MaxPatrol VM версия 2.0

Список поддерживаемых систем

Дата редакции документа: 07.07.2023

Содержание

1. Об этом документе

Документ содержит информацию об основных системах, которые Positive Technologies MaxPatrol VM (далее также — MaxPatrol VM) может сканировать в режиме пентеста, идентификации узлов и на которых может обнаруживать уязвимости.

Документ адресован специалистам, выполняющим установку и интеграцию MaxPatrol VM в организации. Рекомендуется применять документ как источник дополнительной информации о MaxPatrol VM одновременно с другими руководствами по продукту.

Комплект документации MaxPatrol VM включает в себя следующие документы:

— Этот документ.

— Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.

— Руководство оператора — содержит сценарии использования продукта для управления информационными активами организации.

— Руководство по настройке источников — содержит рекомендации по интеграции элементов IT-инфраструктуры организации с MaxPatrol VM для аудита активов.

— Синтаксис языка запроса PDQL — содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с MaxPatrol VM.

В этом разделе

Условные обозначения (см. раздел 1.1)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом

Пример	Описание
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

2. Операционные системы

В этом разделе представлена информация об операционных системах, которые поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста ОС и их версии могут не определиться.

Таблица 2. Операционные системы

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
«РЕД ОС»	7.1—7.3	–	+	+ Только для версии 7.3
ALT Linux	8 СП, 9, 10	–	+	+
Astra Linux CE	Последняя версия	–	+	+
Astra Linux SE	1.5—1.7	–	+	+ Только для версии 1.7
CentOS Linux	7	+	+	+
Debian Linux	8—11	+	+	+
HP HP-UX	11.31	–	+	–
IBM AIX	7	–	+	–
Red Hat Enterprise Linux	4—9	+	+	+
Microsoft Windows	2000, XP, Server 2003, Vista, Server 2008, 7, Server 2008 R2, 8, Server 2012, 8.1, Server 2012 R2, 10 (1507) — 10 (21H2), Server 2016, Server 2019, 11, Server 2022	+	+	+
openSUSE Leap	42.1—15.4	–	+	+
openSUSE Tumbleweed	Последняя версия	–	+	+

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Oracle Enterprise Linux	6—9	–	+	+
Oracle Solaris	10.11—11.4	+	+	–
SUSE Enterprise Linux	11, 12, 15	–	+	+
Ubuntu Linux	18.04—22.04 Только LTS-версии	+	+	+

3. Сетевое оборудование

В этом разделе представлена информация о сетевом оборудовании, которое поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста сетевое оборудование и его версии могут не определиться.

Таблица 3. Сетевое оборудование

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Cisco IOS	Все версии	+	+	+
Cisco IOS XE	Все версии	–	+	+
Cisco IOS XR	Все версии	–	+	+
Cisco Nexus	Все версии	–	+	+
Eltex ESR	Все версии	–	+	–
Eltex MES	Все версии	–	+	–
Palo Alto PAN-OS	Все версии	–	+	+

4. Системы управления базами данных

В этом разделе представлена информация о системах управления базами данных, которые поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста СУБД и их версии могут не определиться.

Таблица 4. СУБД

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
MariaDB	Все версии	+	+	+
Microsoft Access	2000—2019	–	+	+
Microsoft SQL Server	2000—2019	+	+	+
MongoDB	Все версии	+	+	+
MySQL	Все версии	+	+	+
Oracle Database	Все версии	+	+	+
PostgreSQL	Все версии	+	+	+

5. Серверное ПО

В этом разделе представлена информация о серверном программном обеспечении, которое поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста ПО и его версии могут не определиться.

Таблица 5. Серверное ПО

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Apache HTTP Server	Все версии	+	+	+
Apache Tomcat	Все версии	+	+	+
MDaemon Email Server	Все версии	+	+	-
Microsoft Active Directory	Все версии	+	+	+
Microsoft DNS Server	Все версии	+	+	–
Microsoft Dynamics AX	4—2012 R3	–	+	–
Microsoft Exchange	Все версии	+	+	+
Microsoft Internet Information Services	5—10	+	+	+
Microsoft Office Online Server	2016	–	+	-
Microsoft Office Web Apps	2010—2013	–	+	-
Microsoft Project Server	2003—2019	–	+	+
Microsoft SharePoint Foundation	2010—2013	–	+	+
Microsoft SharePoint Server	2003—2019	–	+	+
Microsoft Skype for Business Server	2015—2019	–	+	–
Microsoft System Center Operations Manager	2007—2012	–	+	–
Microsoft System Center Virtual Machine Manager	2008—2012	–	+	–
Microsoft Windows Internet Name Service Server	Все версии	+	+	+
Nginx	1.19 и более новые	+	+	+

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Positive Technologies Application Firewall	Все версии	–	+	–
Veeam Backup & Replication Server	11	–	+	–
VMware vCenter Server	Все версии	+	+	+

6. Системы безопасности

В этом разделе представлена информация о системах безопасности, которые поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста системы безопасности и их версии могут не определиться.

Таблица 6. Список систем безопасности

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
AVG Anti-Virus	2013	—	+	—
AVG Anti-Virus Business Edition	2013	—	+	—
AVG Anti-Virus Free	2013	—	+	—
AVG Internet Security	2013	—	+	—
AVG Internet Security Business Edition	2013	—	+	—
Dr.Web Anti-Virus	3—6	—	+	—
Dr.Web Enterprise Server	6	—	+	—
Dr.Web Security Space	3—8	—	+	—
ESET Endpoint Antivirus	3	—	+	—
ESET Endpoint Security	3—5	—	+	—
ESET NOD32 Antivirus	2—4	—	+	—
ESET Smart Security	3—4	—	+	—
ESET Mail Security	Все версии	—	+	—
ESET File Security	Все версии	—	+	—
Kaspersky Security Center	9—10	—	+	—
Kaspersky Anti-Virus	Все версии	—	+	—
Kaspersky Endpoint Security	Все версии	—	+	—
McAfee AntiVirus Plus	Все версии	—	+	—
McAfee Internet Security	Все версии	—	+	—
McAfee Total Protection	Все версии	—	+	—
McAfee VirusScan Enterprise	8.8	—	+	—

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Norton 360	2004—2013	—	+	—
Norton AntiVirus	2006—2013	—	+	—
Norton Internet Security	2006—2013	—	+	—
Symantec AntiVirus Corporate Edition	9—10	—	+	—
Symantec Endpoint Protection	11—14	—	+	—
Trend Micro Antivirus	16—17	—	+	—
Trend Micro Internet Security	16	—	+	—
Trend Micro Internet Security Pro	16	—	+	—
Trend Micro OfficeScan Client	6—11	—	+	—
Trend Micro OfficeScan Server	6—11	—	+	—
Trend Micro PC-cillin Internet Security	1—15	—	+	—
Trend Micro ServerProtect	5	—	+	—

7. Системы криптографической защиты информации

В этом разделе представлена информация о системах криптографической защиты информации, которые поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста СКЗИ и их версии могут не определиться.

Таблица 7. Список систем криптографической защиты информации

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
«КриптоПро», Administration	Все версии	–	+	–
«КриптоПро», CSP	Все версии	–	+	–
«КриптоПро», JCP	Все версии	–	+	–
«КриптоПро», JTLS	Все версии	–	+	–
«КриптоПро», TLS	Все версии	–	+	–
Gpg4win	Все версии	–	+	–
OpenSSL	Все версии	–	+	–
PGP Desktop	Все версии	–	+	–
ViPNet Client	3—4	–	+	–
ViPNet Coordinator HW	3	–	+	–

8. Приложения

В этом разделе представлена информация о приложениях, которые поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста приложения и их версии могут не определиться.

Таблица 8. Список приложений

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
7-Zip	Все версии	–	+	–
«Яндекс Диск»	Все версии	–	+	–
ActivePerl	Все версии	–	+	–
ActivePython	Все версии	–	+	–
ActiveTcl	Все версии	–	+	–
Adobe Acrobat	Все версии	–	+	+
Adobe Acrobat DC	Все версии	–	+	+
Adobe Acrobat Reader	Все версии	–	+	+
Adobe Acrobat Reader DC	Все версии	–	+	+
Adobe Pepper Flash for Google Chrome	11—32	–	+	–
Ammyy Admin	Все версии	–	+	–
Ansible	2.10—6	–	+	–
Ansible Core	2.10—2.13	–	+	–
AnyDesk	Все версии	+	–	–
Apache HTTP Server (Linux)	2.2—2.4	+	+	+
Apache Struts	Все версии	–	+	–
Apache Subversion	Все версии	–	+	–
Apache Tomcat (Linux)	8—10	+	+	+
Artifactory	6—7	–	+	–
Atlassian Confluence	7 и более новые	–	+	–
Bitwarden	Все версии	–	+	–
Bloodhound	Все версии	–	+	–
Cain & Abel	Все версии	–	+	–

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Check Point GAiA	Все версии	–	+	+
CollabNet Subversion	Все версии	–	+	–
Dashlane Desktop	Все версии	–	+	–
Delphi	Все версии	–	+	–
Deluge	Все версии	–	+	–
Dropbox	Все версии	–	+	–
Mozilla Firefox	Все версии	–	+	+
Firefox ESR	Все версии	–	+	+
Flash Player for Microsoft Internet Explorer	1—32	–	+	–
Foxit Reader	Все версии	–	+	–
GitLab	13—14	–	+	–
Go	Все версии	–	+	–
Google Chrome	Все версии	–	+	+
HAproxy	2	–	+	–
HPE Integrated Lights-Out (iLO)	2—5	+	+	+
Hyper-V	1.0—1.4	–	+	+
iCloud	Все версии	–	+	–
IrfanView	Все версии	–	+	–
iTunes	Все версии	–	+	–
Java Platform	Все версии	–	+	–
JFrog Artifactory	6—7	–	+	–
John the Ripper	Все версии	–	+	–
Kayako Classic	1.19 и более новые	–	+	–
Keeper Password Manager	Все версии	–	+	–
LogMeIn Pro	Все версии	–	+	–
MaxPatrol 8	Все версии	+	+	–
Microsoft .NET Framework	1—4.8	–	+	+
Microsoft Edge	Все версии	–	+	+

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Microsoft Edge (Chromium)	Все версии	–	+	+
Microsoft Excel	2000—2019	–	+	+
Microsoft Excel Viewer	2000—2007SP3	–	+	–
Microsoft Internet Explorer	Все версии	–	+	+
Microsoft Lync	2010—2013	–	+	+
Microsoft OneDrive	Все версии	–	+	–
Microsoft OneNote	2003—2019	–	+	+
Microsoft Office	2003—2019	–	+	+
Microsoft Office Compatibility Pack	2007	–	+	–
Microsoft Office InfoPath	2003—2013	–	+	–
Microsoft Outlook	2003—2019	–	+	+
Microsoft PowerPoint	2003—2019	–	+	+
Microsoft PowerPoint Viewer	2000—2010	–	+	–
Microsoft PowerShell Core	6	–	+	–
Microsoft Pragmatic General Multicast	5.1—6.3	–	+	–
Microsoft Project	2003—2019	–	+	+
Microsoft Publisher	2003—2019	–	+	+
Microsoft Remote Desktop Connection Client	5—10	–	+	+
Microsoft SharePoint Services	2—3	+	+	+
Microsoft Silverlight	1—5	–	+	+
Microsoft Teams	0—1	–	+	–
Microsoft Terminal Services	Все версии	–	+	–
Microsoft Visio	2003—2019	–	+	+
Microsoft Visio Viewer	2003—2013	–	+	–
Microsoft Visual Studio	2010—2019	–	+	+
Microsoft Visual Studio Code	Все версии	–	+	–

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Microsoft Windows Media	6—12	–	+	+
Microsoft Windows Remote Management	Все версии	–	+	–
Microsoft Word	2003—2019	–	+	+
Microsoft Word Viewer	2000—2003	–	+	+
Microsoft XML Core Services	2—6	–	+	+
Mimikatz	Все версии	–	+	–
mIRC	6—7	–	+	–
mRemoteNG	Все версии	–	+	–
Nessus	Все версии	–	+	–
Notepad++	Все версии	–	+	–
OpenOffice	2—4	–	+	–
OpenVPN	Все версии	+	+	–
Opera Web Browser	Все версии	–	+	–
Passwork	4	–	+	–
PDF-XChange Viewer	Все версии	–	+	–
PHP	Все версии	+	+	–
Pidgin	Все версии	–	+	–
Privoxy	3	–	+	–
Python	2—3	–	+	–
Radmin Server	Все версии	+	+	–
Radmin Viewer	Все версии	–	+	–
Ruby	Все версии	–	+	–
SAP GUI	4—7	–	+	–
Signal	Все версии	–	+	–
Skype for Windows	0—7	–	+	–
Slik Subversion	Все версии	–	+	–
SumatraPDF	Все версии	–	+	–
TeamCity	2018—2021	–	+	–
TeamViewer	Все версии	+	+	–

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Techinline Remote Desktop	Все версии	–	+	–
Telegram Desktop	Все версии	–	+	–
Thunderbird	Все версии	–	+	+
TightVNC Server	Все версии	–	+	–
TightVNC Viewer	Все версии	–	+	–
Tor	Все версии	–	+	–
Tor Browser	Все версии	–	+	–
TortoiseSVN	Все версии	–	+	–
uTorrent	Все версии	–	+	–
Veeam Agent for Microsoft Windows	Все версии	–	+	–
Viber	Все версии	–	+	–
VisualSVN Server	Все версии	–	+	–
VLC Media Player	Все версии	–	+	–
VMware ESXi	6—7	–	+	+
VMware Player	Все версии	–	+	–
VMware Tools	Все версии	–	+	–
VMware vCenter	6—7	+	+	+
VMware Workstation	Все версии	–	+	–
WeChat	Все версии	–	+	–
WhatsApp	Все версии	–	+	–
Windows Defender	1—6	–	+	–
Windows Media Center	5	–	+	+
WinPcap	4	–	+	–
WinRAR	Все версии	–	+	–
XenAppServer	6.5	–	+	–
XnView	Все версии	–	+	–
XSpider	4—8	+	+	–
Zabbix Agent	4—6	–	+	–
Zabbix Server	4—6	–	+	–
Zoom	Все версии	–	+	–

9. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

— решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;

— диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;

— разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;

— устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

9.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

9.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

9.3. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

9.3.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста Positive Technologies нужно предоставить:

— номер лицензии на использование продукта;

— файлы журналов и другие наборы диагностических данных, хранящихся в продукте;

— снимки экрана;

— результаты выполнения рекомендаций специалиста технической поддержки;

— каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

9.3.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист Positive Technologies оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

Positive Technologies поставляет пакеты обновления в течение срока обновления, указанного в лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, Positive Technologies обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

9.3.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 9).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 9. Время реакции на запрос и время его обработки

Уровень значимости запроса	**Критерии значимости запроса**	**Время реакции на запрос**	**Время обработки запроса**
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

9.3.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

— о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

— предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;

— проблема классифицирована как неподдерживаемая.

positive technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 170 тысяч акционеров.