



FortiMonitor – Управление сетью и операциями по обеспечению безопасности

Olesya Tarabrina, SE

Fortinet Security Fabric

Обширное

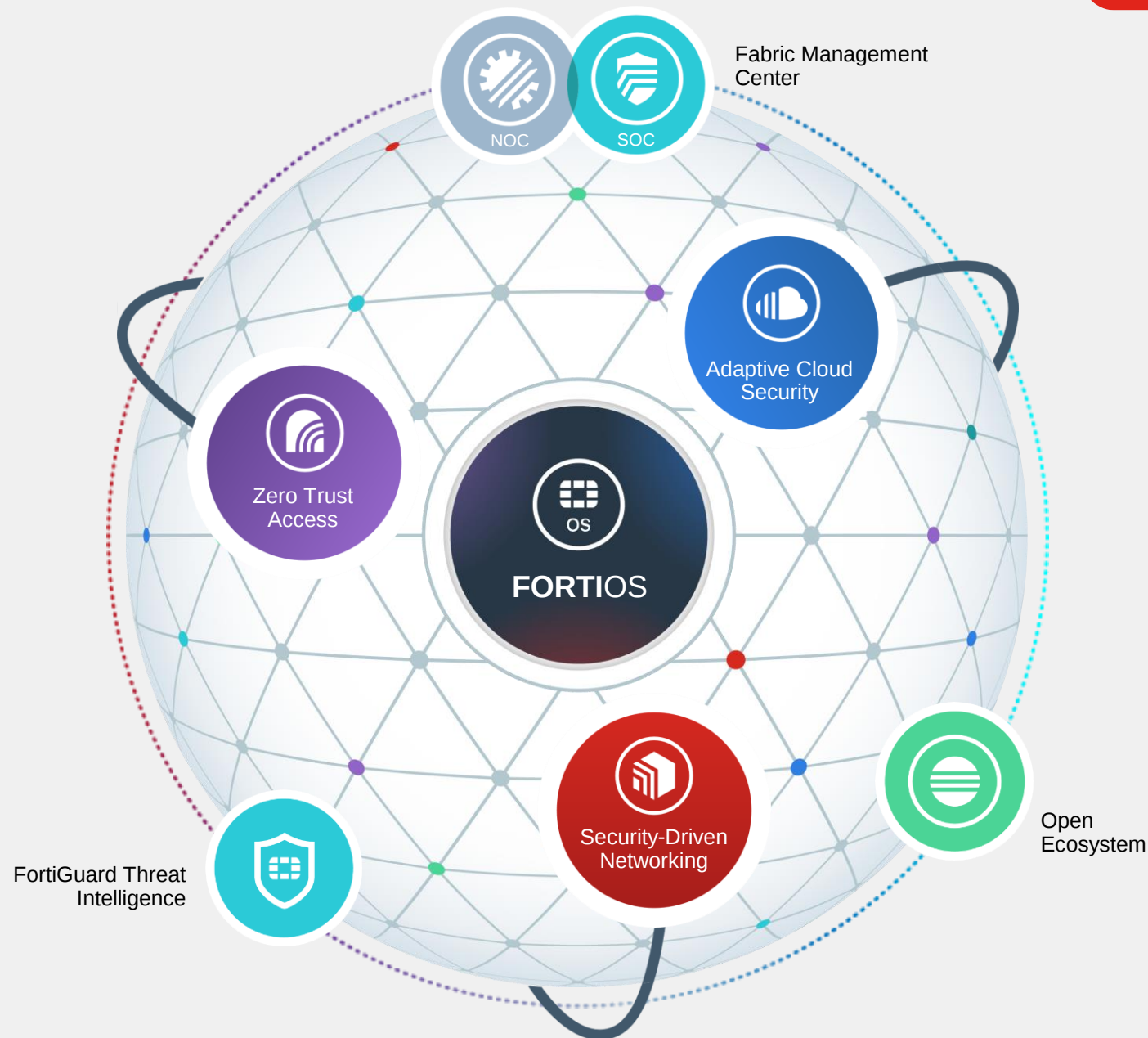
видимость и защита всей поверхности цифровой атаки для лучшего управления рисками

Интегрированное

решение, которое снижает сложность управления и делится информацией об угрозах

Автоматизированное

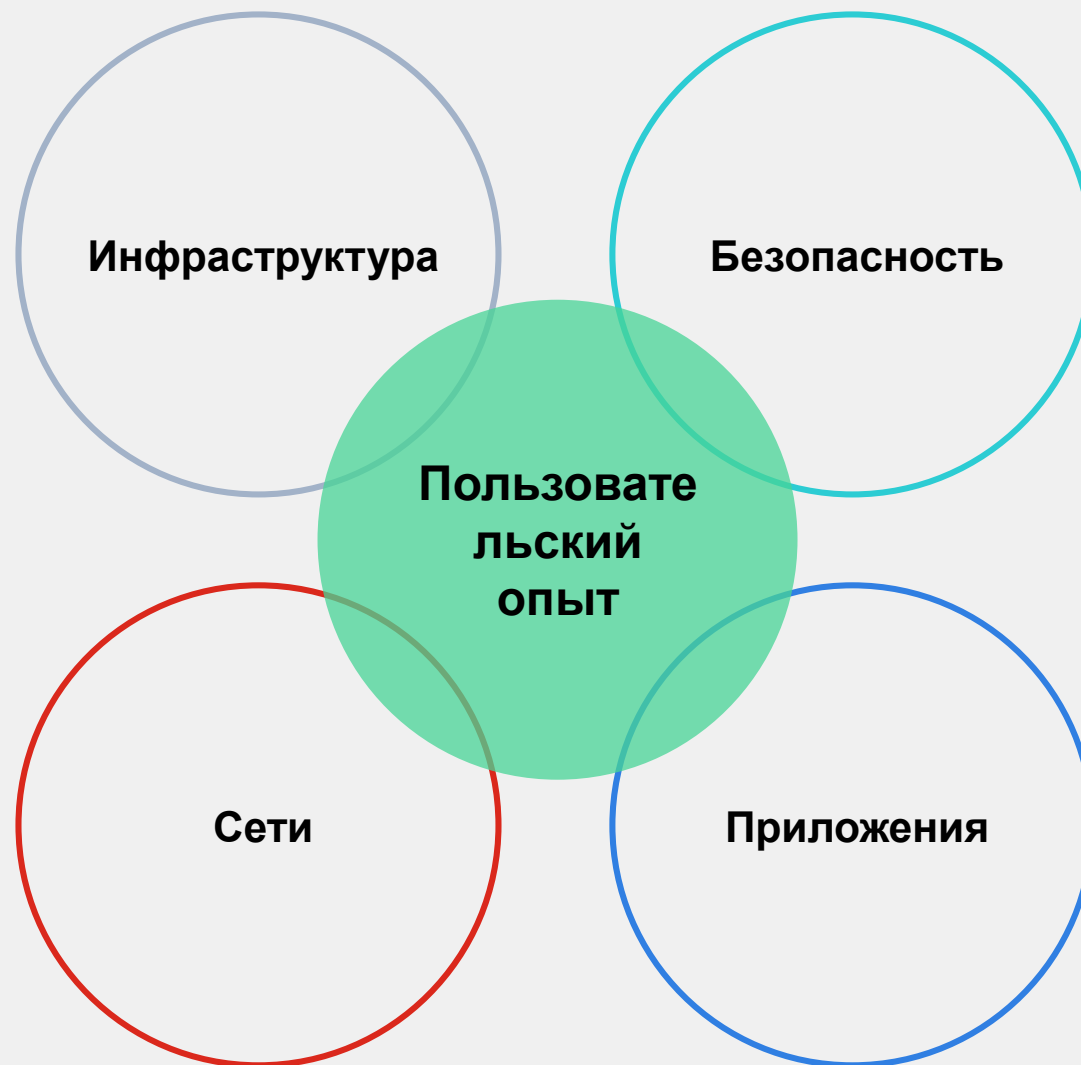
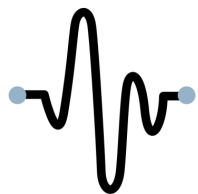
самовосстанавливающиеся сети с безопасностью на основе искусственного интеллекта для быстрой и эффективной работы



Понимание ландшафта мониторинга

**SaaS-Based Network
Performance Monitoring
(NPMD)**

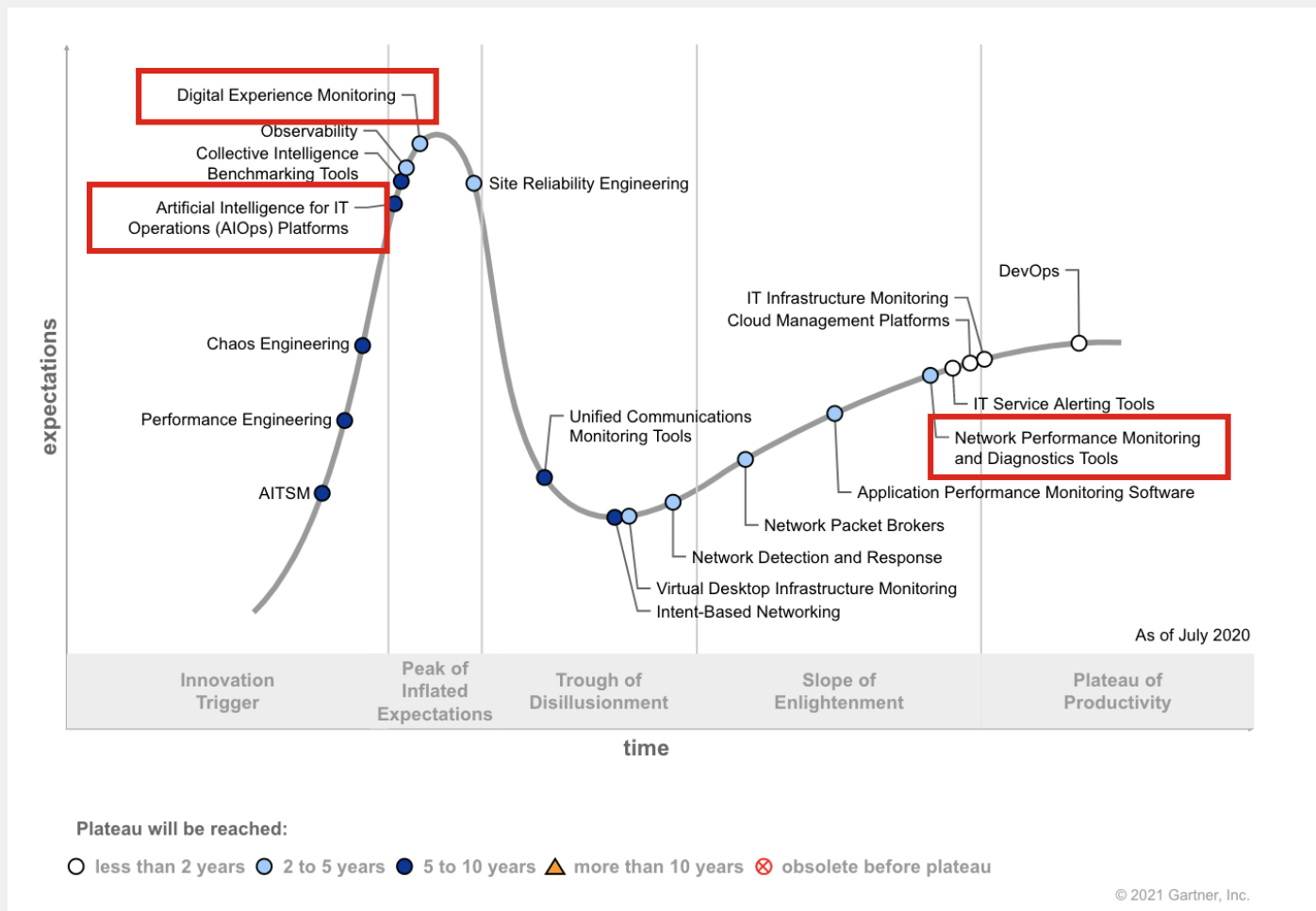
**Digital Experience Monitoring
(DEM)**



Тренды

Корпоративные сети трансформируются, и сетевые операции тоже

К 2024 году 50% НОС-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

Наблюдение

Корреляция

FortiManager, FortiAIops



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

Реагирование

FortiSOAR



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

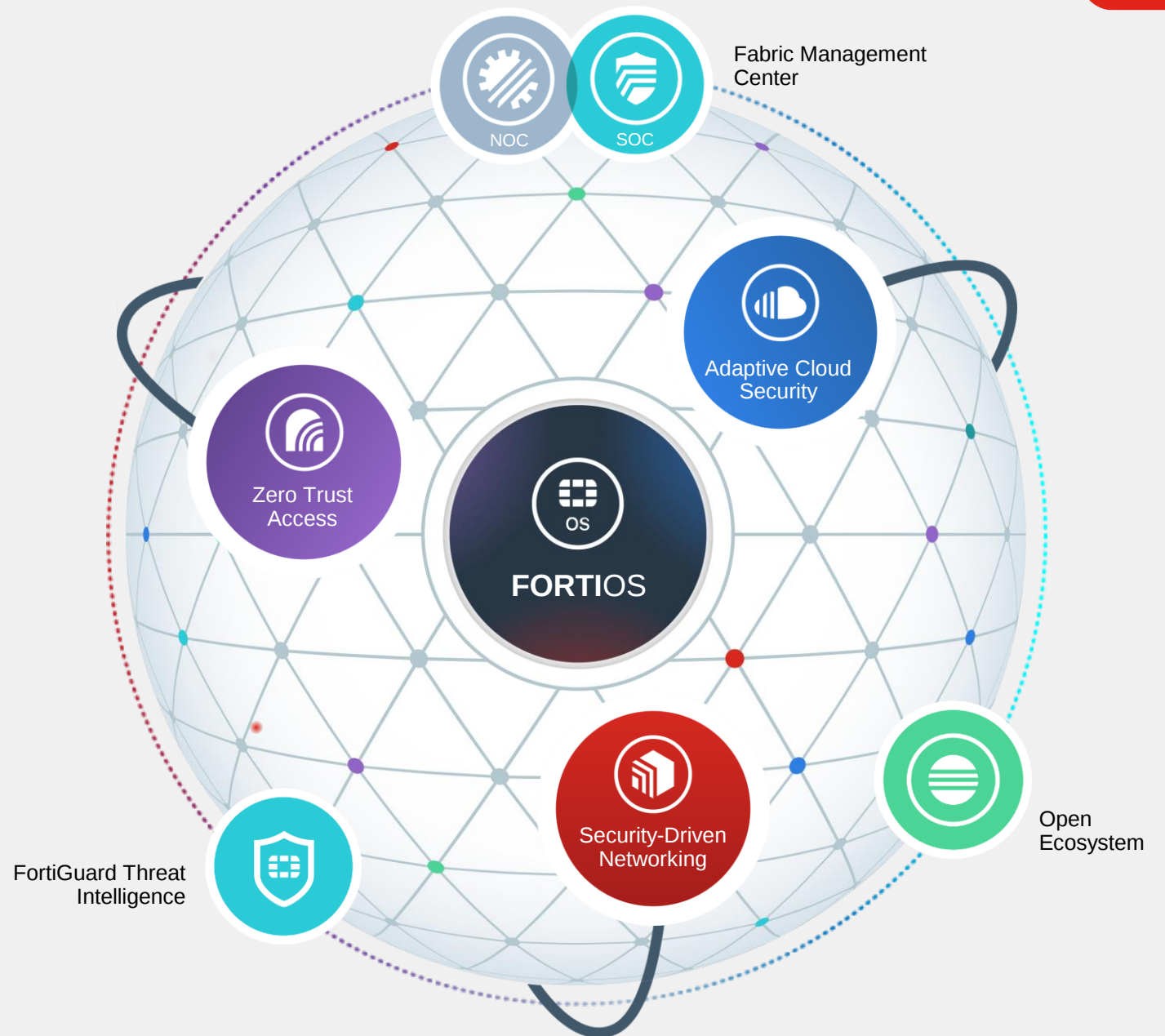
© Fortinet Inc. All Rights Reserved.



Fabric Management Center NOC



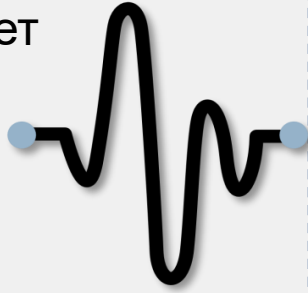
Network Performance Monitoring (NPMD),
Digital Experience Monitoring (DEM) &
Incident Management



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



Gartner

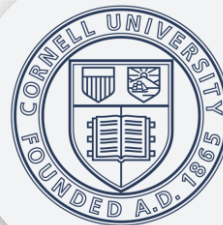
SONY
PICTURES

GoDaddy

Informatica

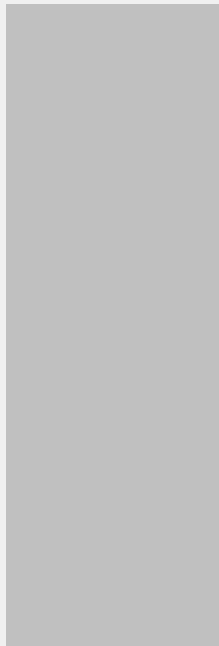
ING

tomtom



ARMOR





Вызовы & Решения



NOC Challenges

Сложность операций для фрагментированных сетей



**Ручные
операции**

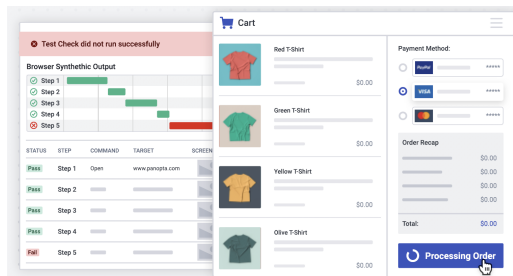


**Наглядность
цифрового опыта**



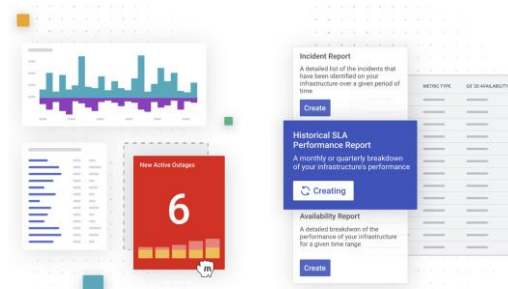
Анализ причин

Ответ FortiMonitor



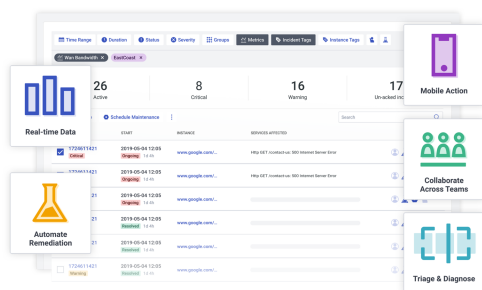
Мониторинг цифрового опыта

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



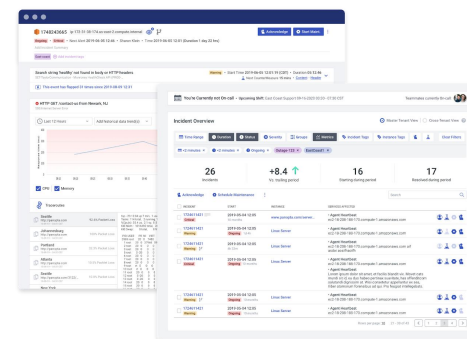
Повышенная видимость

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



Устранение шума

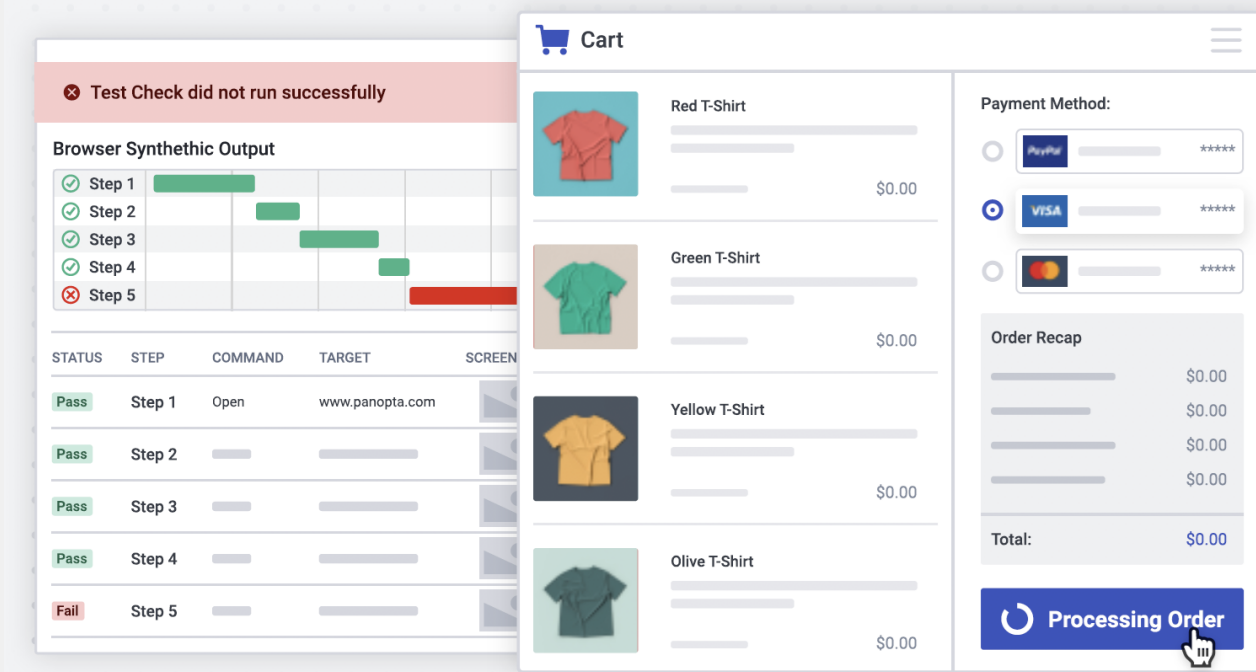
Ускорьте поиск первопричины и сократите количество ручных накладных расходов на диагностику, сортировку и устранение неисправностей.



Автоматическое исправление

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





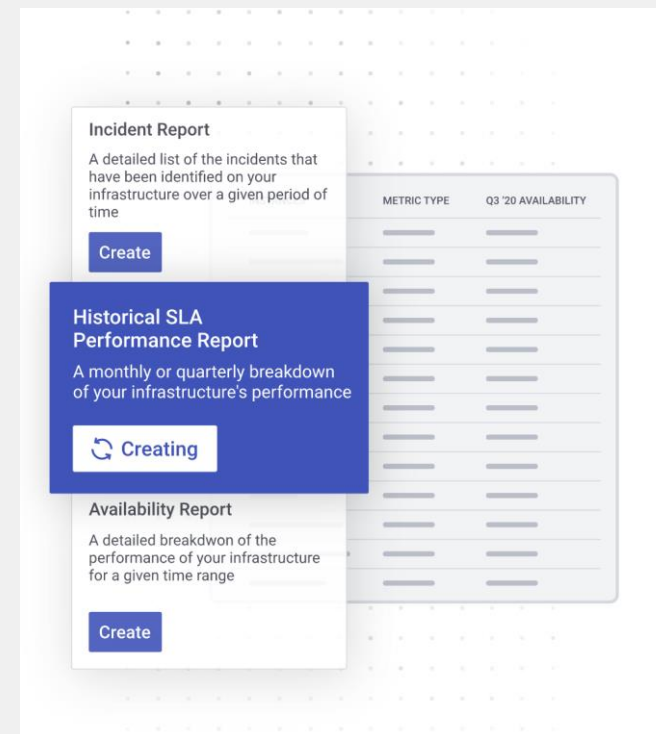
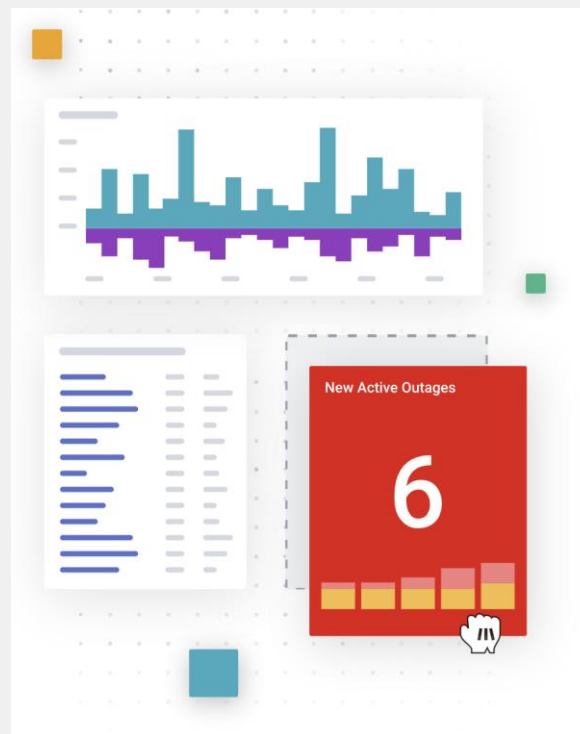
Мониторинг цифрового опыта

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

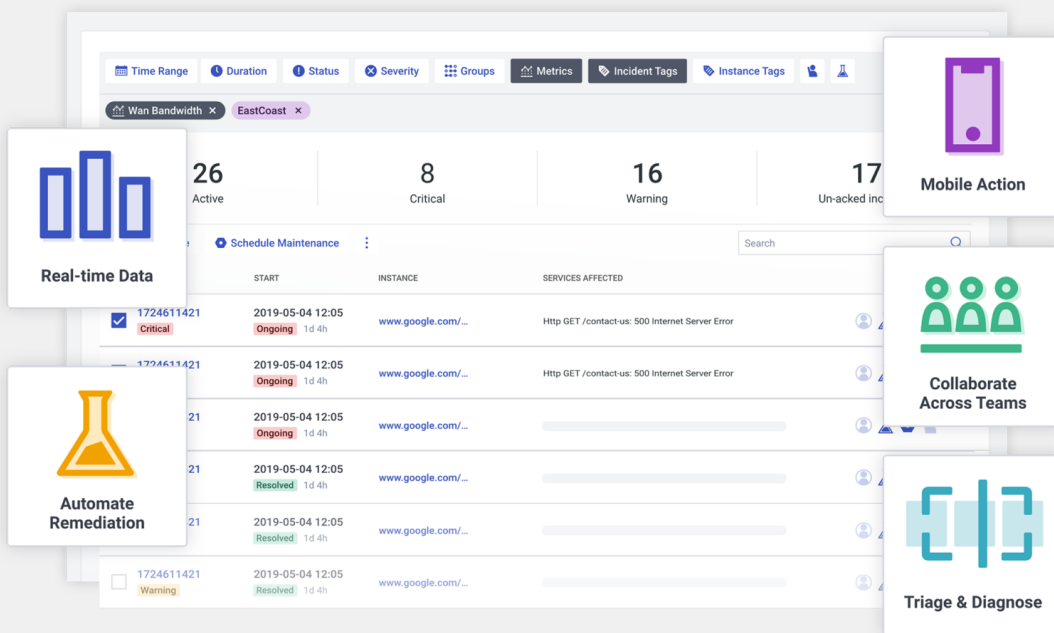
- 1 Получите показатели работоспособности и производительности приложений и систем
- 2 Запускайте тесты с узлов по всему миру, чтобы проверить предоставление услуг
- 3 Используйте синтетику веб-браузера для воспроизведения опыта конечного пользователя

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



Устранение шума

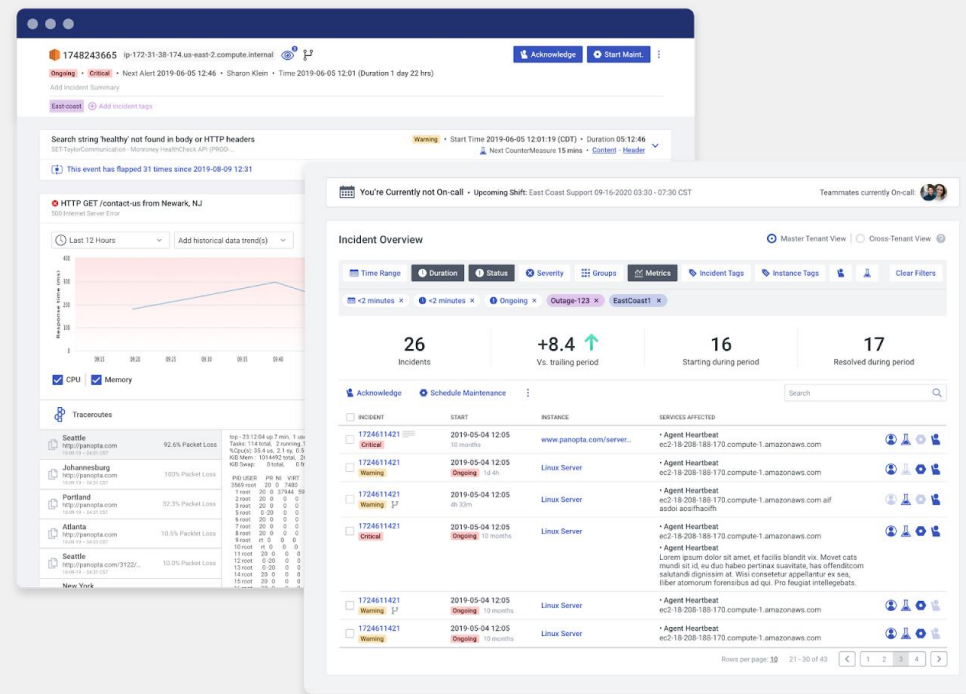
Контролируйте все, но предупреждайте только о том, что важно.

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

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

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?

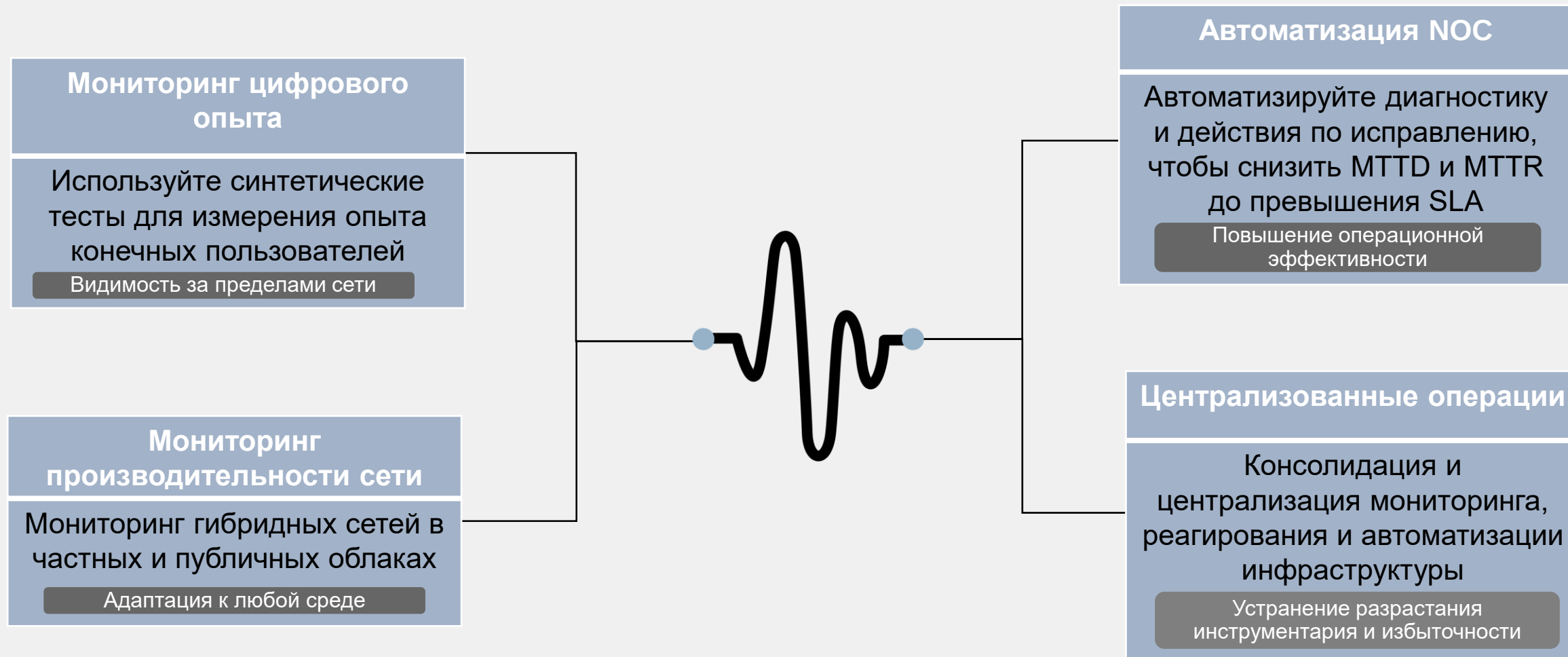
**SaaS-Based Network
Performance Monitoring
(NPMD)**

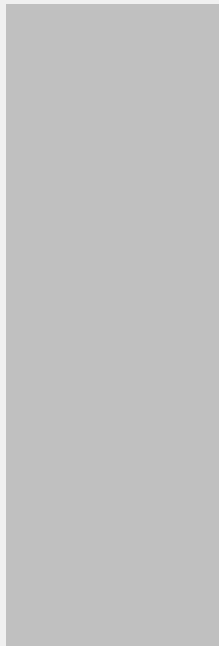
**Digital Experience Monitoring
(DEM)**



Сценарии использования FortiMonitor

Упростите NetOps в мультивендорной среде





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

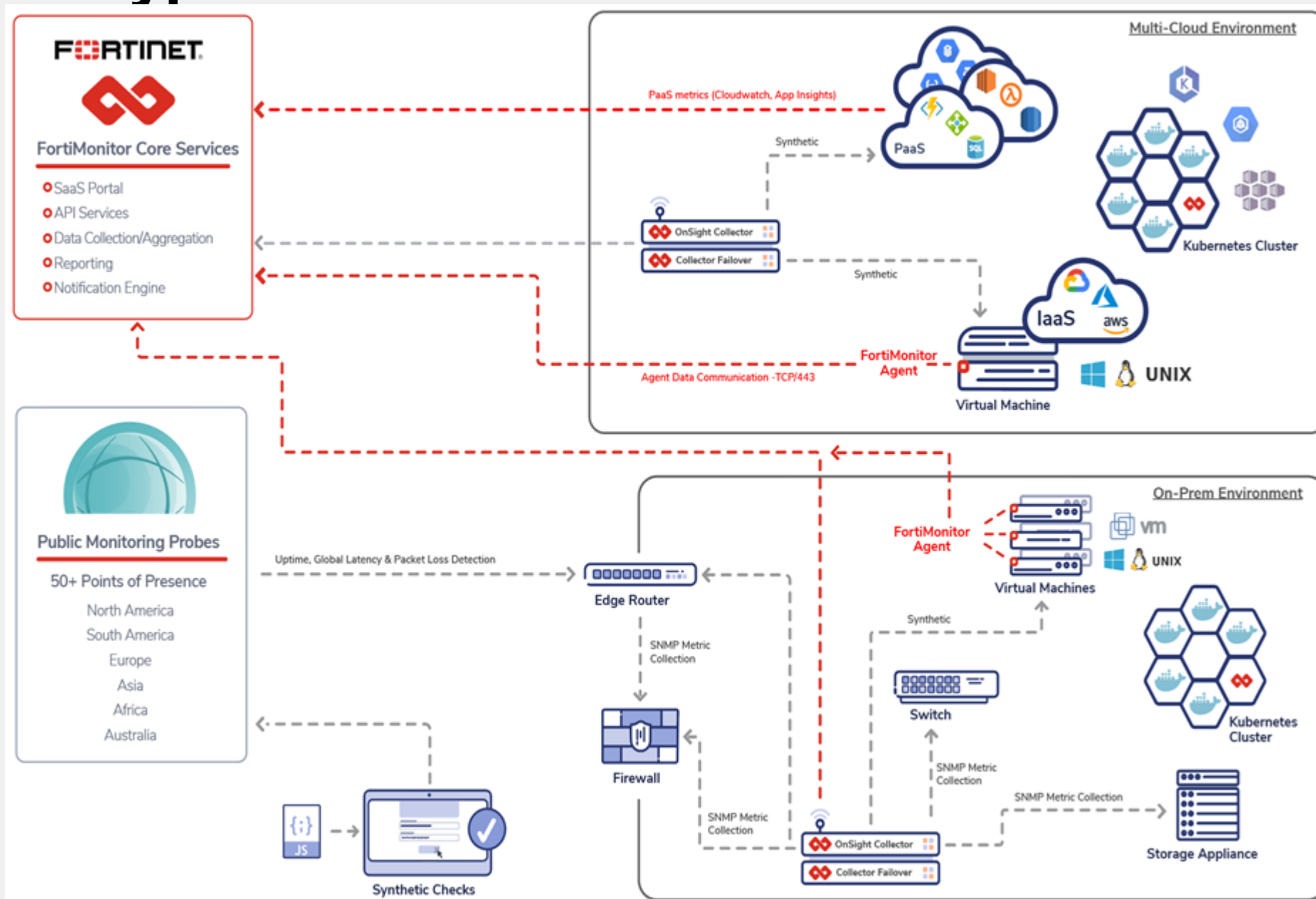
Экономия

- Значительное сокращение сложности развертывания, что позволяет MicroStrategy 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

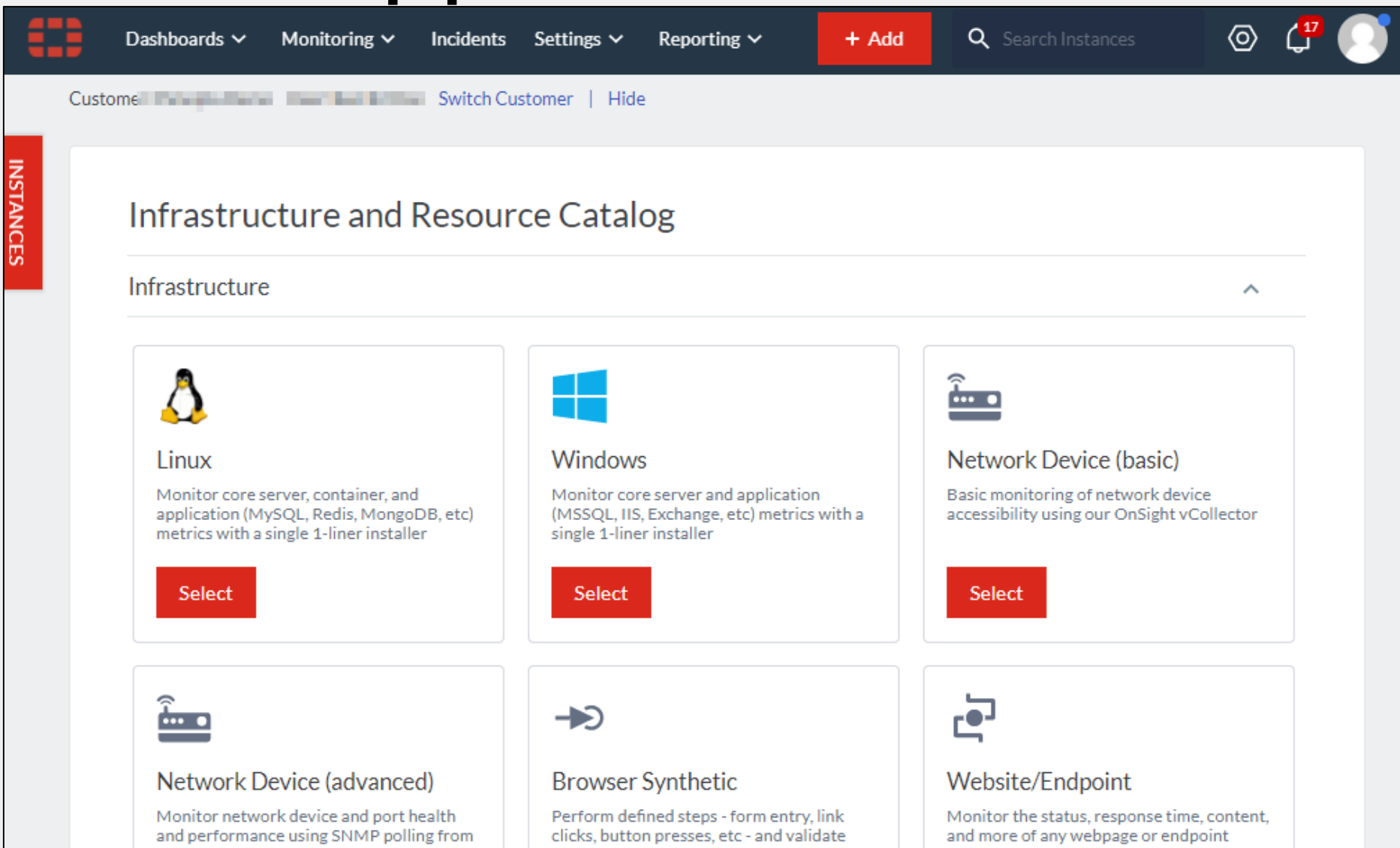
- VMWare Auto Discovery (API based)
- Public Cloud (AWS, Azure) Discovery
- Mass Agent Install
- OnSight Network Scan
- Kubernetes HELM
- REST API
- Вручную через UI



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

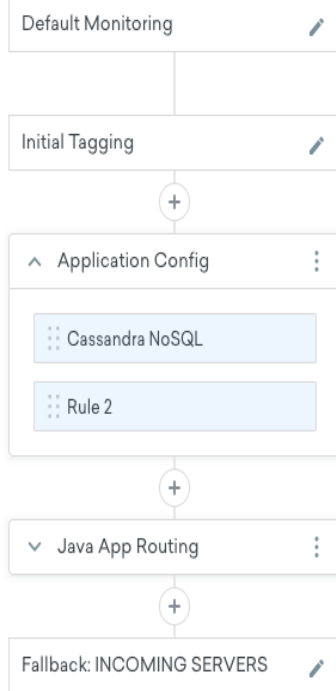
- Мониторинг приложений
- Внешний мониторинг
- Мониторинг сетевых устройств (SNMP)

Monitoring Policy Workflow

Test Workflow

Manage your monitoring configuration from a single workflow. Automate instance grouping, tagging, templates, & [more](#).

Workflow Sequence



Application Config

Cassandra NoSQL

If

Applications: Include Cassandra

Then

Apply Template: Cassandra

And

Set Destination: to Cassandra Nodes

And

Add Tags: database

Discard Changes

Save Changes



Хронология предупреждений

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

Alert Timeline: Linux servers [Edit Details](#) ▼

[+ New Event](#)

Incident Detected

2 MINUTES 2 contacts, 1 integrations, 1 groups A

James Linux
Slack App - Team: Panopta Channel: #slack-demo
Tech Support Demo

10 MINUTES 1 contacts B

Jim Barnes

30 MINUTES 1 integrations C

OpsGenie

Outage Resolved D

Send all clear alerts ☐

Instances

Select the servers and server groups that this schedule applies to. Don't forget to click save when you're done.

[Save Changes](#)

☐ All Instances

- ☐ DNS Servers
- ☐ INCOMING CLOUD E
- ☐ INCOMING SERVERS
- ☐ Linux Servers
- ☐ Monitoring
- ☐ Network Devices
- ☐ Office Infrastructure
- ☐ Templates
- ☐ Windows Servers

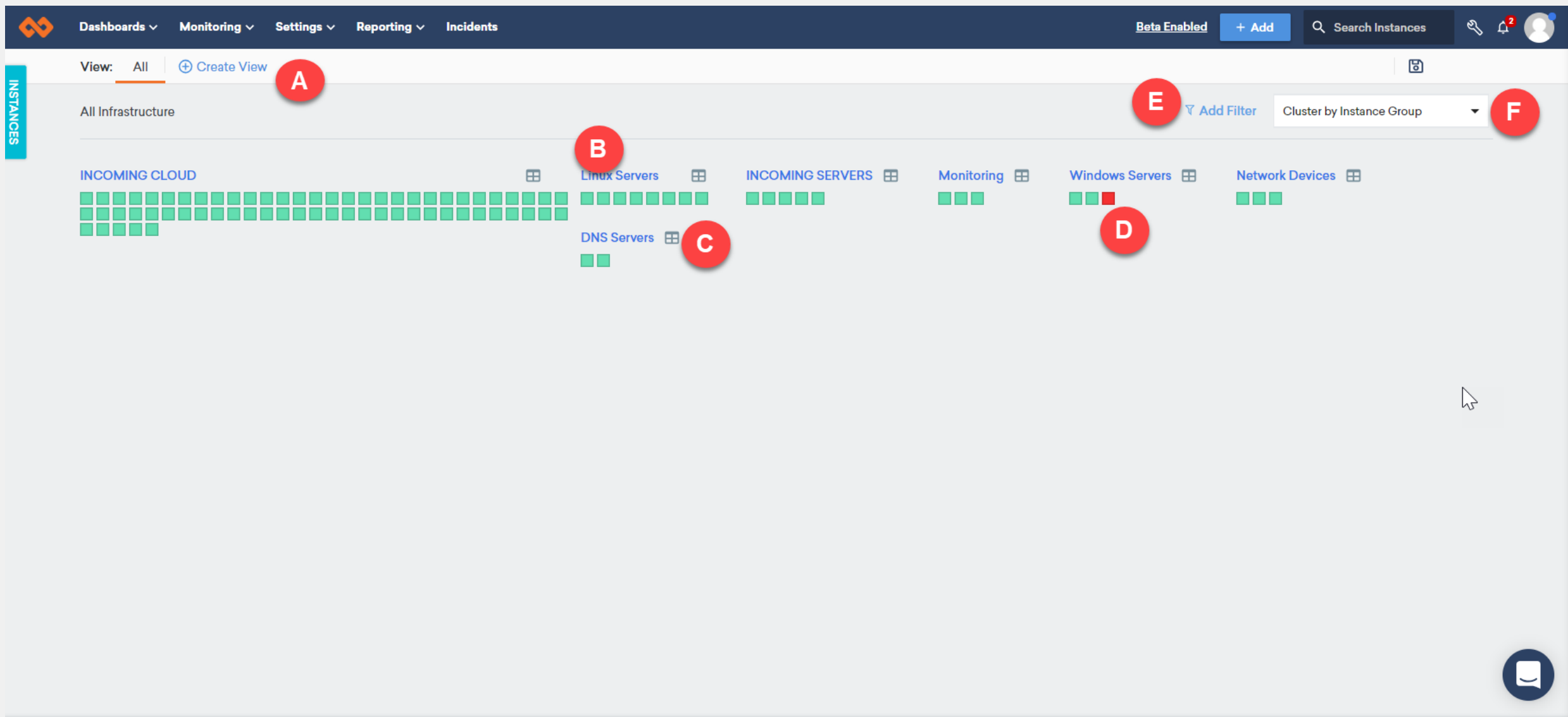


Визуализация

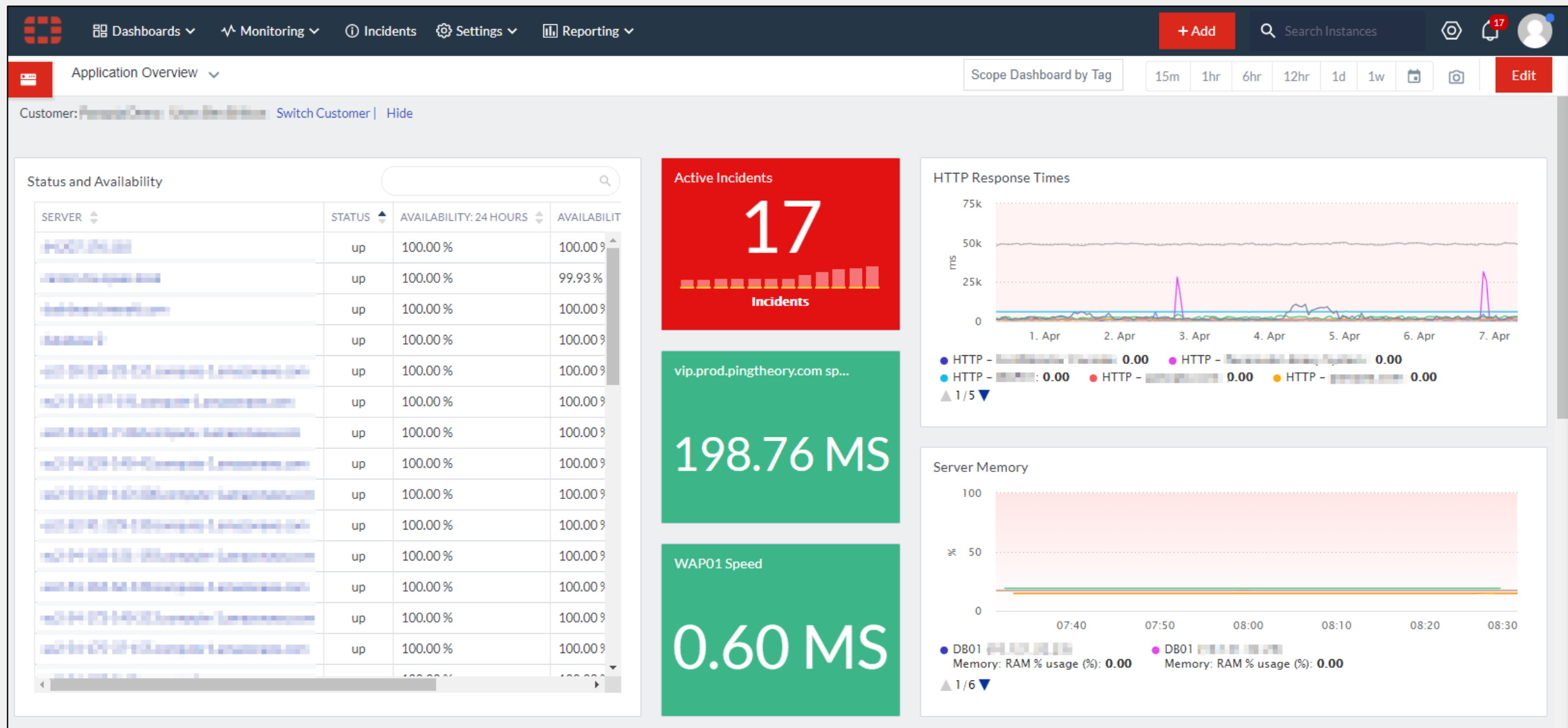
- Инфраструктурная карта
- Дашборд
- Страница сведений об экземпляре
- Страница статуса



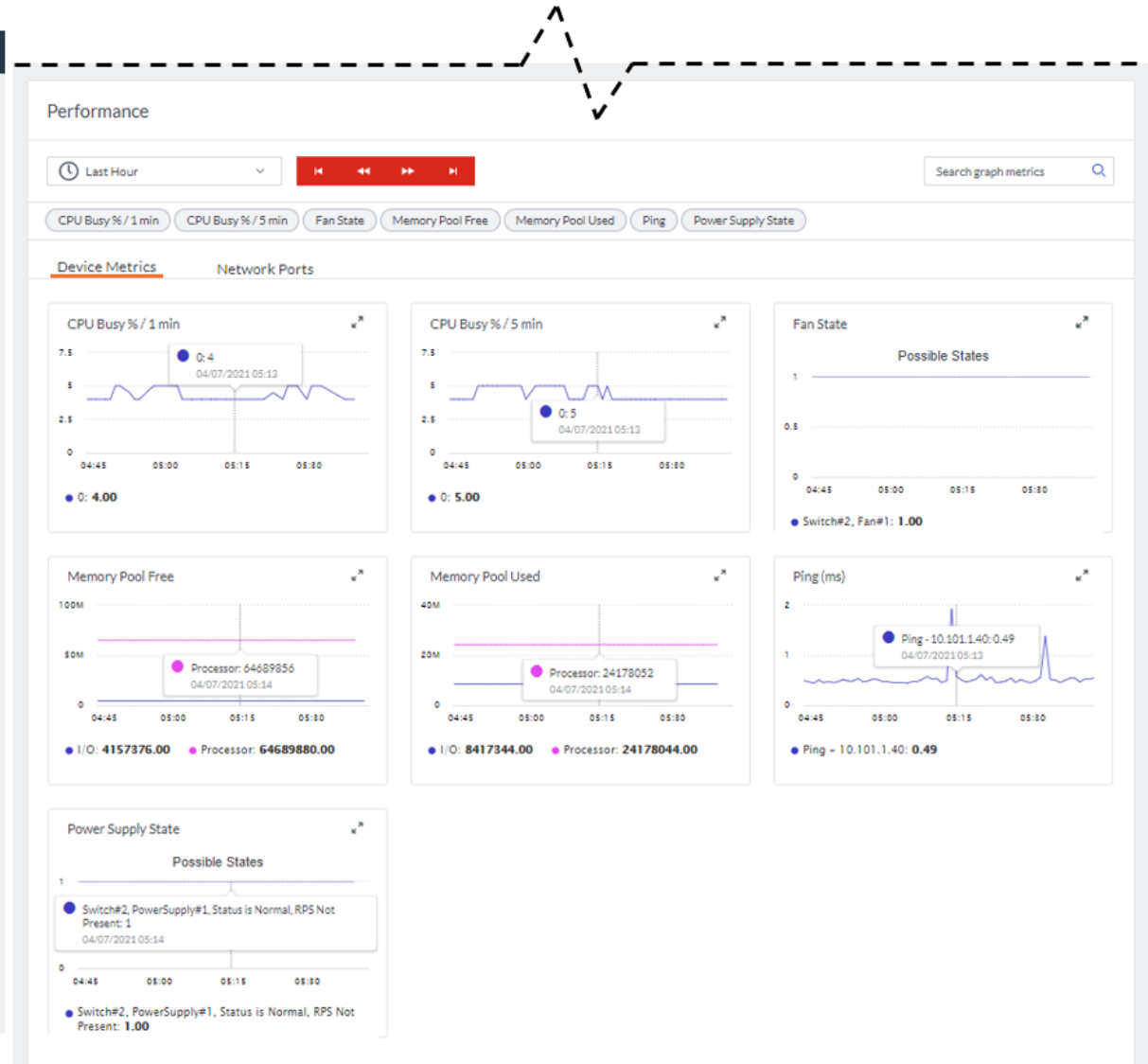
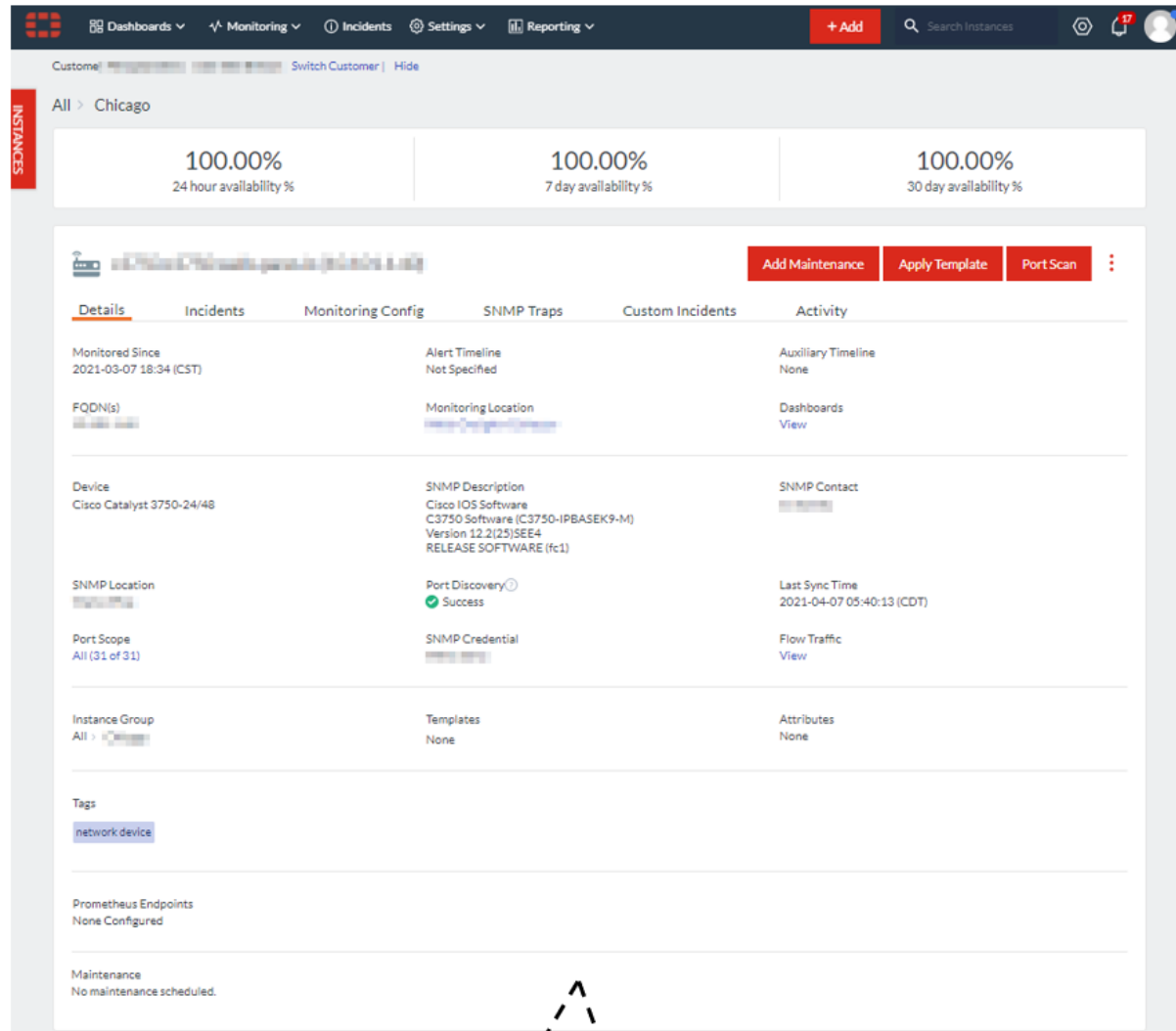
Инфраструктурная карта



Гибкие панели мониторинга на основе виджетов



Подробные сведения о мониторинге устройства



Страница статуса

		Historical Availability							
		Active During Period Warning During Period Outage During Period							
		Outage Details							
		CPU: Usage percentage - Total greater than 90% for more than 5 minutes Triggered at 2019-02-08 06:30:02							
Application Servers		Status	Today	Yesterday	Wed - 02/06	Tue - 02/05	Mon - 02/04	Sun - 02/03	Sat - 02/02
APP01 (10.121.32.21)	A								
APP02 (10.121.32.22)	B								
Database Servers		Status	Today	Yesterday	Wed - 02/06	Tue - 02/05	Mon - 02/04	Sun - 02/03	Sat - 02/02
DB01 (10.121.32.23)									
DB02 (10.121.32.24)									
mongodb.staging (10.121.32.49)									
DNS Servers		Status	Today	Yesterday	Wed - 02/06	Tue - 02/05	Mon - 02/04	Sun - 02/03	Sat - 02/02
ns1.softlayer.com									
ns2.softlayer.com									
Monitoring		Status	Today	Yesterday	Wed - 02/06	Tue - 02/05	Mon - 02/04	Sun - 02/03	Sat - 02/02



Ролевой доступ

INSTANCES

 Dashboards ▾ Monitoring ▾ Settings ▾ Reporting ▾ Incidents

+ Add

Search Instances



Users & Groups

Looking for SSO? It's on our [Integrations page](#). You can learn more about it in our docs.

USERS

GROUPS

ON-CALL SCHEDULES

+ Add User

Delete

Name	Contact Info	Alert Timelines	Roles	Scope
☐ Johnnie Jung	✉ JJ@panopta.com	No Alert Timelines assigned	Contact-only	⋮
☐ Neva Blackmore	✉ nvbm@gmail.com 📞 +17052145569 - SMS 📞 +17052145569 - Voice	No Alert Timelines assigned	Account Admin	All Groups ⋮
☐ Thomas Wayne	✉ t_waynemd@panopta.com ✉ +16305521142 - SMS 📞 +16305521142 - Voice	Basic timeline	Account Admin	All Groups ⋮

1

Showing 1 to 3 of 3 entries



График дежурств

On-call Schedule "T3" :
Escalated

<	>	today	Set Default Contact	May 2018	+ New Event	month	week	day
Sun	Mon	Tue	Wed	Thu	Fri	Sat		
29	30	1	2	3	4	5		
12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]		
12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]		
12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]		
6	7	8	9	10	11	12		
12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]		
12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]		
12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]		
8a Damian Wayne [x]								
13	14	15	16	17	18	19		
12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]		
12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]		
12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]		
20	21	22	23	24	25	26		
12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]		
12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]		
12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	12a Timothy Drake [x]		
8a Damian Wayne [x]								
		8a Damian Wayne [x]		8a Damian Wayne [x]		8a Damian Wayne [x]		
27	28	29	30	31	1	2		
Damian Wayne [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]	12a Cassandra Cain [x]		
Damian Wayne [x]			12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]		
Damian Wayne [x]					12a Timothy Drake [x]	12a Timothy Drake [x]		
12a Cassandra Cain [x]	12a Stephanie Brown [x]	12a Stephanie Brown [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	8a Damian Wayne [x]			
12a Stephanie Brown [x]	12a Timothy Drake [x]	12a Timothy Drake [x]	8a Damian Wayne [x]					



Single Sign-On (SSO)

Single Sign On



Integrate Panopta
with your Okta
installation

[Configure](#)



Integrate Panopta
with your Microsoft
ADFS installation

[Configure](#)



Integrate Panopta
with your SAML-
based SSO provider

[Configure](#)

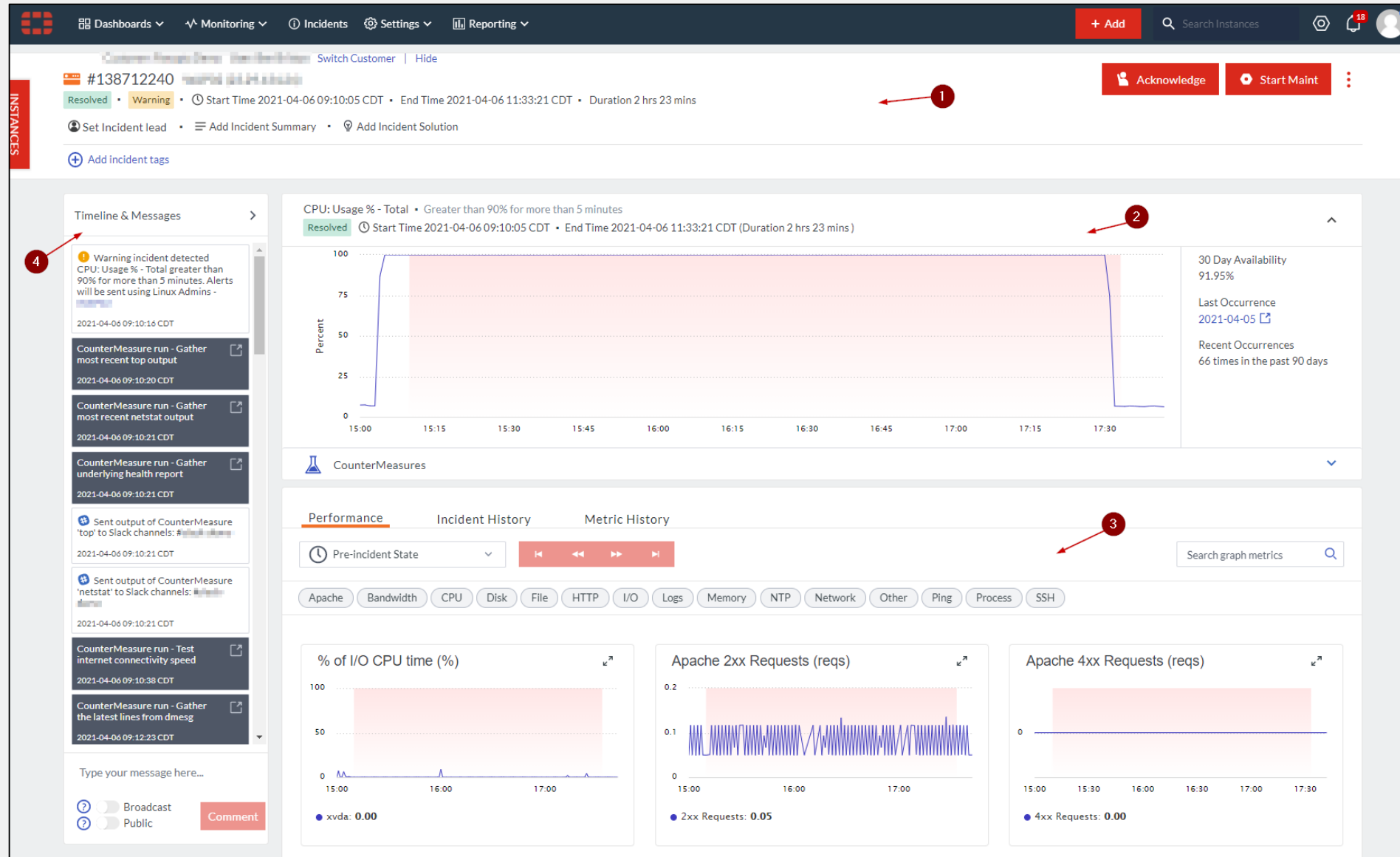
Отчетность

- Предустановленные отчеты
- Запланированные отчеты
- Специальные отчеты

Agent Status Report An audit of the current agent version and status being utilized across your infrastructure Create	Availability Report A detailed breakdown of the performance of your infrastructure for a given time range Create	Capacity Planning Report A report on metric usage trends to assist with capacity planning Create	Historical SLA Performance Report A monthly or quarterly breakdown of your infrastructure's performance Create
Incident Report A detailed list of the incidents that have been identified on your infrastructure over a given period of time Create	Instance Configuration Report Full configuration details on all of your instances Create	Metric Configuration Report Full configuration details on all of your metrics Create	Metric Export Report A report with detailed metric values collected by Panopta Create
MTTR & MTTA Report Breakdown of MTTR and MTTA performance across your infrastructure Create	Tag Audit Report A detailed view into how your tags are utilized across Panopta Create	User Audit Report An audit of all of your current Panopta users Create	User Incident Activity A report of incident activity per user Create
Utilization Report Detailed system resource utilization report, covering core system metrics Create			



Сведения об инциденте



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



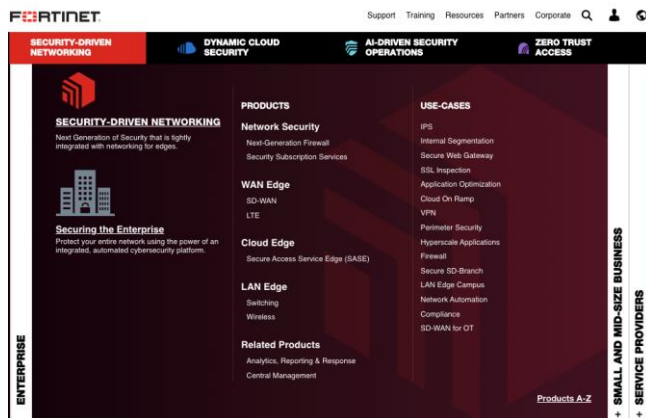
Runbooks



Автоматически запускайте действия по диагностике, сортировке и исправлению

Ресурсы

Страница продукта



www.fortinet.com > FortiMonitor

NSE-институт



NSE FortiMonitor Training

<https://training.fortinet.com/>

Бесплатная пробная версия

Empower your IT team with holistic IT operations management

Experience Panopta with a free 30-day trial that only takes minutes to set up

■ No credit card required ■ Full access to every feature

Passwords must be at least 8 characters long and contain at least one letter, one number, and one special character.

Попробуйте 30-дневную бесплатную пробную версию





FORTINET®