

### Manage Appliances and Manage Groups simplified

The appliance and group management pages under Command Center have been simplified, with obsolete functionality removed and the remaining functions replaced with a new streamlined interface. Manage Appliances allows the managed appliance list to be reviewed and edited, and Manage Groups allows similar functions with groups. The old Group Wizard has been removed completely.

### Asset Detection System sniff range validation fixed

IP address range validation on the Asset Detection System page has been fixed, so that incorrect ranges such as 192.168.2-4.1.154 (note the last period) are no longer accepted.

## Asset Tracker removed

The asset tracker functionality has been removed as it is no longer consistent with the goals of the product.

## New malware test page available

Visiting the page at http://malware-test.netshieldcorp.com will trigger a malware detection event if the Malware Detection System is enabled. Use this page to test your malware and blocking configuration.

## National Vulnerability Database search fixed

Initiating a CVE search from the Audits | National Vulnerability Database page will take the user directly to the latest page on that CVE at the official NVD site.

## Rebranding

As part of our transition from SnoopWall to NETSHIELD Corporation, some text and logos in the user interface have been updated.

# NETSHIELD / Version 10.1 Patch 22 / November 20, 2017

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 22 includes the following:

- Support for Nortel, ProCurve, Cisco, 3Com, and Extreme switches added
- Support for console on serial port added
- Support for manual malware hosts import added
- IP change notifications simplified
- Software update bug fixed
- Asset import/export bugs fixed
- Manage Assets display bugs fixed
- NTP configuration bug fixed
- Added malware block testing page

### Support for Nortel, ProCurve, Cisco, 3Com, and Extreme switches added

- Plugins have been added to support the Nortel 55xx, ProCurve 54xx, and Cisco SG-500 switches.
- The existing Cisco Catalyst plugin has been verified against the Cisco 3750.
- The original plugins to support 3Com and Extreme switches have been replaced with improved versions.
- The generic ProCurve plugin has been fixed to handle later firmware.

### Support for console on serial port added

The appliance console is now available via serial cable. For models that do not include a serial port, the use of a USB-USB null modem cable is also supported. Contact NetSHIELD support for information about compatible cables.

### Support for manual malware hosts import added

A list of malware hosts can now be imported directly into the Malware Detection System, rather than entering them individually.

### IP change notifications simplified

Previously, changes to an asset's IP address were indicated with two separate notifications that used an all-zeros IP address to indicate a missing asset. Changes to an asset's IP address are now reflected in a single notification with a simplified message body.

### Software update bug fixed

A bug that was preventing software updates from being disabled has been fixed.

### Asset import/export bugs fixed

- A bug that was causing imports of large numbers of assets (> 1000) to fail has been fixed.

- Missing assets can now be exported.
- Importing a list of MACs as assets will assign all-zero IP addresses to the assets, instead of 254.254.254.254.
- Error messages regarding missing detection times on import have been removed.

## Manage Assets display bugs fixed

- Assets representing VLAN interfaces are now correctly displayed as system assets.
- In the Missing Assets display, all-zero IP addresses are now displayed as “Unassigned”.

## NTP configuration bug fixed

A bug that was causing manual date/time entry to fail has been fixed.

## Added malware block testing page

Visiting the page http://www.snoopwall.com/malware-test on a monitored asset will now trigger a malware detection event. This is useful for testing the malware detection configuration.

# NETSHIELD / Version 10.1 Patch 21 / October 31, 2017

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 21 includes the following:

- HP ProCurve Support
- Dashboard Performance Fix

### HP ProCurve Support

The HP ProCurve switch plugin has been updated to work correctly with the new switch API. It will support most non-modular HP ProCurve switches.

### Dashboard Performance Fix

A bug that was causing the dashboard to display slowly on appliances with large network logs has been fixed.

# NETSHIELD / Version 10.1 Patch 20 / October 19, 2017

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 20 includes the following:

- Asset Detection Fix

### Asset Detection Fix

A bug that was causing intermittent interference with asset detection has been fixed.

# NETSHIELD / Version 10.1 Patch 19

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 19 includes the following:

- Support for Juniper, HP, and Alcatel switches
- Support for SANs in Certificate Generator
- Command Center in Branch Pro
- Syslog Events Fix
- Allow Multiple IPs Behavior Fix
- Blocking Delay on Class B Networks Fix
- Service Pack Updates from Console
- Miscellaneous Fixes

### Support for Juniper, HP, and Alcatel Switches

Support for Juniper, HP 1920, HP 5130, and Alcatel 62xx switches has been added to SmartSwitch Integration.

### Support for SANs in Certificate Generator

The certificate request generator under System | Manage Server Certificate now supports embedding a Subject Alternative Name (SAN) list into the request. Subject Alternative Name(s) replace the Common Name in the certificate. The SANs can be specified as a list of metadata (hostnames, IPs, email addresses, etc.) to associate with the certificate. It's required for all modern browsers to get the "green padlock". See the online documentation on Custom Certificates for instructions on using this feature.

### Command Center in Branch Pro

The Command Center feature is now available on the Branch Pro. The maximum number of managed appliances has been fixed at 1000 for all platforms.

### Syslog Events Fix

A bug that was preventing syslog events from being sent to remote servers has been fixed.

### Allow Multiple IPs Behavior Fixed

Assets configured to allow multiple IPs will no longer generate untrusted assets or incorrectly configured assets. If an asset with Allow Multiple IPs set changes its IP address, a new asset record will be created in the trusted state, with the new IP, and Allow Multiple IPs set to Yes.

### Blocking Delay on Class B Networks Fix

Blocking times on heavily loaded class B networks have been reduced significantly. However, be aware that a large number of untrusted assets will still limit how fast the appliance can handle a block request. Always trust known assets as soon as possible.

## Service Pack Updates from Console

The user can now update to the latest service pack using the appliance console.

## Miscellaneous Fixes

Blocking then immediately unblocking an asset now shuts off the block properly instead of leaving the asset trusted but blocked. An issue where not entering sniff ranges for every interface could generate errors in the Asset Detection System UI has been fixed. The wording on one of the ADS popups has been rewritten for clarity. The Ping Latency chart has been fixed to update while gathering data. Discoverable fields on the Edit Asset page have been made read-only, as asset detection updates will clear any user-entered information in these fields.

# NETSHIELD / Version 10.1 Patch 18

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 18 includes the following:

- Asset Detection and Blocking Fixes
- Changes to Documentation

### Asset Detection and Blocking Fixes

To improve performance on larger networks, we have retuned the asset detection and blocking for our new hardware platform, increasing asset queue throughput and reducing detection times. We have also cut down on the network traffic generated by our periodic asset sweeps. On the Asset Detection System page, a couple of small fixes include selecting DHCP and IP monitoring by default when turning on ARP detection, and filling in the block/protect range when selecting manual blocking.

### Changes to Documentation

The User Guide, Quick Start Guide, Readme, and Release Notes no longer appear in the Help menu. Instead, there is now a Documentation menu item that takes the user to our online support page, where they may browse the latest versions of these documents as well as FAQs, whitepapers, and other ongoing support features.

# NETSHIELD / Version 10.1 Patch 17

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 17 includes the following:

- Support for Cisco, Dell, and Alcatel Switches Added
- Policies and Regulations Removed
- Miscellaneous Fixes

### Support for Cisco, Dell, and Alcatel Switches Added

The following switches are now supported by SmartSwitch Integration:

- Cisco 3750
- Dell PowerConnect 6248, 5448, 5548
- Alcatel 6248

### Policies and Regulations Removed

As part of an effort to streamline the product and focus on essential functions, the Policies and Regulations menu and functionality has been removed, as well as the Regulations menu item under Appliance Setup.

### Miscellaneous Fixes

The header names in the Malware Log and report have been simplified. A bug that was affecting the Query Vulnerability feature has been fixed.

# NETSHIELD / Version 10.1 Patch 16

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 16 includes the following:

- Packet Sniffing Fix

### Packet Sniffing Fix

A bug has been fixed that was causing packet sniffing to halt under some circumstances after the Asset Detection System configuration was saved.

# NETSHIELD / Version 10.1 Patch 15

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 15 includes the following:

- Asset Detection Rate Limiting Update

### Asset Detection Rate Limiting Update

Adds 250 and 500 broadcasts per second to the ARP sweep rate limiter in the Asset Detection System.

# NETSHIELD / Version 10.1 Patch 14

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 14 includes the following:

- Asset Detection Rate Limiting
- Asset Detection System Advanced Options Cleanup

### Asset Detection Rate Limiting

Assets using outdated PLCs or network stacks may become overwhelmed by the ARP broadcast sweep the appliance periodically sends out to detect assets. The rate at which these packets are sent out can now be set in the Asset Detection System advanced options.

### Asset Detection System Advanced Options Cleanup

Several settings in the advanced options section of the Asset Detection System have been removed as they were obsolete or no longer applicable to the product.

# NETSHIELD / Version 10.1 Patch 13

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 13 includes the following:

- Extended Subnet Limits for Asset Discovery
- Added TLS Disable to Notifications
- Fixed System Statistics Disk Space Display
- Miscellaneous Fixes
- Updated User Guide

### Extended Subnet Limits for Asset Discovery

The subnet range that can be explored during Asset Discovery has been extended to a full class B.

### Added TLS Disable to Notifications

A “TLS Force Off” option has been added to notifications to allow the appliance to communicate with mail servers that are unable to handle TLS or STARTTLS.

### Fixed System Statistics Disk Space Display

The disk space display under System Statistics was displaying incorrect values and has been fixed.

### Miscellaneous Fixes

The malware download service has been fixed to properly handle an interrupted download.
A bug has been fixed that allowed a user to remain logged in across a reboot.

### Updated User Guide

The user guide available from the Help menu has been updated to the latest version.

# NETSHIELD / Version 10.1 Patch 12

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 12 includes the following:

- Switch Integration Fixes

### Switch Integration Fixes

Fixed issue with switch integration plugin for Dell N-Series switches that was interfering with VLAN Roaming and other functions. Removed Juniper from list of switches until new plugin is available.

# NETSHIELD / Version 10.1 Patch 11

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 11 includes the following:

- Malware Download Fix
- Miscellaneous Fixes

### Malware Download Fix

A bug that was corrupting malware signature files if the download was interrupted has been fixed.

### Miscellaneous Fixes

The deprecated Cisco and Custom plugins have been removed from SmartSwitch integration.

# NETSHIELD / Version 10.1 Patch 10

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 10 includes the following:

- Improved Network Status Page
- Fixes to Asset Detection and Malware Engine
- Miscellaneous Fixes

### Improved Network Status Page

The Network Status page now breaks out configuration and link states.

### Fixes to Asset Detection and Malware Engine

A bug that was occasionally preventing missing assets from displaying as active once detected has been fixed. The malware engine now properly resets the never-block cache when assets are removed from the never-block list.

### Miscellaneous Fixes

Background scans are no longer on by default or activated on factory reset.

# NETSHIELD / Version 10.1 Patch 9

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 9 includes the following:

- Command Center Fix

### Command Center Fix

A previous patch caused the Command Center menu to disappear for some appliances. The menu has been restored.

# NETSHIELD / Version 10.1 Patch 8

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 8 includes the following:

- Configurable Asset Auto-Removal
- Fixes to Asset Detection and Blocking
- Fixes to User Interface
- Miscellaneous Fixes

### Configurable Asset Auto-Removal

Under Asset Detection System, the user can now activate auto removal of assets that have not been detected, and specify the time period since detection.

### Fixes to Asset Detection and Blocking

A bug in the sniff range parser was causing incomplete ping sweeps for some range lists. Unblocking from the NetSHIELD Blocking List an asset will now correctly remove the Always Block state from an asset.

### Fixes to User Interface

Changing the Target VLAN setting under Edit Asset no longer fails. Malware Detection log now shows geolocation and search buttons for malware domains.

### Miscellaneous Fixes

The Network Information page under Network Configuration contains redundant information and has been removed. The user can no longer bring up the Edit Asset page for the appliance itself.

# NETSHIELD / Version 10.1 Patch 7

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 7 includes the following:

- Fixes to Command Center
- Fixes to Asset Detection
- Fixes to Malware Detection
- Miscellaneous Fixes

### Fixes to Command Center

A bug that was causing the wait animation to run forever when trusting or untrusting multiple assets on a remote appliance has been fixed.

### Fixes to Asset Detection

IP address changes to known assets will no longer cause new assets with random IP addresses to appear in Manage Assets. A bug that was causing imported assets to appear in the Replicated asset category has been fixed.

### Fixes to Malware Detection

A bug that was causing the malware detection engine to periodically restart has been fixed. Domains detected as part of a TLD entry are now properly removed from the blacklist when the TLD is removed.

### Miscellaneous Fixes

Appliance time will no longer be reset to NTP time on reboot if NTP is off. Factory reset will now shut down the appliance instead of rebooting it. A bug in the Active Directory login process has been fixed. Server certificates are now properly validated when uploaded.

# NETSHIELD / Version 10.1 Patch 6

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 6 includes the following:

- MAC Spoof Setting Fix
- Block/Sniff Range Fix for Class A/B Networks
- Edit Assets Update Fix
- Notification Protocol and Certificate Fix
- Miscellaneous Fixes

### MAC Spoof Setting Fix

A bug that was causing the asset detection engine to ignore the MAC Spoof Alert/Block setting has now been fixed. MAC Spoof alerts and blocks will only occur if they are explicitly turned on.

### Block/Sniff Range Fix for Class A/B Networks

On class A and B networks, the appliance was occasionally detecting and blocking assets outside the set range for certain ranges. This bug has been addressed.

### Edit Assets Update Fix

A bug that was causing the Edit Assets page to crash on updates has been fixed.

### Notification Protocol and Certificate Fix

The SMTP module for notifications has been updated to use TLSv11 and TLSv12 instead of TLSv1 when the later protocols are available. The list of allowed CA intermediate certificates has also been updated.

### Miscellaneous Fixes

The help text for Common Name under Manage Server Certificate has been brought in line with its actual function. Internal debugging logs have been added to the rotation list.

# NETSHIELD / Version 10.1 Patch 5

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 5 includes the following:

- Malware Engine Fix
- Documentation Revisions
- Asset Replication Fix
- Asset Management Fixes
- Inventory Alerts Fix
- Asset Report Fix
- Startup Performance Improvement
- Asset Detection Fix
- System Statistics Fix
- Missing Assets Behavior Enhancement
- Password Characters Fix

### Malware Engine Fix

Fixed a bug that was causing the malware engine to be periodically stopped and restarted.

### Documentation Revisions

Updated the documentation under the Help menu with the latest revisions.

### Asset Replication Fix

Assets on managed appliances now replicate properly to other appliances.

### Asset Management Fixes

Fixed a bug that was causing the appliance information to display improperly under Manage Assets, and another that was preventing the Edit Asset page from working properly.

### Inventory Alerts Fix

Inventory Alerts no longer sends out mistaken notifications for reachable assets.

### Asset Report Fix

Asset Report no longer hangs.

### Asset Detection Fix

Blocks now launch correctly if block range has range in 3$^{rd}$ octet.

### System Statistics Fix

System Statistics page no longer displays multiple duplicate login sessions.

## Missing Assets Behavior Enhancement

Assets that have not been detected for 30 days are now removed from the database.

## Password Characters Fix

Special characters ($, !, @, and so on) may now be used in passwords.

# NETSHIELD / Version 10.1 Patch 4

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 4 includes the following:

- Malware Download Fix

### Malware Download Fix

Fixes a bug that was causing malware signatures not to download under some circumstances.

# NETSHIELD / Version 10.1 Patch 3

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 3 includes the following:

- New User Guide
- Malware and Managed Appliance Blocking Improvements
- Expired License Key Entry Fix
- Restore Database Fix
- Command Center Configuration Export Fix
- Miscellaneous Bugs

### New User Guide

The new NetSHIELD User Guide is now available from the Help menu.

### Malware and Managed Appliance Blocking Fix

The performance and stability of asset blocking for the malware detection and managed appliance systems has been improved.

### Expired License Key Entry Fix

Fixed a bug that was not allowing license keys to be entered for an expired appliance.

### Restore Database Fix

Restore function now properly restores database entries from backup files.

### Command Center Configuration Export Fix

Command center will now correctly export configuration changes to managed appliances.

### Miscellaneous Fixes

Fixes to small bugs including shutdown script taking too long, changing date/time might hang asset queue, and reset asset limits.

# NETSHIELD / Version 10.1 Patch 2

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 2 includes the following:

- Lost License Issue

### Lost License Issue

Fixed a bug which would cause the appliance to lose its license on a restart if the appliance was unable to contact the update server.

# NETSHIELD / Version 10.1 Patch 1

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 1 includes the following:

- Asset Detection and Blocking Function and Performance
- Lost License Issue
- Fixes to NTP and Backup
- Miscellaneous Bugs

### Asset Detection and Blocking Function and Performance

An issue where deleting an asset under block would not cancel the block was fixed, and time from detection to block has been reduced. An IP address change during asset discovery is now handled properly. Assets are now blocked correctly on an appliance restart.

### Lost License Issue

An issue where the appliance would lose its license on startup has been fixed.

### Fixes to NTP and Backup

NTP can now be configured correctly, and appliance files can now be correctly restored.

### Miscellaneous Bugs

Small fixes to the support channel, asset tracker, and switch blocking have been made.

# NETSHIELD / Version 10.1 Patch 0

## Release Notes

***NetSHIELD Appliance*** version 10.1 Patch 0 includes the following:

- New Appliance Kernel

### New Appliance Kernel

The appliance is now running on an LTS 64-bit kernel, providing higher performance and greater stability for all NetSHIELD functions.