Dr.WEB®
Сделано в России

Вы хотите защитить КИИ?

Мы вас обрадуем – начать нужно с другого

www.антивирус.рф
www.drweb.ru

Поскольку времени у нас мало, разберем всего один случай

Dr.WEB®
с 1992 года

Пришел китайский станок лазерной резки. На борту ОС Windows 7

Вставили гарантированно чистую от вирусов флешку, для копирования файлов программ со станка, принесли на рабочий ПК, получили оповещение о вирусе…

Также со станком шло ПО, на usb носителе, при попытке скопировать с него файлы дистрибутивов получили множество детектов, см. вложение.

Поскольку времени у нас мало, разберем всего один случай

Обращение в службу технической поддержки

Dr.WEB®
с 1992 года

ии	Тип	Угроза	Действие	Компонент	Объект
	Инфицирован	Worm.Siggen.12242	В карантине	SpIDer Guard для рабочих станций Windows	G:_WA.nil
	Инфицирован	Trojan.BrowseBan.565	В карантине	SpIDer Guard для рабочих станций Windows	G:\EZCAD2-170\Ezcad2.14.11(20190531) - Lite\J8.exe
	Инфицирован	Trojan.Inject1.10883	В карантине	SpIDer Guard для рабочих станций Windows	G:\EZCAD2-170\Ezcad2.14.11(20190531) - Lite\J8.exe
	Инфицирован	Trojan.Inject1.10883	Вылечен	SpIDer Guard для рабочих станций Windows	G:\EZCAD2-170\Ezcad2.14.11(20190531) - Lite\CorFile2.exe
	Инфицированный архив	Trojan.Inject1.10883	Вылечен	SpIDer Guard для рабочих станций Windows	G:\EZCAD2-170\dirver\MINI卡驱动\2014签名release\CH341SER.EXE
	Инфицирован	Trojan.BrowseBan.565	В карантине	SpIDer Guard для рабочих станций Windows	G:\EZCAD2-100\Ezcad2.14.11(20190531) - Lite\J8.exe
	Инфицирован	Trojan.Inject1.10883	В карантине	SpIDer Guard для рабочих станций Windows	G:\EZCAD2-100\Ezcad2.14.11(20190531) - Lite\J8.exe
	Инфицированный архив	Trojan.Inject1.10883	Вылечен	SpIDer Guard для рабочих станций Windows	G:\EZCAD2-100\dirver\MINI卡驱动\2014签名release\CH341SER.EXE
	Инфицирован	Trojan.Inject1.10883	Вылечен	SpIDer Guard для рабочих станций Windows	G:\EZCAD2-100\Ezcad2.14.11(20190531) - Lite\CorFile2.exe
	Инфицирован	Worm.Siggen.12242	В карантине	SpIDer Guard для рабочих станций Windows	G:_WIFNDNIU.nil

Кстати Worm – это червь, так что возможно злоумышленник, надеялся заразить всю сеть клиента. А может и нет, просто китайский бардак

Dr.WEB®
с 1992 года

- ... несанкционированный вход, через подбор пароля одной из учетных записей
- ... после входа по RDP злоумышленник запустил шифрующий скрипт
- ... судя по последнему отчету, у вас в сети должен быть сервер с адресом _____, на котором видна подозрительная сетевая активность
- ... на сервер … антивирус Dr.Web был установлен уже после шифрования

Из ответов специалистов техподдержки «Доктор Веб» по итогам разбора инцидентов

Dr.WEB®
с 1992 года

Клиент параллельно запросил поставщика в Китае - "это не вирус, просто отключите свой антивирус и работайте спокойно"

Исследование станка выявило, что вредоносный софт не просто там находился – была заражена нужная для работы программа

Dr.WEB®
с 1992 года

Типичная атака “через поставщика”, методы защиты от которой известны давно и достаточно просты. Но используются ли они?

Dr.WEB®
с 1992 года

Защита КИИ – это не только защита промышленных протоколов и контроль целостности на устройствах различного назначения

Это еще и безопасное окружение – которое именно и находится под атакой.

Dr.WEB®
с 1992 года

Лишь 11% пойманных
на USB-накопителях вредоносных
программ были нацелены на АСУ ТП.

Статистика неумолима – гораздо чаще
случаются атаки не на само
промышленное оборудование.

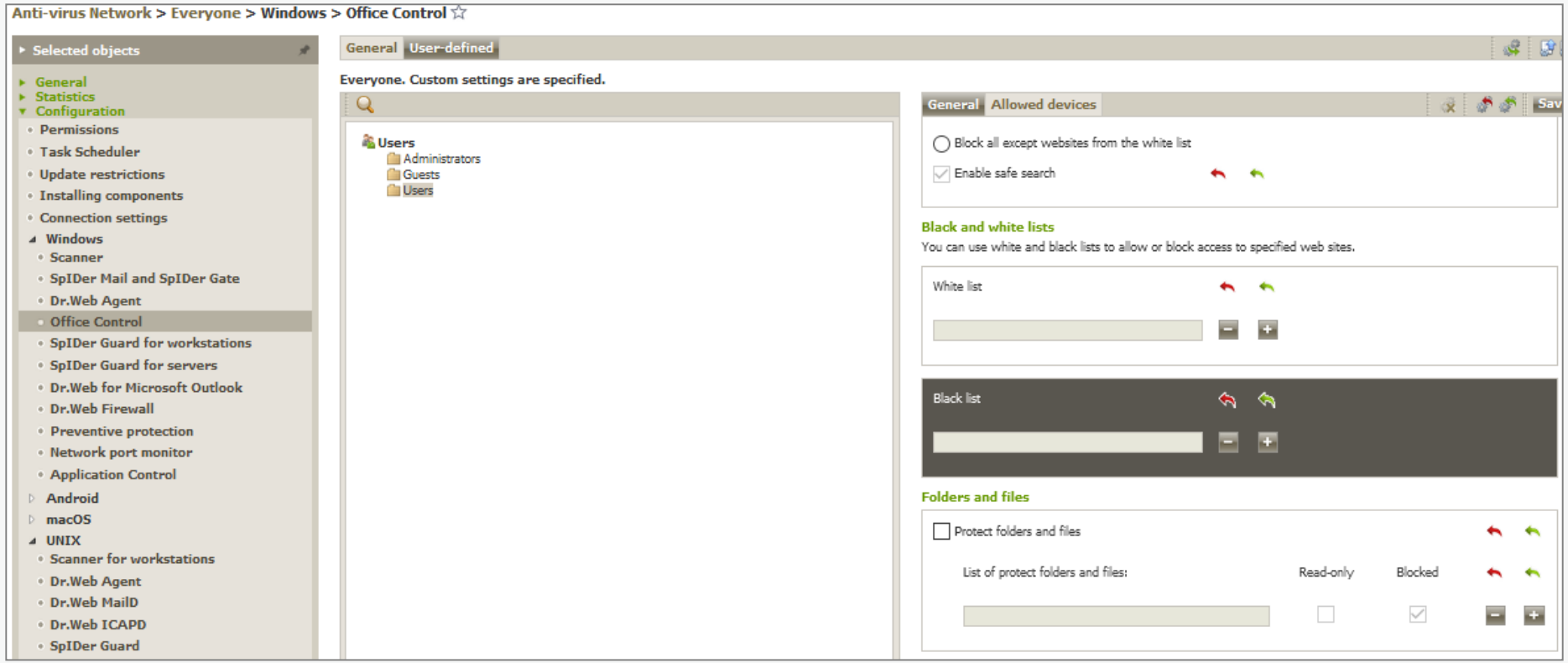
Dr.WEB®
с 1992 года

Dr.Web Enterprise Security Suite

Антивирус – это не только антивирусные базы

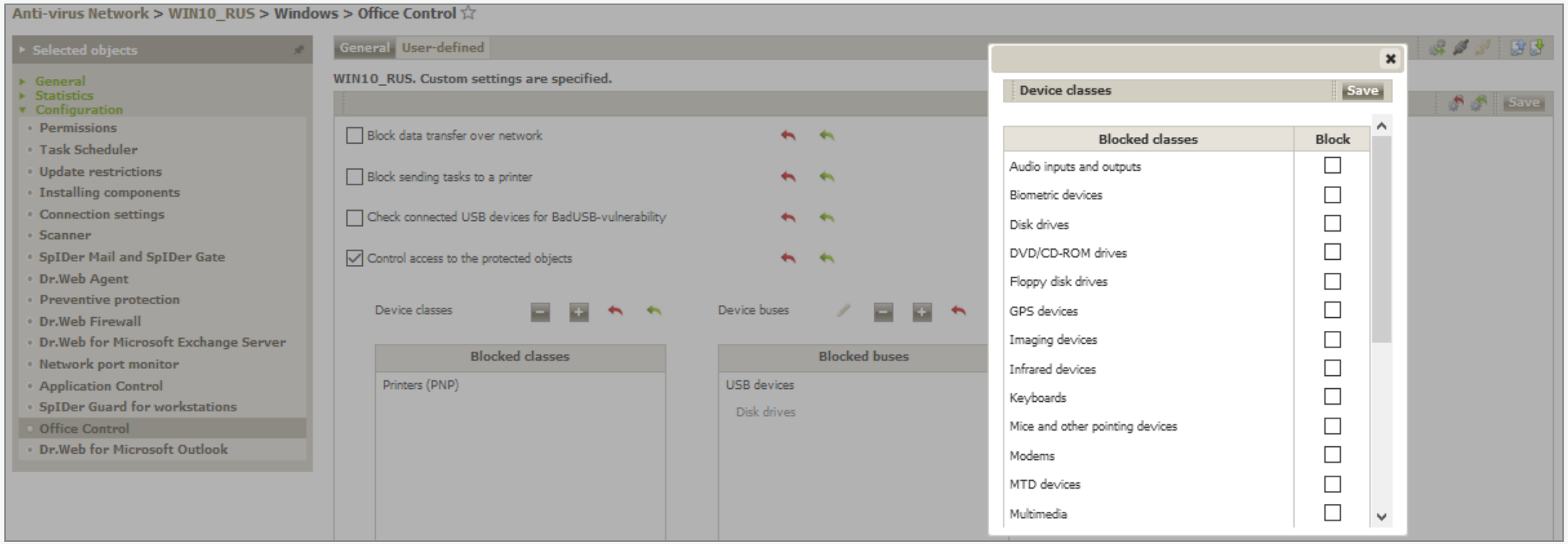
Dr.WEB®
с 1992 года

Доступ только к “чистым” ресурсам
Доступ к ресурсам только в указанное время



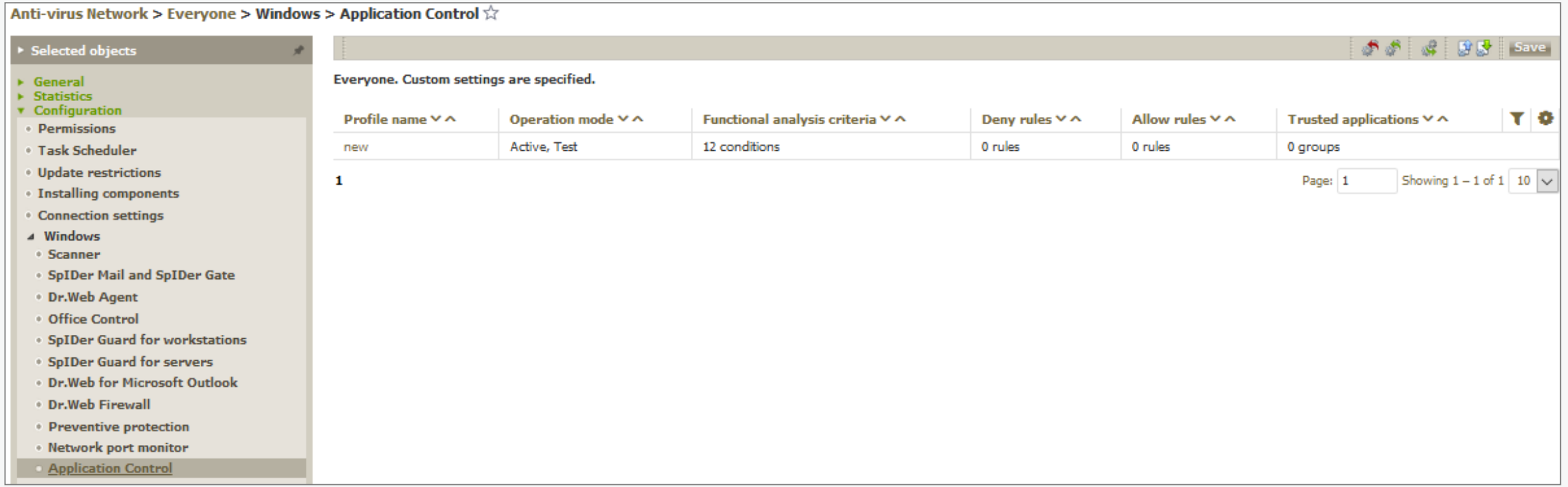
Dr.WEB®
с 1992 года

Контроль использования внешних носителей и оборудования компании



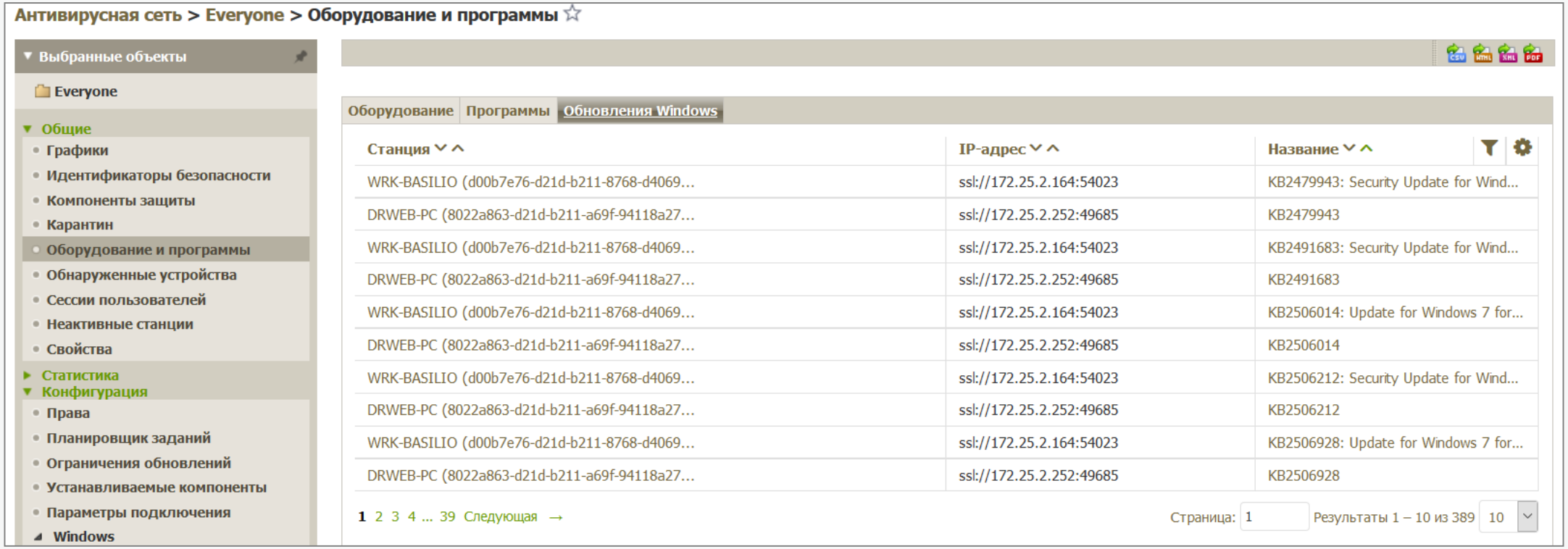
Dr.WEB®
с 1992 года

Контроль запуска программ пользователем (и под его именем)



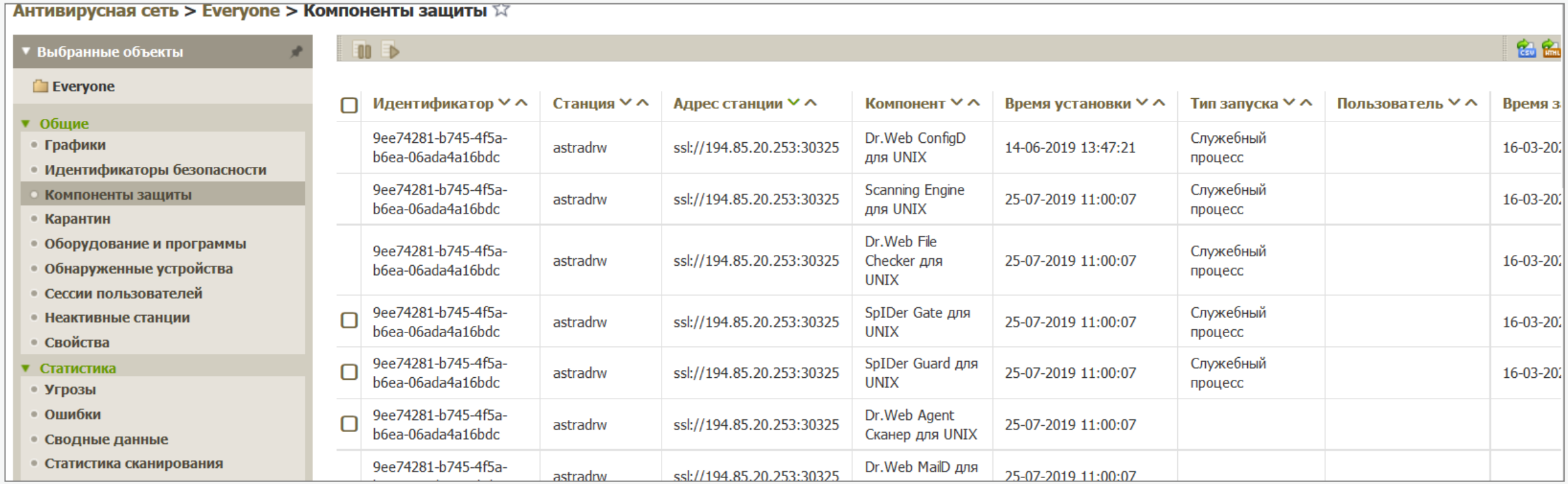
Dr.WEB®
с 1992 года

Контроль установки обновлений безопасности



Dr.WEB®
с 1992 года

Контроль установленных программ
Контроль установленных компонентов защиты



Идентификатор	Станция	Адрес станции	Компонент	Время установки	Тип запуска	Пользователь	Время з
9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	Dr.Web ConfigD для UNIX	14-06-2019 13:47:21	Служебный процесс		16-03-20
9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	Scanning Engine для UNIX	25-07-2019 11:00:07	Служебный процесс		16-03-20
9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	Dr.Web File Checker для UNIX	25-07-2019 11:00:07	Служебный процесс		16-03-20
9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	SpIDer Gate для UNIX	25-07-2019 11:00:07	Служебный процесс		16-03-20
9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	SpIDer Guard для UNIX	25-07-2019 11:00:07	Служебный процесс		16-03-20
9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	Dr.Web Agent Сканер для UNIX	25-07-2019 11:00:07			
9ee74281-b745-4f5a-	astradrw	ssl://194.85.20.253:30325	Dr.Web MailD для	25-07-2019 11:00:07			

Dr.WEB®
с 1992 года

Важно!

Возможности Dr.Web позволяют защищать сотрудников компании, работающих не только внутри локальной сети, но и удаленно – как временно, так и постоянно

Dr.WEB®
с 1992 года

Dr.Web позволяет:

- Обнаруживать и удалять вредоносные программы любого типа и любой сложности
- Применять политики безопасности, принятые в компании, для защиты, в том числе, устройств удаленных сотрудников
- Контролировать состояние защиты, список установленного ПО, установку обновлений…


Dr.WEB®
Сделано в России
ЗАЩИТИ СОЗДАННОЕ
Поддерживаем всех
Российские ОС и оборудование
Альт Линукс, Astra Linux, ОС ROSA, Ред ОС 7.1 Муром, Эльбрус-Д, Эльбрус-8.32
Неподдерживаемые Microsoft версии
ОС Windows 7/Vista/XP
Российское ПО
1С
Valo
Р-Платформа
Новейшие версии Microsoft
Windows 10
© ООО «Доктор Веб», 2003–2020
www.drweb.ru | антивирус.рф

Dr.WEB®
с 1992 года

КИИ?

У вас есть Dr.Web!