FortiMonitor – Управление сетью и операциями по обеспечению безопасности

Olesya Tarabrina, SE

Fortinet Security Fabric

Обширное

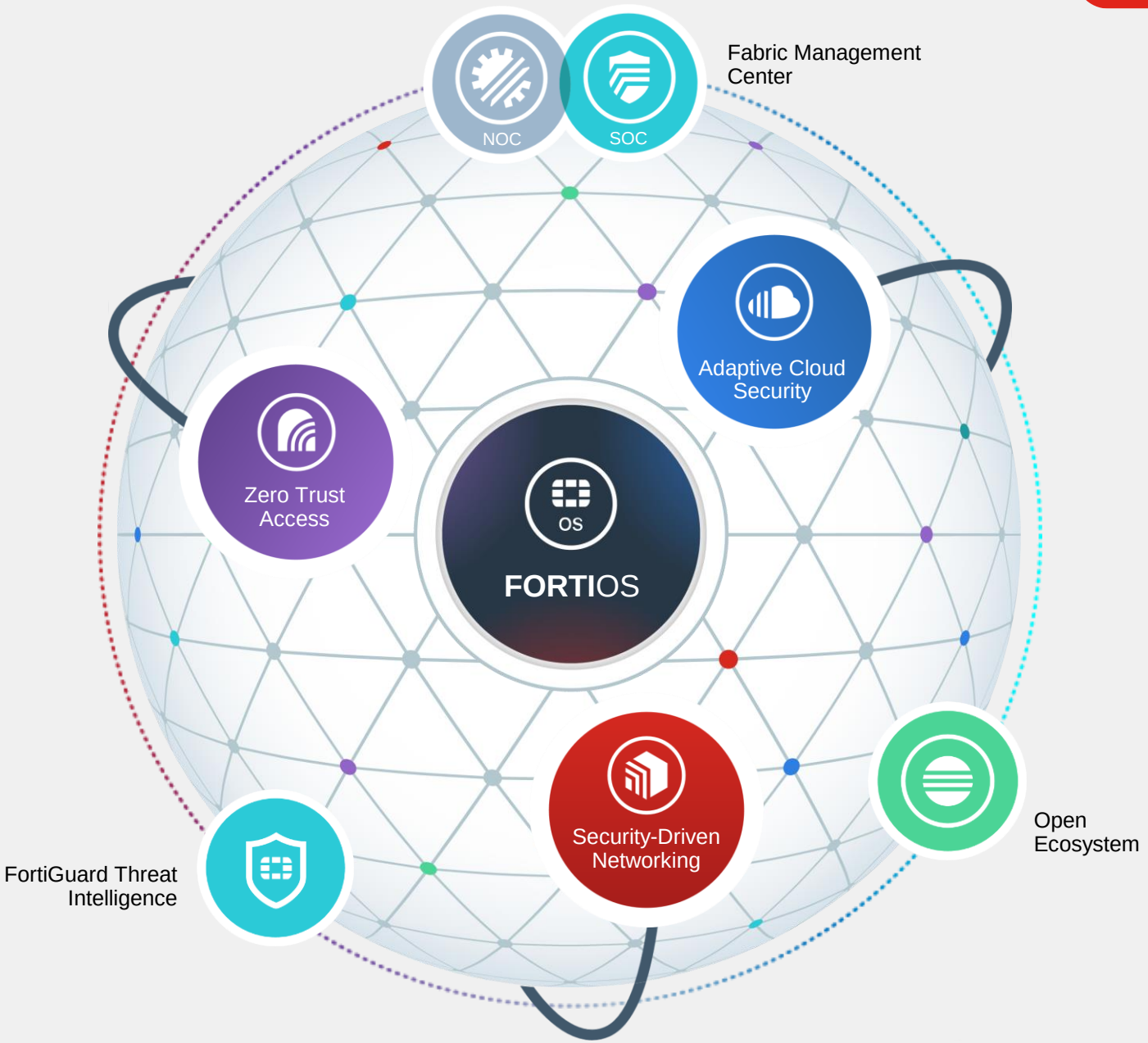
видимость и защита всей поверхности цифровой атаки для лучшего управления рисками

Интегрированное

решение, которое снижает сложность управления и делится информацией об угрозах

Автоматизированное

самовосстанавливающиеся сети с безопасностью на основе искусственного интеллекта для быстрой и эффективной работы



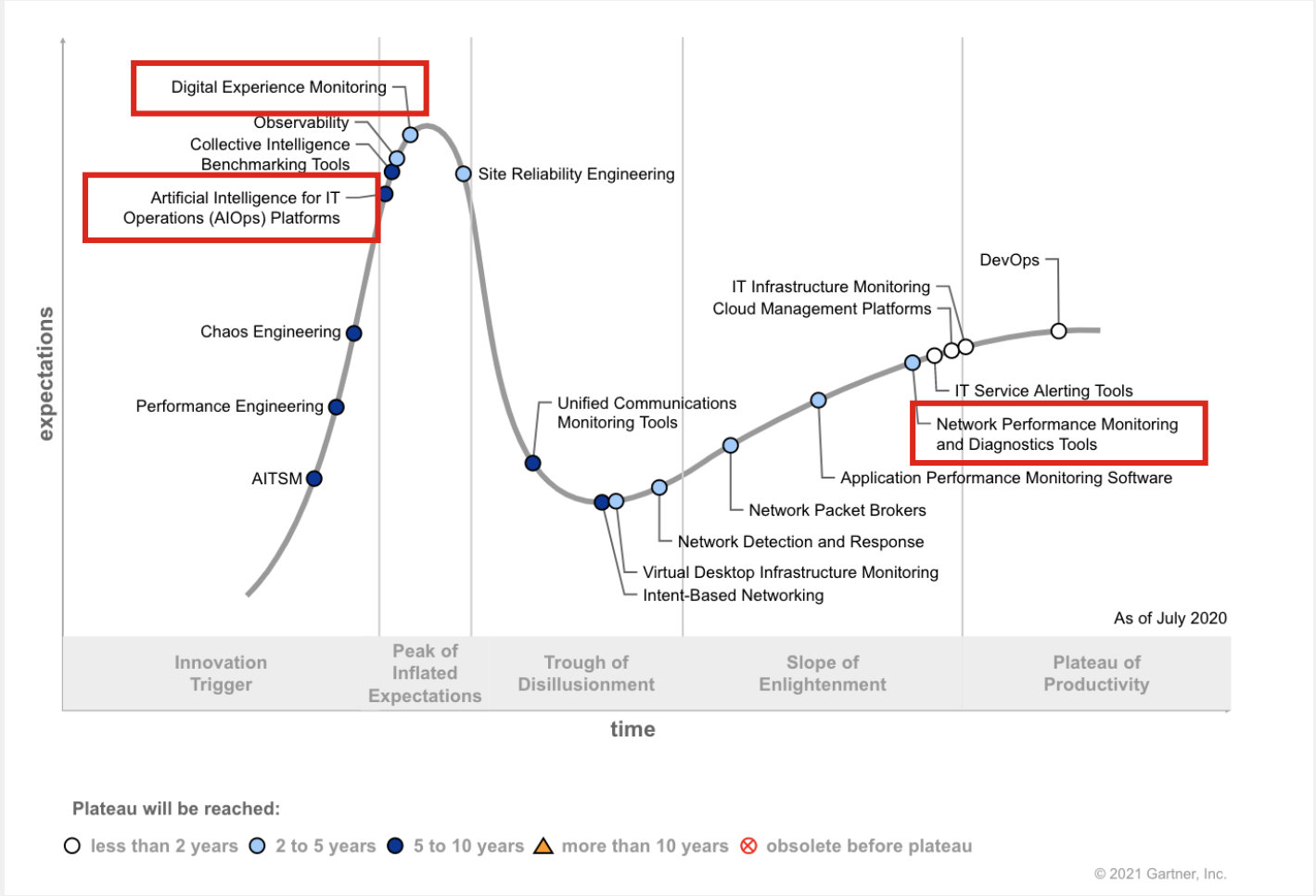
Понимание ландшафта мониторинга

SaaS-Based Network Performance Monitoring (NPMD)

Digital Experience Monitoring (DEM)

Тренды

Корпоративные сети трансформируются, и сетевые операции тоже



К 2024 году 50% NOC-команд должны будут изменить архитектуру своего стека сетевого мониторинга.

Источник: Gartner - Market Guide for Network Performance Monitoring and Diagnostics (G00740014); Gartner Hype Cycle for IT Performance Analysis, 2020 (G00448200)

Представляем AIOps Network Operations

Улучшение TCO для
сетевых операций на 50%+

FortiMonitor

- Сетевой мониторинг
- Обнаружение аномалий
- Аналитика для устранения неполадок

FortiManager, FortiAIOps

- Корреляция WAN, LAN, межсетевого экранирования
- Автоматизация сортировки инцидентов
- Управление изменениями

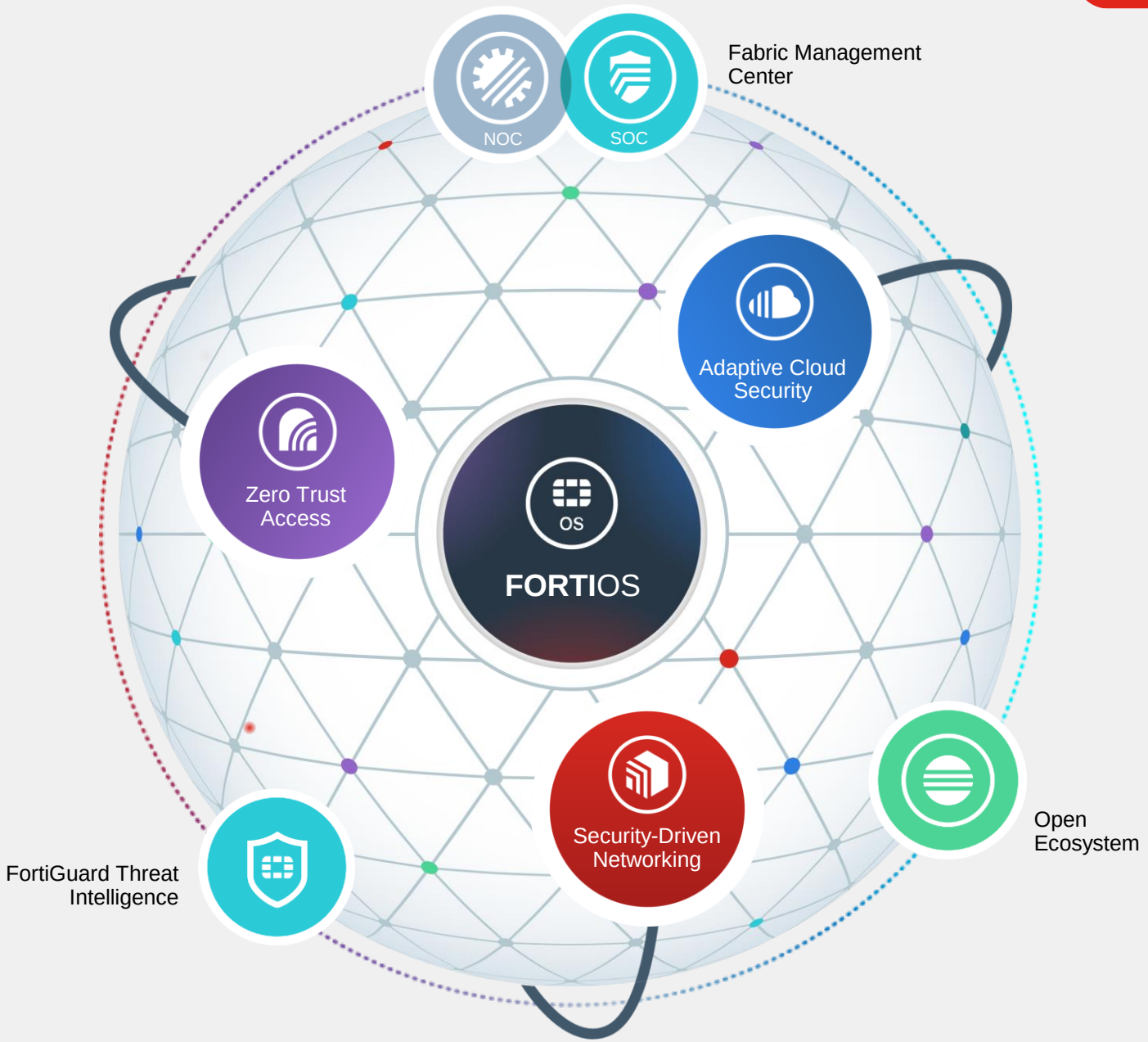
FortiSOAR

- 300+ готовых сценариев
- Встроенные механизмы организации процесса
- NetOps-скрипты

Fabric Management Center NOC

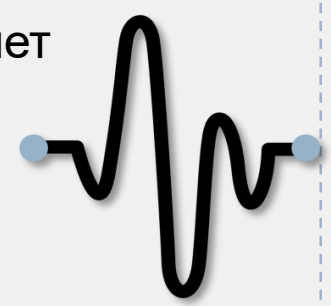
FortiMonitor

Network Performance Monitoring (NPMD), Digital Experience Monitoring (DEM) & Incident Management



FortiMonitor

FortiMonitor (Panopta) - это целостная SaaS-платформа мониторинга, которая объединяет команды и инструменты и позволяет предприятиям проактивно решать проблемы ИТ-инфраструктуры. FortiMonitor наблюдает за работоспособностью и производительностью всей гибридной инфраструктуры и управляет инцидентами непосредственно с единой платформы.



- Основана в 2007 г.
- 400+ клиентов
- Тысячи через партнеров

Вызовы & Решения

NOC Challenges

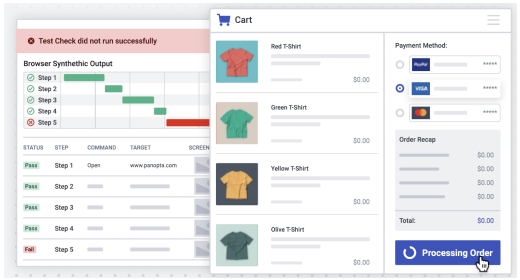
Сложность операций для фрагментированных сетей

Ручные операции

Наглядность цифрового опыта

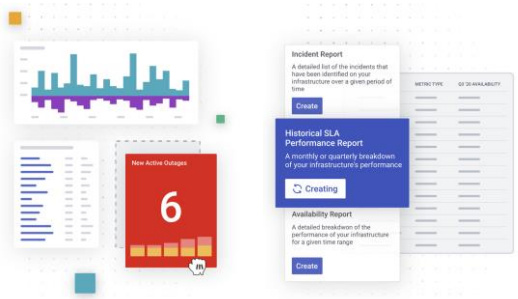
Анализ причин

Ответ FortiMonitor



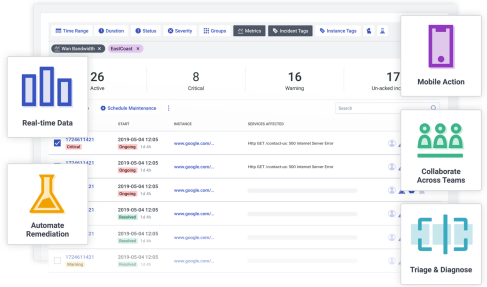
Мониторинг цифрового опыта

Выйдите за рамки показателей и расставьте приоритеты для конечных пользователей, независимо от того, являются они клиентами или сотрудниками.



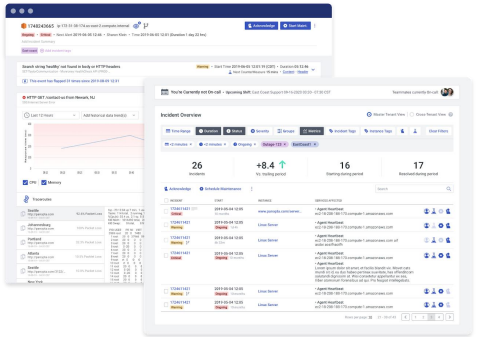
Повышенная видимость

Быстро и легко получайте необходимое представление о работоспособности любого сервера, устройства, сетевого оборудования или приложения.



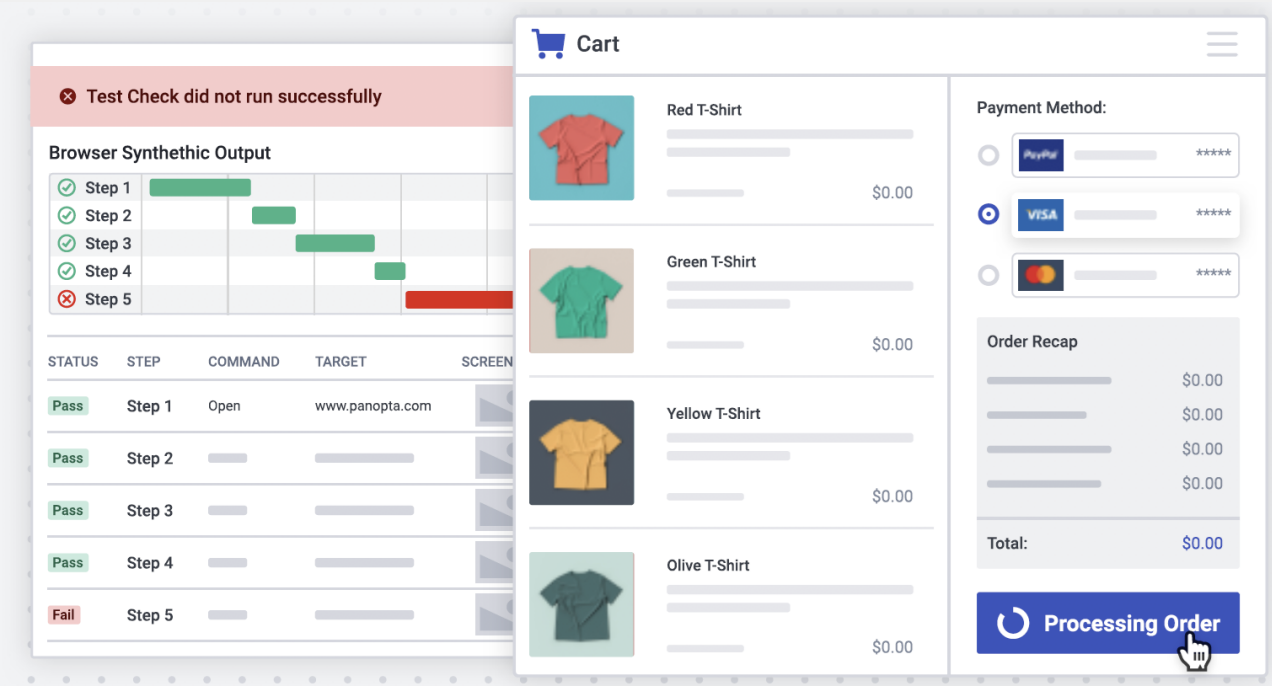
Устранение шума

Ускорьте поиск первопричины и сократите количество ручных накладных расходов на диагностику, сортировку и устранение неисправностей.



Автоматическое исправление

Освободите свою команду от трудоемкого управления инцидентами, чтобы решать проблемы до того, как они возникнут.



1. Получите показатели работоспособности и производительности приложений и систем

2. Запускайте тесты с узлов по всему миру, чтобы проверить предоставление услуг

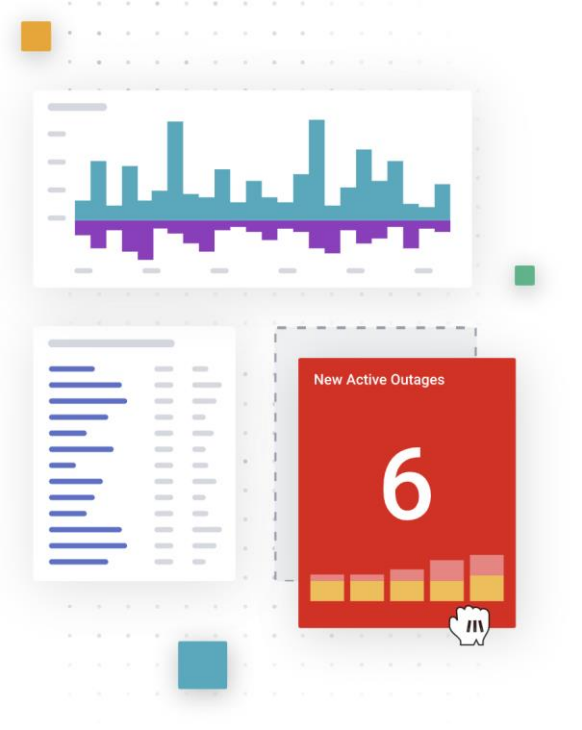
3. Используйте синтетику веб-браузера для воспроизведения опыта конечного пользователя

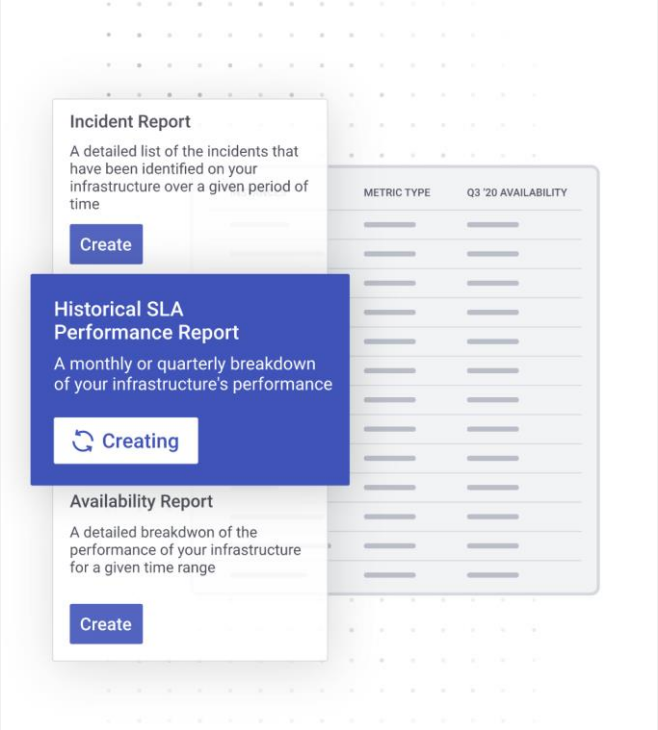
Мониторинг цифрового опыта

Выйдите за рамки показателей и расставьте приоритеты для конечных пользователей независимо от того, являются они клиентами или сотрудниками. Взаимодействие с другими людьми

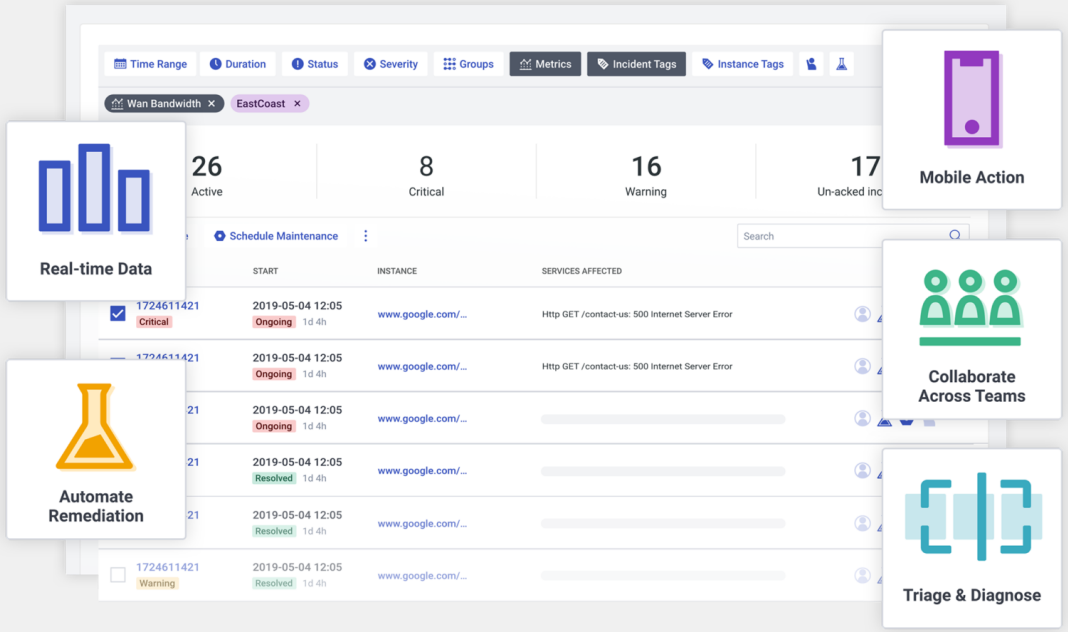
Повышенная видимость

Быстро и легко получайте необходимое представление о работоспособности любого сервера, устройства, сетевого оборудования или приложения.





1. Единый источник достоверной информации для всего вашего предприятия
2. Используйте синтетические проверки для наглядности пользовательского опыта
3. Контроль доступа с опциями для публичных просмотров



1. Получайте оповещения только о том, что действительно важно
2. Используйте автоматизацию для выполнения трудоемких задач
3. Эффективно сообщайте о происшествиях и устраняйте их

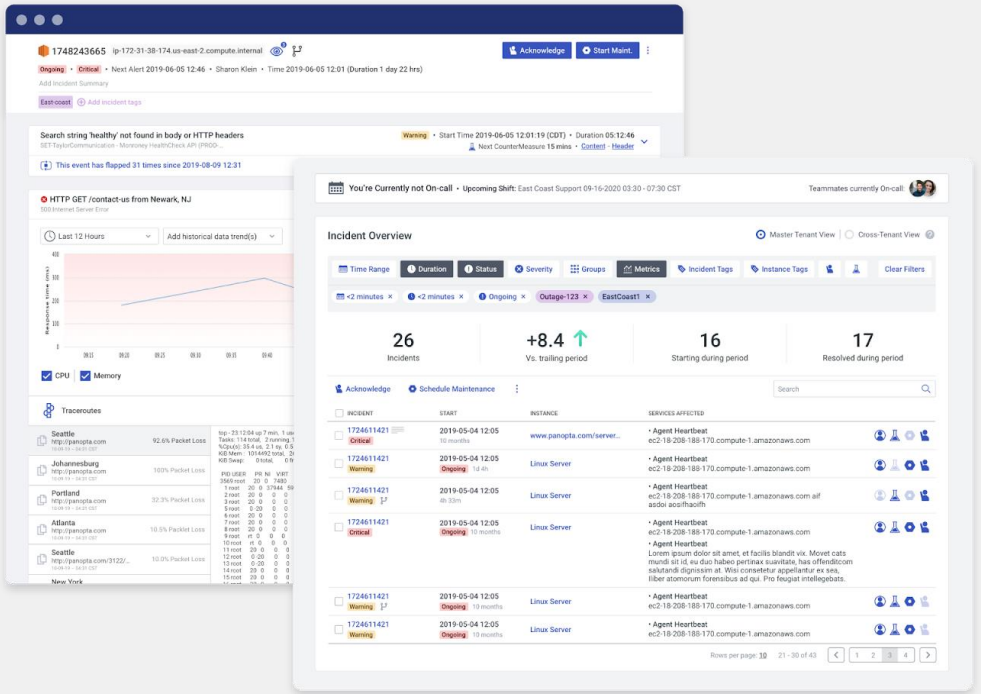
Устранение шума

Контролируйте все, но предупреждайте только о том, что важно.

Ускорьте поиск первопричины и сократите количество ручных накладных расходов на диагностику, сортировку и устранение неисправностей.

Автоматическое исправление

Освободите свою команду от трудоемкого управления инцидентами, чтобы решать проблемы до того, как они возникнут.



1. Автоматизируйте сортировку инцидентов и создание заявок
2. Эффективно сообщайте о происшествиях и устраняйте их
3. Оптимизация реагирования на будущие инциденты

Обзор решения FortiMonitor

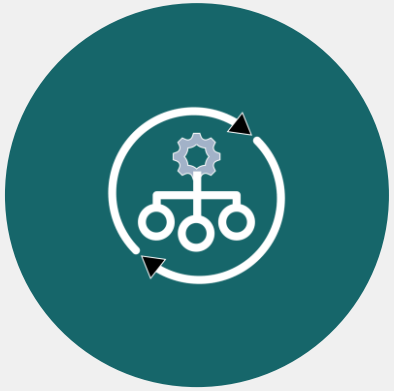
Мониторинг, не зависящий от поставщика

Единая платформа для мониторинга и управления инцидентами для всей инфраструктуры вашего предприятия

Рабочие процессы и оповещения

Создавайте рабочие процессы и оповещения в соответствии с вашей инфраструктурой, чтобы снизить утомляемость от оповещений

Автоматическое исправление



Автоматическая диагностика и устранение проблем до того, как они возникнут

Что делает FortiMonitor?

SaaS-Based Network Performance Monitoring (NPMD)

Digital Experience Monitoring (DEM)

Сценарии использования FortiMonitor

Упростите NetOps в мультивендорной среде

Мониторинг цифрового опыта

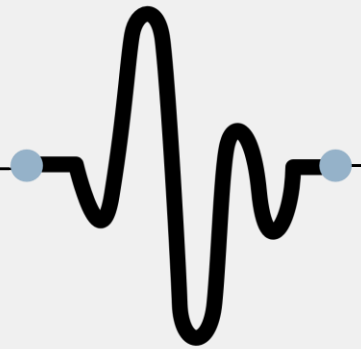
Используйте синтетические тесты для измерения опыта конечных пользователей

Видимость за пределами сети

Мониторинг производительности сети

Мониторинг гибридных сетей в частных и публичных облаках

Адаптация к любой среде



Автоматизация NOC

Автоматизируйте диагностику и действия по исправлению, чтобы снизить MTTD и MTTR до превышения SLA

Повышение операционной эффективности

Централизованные операции

Консолидация и централизация мониторинга, реагирования и автоматизации инфраструктуры

Устранение разрастания инструментария и избыточности

Истории успеха

FortiMonitor улучшил среднее время восстановления (MTTR) на 60%

«Panopta (FortiMonitor) позволила нам достичь единого унифицированного представления о состоянии нашей облачной инфраструктуры и объединить наши корпоративные операции» – **Vijay Chodavarapu, VP of Global Cloud Operations and SRE**

Исходное состояние

Катализатор
Накапливаются нерешенные инциденты, и разрастание поставщиков становится неуправляемым

Вопросы

- Постоянная борьба за понимание внутренних SLA
- Нет единого источника правды и постоянное указание пальцем
- Из-за разрастания инструментов мониторинг невозможно было масштабировать

Подход FortiMonitor

Решение
Консолидация и централизованное управление

Практические результаты

- Перенос AWS, Azure, GCP и размещенной инфраструктуры на платформу
- Маркировка системной логики для управления маршрутизацией
- Надежные синтетические проверки, прием облачных данных и контрмеры

Полученная ценность

Развертывание
Сложные теги и шаблоны для ускорения подключения существующей и расширяемой инфраструктуры

Экономия

- 60% снижение затрат на диагностику и разрешение инцидентов
- NOC обладает единым источником истины
- Доступ руководства к данным SLA в реальном времени

FortiMonitor решает проблемы еще до того, как они возникнут

«Я хочу управлять службой, облачной службой, в которой я понимаю вещи в режиме прогнозирования и предсказуемым образом. Я хочу знать о проблемах до того, как это сделает мой клиент, чтобы я мог принять меры, и мой клиент не пострадал. Это основная причина, по которой я купил Panopta (FortiMonitor)». - ***Roshan Popal, Senior Vice President of Cloud Systems Engineering***

Исходное состояние

Катализатор

Компания MicroStrategy, располагающая командой из более чем 60 сотрудников и обслуживающая более 500+ клиентов, нуждалась в платформе мониторинга, которая могла бы дать им детальный обзор среды своих клиентов, а также единое представление, позволяющее видеть все сразу.

Вопросы

- Отсутствие детальной видимости в среде клиентов
- 1300+ заявок на поддержку в неделю, проблема масштабируемости
- Дорогостоящие решения без специальных показателей

Подход FortiMonitor

Решение

Наличие высокоуровневых представлений о развертываниях и функций автоматической отчетности помогло высшему руководству понять, где они могут регулировать ресурсы.

Практические результаты

- Решение для независимого мониторинга, которое объединяет видимость всех развертываний в одном месте без дополнительных затрат
- Пользовательские панели мониторинга, отчеты, страницы состояния и возможность принимать пользовательские метрики
- Автоматическая диагностика и исправление

Полученная ценность

Развертывание

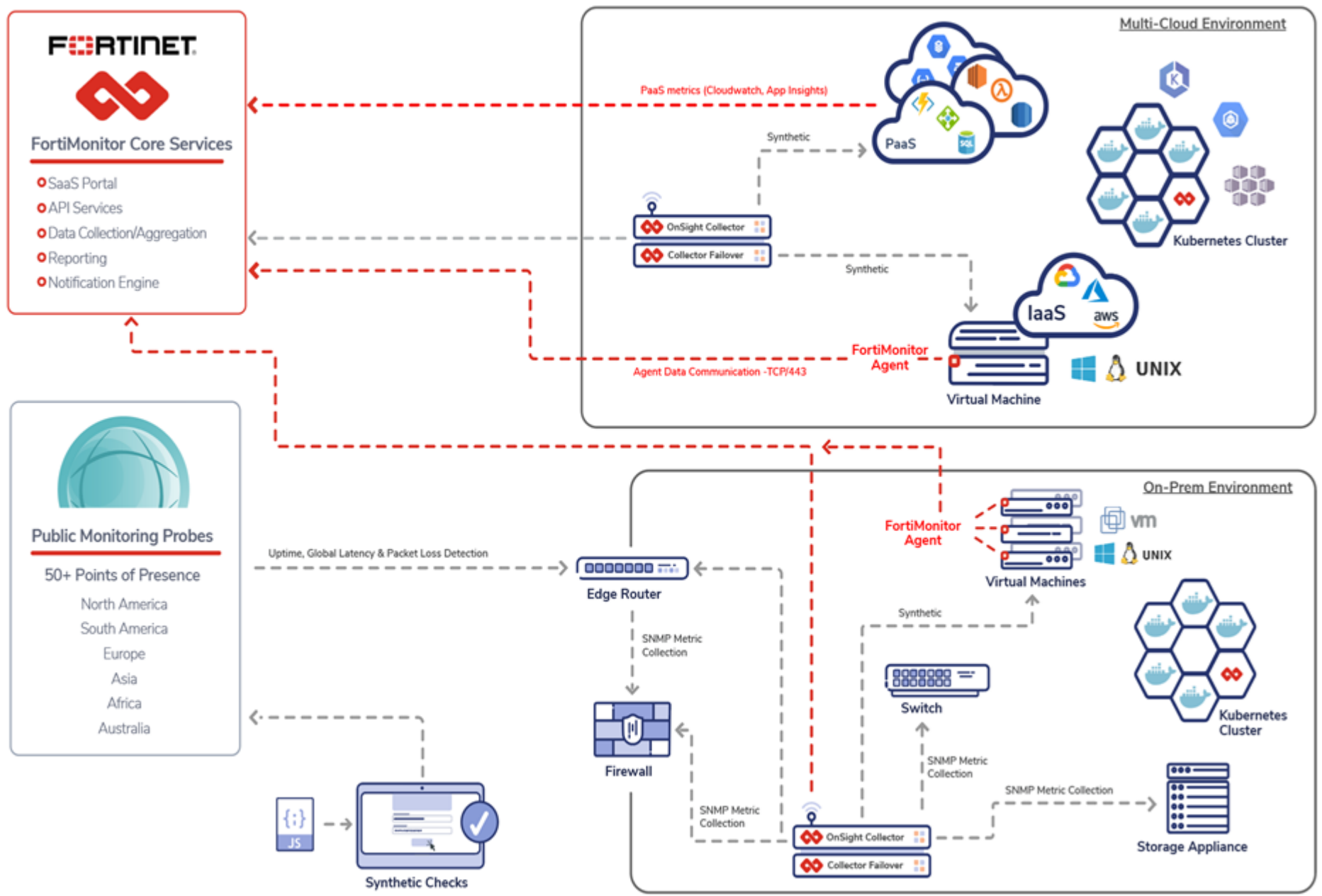
Обеспечение предсказуемости

Экономия

- Значительное сокращение сложности развертывания, что позволяет MircroStrategy предоставлять клиентам более качественное обслуживание.
- Повышение удержания сотрудников и их производительности при одновременном снижении выгорания персонала
- Сниженный MTTR

FortiMonitor

Архитектура



Первичное развертывание

1. Добавление инфраструктуры в FortiMonitor
2. Мониторинг
3. Хронология предупреждений
4. Визуализация
5. Ролевой доступ
6. Отчетность
7. Контрмеры

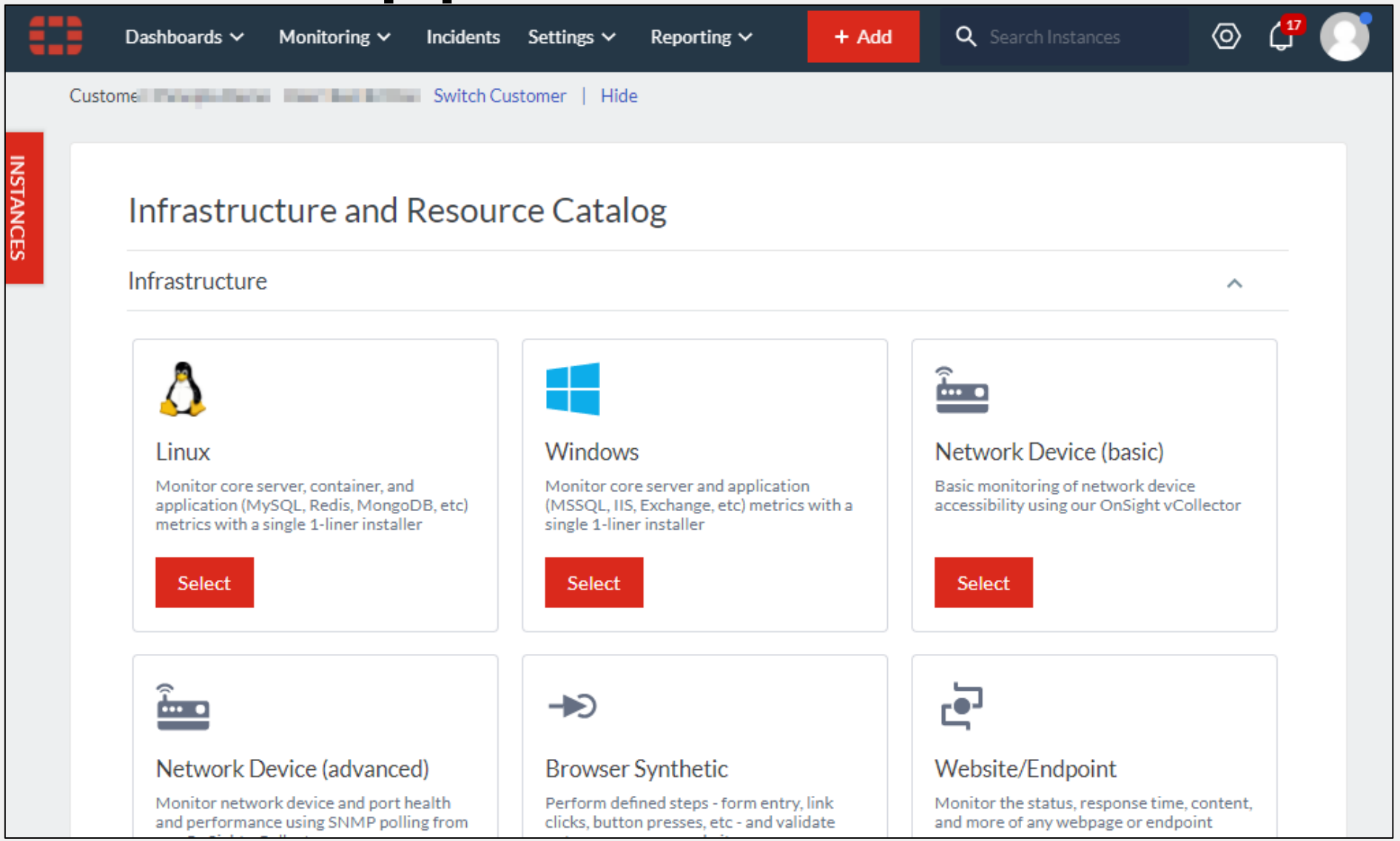
Методы интеграции с инфраструктурой

- VMWare Auto Discovery (API based)
- Public Cloud (AWS, Azure) Discovery
- Mass Agent Install
- OnSight Network Scan
- Kubernetes HELM
- REST API
- Вручную через UI

Методы развертывания и функции

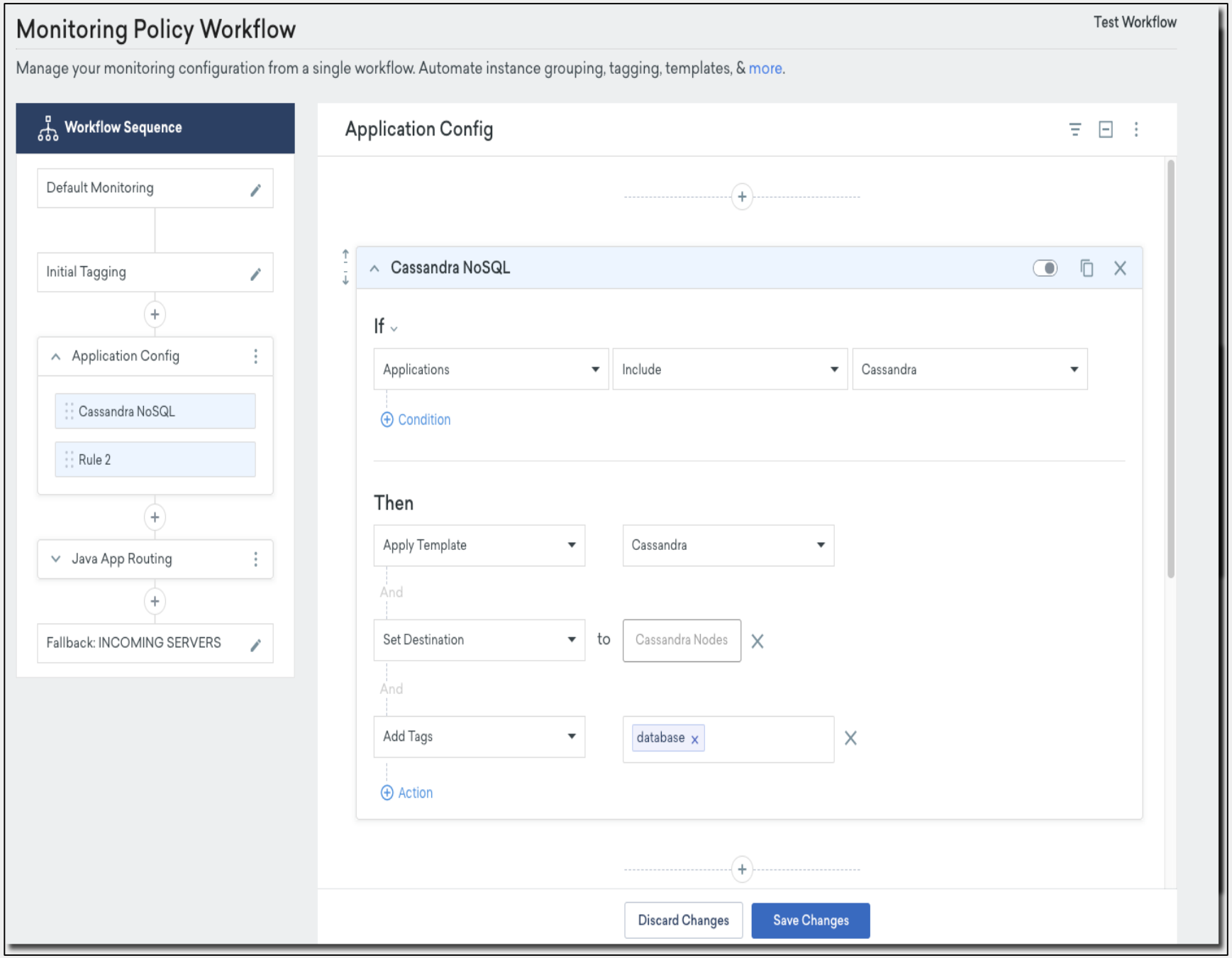
Методы	Функции					Требования	
	External monitoring	Server metrics	SNMP	Counter Measures	Auto-discover instances	Доступ к экземпляру	Сетевой доступ
FortiMonitor Agent	✓	✓		✓		✓	
OnSight Discovery	✓		✓		✓		✓
FortiMonitor Cloud Discovery	✓				✓		
OnSight vCollector installer	✓		✓		✓	✓	✓
Add a basic instance	✓		✓				
Add via API	✓		✓				

Простое добавление новых устройств через графический интерфейс



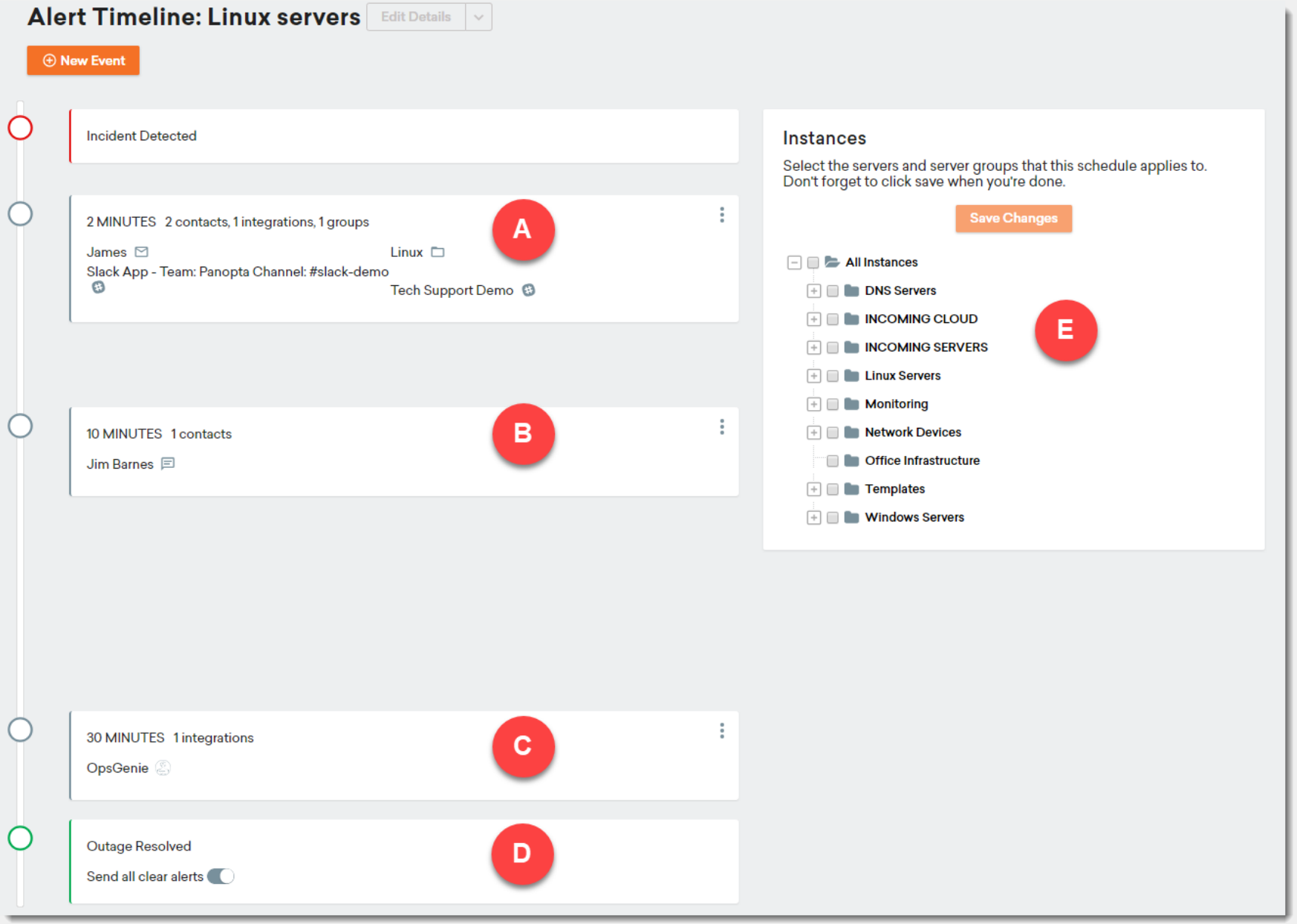
Мониторинг

- Мониторинг приложений
- Внешний мониторинг
- Мониторинг сетевых устройств (SNMP)



Хронология предупреждений

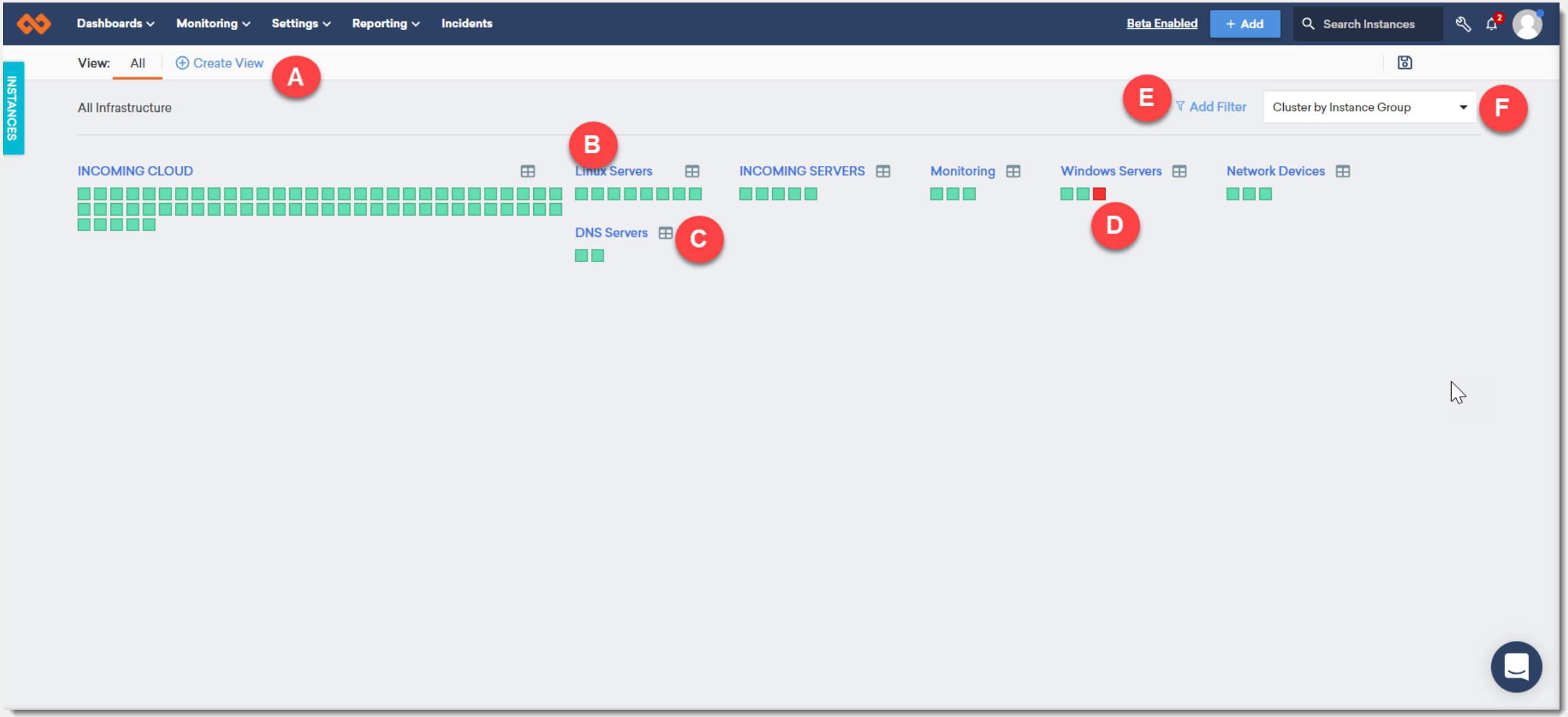
- Кто получает предупреждение
- Какой носитель уведомлений использовать (напрямую или через стороннюю интеграцию)
- Время между идентификацией инцидента и первым и последующими уведомлениями



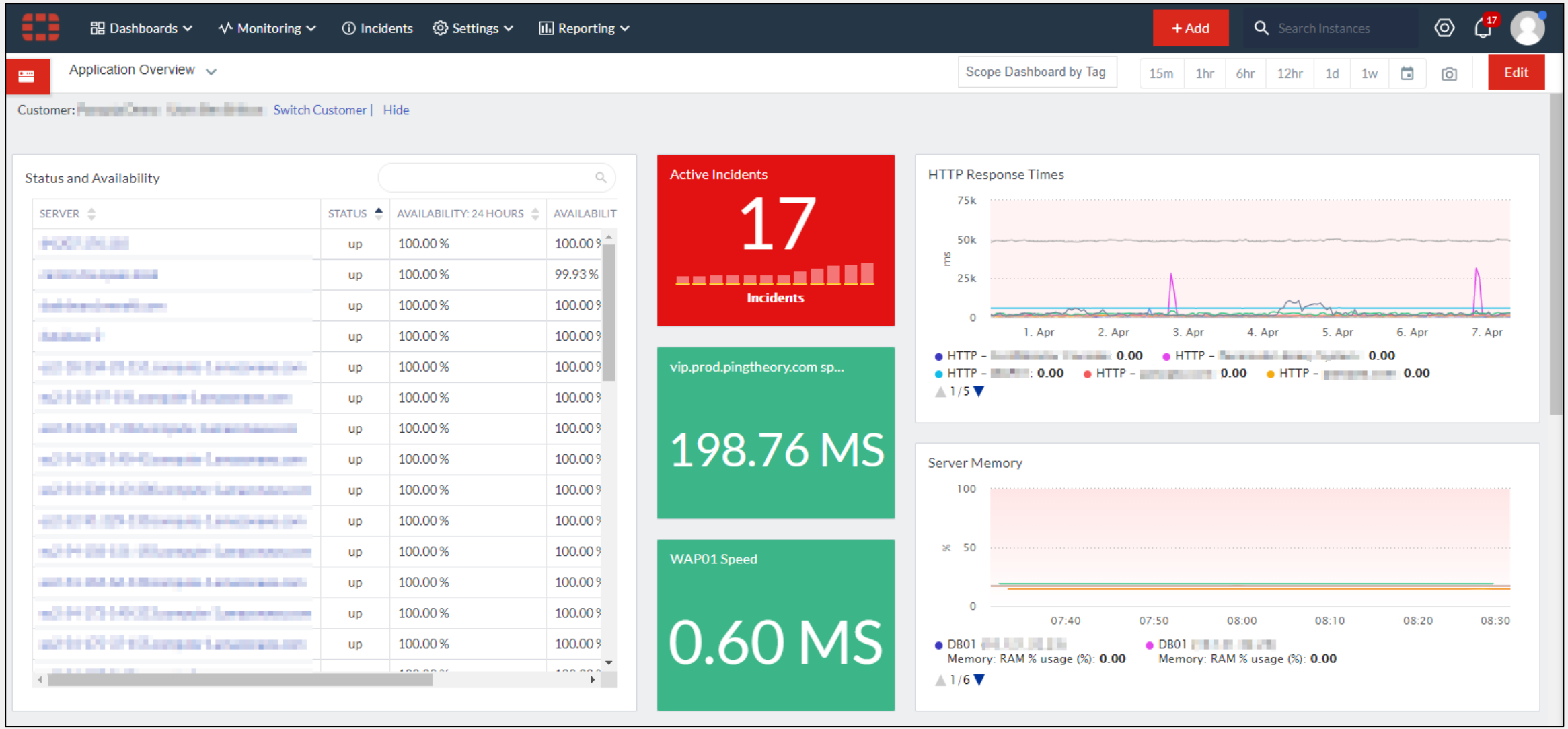
Визуализация

- Инфраструктурная карта
- Дашборд
- Страница сведений об экземпляре
- Страница статуса

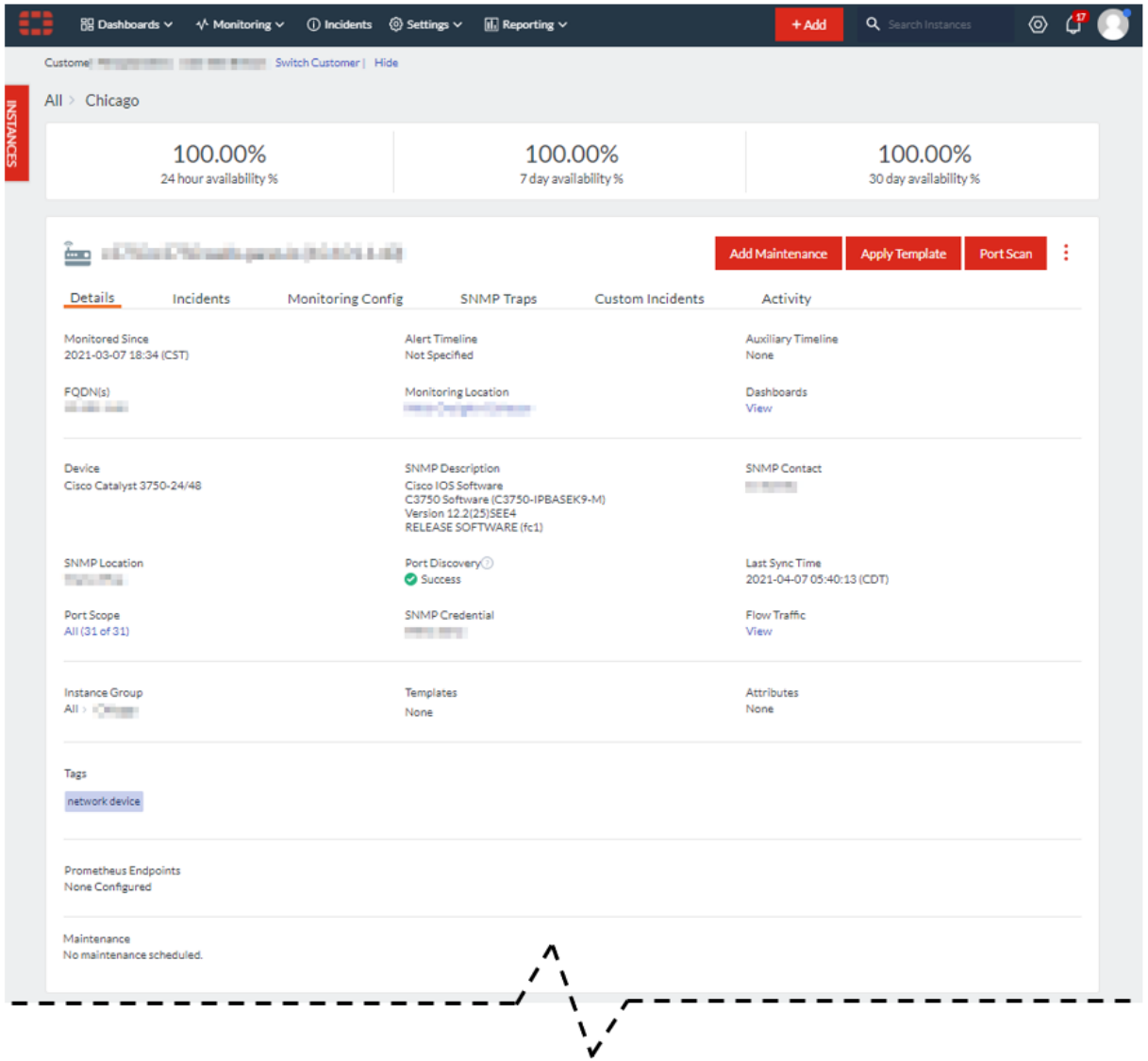
Инфраструктурная карта

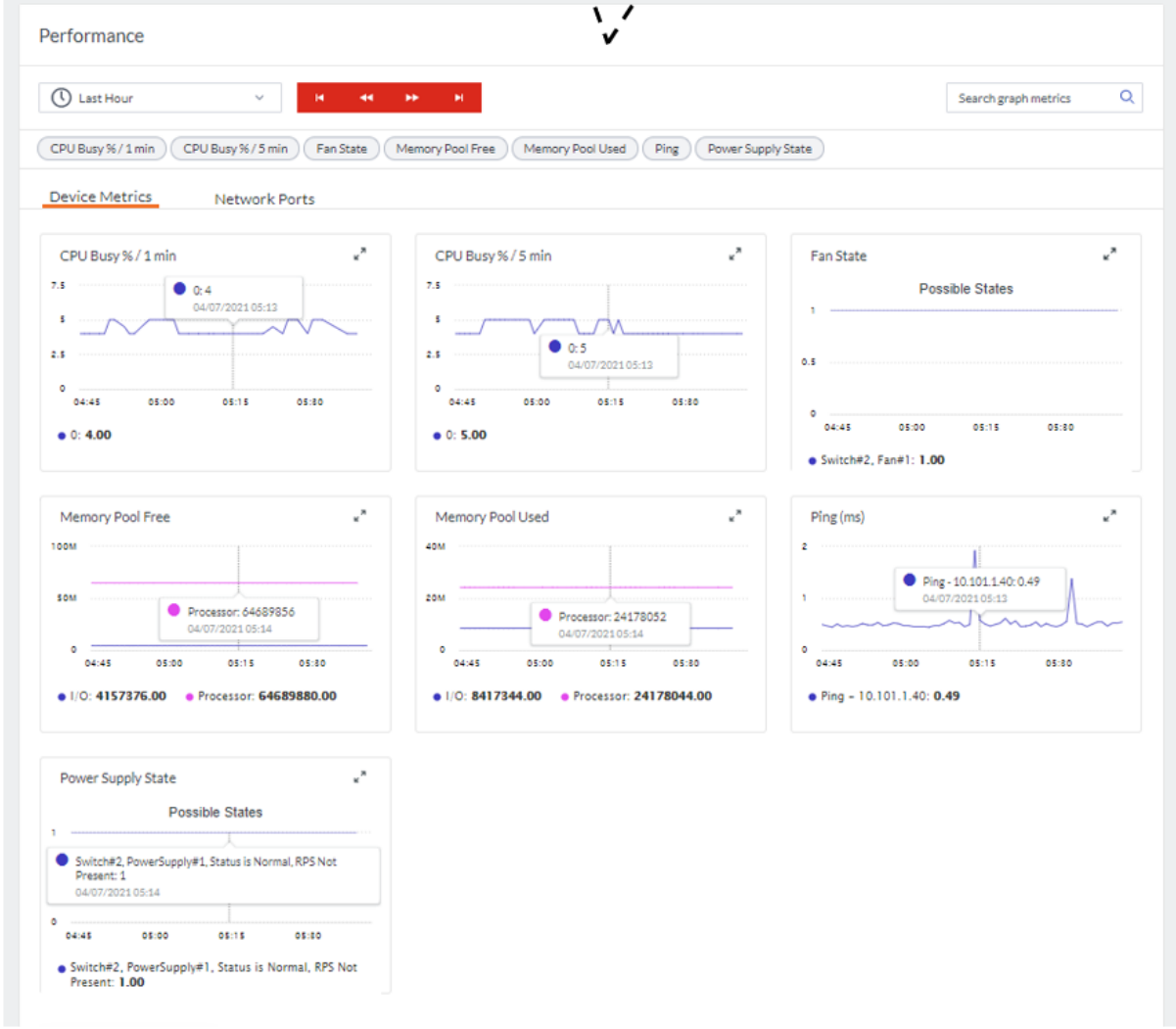


Гибкие панели мониторинга на основе виджетов



Подробные сведения о мониторинге устройства





Страница статуса

Пример: http://status.panopta.com/example

Ролевой доступ

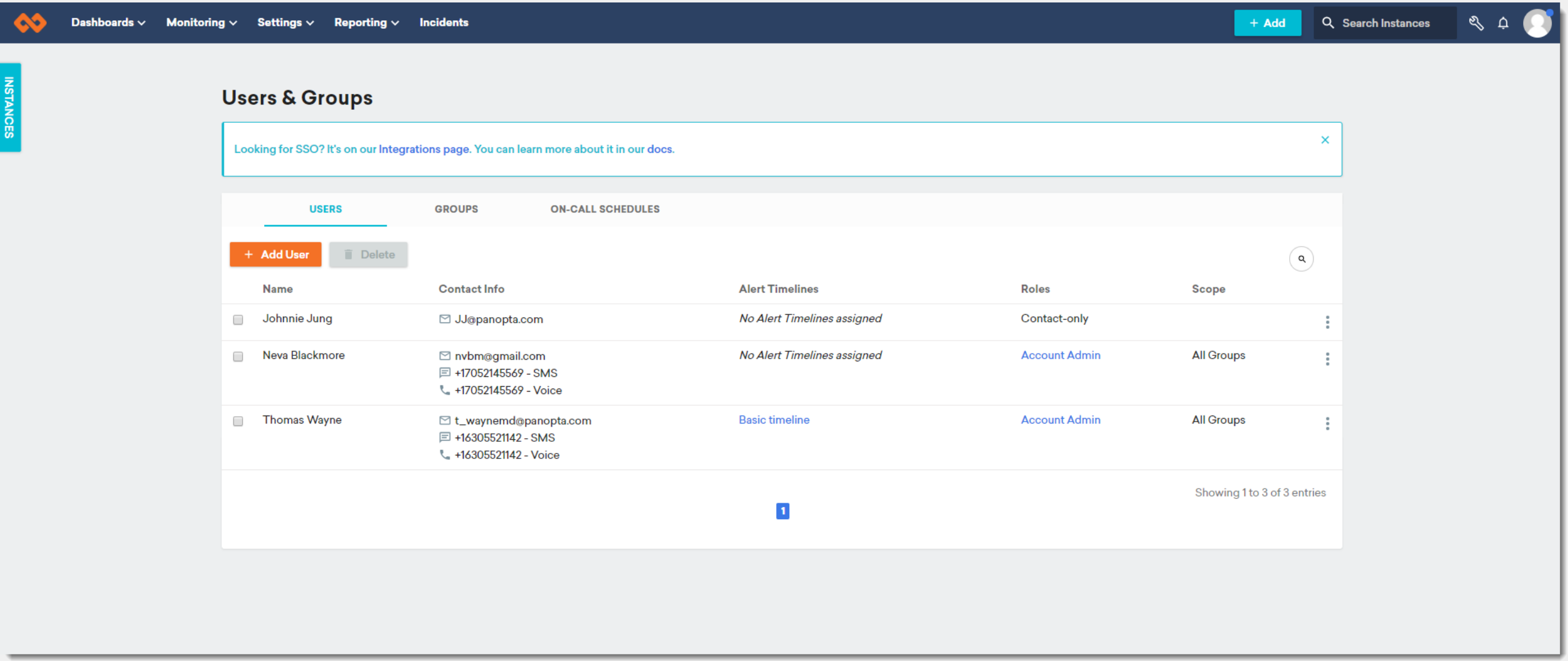
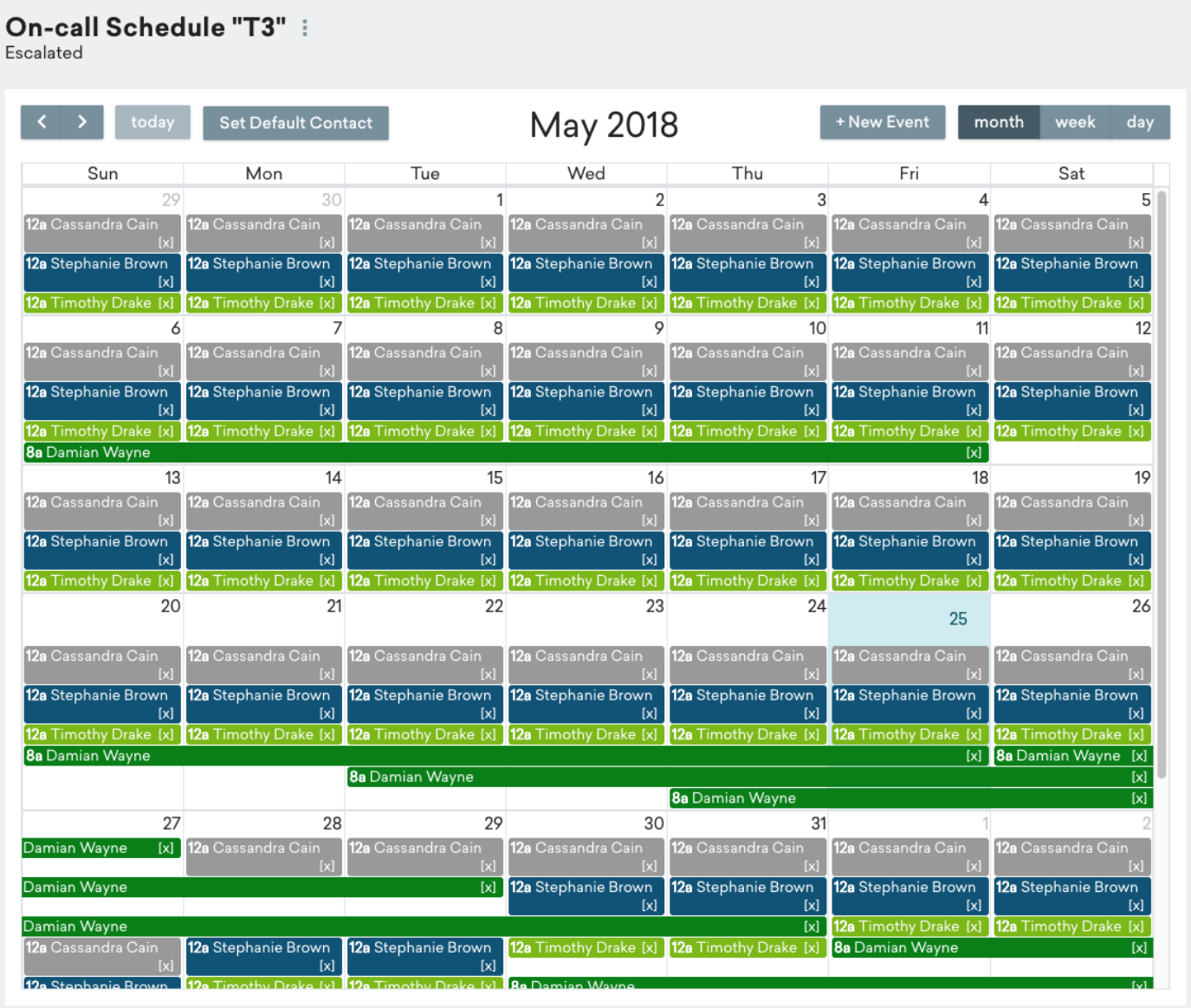
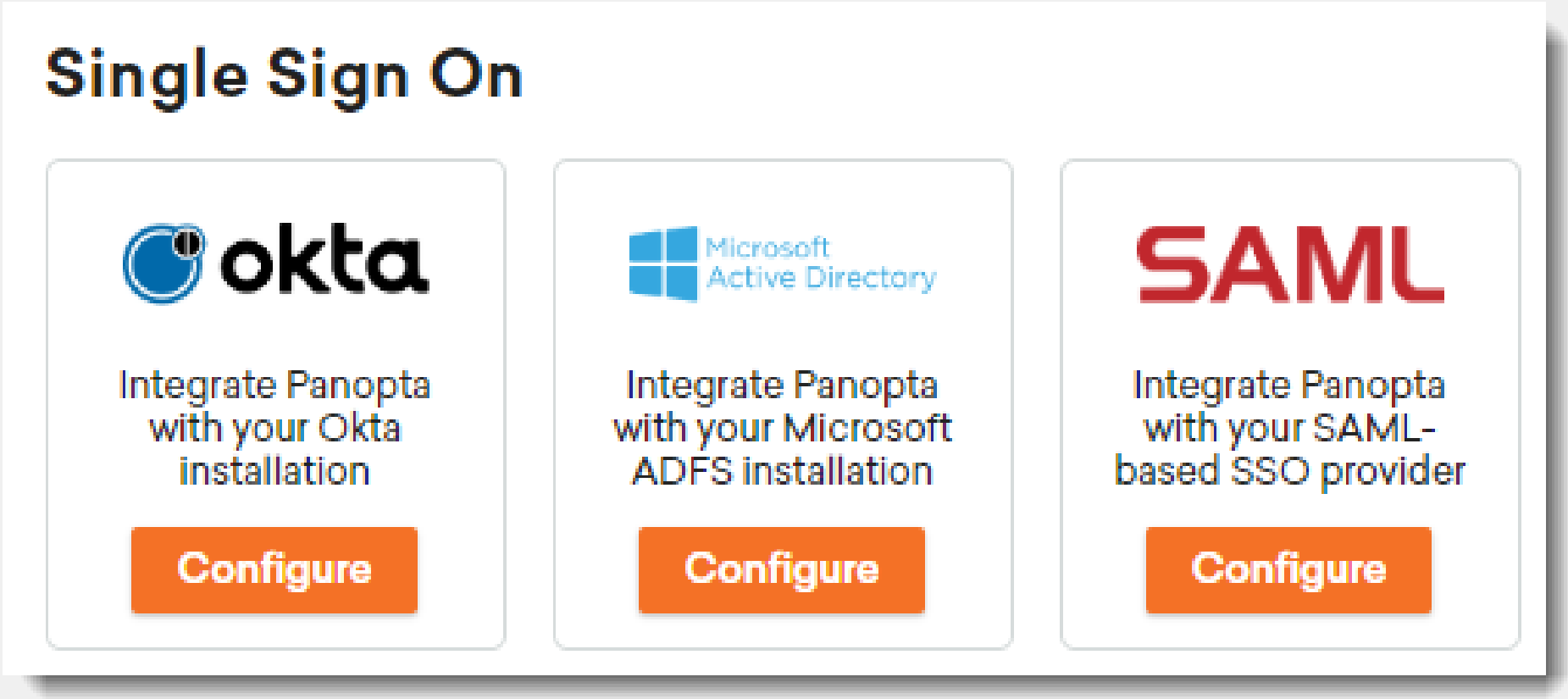


График дежурств

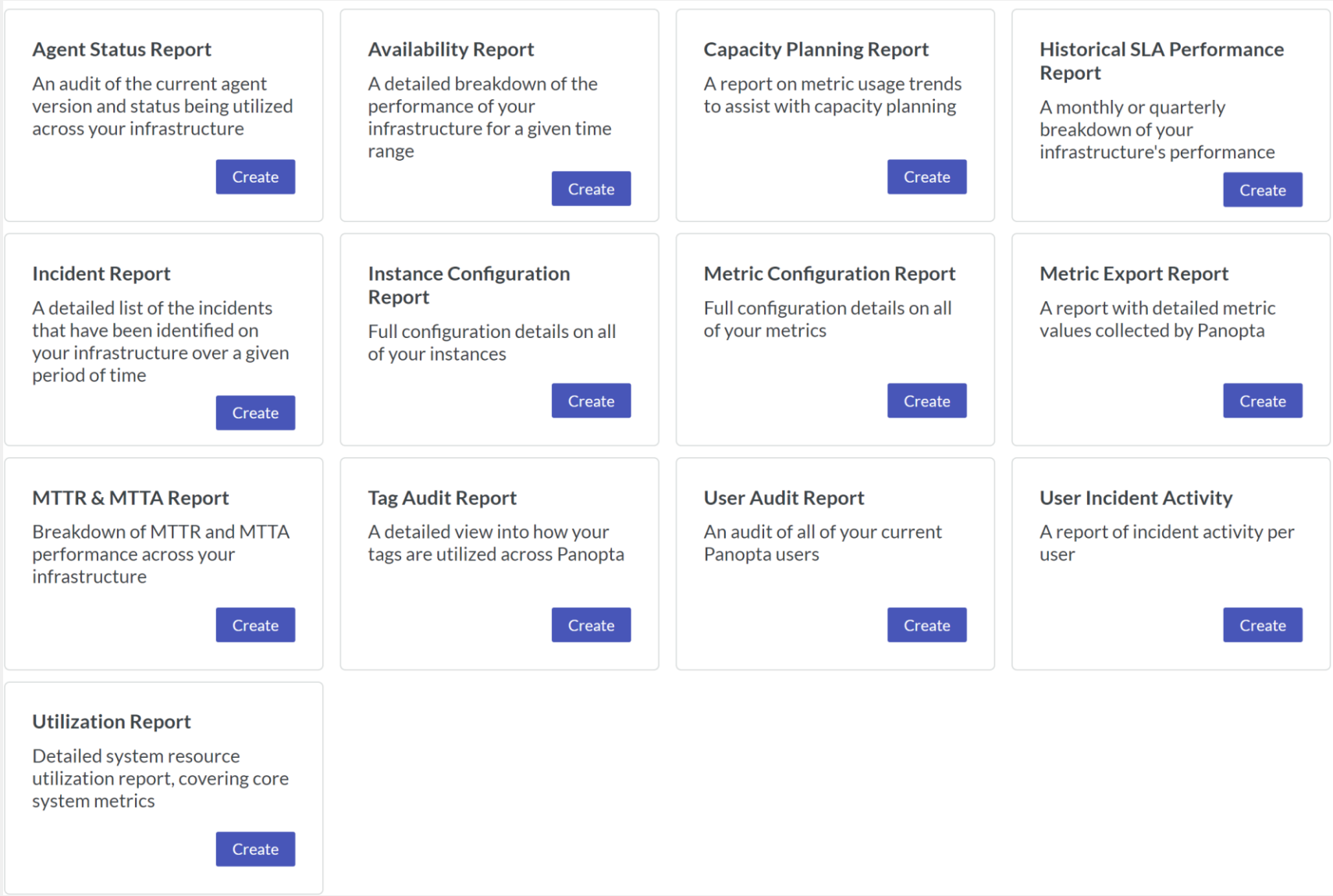


Single Sign-On (SSO)

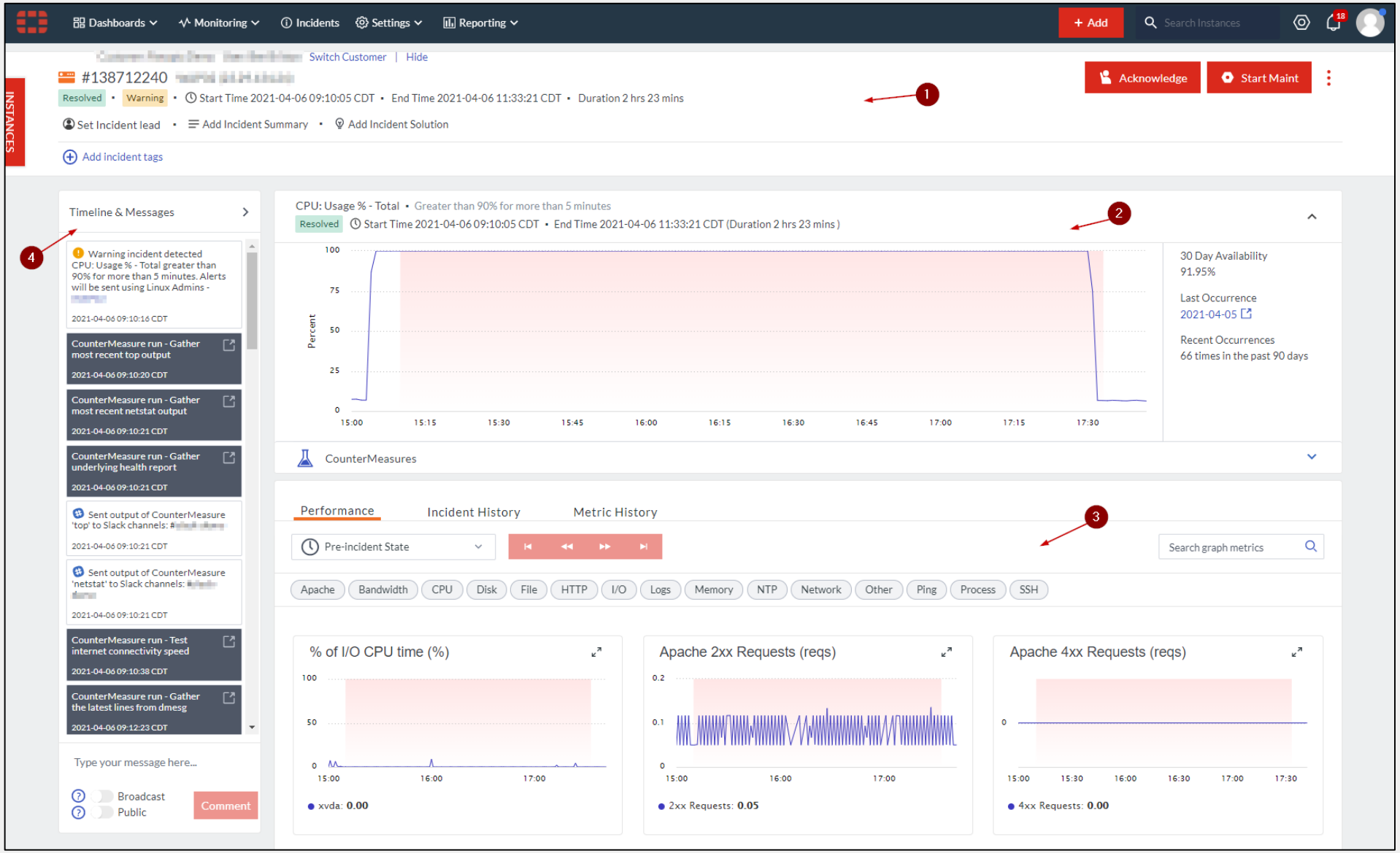


Отчетность

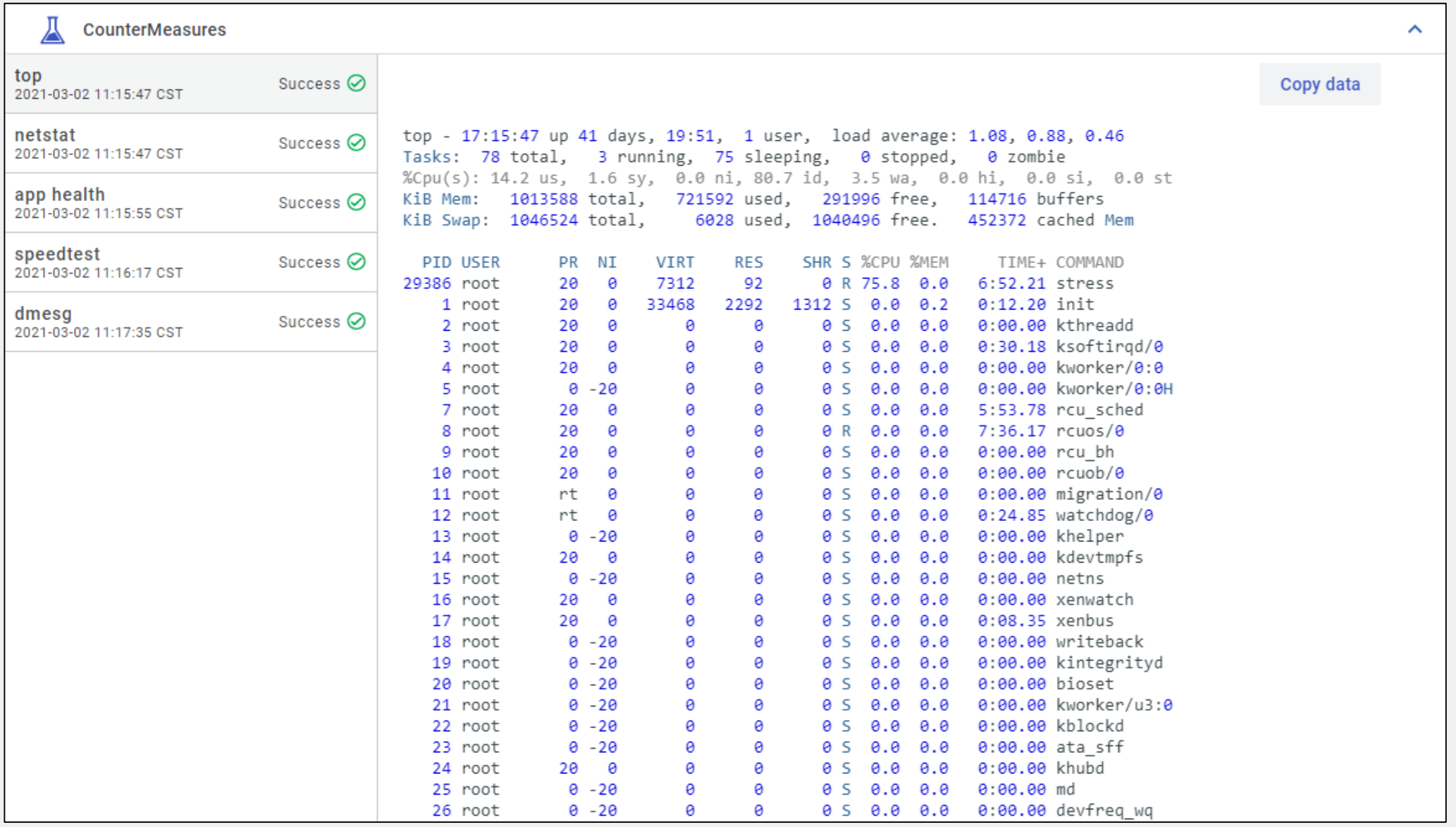
- Предустановленные отчеты
- Запланированные отчеты
- Специальные отчеты



Сведения об инциденте



Пример выходных данных контрмер



Резюме

Три ключевых момента

Мониторинг цифрового опыта (DEM)

Сквозной мониторинг

Отслеживайте опыт конечных пользователей из более чем 50 глобальных внешних точек присутствия, а также изнутри сети

Единый сетевой источник истины (NSoT)

Единая операционная платформа

Поддержка продуктов Fortinet и сторонних производителей. Поддерживает локальные, гибридные и мультиоблачные среды. Независимое от поставщика решение для мониторинга со встроенными функциями оповещения и управления инцидентами

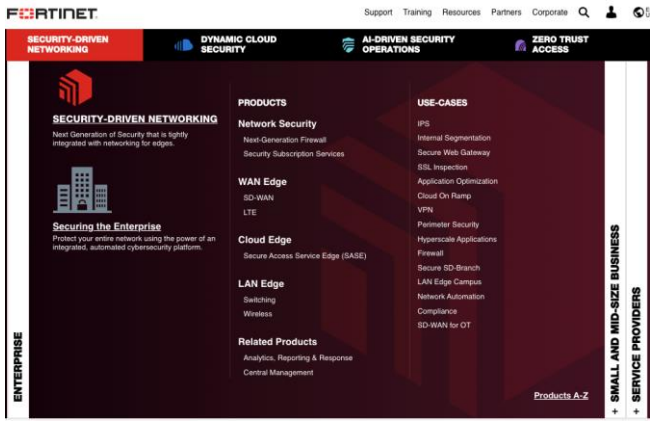
Устранение инцидентов

Runbooks

Автоматически запускайте действия по диагностике, сортировке и исправлению

Ресурсы

Страница продукта



www.fortinet.com > FortiMonitor

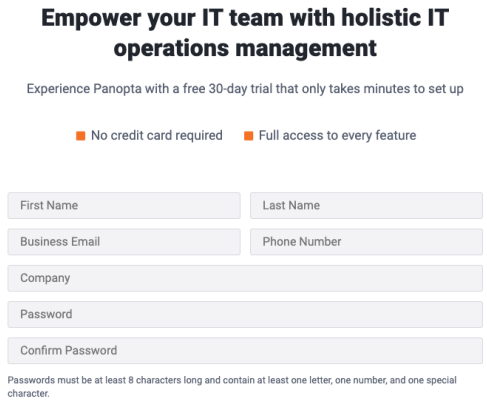
NSE-институт

FORTINET NSE Training Institute

NSE FortiMonitor Training

https://training.fortinet.com/

Бесплатная пробная версия



Попробуйте 30-дневную бесплатную пробную версию


FORTINET