

| Component | OS Type | OS Version                           | System Type | OS Kernel Version                                                                                                                                    | OS Release Date | Support Situation | Minimum Supported Version | Note: Installation reminder                                                                                                      |
|-----------|---------|--------------------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|           | CentOS  | CentOS 5                             | 64-bit      | 2.6.18-8.el5                                                                                                                                         | 12/Apr/2007     | Excluded          |                           | This version is excluded, and no custom package or technical support is provided.                                                |
|           |         | CentOS 5                             | 32-bit      | 2.6.18-8.el5                                                                                                                                         | 12/Apr/2007     | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 5.6                           | 32-bit      | 2.6.18-238.el5                                                                                                                                       | 8/Apr/2011      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 5.6                           | 64-bit      | 2.6.18-238.el5                                                                                                                                       | 8/Apr/2011      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6                             | 64-bit      | 2.6.32-71.el6.x86_64                                                                                                                                 | 10/Jul/2011     | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.1                           | 32-bit      | 2.6.32-131.0.15.el6.i686                                                                                                                             | 9/Nov/2011      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.1                           | 64-bit      | 2.6.32-131.0.15.el6.x86_64                                                                                                                           | 9/Nov/2011      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.2                           | 64-bit      | 2.6.32-220.el6.x86_64                                                                                                                                | 20/Dec/2011     | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.3                           | 32-bit      | 2.6.32-279.el6.i686                                                                                                                                  | 9/Jul/2012      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.3                           | 64-bit      | 2.6.32-279.el6.x86_64                                                                                                                                | 9/Jul/2012      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.4                           | 64-bit      | 2.6.32-358.el6.x86_64                                                                                                                                | 9/Mar/2013      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.5                           | 32-bit      | 2.6.32-431.el6.i686                                                                                                                                  | 1/Dec/2013      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.5                           | 64-bit      | 2.6.32-431.el6.x86_64                                                                                                                                | 1/Dec/2013      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.6                           | 32-bit      | 2.6.32-504.el6.i686                                                                                                                                  | 28/Oct/2014     | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.6                           | 64-bit      | 2.6.32-504.el6.x86_64                                                                                                                                | 28/Oct/2014     | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.7                           | 64-bit      | 2.6.32-573.el6.x86_64                                                                                                                                | 7/Aug/2015      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.8                           | 32-bit      | 2.6.32-642.el6.i686                                                                                                                                  | 25/May/2016     | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.8                           | 64          | 2.6.32-642.el6.x86_64                                                                                                                                | 25/May/2016     | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.9                           | 64          | 2.6.32-696.el6.x86_64                                                                                                                                | 5/Apr/2017      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.10                          | 32          | 2.6.32-754.el6.i686                                                                                                                                  | 3/Jul/2018      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 6.10                          | 64          | 2.6.32-754.el6.x86_64                                                                                                                                | 3/Jul/2018      | Excluded          |                           |                                                                                                                                  |
|           |         | CentOS 7                             | 64          | 3.10.0-123.el7.x86_64                                                                                                                                | 7/Jul/2014      | Supported         | 6.0.4.3341R4              | Specific features are supported. For detailed information on supported features, see the Supported Features sheet.               |
|           |         | CentOS 7.1                           | 64          | 3.10.0-229.el7.x86_64                                                                                                                                | 31/Mar/2015     | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 7.2                           | 64          | 3.10.0-327.el7.x86_64                                                                                                                                | 14/Dec/2015     | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 7.3                           | 64          | 3.10.0-514.el7.x86_64                                                                                                                                | 12/Dec/2016     | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 7.4                           | 64          | 3.10.0-693.el7.x86_64<br>3.10.0-693.el7.x86_64                                                                                                       | 13/Sep/2017     | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 7.5                           | 64          | 3.10.0-862.el7.x86_64<br>5.17.3-1.el7.elrepo.x86_64                                                                                                  | 10/May/2018     | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 7.6                           | 64          | 3.10.0-957.el7.x86_64                                                                                                                                | 3/Dec/2018      | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 7.7                           | 64          | 3.10.0-1062.el7.x86_64                                                                                                                               | 17/Sep/2019     | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 7.8                           | 64          | 3.10.0-1127.el7.x86_64                                                                                                                               | 27/Apr/2020     | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 7.9                           | 64          | 3.10.0-1160.25.1.el7.x86_64<br>5.17.3-1.el7.elrepo.x86_64<br>5.18.0-1.el7.elrepo.x86_64<br>5.19.3-1.el7.elrepo.x86_64<br>5.4.278-1.el7.elrepo.x86_64 | 12/Nov/2020     | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 8                             | 64          | 4.18.0-80.el8.x86_64<br>4.18.0-193.28.1.el8_2.x86_64                                                                                                 | 24/Sep/2019     | Supported         | 6.0.4.3341R4              | Specific features are supported. For detailed information on supported features, see the Supported Features sheet.               |
|           |         | CentOS 8.1                           | 64          | 4.18.0-147.el8.x86_64                                                                                                                                | 15/Jan/2020     | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS Linux release 8.1.1911 (Core) | 64          | 4.18.0-147.5.1.el8_1.x86_64                                                                                                                          |                 | Partial Support   | 6.0.4.3341R4              | not support advanced threat-related features.                                                                                    |
|           |         | CentOS 8.2                           | 64          | 4.18.0-193.el8.x86_64                                                                                                                                | 15/Jun/2020     | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 8.3                           | 64          | 4.18.0-240.el8.x86_64                                                                                                                                | 7/Dec/2020      | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 8.4                           | 64          | 4.18.0-305.3.1.el8.x86_64                                                                                                                            | 3/Jun/2021      | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS 8.5                           | 64          | 4.18.0-348.el8.x86_64                                                                                                                                | 16/Nov/2021     | Supported         | 6.0.4.3341R4              |                                                                                                                                  |
|           |         | CentOS Stream 9                      | 64          | 5.14.0-148.el9.x86_64<br>5.14.0-514.el9.x86_64<br>5.14.0-533.el9.x86_64<br>5.14.0-612.el9.x86_64<br>5.14.0-645.el9.x86_64<br>5.14.0-722.el9.x86_64   | 3/Dec/2021      | Supported         | 6.0.4.3571R4 (SP9)        | This operating system does not support advanced threat-related features.                                                         |
|           |         | CentOS Stream 10 (Coughlan)          | 64          | 6.12.0-170.el10.x86_64                                                                                                                               |                 | Supported         | 6.0.4.3581R4 (SP10)       | This operating system does not support advanced threat-related features.                                                         |
|           |         |                                      | 64          | 6.12.0-248.el10.x86_64                                                                                                                               |                 | Supported         | 6.0.4.3581R4 (SP10)       | This operating system does not support advanced threat-related features.No support for host isolation and domain name isolation. |
|           |         | Ubuntu 10.04                         | 32          | 2.6.32-38-generic-pae                                                                                                                                | 29/Apr/2010     | Excluded          |                           | This version is excluded, and no custom package or technical support is provided.                                                |
|           |         | Ubuntu 10.04.4                       | 32          | 2.6.32-38-generic-pae                                                                                                                                | 16/Feb/2012     | Excluded          |                           |                                                                                                                                  |
|           |         | Ubuntu 10.04.4                       | 64          | 2.6.32-38-server                                                                                                                                     | 16/Feb/2012     | Excluded          |                           |                                                                                                                                  |
|           |         | Ubuntu 11.04                         | 64          | 2.6.38-8-server                                                                                                                                      | 28/Apr/2011     | Excluded          |                           |                                                                                                                                  |
|           |         | Ubuntu 12.04.3                       | 32          | 3.8.0-29-generic                                                                                                                                     | 23/Aug/2013     | Excluded          |                           |                                                                                                                                  |
|           |         | Ubuntu 12.04.3                       | 64          | 3.8.0-29-generic                                                                                                                                     | 23/Aug/2013     | Excluded          |                           |                                                                                                                                  |
|           |         | Ubuntu 13.04                         | 32          | 3.8.0-19-generic                                                                                                                                     | 25/Apr/2013     | Excluded          |                           |                                                                                                                                  |
|           |         | Ubuntu 13.04                         | 64          | 3.8.0-19-generic                                                                                                                                     | 25/Apr/2013     | Excluded          |                           |                                                                                                                                  |
|           |         | Ubuntu 14.04.1                       | 32          | 3.13.0-32-generic                                                                                                                                    | 24/Jul/2014     | Excluded          |                           |                                                                                                                                  |
|           |         | Ubuntu 14.04.1                       | 64          | 3.13.0-32-generic                                                                                                                                    | 24/Jul/2014     | Excluded          |                           |                                                                                                                                  |

Only supports  
CentOS 7, Ubuntu  
18.04, Debian 9.1,  
Red Hat Enterprise  
Linux 7.1, SUSE 15,  
Oracle 8.x, or later

|        |                                 |    |                                                                                |             |                 |                       |                                                                                                                               |
|--------|---------------------------------|----|--------------------------------------------------------------------------------|-------------|-----------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Ubuntu | Ubuntu 16.04                    | 32 | 4.4.0-210-generic                                                              | 21/Apr/2016 | Excluded        |                       |                                                                                                                               |
|        | Ubuntu 16.04                    | 64 | 4.4.0-186-generic                                                              | 21/Apr/2016 | Excluded        |                       |                                                                                                                               |
|        | Ubuntu 17.04                    | 64 | 4.10.0-19-generic                                                              | 13/Apr/2017 | Excluded        |                       |                                                                                                                               |
|        | Ubuntu 18.04                    | 64 | 4.15.0-192-generic                                                             | 26/Apr/2018 | Supported       | 6.0.4.3341R4          | Specific features are supported. For detailed information on supported features, see the Supported Features sheet.            |
|        | Ubuntu 18.04.1                  | 64 | 4.15.0-29-generic                                                              | 26/Jul/2018 | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 18.04.2                  | 64 | 4.18.0-15-generic                                                              | 15/Feb/2019 | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 18.04.3                  | 64 | 5.0.0-23-generic                                                               | 8/Aug/2019  | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 18.04.4                  | 64 | 5.3.0-28-generic                                                               | 12/Feb/2020 | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 18.04.5                  | 64 | 5.4.0-42-generic                                                               | 13/Aug/2020 | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 18.04.6                  | 64 | 4.15.0-156-generic                                                             | 17/Sep/2021 | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        |                                 |    | 5.4.0-84-generic                                                               | 17/Sep/2021 | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 20.04                    | 64 | 5.4.0-126-generic                                                              | 23/Apr/2020 | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 20.04.1                  | 64 | 5.4.0-26-generic<br>5.8.0-28-generic<br>5.11.0-22-generic<br>5.13.0-21-generic | 6/Aug/2020  | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 20.04.2                  | 64 | 5.8.0-43-generic                                                               | 4/Feb/2021  | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 20.04.3                  | 64 | 5.11.0-27-generic                                                              | 26/Aug/2021 | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 20.04.4                  | 64 | 5.13.0-30-generic                                                              | 24/Feb/2022 | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 20.04. 5 LTS             | 64 | 5. 4. 0-125-generic                                                            |             | Partial Support | 6.0.4.3341R4          | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|        | Ubuntu 20.04. 6 LTS             | 64 | 5. 4. 0-144-generic                                                            |             | Partial Support | 6.0.4.3341R4          | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|        | Ubuntu 20.04.2                  | 64 | 5.15.0-46-generic                                                              | 4/Feb/2021  | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 23. 04                   | 64 | 6. 2. 0-39-generic                                                             |             | Supported       | 6. 0. 4. 3571R4 (SP9) | This operating system does not support advanced threat-related features.                                                      |
|        | Ubuntu 22.04                    | 64 | 5.15.0-47-generic                                                              | 21/Apr/2022 | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 22. 04. 1 LTS            | 64 | 5. 15. 0-43-generic                                                            |             | Partial Support | 6.0.4.3341R4          | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|        | Ubuntu 22. 04. 2 LTS            | 64 | 5. 15. 0-60-generic                                                            |             | Partial Support | 6.0.4.3341R4          | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|        | Ubuntu 22. 04. 3 LTS            | 64 | 5. 15. 0-78-generic                                                            |             | Partial Support | 6.0.4.3341R4          | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|        | Ubuntu 22.04.5                  | 64 | 5.15.0-25<br>5.15.0-151-generic<br>5.19.0-41<br>6.2.0-25-generic               |             | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 24.04.1                  | 64 | 6.8.0-31<br>6.8.0-52                                                           |             | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 24.04. 2 LTS             | 64 | 6. 8. 0-53-generic                                                             |             | Partial Support | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 24.04. 3 LTS             | 64 | 6. 8. 0-71-generic<br>6. 14. 0-37-generic                                      |             | Partial Support | 6.0.4.3341R4          | This operating system does not support advanced threat-related features.                                                      |
|        | Ubuntu 24.04. 4 LTS             | 64 | 6. 8. 0-100-generic                                                            |             | Partial Support | 6.0.4.3341R4          |                                                                                                                               |
|        | Ubuntu 24. 10                   | 64 | 6. 11. 0-29-generic                                                            |             | Supported       | 6. 0. 4. 3571R4 (SP9) | This operating system does not support advanced threat-related features.                                                      |
|        | Ubuntu 25. 04                   | 64 | 6. 14. 0-15-generic<br>6. 14. 0-37-generic                                     |             | Supported       | 6. 0. 4. 3571R4 (SP9) | This operating system does not support advanced threat-related features.                                                      |
|        | Ubuntu 25. 10 (Questing Quokka) | 64 | 6. 17. 0-5-generic                                                             | 9/Oct/2025  | Supported       | 6. 0. 4. 3571R4 (SP9) | This operating system does not support advanced threat-related features.                                                      |
|        | Ubuntu 26. 04 LTS               | 64 | 7. 0. 0-14-generic<br>7. 0. 0-15-generic<br>7. 0. 0-22-generic                 |             | Supported       | 6.0.4.3581R4 (SP10)   | This operating system does not support advanced threat-related features.                                                      |
|        | Debian 6.0.0                    | 32 | 2.6.32-5-686                                                                   | 6/Feb/2011  | Excluded        |                       | This version is excluded, and no custom package or technical support is provided.                                             |
|        | Debian 6.0.0                    | 64 | 2.6.32-5-amd64                                                                 | 6/Feb/2011  | Excluded        |                       | This version is excluded, and no custom package or technical support is provided.                                             |

|        |                                   |       |                                                                      |             |           |                     |                                                                                                                    |
|--------|-----------------------------------|-------|----------------------------------------------------------------------|-------------|-----------|---------------------|--------------------------------------------------------------------------------------------------------------------|
| Debian | Debian 7.7                        | 32    | 3.2.0-4-686-pae                                                      | 18/Oct/2014 | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 7.7                        | 64    | 3.2.0-4-amd64                                                        | 18/Oct/2014 | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.0.0                      | 64    | 3.16.0-4-amd64                                                       | 25/Apr/2015 | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.0.0                      | 32    | 3.16.0-4-686-pae                                                     | 25/Apr/2015 | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.1                        | 64    | 3.16.0-4-amd64                                                       | 6/Jun/2015  | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.1                        | 32    | 3.16.0-4-686-pae                                                     | 6/Jun/2015  | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.2                        | 64    | 3.16.0-4-amd64                                                       | 5/Sep/2015  | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.4                        | 32    | 3.16.0-4-686-pae                                                     | 2/Apr/2016  | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.4                        | 64    | 3.16.0-4-amd64                                                       | 2/Apr/2016  | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.7.1                      | 32    | 3.16.0-4-686-pae                                                     | 14/Jan/2017 | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.7.1                      | 64    | 3.16.0-4-amd64                                                       | 14/Jan/2017 | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.8.0                      | 64    | 3.16.0-4-686-pae                                                     | 6/May/2017  | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.8.0                      | 32    | 3.16.0-4-amd64                                                       | 6/May/2017  | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.10.0                     | 64    | 3.16.0-4-amd64                                                       | 9/Dec/2017  | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 8.10.0                     | 32    | 3.16.0-4-686-pae                                                     | 9/Dec/2017  | Excluded  |                     | This version is excluded, and no custom package or technical support is provided.                                  |
|        | Debian 9.1.0                      | 64    | 4.9.0-3-amd64                                                        | 22/Jul/2017 | Supported | 6.0.4.3341R4        | Specific features are supported. For detailed information on supported features, see the Supported Features sheet. |
|        | Debian 9.1.0                      | 32    | 4.9.0-3-686-pae                                                      | 22/Jul/2017 | Supported | 6.0.4.3341R4        |                                                                                                                    |
|        | Debian 9.13.0                     | 64    | 4.9.0-13-amd64                                                       | 18/Jul/2020 | Supported | 6.0.4.3341R4        |                                                                                                                    |
|        | Debian 9.13.0                     | 32    | 4.9.0-13-686-pae                                                     | 18/Jul/2020 | Supported | 6.0.4.3341R4        |                                                                                                                    |
|        | Debian 9.6.0                      | 64    | 4.9.0-8-amd64                                                        | 10/Nov/2018 | Supported | 6.0.4.3341R4        |                                                                                                                    |
|        | Debian 9.6.0                      | 32    | 4.9.0-8-686-pae                                                      | 10/Nov/2018 | Supported | 6.0.4.3341R4        |                                                                                                                    |
|        | Debian 9.7.0                      | 64    | 4.9.0-8-amd64                                                        | 23/Jan/2019 | Supported | 6.0.4.3341R4        |                                                                                                                    |
|        | Debian 9.7.0                      | 32    | 4.9.0-8-686-pae                                                      | 23/Jan/2019 | Supported | 6.0.4.3341R4        |                                                                                                                    |
|        | Debian 9.11                       | 32/64 | 4.9.0-11-amd64                                                       |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian GNU/Linux 10.13 (buster)   | 32/64 | 4.19.0-27-amd64                                                      |             | Supported | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                           |
|        | Debian GNU/Linux 11.0 (bullseye)  | 32/64 | 5.10.0-8-amd64                                                       |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian GNU/Linux 11.2 (bullseye)  | 32/64 | 5.10.0-10-amd64                                                      |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian GNU/Linux 11.3 (bullseye)  | 32/64 | 5.10.0-13-amd64                                                      |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian 11.4                       | 32/64 | 5.10.0-16-amd64                                                      |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian GNU/Linux 11.5 (bullseye)  | 32/64 | 5.10.0-18-amd64                                                      |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian GNU/Linux 11.6 (bullseye)  | 32/64 | 5.10.0-20-amd64                                                      |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian GNU/Linux 11.7 (bullseye)  | 32/64 | 5.10.0-22-amd64                                                      |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian GNU/Linux 11.8 (bullseye)  | 32/64 | 5.10.0-26-amd64                                                      |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian 11.9                       | x64   | 5.10.0-28<br>6.1.0-27                                                |             | Supported | 6.0.4.3341R4        |                                                                                                                    |
|        | Debian GNU/Linux 11.10 (bullseye) | x64   | 5.10.0-30-amd64                                                      |             | Supported | 6.0.4.3581R4 (SP10) |                                                                                                                    |
|        | Debian 11.11                      | 32/64 | 5.10.0-37-amd64                                                      |             | Supported | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                           |
|        | Debian GNU/Linux 12.0 (bookworm)  | 32/64 | 6.1.0-9-amd64                                                        |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian GNU/Linux 12.1 (bookworm)  | 32/64 | 6.1.0-10-amd64                                                       |             | Supported | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                           |
|        | Debian GNU/Linux 12.2 (bookworm)  | 32/64 | 6.1.0-13-amd64<br>6.1.0-41-amd64                                     |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian GNU/Linux 12.4             | 32/64 | 6.1.0-15-amd64                                                       |             | Supported | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                           |
|        | Debian 12.5                       | x64   | 6.1.0-18<br>6.1.0-27                                                 |             | Supported | 6.0.4.3341R4        |                                                                                                                    |
|        | Debian GNU/Linux 12.6 (bookworm)  | 32/64 | 6.1.0-22-amd64                                                       |             | Supported | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                           |
|        | Debian GNU/Linux 12.7 (bookworm)  | 32/64 | 6.1.0-25-amd64                                                       |             | Supported | 6.0.4.3571R4 (SP9)  |                                                                                                                    |
|        | Debian GNU/Linux 12.8 (bookworm)  | 32/64 | 6.1.0-27-amd64                                                       |             | Supported | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                           |
|        | Debian 12.9                       | 32/64 | 6.1.0-29-amd64                                                       |             | Supported | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                           |
|        | Debian GNU/Linux 12.10 (bookworm) | x64   | 6.1.0-28-amd64<br>6.1.0-33-amd64<br>6.1.0-34-amd64<br>6.1.0-32-amd64 |             | Supported | 6.0.4.3581R4 (SP10) |                                                                                                                    |
|        | Debian 12.11                      | 32/64 | 6.1.0-37-amd64                                                       |             | Supported | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                           |
|        | 飞牛Fn0S (Debian 12.12)             | 32/64 | 6.12.18-trim                                                         |             | Supported | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                           |
|        | Debian GNU/Linux 12.12 (bookworm) | x64   | 6.1.0-39-amd64                                                       |             | Supported | 6.0.4.3581R4 (SP10) |                                                                                                                    |
|        | Debian GNU/Linux 12.13 (bookworm) | x64   | 6.1.0-42-amd64<br>6.1.0-44-amd64                                     |             | Supported | 6.0.4.3581R4 (SP10) |                                                                                                                    |

|                  |                  |                                                 |     |                                                    |             |                 |                     |                                                                                                                               |
|------------------|------------------|-------------------------------------------------|-----|----------------------------------------------------|-------------|-----------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Athena EPP Agent | Debian GNU/Linux | Debian GNU/Linux 12.14 (bookworm)               | x64 | 6.1.0-47-amd64                                     |             | Partial Support | 6.0.4.3571R4 (SP9)  | Please contact TAC for the Agent installation method.                                                                         |
|                  |                  | Debian GNU/Linux 13.0 (trixie)                  | x64 | 6.12.38+deb13-amd64                                |             | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                      |
|                  |                  | Debian GNU/Linux 13.1 (trixie)                  | x64 | 6.12.43+deb13-amd64                                |             | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
|                  |                  | Debian GNU/Linux 13.2 (trixie)                  | x64 | 6.12.57+deb13-amd64                                | 9/Aug/2025  | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
|                  |                  | Debian GNU/Linux 13.3 (trixie)                  | x64 | 6.12.63+deb13-amd64                                |             | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                      |
|                  |                  |                                                 | x64 | 6.8.12-17-pve                                      |             | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                      |
|                  |                  | Debian GNU/Linux 13.4 (trixie)                  | x64 | 6.12.73+deb13-amd64                                |             | Partial Support | 6.0.4.3591R4 (SP11) | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|                  |                  | Debian GNU/Linux 13.5 (trixie)                  | x64 | 6.12.86+deb13-amd64<br>6.12.95+deb13-amd64         |             | Partial Support | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
|                  |                  | Debian GNU/Linux 13.6 (trixie)                  | x64 | 6.12.94+deb13-amd64                                |             | Partial Support | 6.0.4.3591R4 (SP11) | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|                  | Red Hat          | Red Hat Enterprise Linux 5.4                    | 64  | 2.6.18-164.el5                                     | 2/Sep/2009  | Excluded        |                     | This version is excluded, and no custom package or technical support is provided.                                             |
|                  |                  | Red Hat Enterprise Linux 5.6                    | 64  | 2.6.18-238.el5                                     | 13/Jan/2011 | Excluded        |                     |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 6                      | 32  | 2.6.32-71.el6.i686                                 | 9/Nov/2010  | Excluded        |                     |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 6                      | 64  | 2.6.32-71.el6.x86_64                               | 9/Nov/2010  | Excluded        |                     |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 6.2                    | 32  | 2.6.32-220.el6.i686                                | 6/Dec/2011  | Excluded        |                     |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 6.2                    | 64  | 2.6.32-220.el6.x86_64                              | 6/Dec/2011  | Excluded        |                     |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 6.4                    | 32  | 2.6.32-358.el6.i686                                | 21/Feb/2013 | Excluded        |                     |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 6.4                    | 64  | 2.6.32-358.el6.x86_64                              | 21/Feb/2013 | Excluded        |                     |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 6.7                    | 32  | 2.6.32-573.el6.i686                                | 22/Jul/2015 | Excluded        |                     |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 6.7                    | 64  | 2.6.32-573.el6.x86_64                              | 22/Jul/2015 | Excluded        |                     |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 6.9                    | 32  | 2.6.32-696.el6.i686                                | 21/Mar/2017 | Excluded        |                     | Specific features are supported. For detailed information on supported features, see the Supported Features sheet.            |
|                  |                  | Red Hat Enterprise Linux 6.9                    | 64  | 2.6.32-696.el6.x86_64                              | 21/Mar/2017 | Excluded        |                     |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux Server 7.0 (Maipo)     | 64  | 3.10.0-123.el7.x86_64                              |             | Supported       | 6.0.4.3581R4 (SP10) |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 7.1                    | 64  | 3.10.0-229.el7.x86_64                              | 5/Mar/2015  | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 7.3                    | 64  | 3.10.0-514.el7.x86_64                              | 3/Nov/2016  | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 7.4                    | 64  | 3.10.0-693.el7.x86_64                              | 31/Jul/2017 | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 7.5                    | 64  | 3.10.0-862.el7.x86_64                              | 10/Apr/2018 | Supported       | 6.0.4.3571R4 (SP9)  |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 7.6                    | 64  | 3.10.0-957.el7.x86_64<br>5.5.4-1.el7.elrepo.x86_64 | 30/Oct/2018 | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 7.7                    | 64  | 3.10.0-1062.el7.x86_64                             | 6/Aug/2019  | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 7.9                    | 64  | 3.10.0-1160.el7.x86_64                             | 29/Sep/2020 | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 8                      | 64  | 4.18.0-80.el8.x86_64                               | 7/May/2019  | Supported       | 6.0.4.3341R4        | This operating system does not support advanced threat-related features.                                                      |
|                  |                  | Red Hat Enterprise Linux 8.1 (Ootpa) (RHEL 8.1) | 64  | 4.18.0-147.el8.x86_64                              |             | Supported       | 6.0.4.3571R4 (SP9)  |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 8.2                    | 64  | 4.18.0-193.el8.x86_64                              | 28/Apr/2020 | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 8.3 (Ootpa)            | 64  | 4.18.0-240.el8.x86_64                              |             | Supported       | 6.0.4.3571R4 (SP9)  |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 8.4                    | 64  | 4.18.0-293.el8.x86_64                              |             | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 8.5                    | 64  | 4.18.0-348.el8.x86_64                              |             | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 8.6                    | 64  | 4.18.0-372.9.1.el8.x86_64                          |             | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 8.7                    | 64  | 4.18.0-425.3.1.el8.x86_64                          |             | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 8.8                    | 64  | 4.18.0-477.10.1.el8_8.x86_64                       |             | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 8.9                    | 64  | 4.18.0-513.5.1.el8_9.x86_64                        |             | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|                  |                  | Red Hat Enterprise Linux 8.10 (Ootpa)           | 64  | 4.18.0-553.el8_10.x86_64                           |             | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
|                  |                  | Red Hat Enterprise Linux 9.0                    | 64  | 5.14.0-70<br>5.14.0-427<br>5.14.0-547              |             | Supported       | 6.0.4.3341R4        |                                                                                                                               |

|      |                                          |    |                                             |             |                 |                     |                                                                                                                                |
|------|------------------------------------------|----|---------------------------------------------|-------------|-----------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------|
|      | Red Hat Enterprise Linux 9.1             | 64 | 5.14.0-162                                  |             | Supported       | 6.0.4.3341R4        |                                                                                                                                |
|      | Red Hat Enterprise Linux 9.2             | 64 | 5.14.0-284                                  |             | Supported       | 6.0.4.3341R4        |                                                                                                                                |
|      | Red Hat Enterprise Linux 9.3             | 64 | 5.14.0-362                                  |             | Supported       | 6.0.4.3341R4        |                                                                                                                                |
|      | Red Hat Enterprise Linux 9.4             | 64 | 5.14.0-427.13.1.el9_4.x86_64                |             | Supported       | 6.0.4.3341R4        |                                                                                                                                |
|      | Red Hat Enterprise Linux 9.5 (Plow)      | 64 | 5.14.0-503.11.1.el9_5.x86_64                |             | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                       |
|      | Red Hat Enterprise Linux 9.6 (Plow)      | 64 | 5.14.0-570.12.1.el9_6.x86_64                |             | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                       |
|      | Red Hat Enterprise Linux 9.7 (Plow)      | 64 | 5.14.0-611.5.1.el9_7.x86_64                 |             | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                       |
|      | Red Hat Enterprise Linux 9.8 (Plow)      | 64 | 5.14.0-687.5.3.el9_8.x86_64                 |             | Partial Support | 6.0.4.3591R4 (SP11) | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features.  |
|      | Red Hat Enterprise Linux 10.0 (Coughlan) | 64 | 6.12.0-55.9.1.el10_0.x86_64                 |             | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                       |
|      | Red Hat Enterprise Linux 10.2 (Coughlan) | 64 | 6.12.0-211.7.3.el10_2.x86_64                |             | Partial Support | 6.0.4.3581R4 (SP10) | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features.  |
| SUSE | SUSE 11.x                                |    | /                                           | 24/Mar/2009 | Excluded        |                     | This version is excluded, and no custom package or technical support is provided.                                              |
|      | SUSE Linux Enterprise Server 12 GA       | 64 | 3.12.28-4-default                           |             | Supported       | 6.0.4.3571R4 (SP9)  | Need to pay attention to the function support boundary                                                                         |
|      | SUSE Linux Enterprise Server 12 SP1      | 64 | 3.12.49-11-default<br>3.12.59-60.45-default |             | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                       |
|      | SUSE Linux Enterprise Server 12 SP2      | 64 | 4.4.21-69-default                           |             | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                       |
|      | SUSE Linux Enterprise Server 12 SP3      | 64 | 4.4.73-7-default                            |             | Partial Support | 6.0.4.3341R4        | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features.  |
|      | SUSE Linux Enterprise Server 12 SP4      | 64 | 4.12.14-94.41-default                       |             | Supported       | 6.0.4.3571R4 (SP9)  | Need to pay attention to the function support boundary                                                                         |
|      | SUSE Linux Enterprise Server 12 SP5      | 64 | 4.12.14-120-default                         |             | Supported       | 6.0.4.3571R4 (SP9)  | Need to pay attention to the function support boundaryThis operating system does not support advanced threat-related features. |
|      | SUSE Linux Enterprise Server 15 SP1      | 64 | 4.12.14-195-default                         |             | Partial Support | 6.0.4.3341R4        | Need to pay attention to the function support boundary                                                                         |
|      | SUSE Linux Enterprise Server 15 SP2      | 64 | 5.3.18-22-default                           |             | Partial Support | 6.0.4.3341R4        | Need to pay attention to the function support boundary                                                                         |

|              |                                     |       |                                         |             |                 |                       |                                                                                                                               |
|--------------|-------------------------------------|-------|-----------------------------------------|-------------|-----------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------|
|              | SUSE Linux Enterprise Server 15 SP3 | 64    | 5. 3. 18-57-default                     |             | Partial Support | 6.0.4.3341R4          | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|              | SUSE Linux Enterprise Server 15 SP4 | 64    | 5. 14. 21-150400. 22-default            |             | Partial Support | 6.0.4.3341R4          | Need to pay attention to the function support boundary                                                                        |
|              | SUSE Linux Enterprise Server 15 SP5 | 64    | 5.14.21-150500.53-default               |             | Partial Support | 6.0.4.3341R4          | This operating system does not support advanced threat-related features.                                                      |
|              | SUSE Linux Enterprise Server 15 SP6 | 64    | 6. 4. 0-150600. 21-default              |             | Partial Support | 6.0.4.3341R4          | This operating system does not support advanced threat-related features.                                                      |
|              | SUSE Linux Enterprise Server 15 SP7 | 64    | 6. 4. 0-150700. 51-default              |             | Partial Support | 6.0.4.3341R4          | This operating system does not support advanced threat-related features.                                                      |
|              | SUSE 15                             |       | /                                       | 16/jul/2018 | Supported       | 6.0.4.3341R4          | Specific features are supported. For detailed information on supported features, see the Supported Features sheet.            |
|              | SUSE Linux Enterprise Server 16.0   | 64    | 6. 12. 0-160000. 5-default              | 4/Nov/2025  | Supported       | 6.0.4.3581R4 (SP10)   | This operating system does not support advanced threat-related features.                                                      |
| Oracle Linux | Oracle Linux 5.x                    | 32/64 |                                         | 1/jun/2007  | Excluded        |                       | This version is excluded, and no custom package or technical support is provided.                                             |
|              | Oracle Linux 6.x                    | 32/64 |                                         | 1/Feb/2011  | Excluded        |                       |                                                                                                                               |
|              | Oracle Linux Server 7.0             | 64    | 3. 8. 13-35. 3. 1. e17uek. x86_64       |             | Supported       | 6.0.4.3581R4 (SP10)   | This operating system does not support advanced threat-related features.                                                      |
|              | Oracle Linux Server 7.1             | 64    | 3. 8. 13-55. 1. 6. e17uek. x86_64       |             | Supported       | 6.0.4.3581R4 (SP10)   | This operating system does not support advanced threat-related features.                                                      |
|              | Oracle Linux Server 7.2             | 64    | 3. 8. 13-98. 7. 1. e17uek. x86_64       |             | Supported       | 6.0.4.3581R4 (SP10)   | This operating system does not support advanced threat-related features.                                                      |
|              | Oracle Linux Server 7.3             | 64    | 4. 1. 12-61. 1. 18. e17uek. x86_64      |             | Supported       | 6.0.4.3581R4 (SP10)   | This operating system does not support advanced threat-related features.                                                      |
|              | Oracle Linux Server 7.4             | 64    | 4.1.12-94.3.9.e17uek.x86_64             |             | Supported       | 6. 0. 4. 3571R4 (SP9) | This operating system does not support advanced threat-related features.                                                      |
|              | Oracle Linux Server 7.5             | 64    | 4.1.12-112.16.4.e17uek.x86_64           |             | Supported       | 6.0.4.3581R4 (SP10)   | This operating system does not support advanced threat-related features.                                                      |
|              | Oracle Linux Server 7.6             | 64    | 4. 14. 35-1818. 3. 3. e17uek. x86_64    |             | Partial Support | 6.0.4.3341R4          | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|              | Oracle Linux Server 7.7             | 64    | 4. 14. 35-1902. 3. 2. e17uek. x86_64    |             | Supported       | 6.0.4.3581R4 (SP10)   | This operating system does not support advanced threat-related features.                                                      |
|              | Oracle Linux Server 7.8             | 64    | 4. 14. 35-1902. 300. 11. e17uek. x86_64 |             | Supported       | 6.0.4.3581R4 (SP10)   | This operating system does not support advanced threat-related features.                                                      |
|              | oracle Linux server 7.9             | 64    | 5. 4. 17-2102. 201. 3. e17uek. x86_64   |             | Supported       | 6. 0. 4. 3571R4 (SP9) | This operating system does not support advanced threat-related features.                                                      |
|              | Oracle Linux 8.x                    | 64    | /                                       | 1/jul/2019  | Supported       | 6.0.4.3341R4          | Specific features are supported. For detailed information on supported features, see the Supported Features sheet.            |
|              | Oracle Linux 9.x                    | 64    |                                         | 1/jun/2022  | Supported       | 6.0.4.3341R4          |                                                                                                                               |
| AlmaLinux    | Oracle Linux Server 10.1            | 64    |                                         |             | Supported       | 6.0.4.3581R4 (SP10)   | This operating system does not support advanced threat-related features.                                                      |
|              | AlmaLinux 8.3                       | 64    | /                                       |             | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|              | AlmaLinux 8.4 (Electric Cheetah)    | 64    | 4. 18. 0-305. e18. x86_64               |             | Supported       | 6. 0. 4. 3571R4 (SP9) | This operating system does not support advanced threat-related features.                                                      |
|              | AlmaLinux 8.5 (Arctic Sphynx)       | 64    | 4. 18. 0-348. e18. x86_64               |             | Supported       | 6. 0. 4. 3571R4 (SP9) | This operating system does not support advanced threat-related features.                                                      |
|              | AlmaLinux 8.6 (Sky Tiger)           | 64    | 4. 18. 0-372. 9. 1. e18. x86_64         |             | Supported       | 6. 0. 4. 3571R4 (SP9) |                                                                                                                               |
|              | AlmaLinux 8.7 (Stone Smilodon)      | 64    | 4. 18. 0-425. 3. 1. e18. x86_64         |             | Supported       | 6. 0. 4. 3571R4 (SP9) |                                                                                                                               |
|              | AlmaLinux 8.8 (Sapphire Caracal)    | 64    | 4.18.0-477.10.1.el8_8.x86_64            |             | Supported       | 6.0.4.3581R4 (SP10)   |                                                                                                                               |
|              | AlmaLinux 8.9                       | 64    | /                                       |             | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|              | AlmaLinux 9.0 (Emerald Puma)        | 64    |                                         |             | Supported       | 6.0.4.3581R4 (SP10)   |                                                                                                                               |
|              | AlmaLinux 9.1 (Lime Lynx)           | 64    |                                         |             | Supported       | 6. 0. 4. 3571R4 (SP9) | This operating system does not support advanced threat-related features.                                                      |
|              | AlmaLinux 9.2                       | 64    |                                         |             | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|              | AlmaLinux 9.3                       | 64    |                                         |             | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|              | AlmaLinux 9.4                       | 64    |                                         |             | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|              | AlmaLinux 9.5                       | 64    |                                         |             | Supported       | 6.0.4.3341R4          |                                                                                                                               |
|              | AlmaLinux 9.6                       | 64    |                                         |             | Supported       | 6. 0. 4. 3571R4 (SP9) | This operating system does not support advanced threat-related features.                                                      |
|              | AlmaLinux 9.7 (Moss Jungle Cat)     | 64    | 5. 14. 0-570. 52. 1. e19_6. x86_64*rt   |             | Supported       | 6. 0. 4. 3571R4 (SP9) | This operating system does not support advanced threat-related features.                                                      |

|             |                                          |    |                                                                                              |  |                 |                     |                                                                                                                               |
|-------------|------------------------------------------|----|----------------------------------------------------------------------------------------------|--|-----------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------|
|             | AlmaLinux 9.8 (Olive Jaguar)             | 64 | 5.14.0-687.5.3.el9_8.x86_64                                                                  |  | Partial Support | 6.0.4.3581R4 (SP10) | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|             | AlmaLinux 10.0 (Purple Lion)             | 64 | 6.12.0-55.30.1.el10_0.x86_64                                                                 |  | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                      |
|             | AlmaLinux 10.1 (Heliotrope Lion)         | 64 | 6.12.0-124.20.1.el10_1.x86_64                                                                |  | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                      |
|             | AlmaLinux 10.2 (Lavender Lion)           | 64 | 6.12.0-211.7.3.el10_2.x86_64                                                                 |  | Partial Support | 6.0.4.3581R4 (SP10) | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
| Rocky Linux | Rocky Linux release 8.3                  | 64 | 4.18.0-240.22.1.el8.x86_64                                                                   |  | Supported       | 6.0.4.3571R4 (SP9)  |                                                                                                                               |
|             | Rocky Linux 8.4                          | 64 |                                                                                              |  | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|             | Rocky Linux release 8.5 (Green Obsidian) | 64 | 4.18.0-348.el8.0.2.x86_64                                                                    |  | Supported       | 6.0.4.3571R4 (SP9)  |                                                                                                                               |
|             | Rocky Linux 8.6 (Green Obsidian)         | 64 | 4.18.0-372.9.1.el8.x86_64                                                                    |  | Supported       | 6.0.4.3571R4 (SP9)  |                                                                                                                               |
|             | Rocky Linux 8.7                          | 64 |                                                                                              |  | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|             | Rocky Linux 8.8                          | 64 |                                                                                              |  | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|             | Rocky Linux 8.9 (Green Obsidian)         | 64 | 4.18.0-513.5.1.el8_9.x86_64                                                                  |  | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
|             | Rocky Linux 8.10                         | 64 | 4.18.0-553.el8_10.x86_64<br>4.18.0-553.40.1.el8_10.x86_64                                    |  | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|             | Rocky Linux 9.0 (Blue Onyx)              | 64 | 5.14.0-70.13.1.el9_0.x86_64                                                                  |  | Supported       | 6.0.4.3581R4 (SP10) |                                                                                                                               |
|             | Rocky Linux 9.1 (Blue Onyx)              | 64 | 5.14.0-162.6.1.el9_1.x86_64                                                                  |  | Supported       | 6.0.4.3581R4 (SP10) |                                                                                                                               |
|             | Rocky Linux 9.2                          | 64 | 5.14.0-284.11.1.el9_2.x86_64                                                                 |  | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|             | Rocky linux 9.3 (Blue Onyx)              | 64 | 5.14.0-362.8.1.el9_3.x86_64                                                                  |  | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
|             | Rocky Linux release 9.4 (Blue Onyx)      | 64 | 5.14.0-427.13.1.el9_4.x86_64                                                                 |  | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
|             | Rocky Linux 9.5 (Blue Onyx)              | 64 | 5.14.0-503.14.1.el9_5.x86_64                                                                 |  | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
|             | Rocky Linux 9.6 (Blue Onyx)              | 64 | 5.14.0-570.17.1.el9_6.x86_64<br>5.14.0-570.33.2.el9_6.x86_64<br>5.14.0-570.33.2.el9_6.x86_64 |  | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
|             | Rocky Linux 9.7 (Blue Onyx)              | 64 | 5.14.0-611.9.1.el9_7.x86_64<br>5.14.0-611.5.1.el9_7.x86_64                                   |  | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
|             | Rocky Linux release 10.0 (Red Quartz)    | 64 | 6.12.0-55.12.1.el10_0.x86_64                                                                 |  | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                      |
|             | Rocky Linux 10.1 (Red Quartz)            | 64 | 6.12.0-124.8.1.el10_1.x86_64<br>6.12.0-124.45.1.el10_1.x86_64                                |  | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                      |
|             | Rocky Linux 10.2 (Red Quartz)            | 64 | 6.12.0-211.16.1.el10_2.0.1.x86_64                                                            |  | Partial Support | 6.0.4.3581R4 (SP10) | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|             | Alibaba Cloud Linux 3.2104 LTS           | 64 | 5.10.134-18.al8.x86_64                                                                       |  | Supported       | 6.0.4.3341R4        |                                                                                                                               |
|             | Alibaba Cloud Linux 2.1903 LTS           | 64 | 4.19.91-28.2.al7.x86_64<br>4.19.91-28.5.al7.x86_64                                           |  | Supported       | 6.0.4.3341R4        |                                                                                                                               |

|                     |                                                       |    |                                                    |  |                 |                     |                                                                                                                               |
|---------------------|-------------------------------------------------------|----|----------------------------------------------------|--|-----------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Alibaba Cloud Linux | Alibaba Cloud Linux 3.2104 U11 (OpenAnolis Edition)   | 64 | 5.10.134-18.al8.x86_64                             |  | Partial Support | 6.0.4.3341R4        | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|                     | Alibaba Cloud Linux 3.2104 U10 (Pro Edition)          | 64 | 5.10.134-010.ali5000.pro.al8.x86_64                |  | Partial Support | 6.0.4.3341R4        | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|                     | Alibaba Cloud Linux 3.2104 U13.3 (OpenAnolis Edition) | 64 | 5.10.134-19.8.al8.x86_64                           |  | Supported       | 6.0.4.3601R4 (SP12) |                                                                                                                               |
| PlatOS              | PlatOS 1.3 (LTS)                                      | 64 | 4.18.0-372.85.1.192.p01.x86_64                     |  | Supported       | 6.0.4.3341R4        |                                                                                                                               |
| CloudLinux          | CloudLinux 8.8 (Anatoly Filipchenko)                  | 64 | 4.18.0-477.10.1.lve.e18.x86_64                     |  | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
|                     | CloudLinux 8.10 (Vladimir Aksyonov)                   | 64 | 4.18.0-553.lve.e18.x86_64                          |  | Supported       | 6.0.4.3571R4 (SP9)  | This operating system does not support advanced threat-related features.                                                      |
| Fedora              | Fedora Linux 44 (Server Edition)                      | 64 | 6.19.10-300.fc44.x86_64                            |  | Partial Support | 6.0.4.3581R4 (SP10) | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
| veLinux             | veLinux 1.0 (Debian GNU/Linux 10.9 (buster))          | 64 | 5.4.250-10-velinux1u4-amd64                        |  | Partial Support | 6.0.4.3601R4 (SP12) | Please contact TAC for the Agent installation method.This operating system does not support advanced threat-related features. |
|                     | veLinux 1.0 CentOS (CentOS Linux 7.9)                 | 64 | 5.4.250-9.2.ve1.x86_64                             |  | Supported       | 6.0.4.3601R4 (SP12) | This operating system does not support advanced threat-related features.                                                      |
|                     | veLinux 2.0 CentOS (CentOS Stream 9)                  | 64 | 5.15.152-7.1.ve2.x86_64<br>5.15.152-7.4.ve2.x86_64 |  | Supported       | 6.0.4.3601R4 (SP12) | This operating system does not support advanced threat-related features.                                                      |
| Amazon              | Amazon Linux 2023.11.20260514                         | 64 | 6.18.25-57.109.amzn2023.x86_64                     |  | Supported       | 6.0.4.3581R4 (SP10) | This operating system does not support advanced threat-related features.                                                      |