FortiNAC

Контроль доступа к сетевой среде - новые технологии в портфеле решений
Fortinet и **Bradford Networks**

2018

Сегодня

2.4 млрд — Подключенных “things” в корпоративных сетевых инфраструктурах

11 млн — Скомпрометировано (2016)

256 дней — На обнаружение угрозы (без специальных средств)

2020

6.9 млрд — Подключенных “things” в корпоративных сетевых инфраструктурах

1.5 млрд человек — Потенциально уязвимы

No DECLINE — Снижения не ожидается в обозримом будущем

Реальный вызов = 1 Достаточно только одного

Один из наиболее быстро развивающихся сегментов на рынке кибербезопасности

Growing Addressable Market

NAC Market

$685 Million

26% YoY growth

Gartner, Market Guide for Network Access Control, May 2017

К 2019 году 40% крупных предприятий будут требоваться специализированные и автоматизированные средства для выполнения нормативных обязательств на случай возникновения серьезных инцидентов информационной безопасности

Market Analysis

Драйверы роста & Тренды

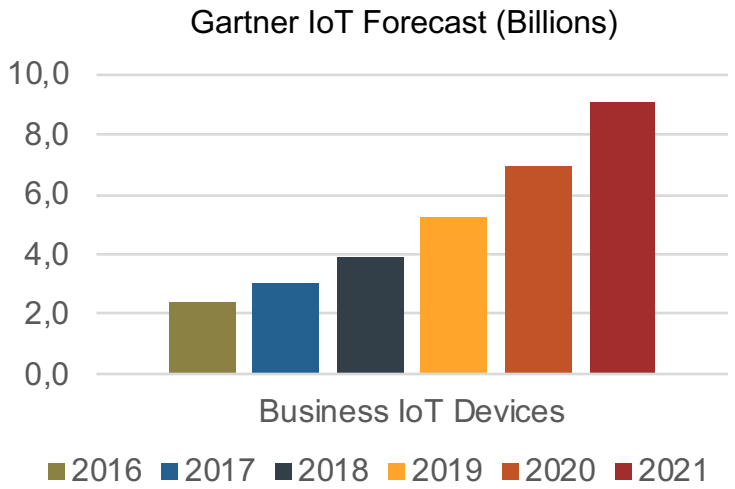
Идентификация и мониторинг IoT
Автоматизация применения политики на основе аутентификации, обнаружения, конфигурации, либо роли конечных узлов

Повышение осведомленности (Network Visibility)
Снижение рисков, связанных с наличием в составе инфраструктуры узлов/устройств, не отвечающих заданным требованиям

Соответствие и аудит
Доказательство, что предприятие осуществляет контроль и мониторинг своей сетевой инфраструктуры

Взрывной рост IoT как драйвер рынка

The IoT Market Will Be Massive



- Прогноз Gartner - рынок IoT будет интенсивно расти от показателей в 2,3 млрд устройств в 2016 г. до 9,1 млрд устройств в 2021 г.
- К 2020 году более 25% выявленных угроз на предприятиях будут связаны с IoT, хотя на IoT будет приходиться менее 10% бюджетов

Gartner: Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017

Драйверы роста IoT

Снижение стоимости Интернет-подключения

Увеличение инвестиций в решения и системы IoT крупными предприятиями и инфраструктурами

Расширение возможности подключения к Интернету из-за расширяющегося покрытия Wi-Fi и других беспроводных технологий

Source: Gartner, BI Intelligence, IHS Technology.

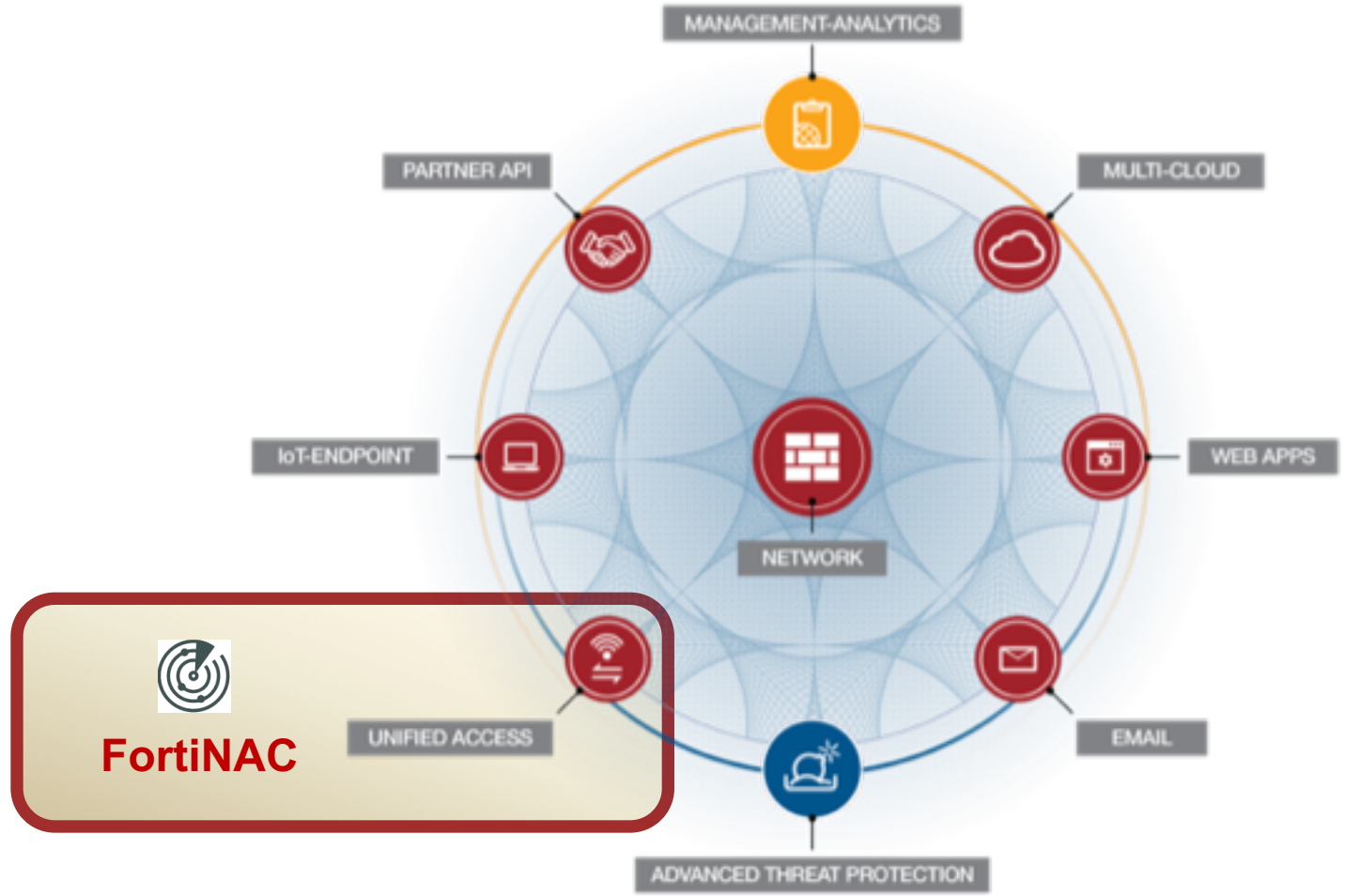
FortiNAC

Контроль и управление доступом

FortiNAC – как элемент расширения Фабрики Безопасности

Приобретение компании Bradford Networks

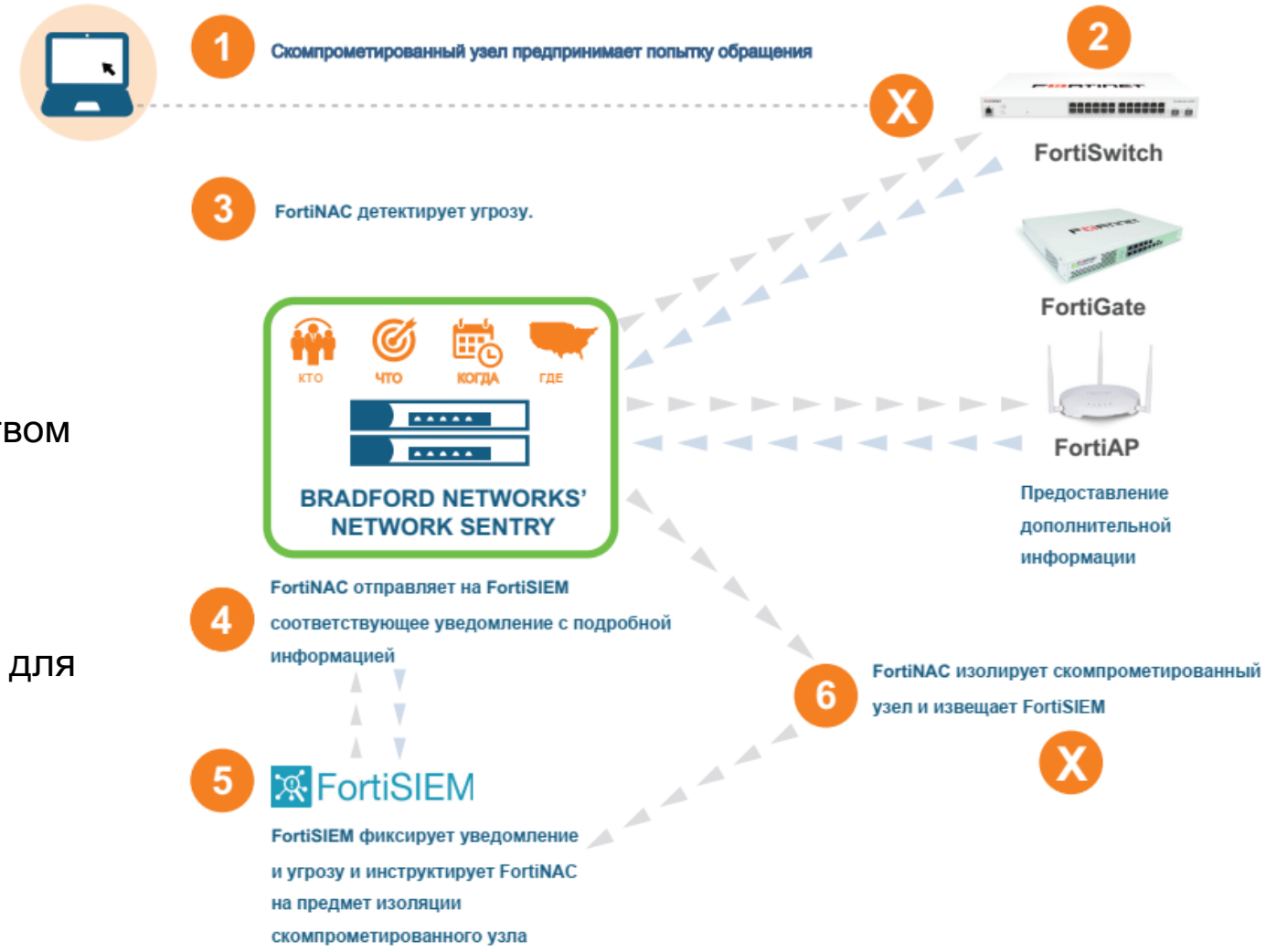
- Расширение портфеля решений Fortinet
- Расширение функциональности контроля доступа
- Повышение уровня осведомленности и защищенности
- Обогащение Фабрики Безопасности



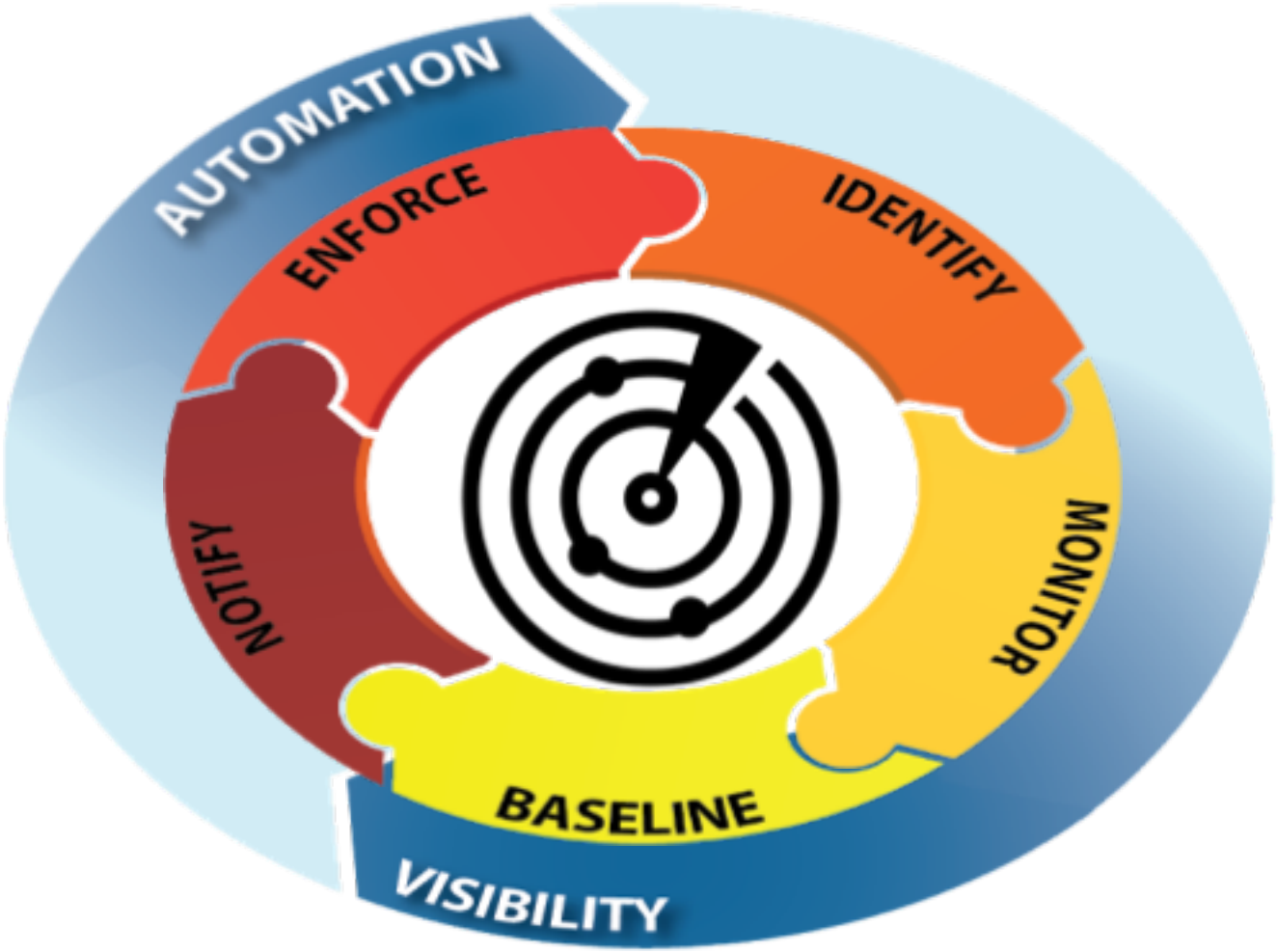
FortiNAC в действии

Как это работает:

1. Попытка обращения
2. Фиксация обращения сетевым устройством и передача информации FortiNAC
3. Детектирование угрозы/несоответствия
4. Обмен данными в рамках Фабрики Безопасности – FortiSIEM
5. Формирование и получение инструкций для противодействия
6. Изоляция скомпрометированного узла



FortiNAC в действии



Обнаружение:
- Оборудования и устройств сетевой инфраструктуры
- Конечные узлы

Чтение:
- CAM tables,
- ARP caches,
- Forwarding DB

Идентификация (для всех конечных узлов):
- MAC
- IP
- Port
- AP
- SSID

Нотификация:
- на основе “what if” сценариев

Профилирование: Endpoint Profiling, Fingerprint, TCP/UDP…
Ассоциирование: User to Device Association
Сеть: Provisioning
Оценка: Endpoint Compliance/Posturing

Контроль:
- Port Level Control,
- Lock it down

FortiNAC - уровни лицензирования

	Basic	Plus	Pro
Описание	Простое, легко внедряемое решение по отслеживанию всех устройств сети, автоматизации процессов авторизации и блокировок доступа при необходимости	Полная функциональность Базовой лицензии - плюс расширенный функционал контроля доступа и провиженинга для пользователей, гостей и устройств сети	Максимальная функциональность – лицензия Premier предлагает отслеживание устройств сети в реальном времени, полный контроль и управление доступом и автоматизированные средства ответной реакции.
Применение	Предприятие нуждается в решении по контролю устройств и защите IoT, но не нет необходимости в более глубоком контроле пользователей/сетей или внедрении автоматизированной ответной реакции на угрозы или несоответствия	Для предприятий, нуждающихся в полнофункциональном и гибком NAC-решении с обеспечением отслеживания и контроля устройств сети, но не требующих функций автоматизированной реакции на угрозы или несоответствия	Для предприятий, которые хотят иметь полную видимость устройств сети, гибкое решение NAC для контроля и управления доступом, а также, точную сортировку событий и автоматизированную реакцию на угрозы или несоответствия угроз в режиме реального времени.
Осведомленность (Visibility)			
Контроль			
Реакция			

FortiNAC - уровни лицензирования

	FortiNAC LICENSE TYPES		BASIC	PLUS	PRO
Visibility	Network	Network Discovery	•	•	•
	User	Persistent Agent		•	•
		Domain Authorization		•	•
		Captive Portal		•	•
	Endpoint	Rogue Identification	•	•	•
		Captive Portal		•	•
		Device Profiling & Classification	•	•	•
		Domain Authorization	•	•	•
		MDM Integration	•	•	•
Automation / Control		Network Access Policies		•	•
		BYOD / Onboarding		•	•
		Guest Management		•	•
		IoT Onboarding with Sponsor	•	•	•
		Endpoint Compliance		•	•
		Rogue Device Detection & Restriction	•	•	•
		Web & Firewall Single Sign On		•	•
		Firewall Segmentation	•	•	•
Incident Response		Event Correlation			•
		Extensible Actions & Audit Trail			•
		Alert Criticality & Routing			•
		Guided Triage Workflows			•
Integrations		Inbound Security Events			•
		Outbound Security Events		•	•
		REST API		•	•
Reporting		Live Reporting		•	•
		Historical Analytics		•	•

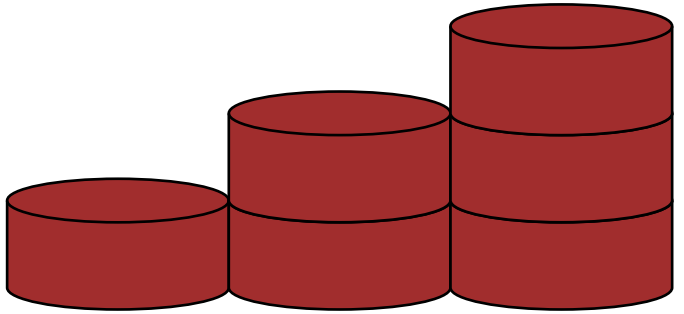
Варианты исполнения FortiNAC

ПАК – программно-аппаратный комплекс

- 3 Control & Application Appliances
- 2 Control Appliances
- 2 Application Appliances
- Manager
- Analytics Server

Виртуальные машины

- Control / Application VM
- Manager VM
- Analytics VM



Уровни лицензирования

1. **Basic**
   - Детектирование
2. **Plus**
   - Детектирование и контроль
3. **Pro**
   - Детектирование, контроль и реакция

Функции сервера контроля - Control Server

- Функционал обработки данных и «принятия решения» согласно настроенных политик
- Реализация взаимодействия с коммутационным оборудованием инфраструктуры
  - Command Line Interface (CLI) sessions via telnet or SSH
  - SNMP communications to read/write data from/to the switch
  - Trap receiver for MAC notification and link up/down traps
- Поддержка базы данных
  - Adapter/Host/User Tables, Connection Table, Scan Results, etc
  - Identifies which policies are active on which ports/switches
- Сервер RADIUS
  - All RADIUS Authentication requests
- Обычно располагается в сегменте управления коммутационным оборудованием – в «management VLAN»

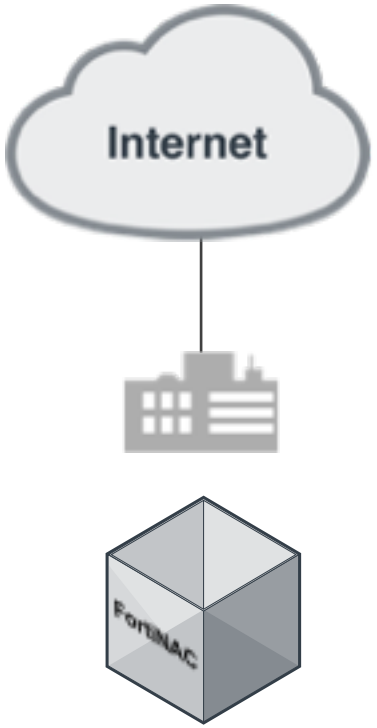
Функции сервера приложений - Application Server

- Поддерживает клиентские соединения
- Поддерживает службы DHCP, DNS, Web services для “Isolation VLANs” или/и captive portal
  - » DHCP relay/helpers on the Isolation VLAN(s) will point to the Application Server
- Поддерживает текущие соединения с агентами
- Располагается в пользовательских/продуктивных сегментах инфраструктуры
- Обеспечивает функции профилирования
  - » NMAP scans are run from the Application Server
  - » DHCP fingerprinting is done from the Application Server

Варианты внедрения

Четыре возможных варианта дизайна решения

Варианты внедрения - Малый (1/2)



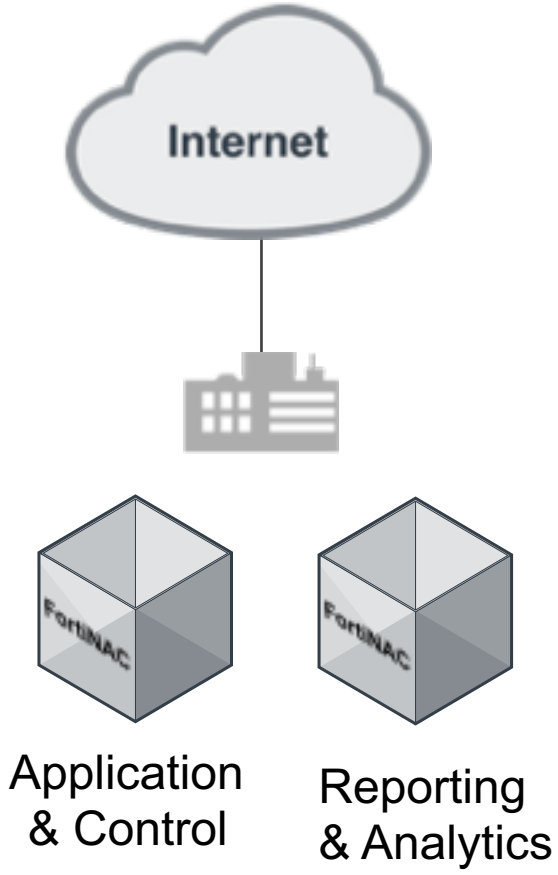
Application
& Control

Архитектурные элементы:

Application & Control – все-в-одном

- Решение реализуется на базе единого ПАК с функционалом Application и Control серверов
- Подходит для небольших и средних предприятий/организаций, с объемом инфраструктуры 250-15000 портов доступа

Варианты внедрения - Малый (2/2)

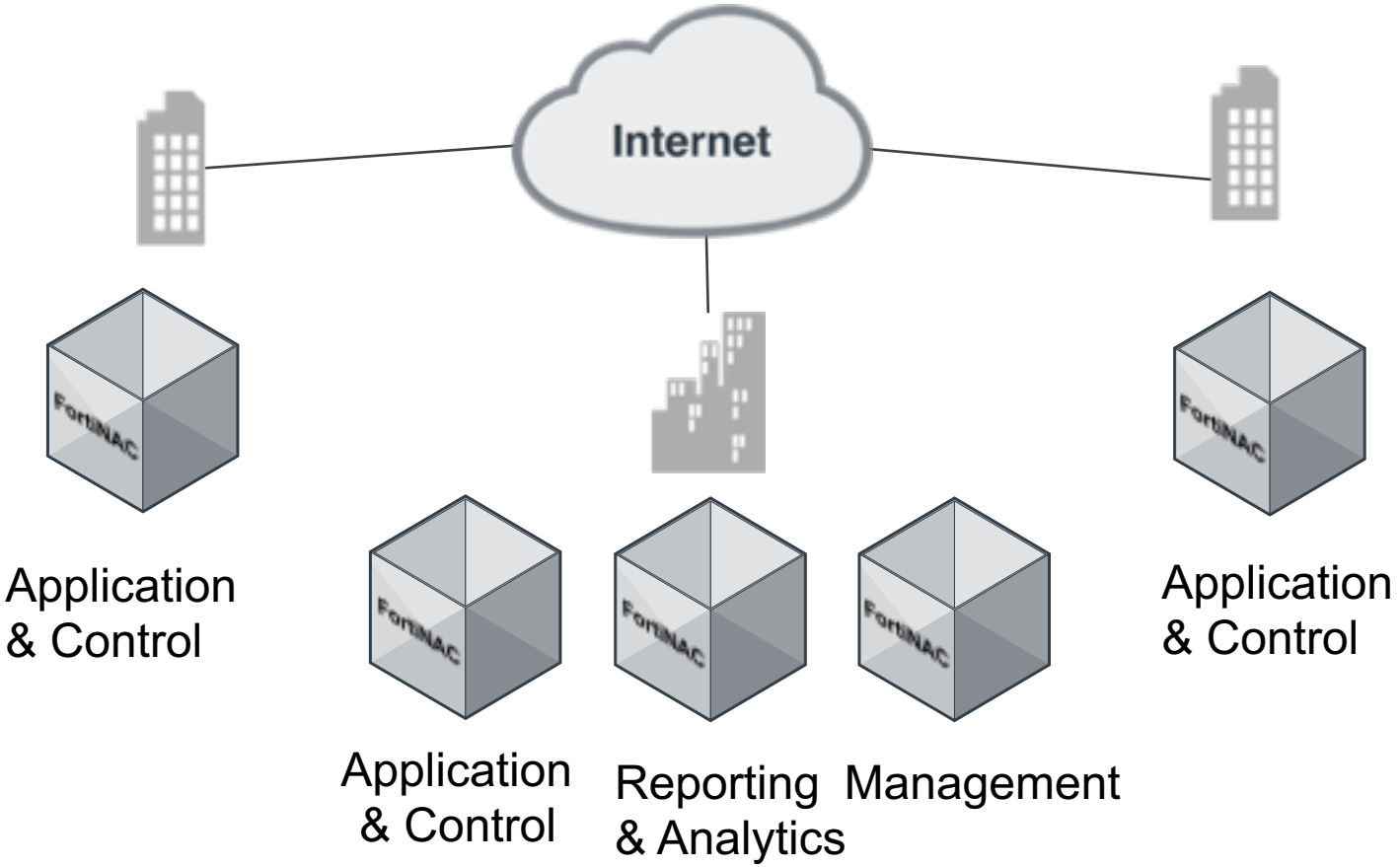


Архитектурные элементы:

Application & Control – все-в-одном

- Решение реализуется на базе единого ПАК с функционалом Application и Control серверов
- Опционально – отдельный ПАК с выделением функционала Аналитики и Отчетности
- Подходит для небольших и средних предприятий/организаций, с объемом инфраструктуры 250-15000 портов доступа

Варианты внедрения - Средний

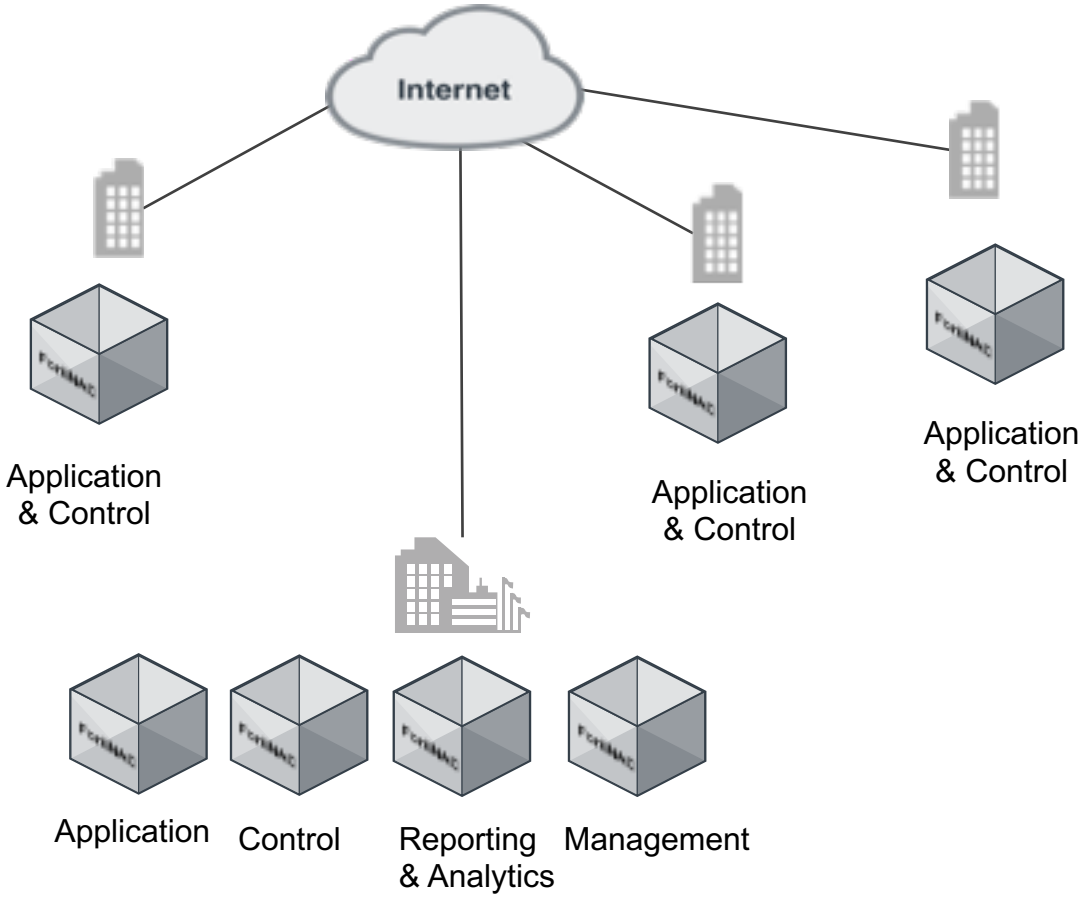


Архитектурные элементы:

Решение реализуется на базе нескольких ПАК(VM):

- ПАК Application & Control – по количеству площадок внедрения
- ПАК Reporting & Analytics
- ПАК Management
- Подходит для средних предприятий/организаций, с объемом инфраструктуры 12000-60000 портов доступа

Варианты внедрения – для крупных инфраструктур



Архитектурные элементы:

Решение реализуется на базе нескольких ПАК(VM):

- ПАК Application & Control – по количеству площадок внедрения (кроме головной)
- ПАК Application
- ПАК Control
- ПАК Reporting & Analytics
- ПАК Management
- Подходит для средних предприятий/организаций, с объемом инфраструктуры 20000-75000 портов доступа

FortiNAC в деталях

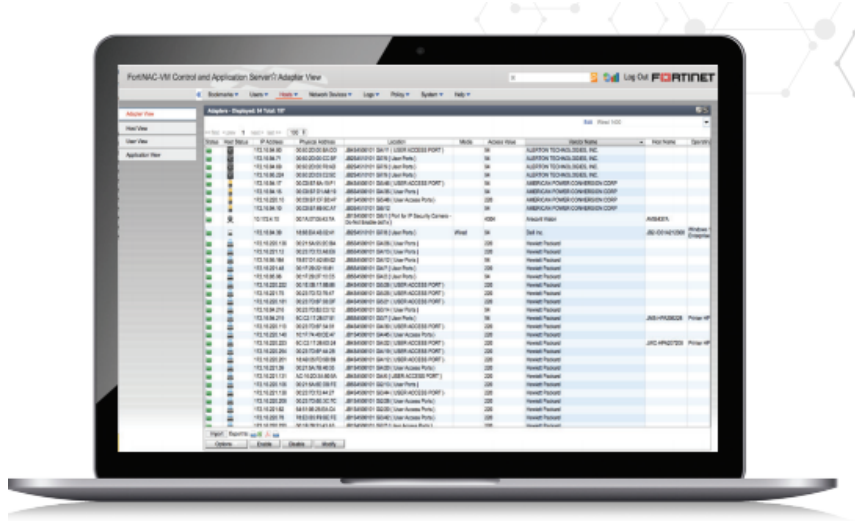
Основной функционал и возможности

FORTINET

FortiNAC – защита и управление доступом к среде

Отслеживание каждого устройства и пользователя

- Детальное профилирование устройств посредством использования различных источников информации и анализа поведения для точного определения и описания всей сетевой инфраструктуры



Расширение функций контроля сети – поддержка сторонних устройств

- Поддержка функций внедрения политик и изменений конфигураций для коммутационного и беспроводного оборудования более 70 производителей.
- Обогащение Фабрики Безопасности Fortinet

Автоматизированная ответная реакция

- Секундная реакция на возникающие события – изоляция угрозы до ее распространения
- Широкий спектр средств автоматизации – изменений конфигураций устройств при обнаружении несоответствующего поведения

FortiNAC – Комплексная безопасность сетевого окружения

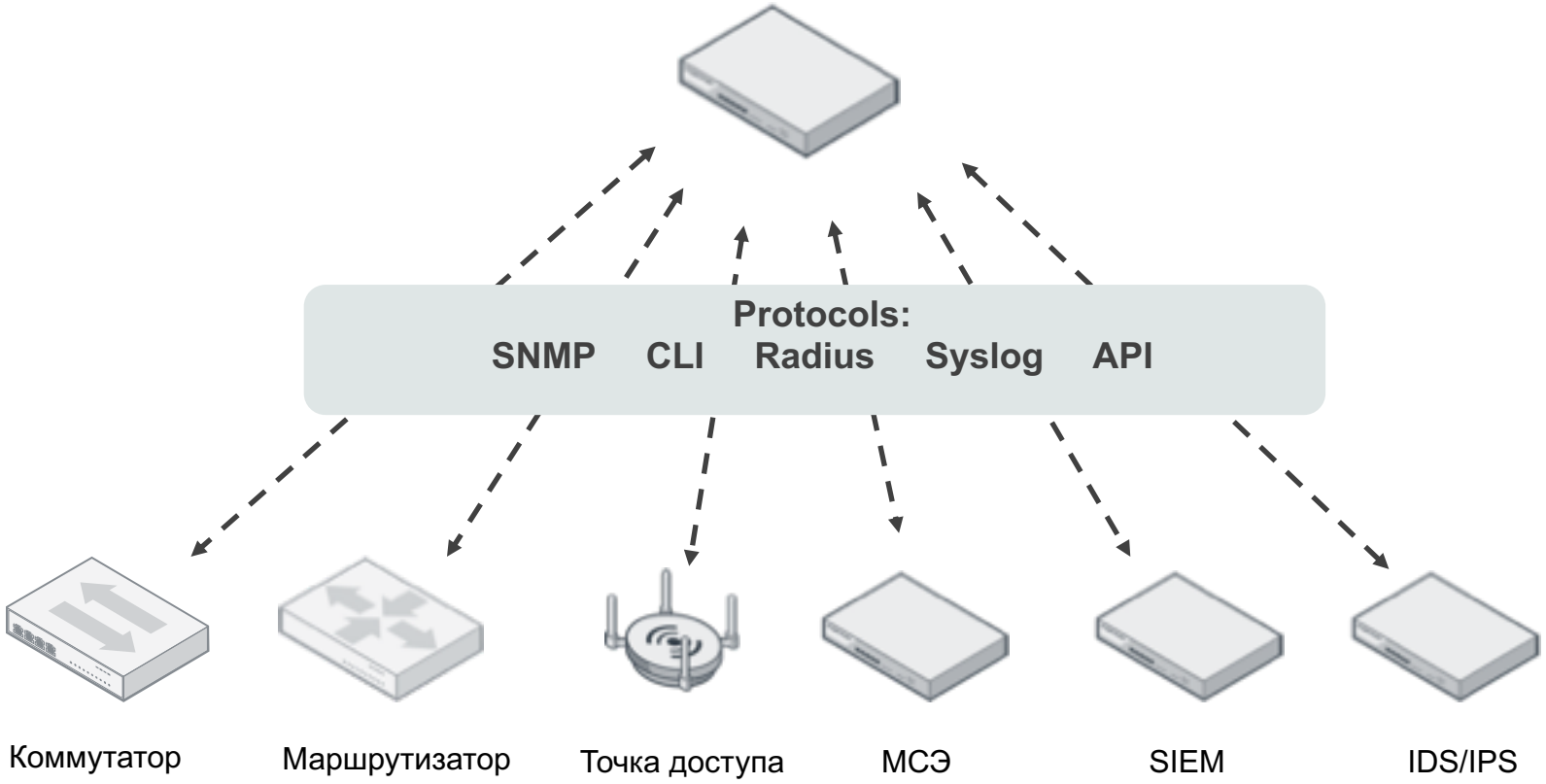
Осведомленность (Visibility)

- **Обнаружение всех устройств инфраструктуры, IoT, пользователей и приложений**
- **Получение данных: RADIUS, CLI, SNMP, Syslog, MDM, DHCP, LDAP**
  - » Возможности идентификации более 1500 типов устройств
- **Мульти-вендорные проводные и беспроводные подключения**
  - » Получение данных от оборудования практически всех вендоров
- **Идентификация и профилирование каждого конечного узла**
  - » Возможности создания политик на основе типа устройства
  - » Расширение возможностей управления уязвимостями и патчами на конечные узлы, не использующие FortiClient
- **Самостоятельная регистрация для упрощения управления гостевым доступом**

Осведомленность: конечные узлы, пользователи, приложения

Осведомленность: сбор данных без установки агентов

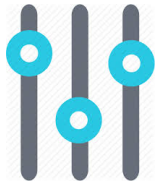
различные источники получения информации



Осведомленность: идентификация конечных узлов

- Классификация устройств
  - » В автоматическом или ручном режиме
    - Sponsor Notification
  - » Тип устройства
  - » Подтверждение при подключении
  - » Блокировка при неуспешном подтверждении
- 13 методов профилирования
  - » Большое кол-во методов профилирования повышает уровень доверия

FortiNAC – Комплексная безопасность сетевого окружения



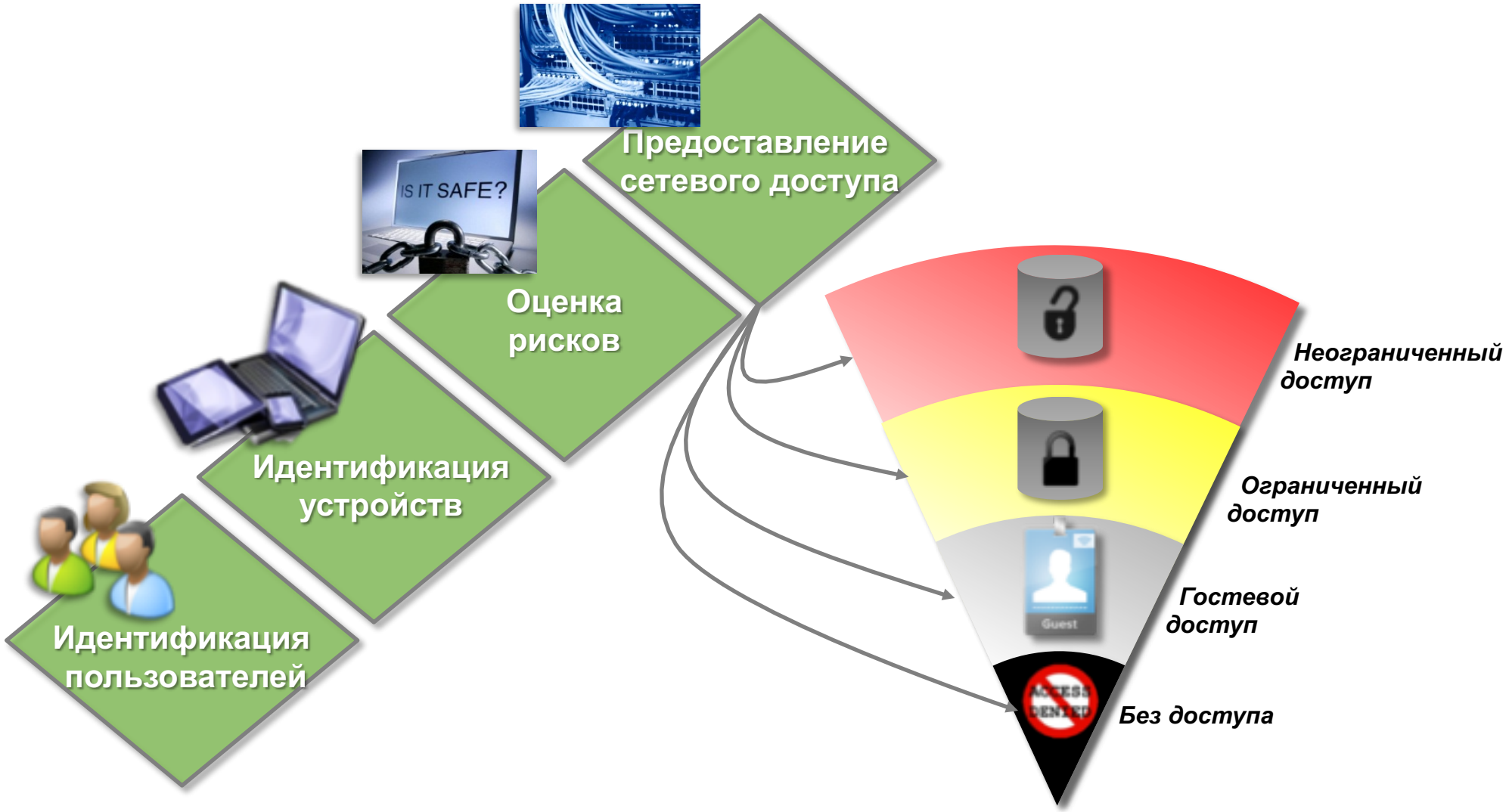
Контроль

- **Автоматизированные процессы аутентификации и авторизации**
  - » Глубоко детализированные профили для устройств и пользователей допускают автоматический контролируемый доступ к сетевой среде
  - » Фиксация роли, локации, времени и других метрик устройств

- **Динамический контроль доступа к сетевой среде**
  - » Предоставление/блокировка доступа на основе динамических изменений в активности устройства или профиле

- **Микро-сегментирование**
  - » Точная и детальная идентификация устройств позволяет выполнить микросегментацию сетевой инфраструктуры
  - » Устройства имеют ограниченный контролируемый доступ для снижения возможной площади атаки/распространения угрозы

Контроль: Динамический доступ к сетевой среде

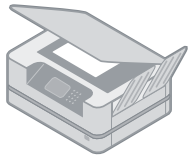


FortiNAC – Комплексная безопасность сетевого окружения

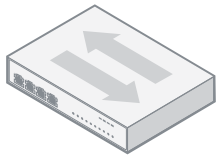
Автоматизированная реакция на угрозы/несоответствия

- **Мост между SOC & NOC**
  - » Немедленная реакция – по факту появления события безопасности
- **Быстрая и эффективная сортировка событий безопасности**
  - » В соответствии с настроенными правилами автоматизации, секундная реакция может быть реализована при обнаружении подозрительного/плохого поведения
- **Ускорение процесса расследования угроз/инцидентов**
  - » Доступна вся комплексная историческая информация по устройствам
- **Точечное применение мер сдерживания и противодействия**
  - » Карантин, предоставление доступа только в Интернет и т.п.

Динамическое профилирование устройств

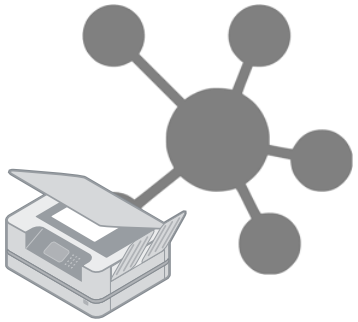


1. Принтер подключился к сети



2. На FortiNAC направлен MAC notification trap

3. FortiNAC Профилирует устройство как «принтер»



4. FortiNAC Информирует Фабрику о предоставлении соответствующего доступа

Сдерживание угроз на границе сети

1. Пользователь подключает инфицированный ноутбук

2. FGT отправляет событие на FortiNAC

3. FortiNAC помещает узел в карантин на уровне доступа

4. Угроза сдержана на уровне коммутатора доступа

Ключевые отличительные особенности решения

› Двунаправленные API для интеграции FortiNAC с решениями сторонних производителей

› Поддержка «из коробки» более 1500 типов и наименований сетевых устройств и возможность детектировать и учитывать любой конечный узел, имеющий IP-адрес

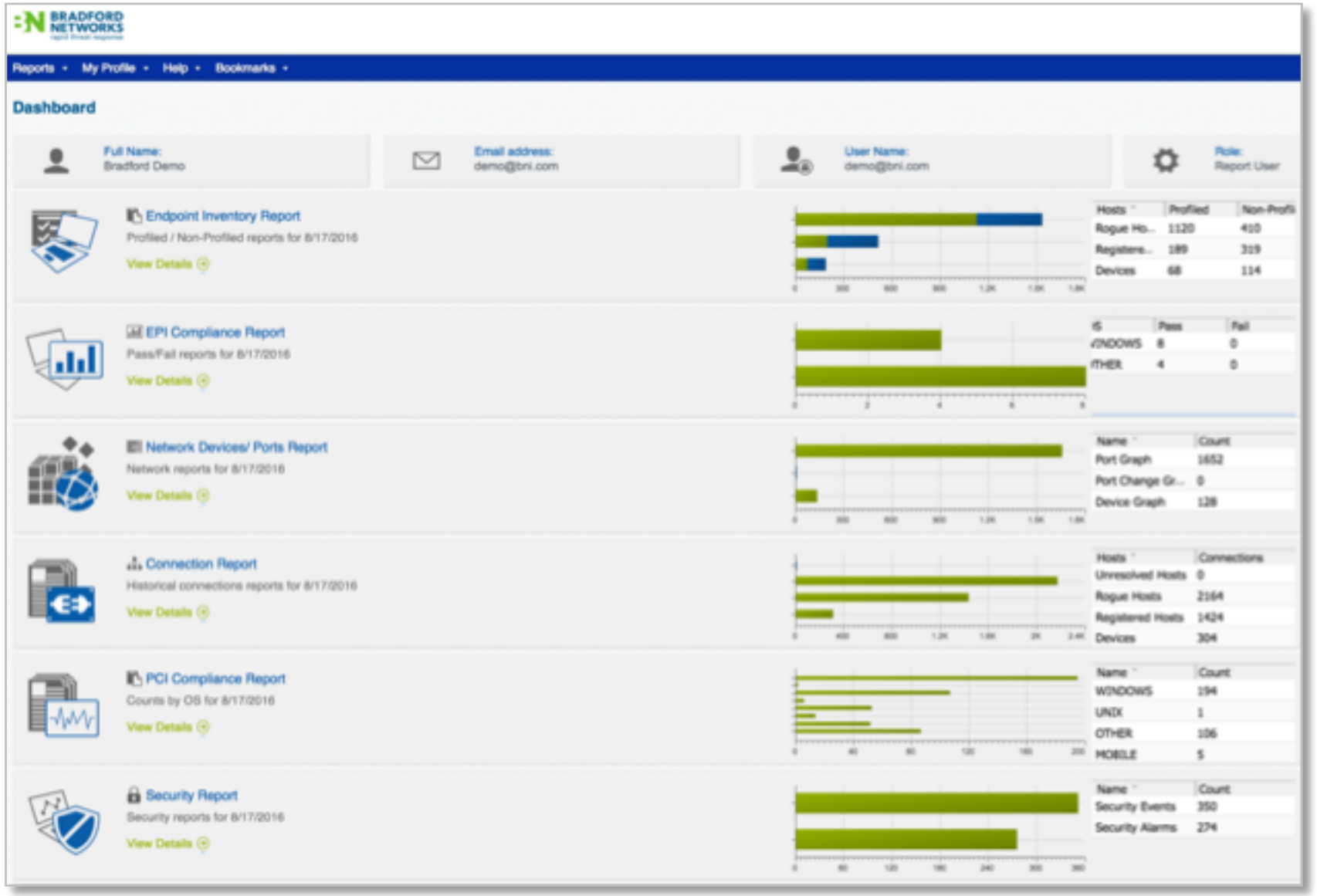
› Возможность динамического обеспечения микросегментации сетевой инфраструктуры на базе различных атрибутов устройств и конечных узлов – роли, профиля, использования приложений и др.

› Архитектура решения не требует мониторинга сетевого трафика, таким образом избегая необходимости внедрения отдельного ПАК в каждой локации в распределенных инфраструктурах

› Решение может быть легко развернуто в инфраструктуре ISP и MSSP в виртуальном виде с предоставлением соответствующих опций

› Имеет возможность создавать детальные профили устройств, которые могут быть очень важны по мере развития IoT в составе инфраструктуры

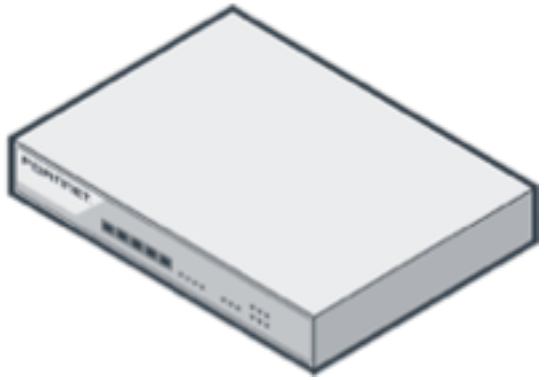
FortiNAC – Аналитика и Отчетность



Безопасность в мире IoT

FortiNAC

Network Access Control



- Идентификация, профилирование всех конечных узлов, IoT, устройств, пользователей, приложений
- Сегментация сети на основе характеристик конечных узлов и поведения
- Динамическая оценка риска и автоматическое применение мер противодействия, в том числе для устройств сторонних производителей

Watching Every Node on the Network

Сравнение с конкурентами

Небольшая Battle card

Сравнение встроенного функционала

	Fortinet FortiNAC	Aruba ClearPass	Cisco ISE	ForeScout CounterACT
Choice of Authentication (802.1X, non-AAA, Captive Portal, WebAuth, MACauth)	✓	✓	O Weak sequential support	✗ Weak .1X support
Multivendor Support	✓	✗ Limited	✗ Limited	✗ Limited
Profiling (no additional license)	✓	✓	✗	✓
Basic guest (included)	✓	✓	✓	✗
Can use privileged SSH / SNMP access for enforcement	✓	✗	✓	✗

Сравнение функционала BYOD

	Fortinet FortiNAC	Aruba ClearPass	Cisco ISE	ForeScout CounterACT
Secure Onboarding (iOS, Android, Chromebooks)	✓	✓	✓	✗ Requires 3rd Party Servers
Device provisioning workflows (BYOD and Device Registration-non smartphones, tablets, laptops)	✓	✓	✓	✗
MDM integration included in base license	✓	✓	✗ Requires Apex License	✗ Requires Licensed Plugins

Сравнение функционала управления гостевым доступом

	Fortinet FortiNAC	Aruba ClearPass Guest	Cisco ISE	ForeScout CounterACT
Social Login Support	✓	✓	✗ Limited Social Login Support	✗
Highly Customizable Guest Portal	✓	✓	✗	✗
Sponsor Option	✓	✓	✓	✗

Проверка конечных узлов

	Fortinet FortiNAC	Aruba ClearPass	Cisco ISE	ForeScout CounterACT
Third party integration included	✓	✓	✗	✗
Integration with 70+ EPP vendors	✓	✓	✗	✗
Can Block USB devices	✓	✓	✓	✗
Device evaluated before allowed on network	✓	✓	✓	✗

Автоматизированная реакция на угрозы

	Fortinet FortiNAC	Aruba ClearPass	Cisco ISE	ForeScout CounterACT
Event Correlation Engine	✓	✗	✗	✗
Extensible Actions	✓	✗	✗	✓
Audit Trail	✓	✗	✗	✓
Forensics & Trending	✓	✗	✗	✗

Слабости решения Cisco

- Very limited 3rd party integration
  - Cisco works best with… *Cisco*! (must be newer switches with right OS)
  - 3rd party integration is charged as a subscription
- Appliance licenses are all subscription
  - Requires additional licensing for profiling
  - Not IoT friendly
  - PLUS and APEX license are subscription only
- Scalability issues in large deployments
- Multi-Factor Authentication (MFA/2FA) through RADIUS only


FORTINET
NETWELL