

КОНТРОЛЬ СОСТОЯНИЯ СЕТИ

С ПЛАТФОРМОЙ
NETOPIA FIREWALL COMPLIANCE

- АНАЛИЗ СООТВЕТСТВИЯ КОНФИГУРАЦИЙ СЕТЕВЫХ УСТРОЙСТВ ЗАДАНЫМ СТАНДАРТАМ.
- АНАЛИЗ И ОПТИМИЗАЦИЯ ПРАВИЛ СЕТЕВОГО ДОСТУПА.
- РАСЧЁТ ВОЗМОЖНЫХ ВЕКТОРОВ АТАК С УЧЁТОМ НАСТРОЕК СЕТЕВОГО ОБОРУДОВАНИЯ.
- ВИЗУАЛИЗАЦИЯ СЕТЕВОЙ ИНФРАСТРУКТУРЫ.
- ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ.
- АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ ДОСТУПОВ.



КАКИЕ ПРОБЛЕМЫ МЫ РЕШАЕМ?

Основные проблемы

Спешная миграция межсетевых экранов с зарубежных на российские

Отсутствие единообразия в настройке сетевых устройств

Отсутствие видения общей «картины» сетевых доступов

Отсутствие контроля за изменениями конфигураций сетевого оборудования

Слишком большое количество сетевых правил, сложно проводить их оптимизацию

Слишком большое количество критичных уязвимостей, недостаточно ресурсов на своевременное устранение их всех



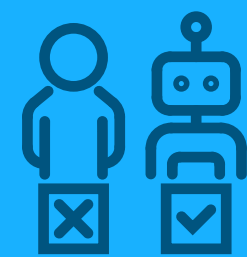
МОДУЛЬНАЯ ПЛАТФОРМА NETOPIA FIREWALL COMPLIANCE



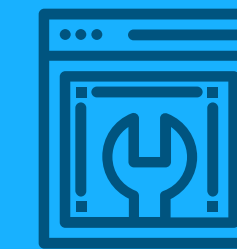
Возможные сценарии



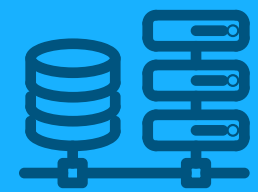
АНАЛИЗ И ОПТИМИЗАЦИЯ
ПРАВИЛ ДОСТУПА



КОНТРОЛЬ СЕГМЕНТАЦИИ СЕТИ



АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ
ЖИЗНЕННЫМ ЦИКЛОМ
ДОСТУПОВ



НЕПРЕРЫВНЫЙ АУДИТ
И РЕСЕРТИФИКАЦИЯ ПРАВИЛ



АНАЛИЗ ВЕКТОРОВ АТАК
И УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ



ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ

Netopia Firewall Compliance



FIREWALL
ASSURANCE



CHANGE
MANAGEMENT



NETWORK
ASSURANCE



VULNERABILITY
CONTROL

СРАВНЕНИЕ С КОНКУРЕНТАМИ



				
Network Assurance				
Сбор конфигураций (в т.ч офлайн)	+	+	+ -	+
Широкая поддержка российских вендоров (в т.ч. PT NGFW)	+	-	-	+ -
Контроль конфигураций	+	+	+	+
База проверок (hardening) по российским вендорам	+	-	-	+
Карта сети	+	+	+	+
Firewall Assurance				
Анализ сетевой доступности	+	+	+	+
Анализ и оптимизация правил	+	+	+	+
Поиск по объектам внутри правил	+	+	+	-
Vulnerability Control				
Приоритизация уязвимостей	+	+	-	-
Построение векторов атак	+	+	-	-
Change Management				
Изменение сетевых политик на устройстве	+	+	+	+

ПОДДЕРЖИВАЕМЫЕ СИСТЕМЫ

Email

BPM-системы

SIEM

AD/LDAP



Vulnerability Management

IPAM

Security Scanner

ITSM

ИНТЕГРИРУЕМЫЕ СИСТЕМЫ

NAUMEN

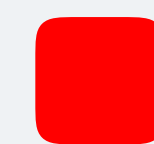
NAUMEN SERVICE DESK

BPMSOFT

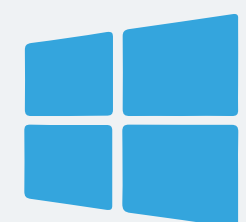
BPM SOFT

**Security
Vision**

SECURITY VISION VM

 **positive technologies**

POSITIVE TECHNOLOGIES VM / POSITIVE TECHNOLOGIES MAXPATROL 8

 Microsoft
Active Directory

MICROSOFT ACTIVE DIRECTORY / LDAP



IPAM



SIEM



EMAIL

ДОБАВЛЕНИЕ СИСТЕМ ВОЗМОЖНО ПО ЗАПРОСУ

СПИСОК ПОДДЕРЖИВАЕМОГО ОБОРУДОВАНИЯ И ПО



IOS

ASA Firewall



UserGate

FORTINET®



HUAWEI



CHECK POINT™

Контигент

с•терра



positive technologies



В БЛИЖАЙШЕЕ ВРЕМЯ:



Модуль	Описание	Лицензирование
Network Assurance	Анализ соответствия конфигураций сетевых устройств заданным стандартам; ретроспективный анализ изменений конфигураций, анализ настроек на Hardening и Best Practice, построение карты сети и визуализация сетевой инфраструктуры.	По количеству маршрутизирующих устройств.
Firewall Assurance	Анализ пути прохождения трафика и контроль доступа. Анализ правил доступа, политик и их оптимизация (затенённые правила, давно не работающие правила, правила со слишком большим избыточным доступом и другие оптимизации). Контроль наличия или отсутствия доступа в правилах межсетевых экранов по всему пути прохождения трафика.	По количеству межсетевых экранов. Включает в себя модуль Network Assurance. FA NA
Change Management	Управление изменениями политик межсетевых экранов в автоматизированном режиме с поддержкой цепочек согласований, присвоением номера тикетов правилам, интеграцией с существующими системами управления изменениями в организации (ITSM, PAM и др.) посредством API.	По количеству межсетевых экранов, на которых будут проводиться изменения политик доступа. Для работы модуля обязательно наличие лицензии «Firewall Assurance». ЛИЦЕНЗИОННЫЕ ТРЕБОВАНИЯ: CM FA
Vulnerability Control	Корреляция текущих уязвимых активов с их доступностью по сети: из интернета, из сетей подрядчиков или иных внешних источников. Приоритизация устранения уязвимостей исходя из их достижимости. Выявление векторов атак и достижимости по сети критических защищаемых данных через существующие уязвимости (Multi-hop атаки).	По количеству активов в сети. Для эффективной работы модуля требуется как можно более полная информация о сети из модулей «Firewall Assurance» (обязательно) и «Network Assurance». ЛИЦЕНЗИОННЫЕ ТРЕБОВАНИЯ: VC FA NA

ОЦЕНИТЕ ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ РЕШЕНИЯ NETOPIA FIREWALL COMPLIANCE!

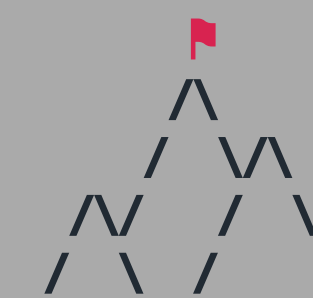


ООО «НЕТОПИЯ»

121205, г. Москва, муниципальный округ Можайский, территория инновационного центра «Сколково», б-р Большой, д. 42, стр. 1, этаж 2, помещение № 162/№ 4

Порядковый номер
в реестре отечествен-
ного ПО — 17109

Резиденты
Сколково



ПРЕМИЯ
ЦИФРОВЫЕ
ВЕРШИНЫ 2025

+7 (495) 255-35-82 / info@netopia.pro