AV Defender version branching

The AV Defender 6.6.2.49 and 6.4.2.79 update introduces a split version for Security Manager users, based on the operating system of the device.

- **AV Defender 6.6.x for Windows Modern Operating Systems**: designed for Windows 7/Windows Server 2008 R2 and higher, this version no longer installs on legacy operating systems.
- **AV Defender 6.4.x for Windows Legacy Operating Systems**: designed for Windows XP and Windows Vista families, including corresponding embedded and server versions, this version does not install on modern operating systems.

AV Defender installations after this update will receive the version corresponding to the operating system.

Information on both branches are included in these release notes.

Security Manager | AV defender 6 is an integrated AV offering available for all Security Manager | AV Defender clients as a licensable option for users using SolarWinds N-central. Management and deployment are done through your Security Manager | AV Defender server.
AV Defender Version 6.6.2.49

Enhancements

New installations automatically get the latest version of Advanced Threat Control (ATC) 4.0.

ATC 4.0 highlights:

- Under-the-hood improvements deliver better proactive heuristics and allow faster response to new threats or false positives.
- Better detection of script-based and PowerShell attacks.
- ATC 4.0 groups related processes and evaluates actions for improved efficacy.
- Improved mechanism for detecting potential Process Doppelgänging attacks.
- Added support for the system variable `%AllUsersProfile%` to specify paths for product modules.

Resolved issues in this build

- The firewall module that caused critical errors (BSOD) when using the Linux Subsystem on endpoints running Windows 10 "Redstone 1" or "Redstone 4".
- The issue that prevented quarantined files from being restored on network paths when using the local user interface.
- The issue that caused high RAM usage on Relay and many queued endpoints connections in specific situations.
- Relay issue causing the error code 87 when deploying the product through Relay as well as other Relay issues.
- Advanced Threat Control causing a critical error (BSOD) when using CodeSoft.
- The issue with Advanced Threat Control that prevented CCH Prosystems Tax from being installed on endpoints.
- Issue causing error when applying a policy with already existing settings.
AV Defender Version 6.4.2.79

Enhancements

- Improved mechanism for detecting potential Process Doppelgänging attacks.
- Added support for the system variable \%AllUsersProfile\% to specify paths for product modules.

Resolved issues in this build

- Fixed an issue that prevented quarantined files from being restored on network paths when using the local user interface.
AV Defender Version 6.2.36.1014

Enhancements

- Added support for the installation of the March 13th Microsoft security patches (KB4088877, KB4088880, ADV180002) for Windows Server 2012, Windows Server 2008 and Windows 8 Embedded.
- To configure an email address in the About window so that it opens the default email application on the endpoint, it must be added with the "mailto:" prefix in the policy. The "mailto:" prefix is no longer displayed in the About window.
- Introduced a Signature Update fallback mechanism that loads the last working antimalware signatures in case of faulty updates.
- Added support for uninstalling the following incompatible security products:
  - McAfee Endpoint Security Adaptive Threat Protection
  - McAfee Product Improvement Program
  - McAfee Client Proxy

Resolved issues in this build

- Fixed an issue where saving Excel files accessed from the network resulted in temporary files not being deleted.
- Fixed an issue where Content Control was blocking an application from connecting to the console port of an equipment.
- Fixed an issue where Content Control was blocking access to the nest.com web page.
- Fixed a compatibility issue with Symantec DLP solution causing problems with file downloads and video streaming in some cases.
- Fixed an issue that caused Content Control to block an internal application.
- Fixed an issue that caused Content Control to block SSL websites in Google Chrome.
- In some cases, Content Control was slowing down the Oracle application. The issue is now fixed.
- In some cases, files from Quarantine were not properly deleted. The issue is now fixed.
- Fixed an issue with firewall blocking RDP connections in the local network when the Network Discovery option was set to Remote.
- Fixed an issue where the Relay was not removing older versions of malware signatures.
- Fixed an issue causing error message -2009 when trying to update the product via Relay.
- Some Microsoft Lync Server 2013 recommended locations were missing from the built-in exclusions. The issue is now fixed.
- Repairing the installation while the Endpoint Security Service was not running resulted in AV Defender being uninstalled. The issue is now fixed.
AV Defender Version 6.2.31.985

Enhancements

- Made various improvements across the product for better detection and faster access of network shares.
- Added compatibility with Mozilla Firefox 58.0 for SSL traffic scanning.
- Local users can no longer restore files to paths protected by Windows User Account Control.

Resolved issues in this build

- In some situations, the users could experience slowdowns for applications running from Samba network shares. The issue is now fixed.
- Fixed an issue where the Firewall module did not start after upgrading from very old versions.
- Fixed a communication issue that occurred on Windows Server 2003 after upgrading to the new version of Update Server.
- Fixed an issue with on-access scanning blocking the execution of Potentially Unwanted Applications (PUA) even though the option to scan for PUA was disabled.
- Fixed an issue with Microsoft Exchange Server 2016 where the product failed to scan emails after Cumulative Update 8.
AV Defender Version 6.2.28.973

Enhancements

- Added support for installation of January 3rd Microsoft security patches (KB4056892, KB4056890, KB4056898, KB4056897). This update will automatically deliver a specific registry key that enables the delivery of these security patches through Windows Update.
- Improved the scanning for fileless attacks.

Resolved issues in this build

- Fixed an issue where the Application Control log folder increased in size until it filled the disk.
- Fixed an issue where Content Control was still processing some web pages when disabled.
- Fixed an issue where the upgrade failed due to a ‘looped’ uninstallation of the previously installed product.
- An issue caused multiple tmp* folders being created in C:\Windows\Temp by the scanning engine has been resolved.
- Fixed an issue where a device scanning task started for each user logged on the endpoint.
- In some situations, scheduled Full Scan tasks were running twice. The issue is now fixed.
- Fixed an issue where Scan SSL activation was blocking Google Hangouts.
- Web Access Control exclusions failed to apply for websites which included, in their URLs, a similar group of letters as the ones from the Internet domain name (i.e. *ru). The issue is now fixed.
- Fixed the failed redirection of the product Signatures and ThreatScanner folders onto Thawed partition on endpoints with Faronics Deep Freeze.
- Fixed an Update Server issue, which sometimes failed to communicate with the endpoints as expected.
- Fixed an issue where, in some cases, the Bitdefender security services blocked the terminal server after a certain number of sessions.
- An issue which caused the Firewall module to malfunction due to a stopped driver has been resolved.
- Fixed an issue occurred on some Citrix PVS systems where the product installation failed at 82% with BSOD after restart when the Firewall was also installed.
- Addressed a proxy server issue that prevented the endpoints to connect to Bitdefender cloud services.
- Fixed an incompatibility with Windows Firewall that caused network issues on Windows 7 endpoints after updating the product to version 6.2.24.937.
- A conflict between Bitdefender and Windows Firewall caused connectivity issues.
- Fixed the error code 3 occurred during the signature update, which caused the endpoints to appear as outdated.
- Fixed an issue where HTTPS web pages were blocked on some machines because the security certificate validation was taking too long.
- Fixed the vulnerability FG-VD-17-019 reported by the Fortinet FortiGuard Labs through responsible disclosure.
- Addressed a vulnerability discovered by Hossein Lotfi, Secunia Research at Flexera Software, and reported through responsible disclosure.
- Fixed the error code 3, received during signature update.
- Fixed the delayed connection to an RDS Server that occurred when on-access scanning was enabled.
- Fixed an issue where Windows Firewall Configuration Provider was detected as an incompatible security product.
- Fixed an incompatibility issue of the Content Control module with Avaya application.
- Fixed an issue where the product did not support MAC addresses with lowercase letters for networks defined in the security policies.
- On certain Windows Server machines, the product signatures were being reported as out of date in Control Center. The issue is now fixed.
- Fixed an issue where the product was downgrading to a previous version when using a silent installation.

Known issues

- Only one Anti-malware event is generated for an archive with multiple infected files when the Scan Action is set to Take No Action.
AV Defender Version 6.2.19.899

Enhancements

- Made several improvements to the installation process to address the removing of incompatible security products, the replacement of Endpoint Security by Bitdefender versions and the cleaning procedure.
- Bitdefender Endpoint Security Tools is now compatible with Windows Server Core 2016.

Resolved issues in this build

- A compatibility issue with the latest update from Microsoft on Windows 8.1 and Windows Server 2012 R2 systems.
- Fixed the Microsoft Application Verifier vulnerability CVE-2017-6186.
- The Firewall module was disabled after upgrading the operating system from Windows 7 to Windows 10 Creators Update.
- Fixed issue where endpoints were automatically restarting during the product update, although the “Postpone reboot” option was selected and “If needed, reboot after installing updates” was disabled in the security policy settings.
- Fixed issue where the option “Take no action”, configured in Control Center for infected and suspicious files detected at on-access scanning, was automatically changed to “Deny access” when opening the Power User mode.
- Fixed issue that caused 100% CPU usage when using a proxy with Kerberos/NTLM authentication.
AV Defender Version 6.2.19.890

Enhancements

- Improved submission options for 3rd party integrations.
- AVC and anti-malware are now the only modules available for Windows XP and 2003.

Resolved issues in this build

- In some situations, the scheduled on-demand scan tasks started immediately after the endpoints resumed from sleep or hibernation.
- An edge case where scheduled scan tasks from the past started when the user applied a policy on a new endpoint.
- Assignment rules were in some cases incorrectly applied on SSID for wireless connection.
- An issue where increased Internet traffic generated on endpoints when various proxy servers were configured in Internet Explorer.
- BSOD generated by Firewall module during boot process after upgrade to Windows 10 has been resolved.
- Critical error occurred where starting certain Windows 8.1 applications via Application Jukebox Player.
- In some situations, endpoints in large networks and with Bitdefender Endpoint Security Tools installed were sending Internet Control Message Protocol (ICMP) broadcasts that generated high volumes of network traffic.
- Occasionally, Internet browsers were experiencing temporary connectivity losses when AVC was installed on endpoint. The issue is now fixed.
- Addressed an issue where starting a Reconfigure Client task during malware signature update affected the Bitdefender update service.
- Internet Explorer plugin issue caused browser to stop working when accessing specific URLs and Antiphising module was active.
- An issue occurred where the applied Firewall rules did not preserve Power User setting.
- An issue where the handshake.html or refresh.html files were being downloaded in the browser when accessing some secured websites, such as LinkedIn or banking websites, while the ScanSSL was enabled via new Content Control components.
- In some cases, Critical issue (BSOD) on full scan was reported.
- After changing the update server download location the signatures were unable to be downloaded. The issue is now resolved.
- An issue where upgrades from endpoint security v5 to v6 was failing has been resolved.

Known issues

The product installation may not work on Windows Vista, Windows 7, Windows Server 2008 and Windows Server R2 operating systems due to a known Microsoft issue. This is not related to Bitdefender and can be fixed on Windows 7 and Windows Server 2008 R2 with this KB article.
AV Defender Version 6.2.15.860

Enhancements

- Notification pop-ups can now be enabled or disabled based on the module and severity of the events.
- The AVC module has further controls by blocking unauthorized applications and processes from running.
- The Anti-Ransomware vaccine, which immunizes endpoints against known ransomware, has now been added.
- Added support for Anti-exploit techniques that further augments existing technologies to fight targeted attacks.
- Improved protection mechanism to enhance malware detection rate.

Resolved issues in this build

- In some situations, the configured proxy servers were not being used.
- Filters were not properly applied for certain web categories in AVC, in some cases.
- BSOD occurred, in some cases, for the AVC module that was enabled on Windows Server 2012 R2 machines.
- Error 160 that occurred on scheduled reboots after update when set hour was only a single digit.
- Vulnerability OpenSSL CVE-2016-6304 was addressed.
- An issue where high CPU usage in virtual environments with NTLM Proxy has been resolved.
- Slow down caused on certain VMware workstations has been addressed.
- Locked hard-drive issue where endpoints running Windows Server 2012/R2 at server reboot with Device Control activated has been resolved.
- Delayed reboot on Windows 7 32-bit systems has been resolved.
AV Defender Version 6.2.9.799

Enhancements

- Improvement to the protection mechanism which enhances the malware detection rate.
- Support for Windows 10 Redstone.
- Support for Scan SSL in the Firefox 64-bit browser.
- Built-in antimalware exclusions mechanism has been improved.
- Integrated OpenSSL version 1.0.1s.
- Added exclusions for Systems Center Configuration Manager 2012 (SCCM 2012) following Microsoft recommendations.
- All packages now archive with WinRAR version 5.31.
- Improved product and signatures update verification mechanisms.
- Made several improvements to the installation process that address the replacement of previous versions.
- Improved the signature updating mechanism.
- Improved endpoint resource consumption during update operations.
- Improved cleanup process on install.
- Improved memory usage.

Resolved issues in this build

- In some situations, Windows 10 systems displayed BSOD when scanning EFS encrypted files through the File System Redirector.
- Fixed the ZDI-CAN-3749 and ZDI-CAN-3829 vulnerabilities reported by ZeroDay Initiative through responsible disclosure.
- OpenSSL vulnerability CVE-2016-2017 was remedied.
- An issue where the DataProtection module incorrectly blocked web pages based on partial word match.
- Installation error code 234 occurred, in some situations, when the Firewall Module was installed.
- In some situations, when the user was logged in Windows, the desktop icon did not appear in the Windows Notifications area and all protections modules were disabled.
- In some situations, the deployment was unsuccessful when installing the Firewall module.
- Firewall rules using the environment variable %localappdata% was not applying to the endpoints.
- Fixed an issue that was preventing users from creating or updating certain security certificates.
- In some situations, websites with self-signed certificates did not load using the Advanced option in Google Chrome when SSL scan was enabled.
- Device Control reports contained false blocked events on devices that were not used at the time.
- An issue that caused on-access scanning to turn off and return error message “Could not connect to Security Server” has been resolved.
- An issue where Content Control had prevented emails from being downloaded to Thunderbird and Outlook.
- Addressed several scenarios that were causing product crashes.
- Fixed an issue that was causing Windows 10 systems to enter in recovery mode after installing the product and rebooting the machine.
- Fixed a BSOD with a REFERENCE_BY_POINTER error, occurred on Windows 10 Professional x64 systems during scanning the encrypted folder C:\Windows\CSC.
- Error code 1460, received when on-demand scans tasks were run.
- Fixed an issue with Firewall profiles which were improperly set when using unusual network masks.
- Content Control was cropping incoming emails.
- BSOD occurred in rare situations when installing the product with Content Control module.
- Addressed failed installation scenario in which the notification message improperly displayed installation was successful.
- AVC module that was causing backups to fail when using VSS and Veeam.
- Web page load failure in Google Chrome version 38.0.2125.101 when AVC was enabled.
- A corner case was discovered that prevented full scans from completing successfully.
- Addressed a vulnerability that implied the possibility of remote execution.
- In some situations, HP machines with specific hardware configuration were starting Windows OS in recovery mode.
- In some situations, update to endpoints was not performed.
- The firewall module was malfunctioning on certain Windows 10 machines, when added and with Content Control enabled.
- In some situations, scans that finished immediately were displayed with 0% scan progress.
- The security agent reconfiguration failed when an uninstall password was set.
- In some specific situations, the product downloaded a higher amount of signatures than necessary during update.
- If the update required a reboot and the reboot was scheduled with day and hour of the week, only the hour was taken into account.
- In some situations, the security agent used an abnormally large amount of RAM.
- The Firewall module could not install on endpoint after system upgrade to Windows 10.
- Microsoft Surface Pro tablets were improperly detected as virtual machines.
- After upgrade to Windows 10, the Firewall module was reported as disabled in the Windows Action Center.
- Installation was crashing one endpoints with high CPU usage.
- In some situations, the agent deployment on Windows 8.1 systems had failed.
- Built-in firewall rules issues occurred when accessing an Active Directory domain or when connecting through Remote Desktop Connection.
- In some situations, when repairing the product files and a system reboot was required, the system entered a reboot loop.
- Blocked process occurred in certain situations, was causing the endpoint to run slow.