U-Series Appliance Hardening Reference

This guide provides a reference for the hardening techniques applied to your Windows Server 2022 U-Series Appliance.

Due to the nature of the data contained within an appliance and the operational roles it performs, BeyondTrust has secured the platform with multiple layers of security to ensure the attack risk surface is as minimal as technologically possible. This includes using software security solutions embedded in the product, restricting access to the operating system, restricting the installation of third-party applications, not allowing outbound browser communications, and hardening the solution to industry standards.

Security Technology

The U-Series Appliance contains operating system hardening and multiple layers of security to prevent an attack. Below are configuration, software, best practices, and design considerations implemented in order to protect the appliance from malicious activity.

Configuration Changes

- Feature Based Access:
  - Windows services are enabled or disabled as needed, based on the features enabled on the appliance.
  - Components are logically separated and can be hardened individually.
  - Windows Server service is disabled by default.
- Limited Exposed Services:
  - All non-required services are disabled and uninstalled.
  - Support for third-party software installations is prohibited, except where noted in supported "Appliance Software Extensions and Modifications" on page 2 below.
  - Changing the configuration of appliance features is not permitted.
- Windows Firewall is enabled:
  - All non-essential inbound ports are disabled, except those used by BeyondTrust software.

Software Protection

- Microsoft Windows Defender
- BeyondTrust Endpoint Privilege Management

Design Consideration

- Automatic backup with encryption and password protection is configured.

Security Best Practices

- Browser communications required over HTTPS
- User installable SSL certificates

- Disabled local browser
- RDP access disabled by default
- Complex password required for all configurations
- Hardened to Center for Internet Security (CIS) and Security Technical Implementation Guides (STIGs) standards

Secure Auto Update

- BeyondTrust Updater:
  - Embedded on the appliance.
  - Provides proxy services and change management for updates.
  - SSL is required for updates on appliances.
  - Updates are validated by serial number for licenses.
  - Updated binaries (contents) are digitally signed.
- Security Update Package Installer (SUPI):
  - Secure download of pre-screened and validated Windows Updates.
  - Install process can be performed locally or initiated remotely.
- BeyondTrust U-Series Appliances adhere to the following schedule for risk mitigation:
  - Operating system and database critical vulnerabilities not mitigated by Appliance Hardening and Security: 7 days from patch release.
  - Operating system and database critical vulnerabilities mitigated by Appliance Hardening and Security: 90 Days from patch release.
  - BeyondTrust critical vulnerabilities regardless of type: 30 days from identification.

Encryption

- Credentials stored within Password Safe are protected using AES256.
- Password Safe data in transit is encrypted with TLS v1.2.

Appliance Software Extensions and Modifications

- Joining the appliance to a Microsoft Windows domain is permitted, only when the instructions are provided by a BeyondTrust Support representative and they are strictly followed. Failure to follow the given procedure exactly can decrease the hardening of the appliance and lead to technical problems with its normal operation.
- The following third-party vendor supplied software is supported for installation on the appliance by end users:
  - Thales for HSM Integration

> ***Note:*** *The installation of any third-party software on the appliance, or modifications to the appliance, its settings or its associated software, that are not explicitly referenced within this guide, or are implemented without the guidance of a BeyondTrust representative, may void your warranty.*

Center for Internet Security Compliance Report

CIS is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

The CIS Controls and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals. The U-Series Appliances produced by BeyondTrust are hardened to the CIS Benchmark for Windows Server 2022, Level 2 Member Server as a profile.

Reference

- CIS Homepage: https://www.cisecurity.org/
- CIS Benchmark for Microsoft Windows Server 2022 Benchmark: https://www.cisecurity.org/benchmark/microsoft_windows_server/
- Level 2 Member Server profile

Security Technical Implementation Guides

STIGs provide configurable operational security guidance for products being used by the DoD.

The appliances produced by BeyondTrust are regularly scanned against the Security Content Automation Program (SCAP) checklist, as defined by NIST. The results of these scans are listed below.

Assessment Summary

- Score - 99%
  - Passed: 218
  - Not Applicable: 53
  - Open: 4
    - CAT I: 0
    - CAT II: 4
    - CAT III: 0
- DISA STIG v1.2.3
- Appliance Image: 2023-R10

> ***Note:** A list of the **Not Applicable** findings can be provided upon request.*

Open Findings

Category 11:

- Windows Server 2022 must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs (V-254245, WN22-00-000080).

  - Response: The appliance hardening includes BeyondTrust Endpoint Privilege Management for Windows; however, it is not configured in a deny-all, permit-by-exception policy out-of-the-box.
- Windows Server 2022 must have a host-based intrusion detection or prevention system (V-254249, WN22-00-000120).
  - Response: The appliance doesn't include a built-in HIDS or HIPS system; however, it does provide log exporting capabilities. Logs can be exported and consumed by the customer's own HIDS/HIPS system.
- Windows Server 2022 system files must be monitored for unauthorized changes (V-254259, WN22-00-000220).
  - Response: The appliance hardening includes file integrity monitoring (FIM); however, it doesn't monitor against a baseline on a weekly basis.
- Windows Server 2022 generates security audits user right must only be assigned to Local Service and Network Service (V-254502, WN22-UR-000120).
  - Response: Service accounts associated with BeyondTrust applications require permissions to generate security audits.

> ***Note:*** *The following STIG recommended hardening modifications, found in* ***Security and Compliance > Local Computer Policy*** *in the web console, were applied prior to scanning:*
>
> - ***LAN Manager Authentication Level*** *is set to* ***Send NTLMv2 esponse only. Refuse LM &NTLM****. Out of the box, the appliance is configured to* ***Send NTLMv2 response only. Refuse LM****.*
> - ***FIPS Mode*** *is enabled.*