# NETSCOUT Omnis Security

Omnis Network and Cyber Security Platform – специализированная, интеллектуальная платформа для обнаружения угроз в сети организации, а также решения задач по расследованию инцидентов кибербезопасности.

### Платформа для обнаружения и реагирования на сетевые угрозы

Современные корпоративные сети постоянно трансформируются, охватывая сети обработки данных, офисные сети, разветвлённую структуру филиалов, а теперь виртуальные и публичные, облачные платформы. Используемые средства защиты далеко не всегда соответствуют всем новым стандартам и требованиям к защищенности, при этом количество кибератак растет ежегодно. В свою очередь, увеличение количества инструментов кибербезопасности, приводит к накоплению огромного количества данных. Отсутствие полного понимания и контроля работы сети, приводит к снижению эффективности работы SOC, снижая время реагирования, скорость и эффективность обнаружения угроз. Для решения всех этих проблем, организации должны собрать и проанализировать максимальное количество исходных данных ИТ-инфраструктуры (логи, «сырой» трафик, Netflow и информацию о работе арендованных каналов связи), серверных платформ. При этом, требуется обогатить эти данные сведениями об угрозах и бизнес-транзакциях. Платформа NETSCOUT® позволяет решить все эти задачи при помощи Omnis® Security - система анализа, обнаружения, реагирования и расследования киберугроз.

### Эффективная кибербезопасность начинается с полной прозрачности и видимости сети

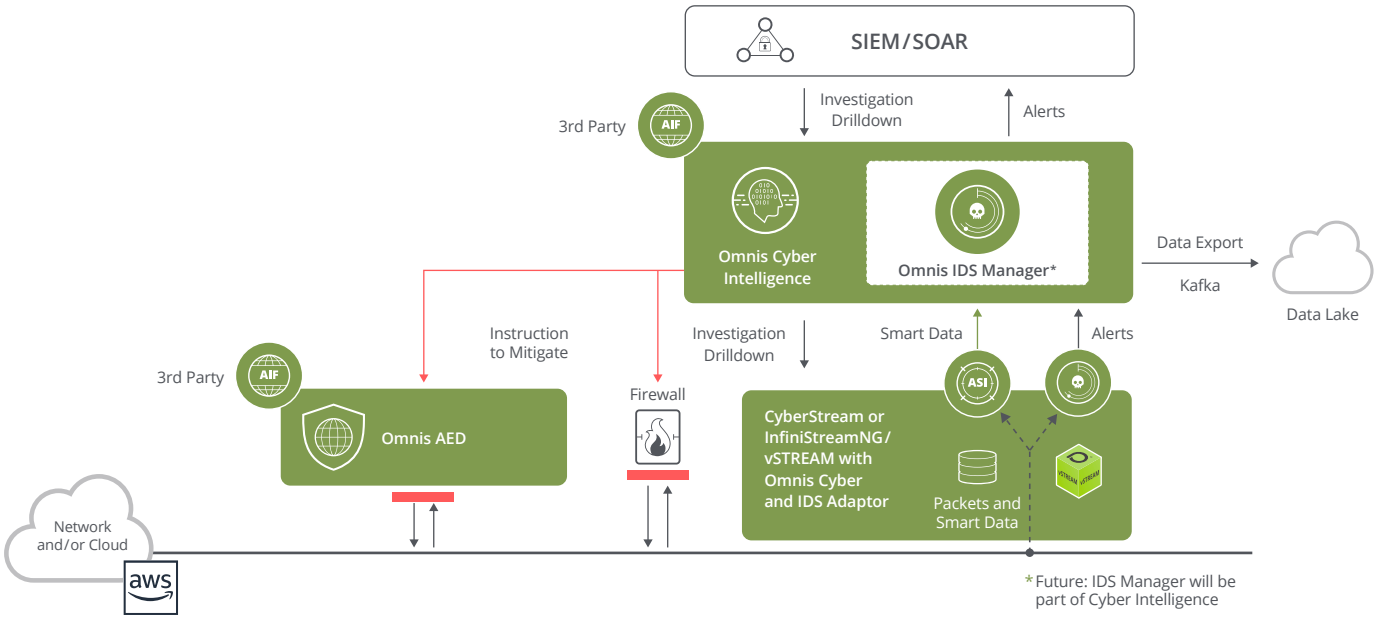
Вы не можете защитить себя от того, чего не видите и не контролируете. Это фундаментальная аксиома кибербезопасности. В современной, сложноустроенной инфраструктуре, включающей технологически устаревшие сети, множество удаленных офисов, сотрудников, работающих посредством VPN, корпоративных и частных облачных сред, только контроль работы каждого сервиса в сети позволит защититься от киберугроз.

Более 30 лет NETSCOUT предоставляет Заказчикам решение по детальному анализу сетевого трафика, а также мониторингу прикладного уровня всей цифровой инфраструктуры. В компании NETSCOUT данный подход получил название “Видимость без границ”. Такой уровень видимости является основополагающим требованием для эффективного обнаружения и реагирования на угрозы информационной безопасности.

NETSCOUT Omnis Security использует известную платформу InfiniStreatmNG® (ISNG). ISNG является масштабируемой платформой для сбора, обработки и длительного хранения сетевых пакетов,а также для обеспечения комплексной и последовательной видимости физической, виртуальной или облачной среды.

## ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА ПЛАТФОРМЫ

- Для съёма данных с сети используется высоко масштабируемое сетевое оборудование, способное обеспечить эффективную всестороннюю видимость трафика сети.
- Многочисленные методы обнаружения сетевых уязвимостей при помощи использования аналитических данных об угрозах, поведенческого анализа, данных из различных источников и глубокого анализа работы бизнес-сервисов.
- Контекстный анализ и детальное расследование с помощью обработки большого объема трафика, механизм обогащения метаданными и эффективности (KPI), такие, как коды ошибок, время отклика, глубокого анализа пакетов трафика.
- Корректировка политик безопасности защиты периметра (например, NGFW) на основании оценки результатов анализа сетевых пакетов и событий безопасности.
- Использование имеющихся источников метаданных и пакетов сценариев, использование открытого API упрощает автоматизацию работы технических подразделений.




ISNG поддерживает множество различных платформ, сетевых интерфейсов и систем хранения:

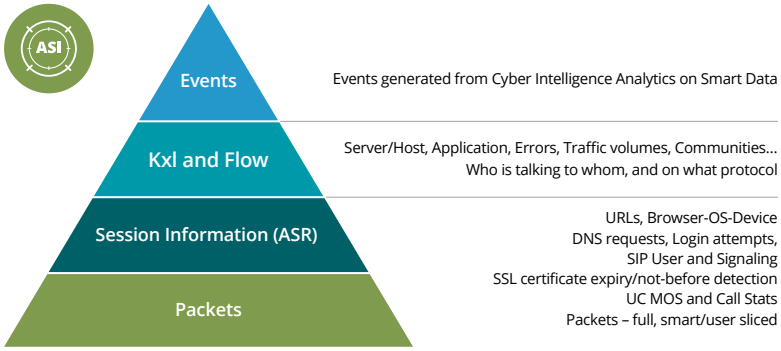
- Устройство реализовано, как в виде фирменного оборудования - сервера от компании NETSCOUT и ПО устанавливаемого на сертифицированные bare metal сервера, так и 100% виртуального исполнения (vSTREAM®). ISNG работает с облачными или виртуальными средами, например Amazon Web Services, Google Cloud, Microsoft Azure, Oracle Cloud Infrastructure и VMware NSX-V и NSX-T.
- Захват и обработка пакетов на скорости до 100 Гбит/с.
- Локальное дисковое хранилище емкостью в несколько сотен терабайт для локального хранения метаданных и сетевых пакетов.

Используя запатентованную технологию Adaptive Service Intelligence® (ASI), устройство ISNG преобразует исходные сетевые пакеты в индексированные метаданные (называются NETSCOUT “Smart Data”). NETSCOUT Smart Data содержит такую информацию, как:

- 5 параметров ключевых данных о сессии (IP-адрес источника и назначения, порт источника и назначения и поле с обозначением типа сетевого протокола).
- Ключевые показатели сервиса – коды ошибок, показатели задержек и т.д.
- Данные из SIP сессии, включая информацию о пользователях и служебные данные.
- DNS-запросы/ответы, URI, типы браузеров и устройств.
- И многое другое.

Помимо расширенных метаданных платформа ISNG также хранит сжатые исходные пакеты трафика.

Созданные ISNG и ASI Smart Data обеспечивают всестороннюю видимость всей цифровой инфраструктуры. И этот единый источник надежных метаданных может быть легко доступен для использования в NetOps и SecOps.




## Многочисленные методы обнаружения угроз на основе сети

Используя инструментарий NETSCOUT ISNG и интеллектуальные метаданные, и пакеты, полученные с помощью ASI, Omnis Security обеспечивает множество методов обнаружения киберугроз.

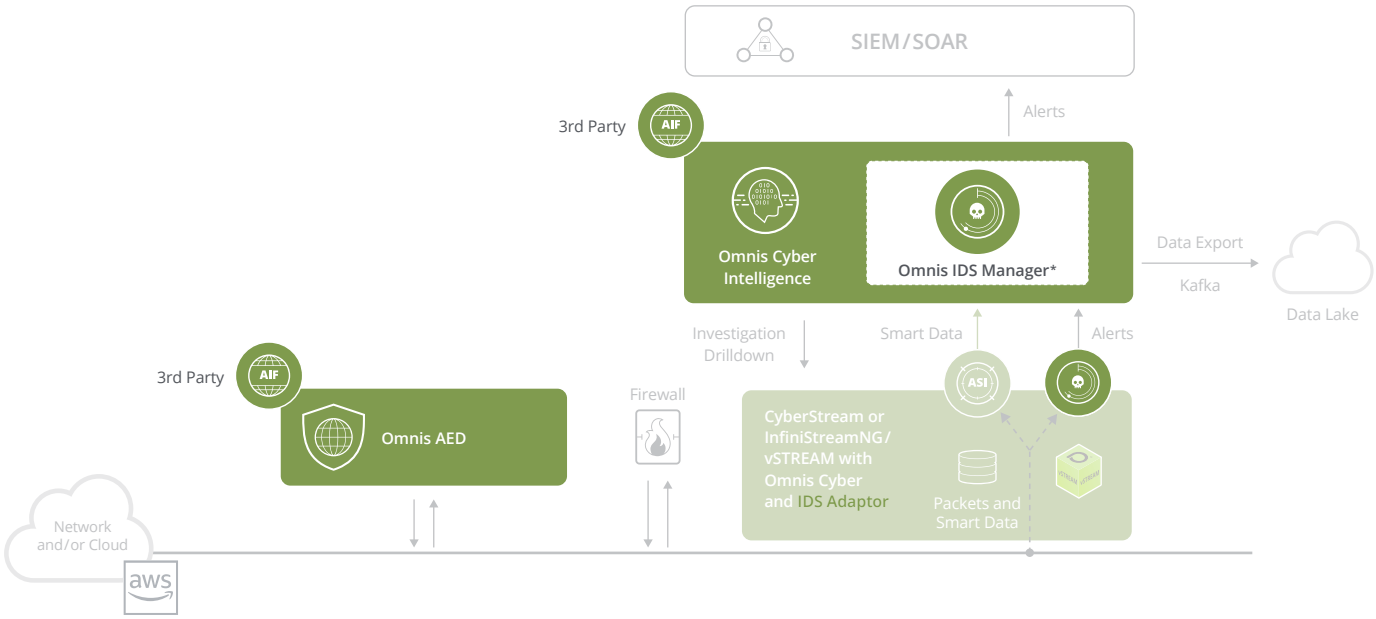
- **Omnis Cyber Intelligence** – является централизованной консолью для платформы Omnis Security, Cyber Intelligence анализирует данные, собранные коллекторами ISNG, применяет baseline сети, а также использует данные базы сигнатур ATLAS® (или сторонних поставщиков) для обнаружения всех типов киберугроз, запуска workflow, визуализации и расследования. События из Cyber Intelligence могут быть отправлены в SIEM-систему, а исходные данные могут быть экспортированы в системы для дальнейшего анализа аналитическими комплексами.
- **Omnis Intrusion Detection System (IDS)** – сервер или дополнительный модуль для ISNG, Omnis IDS предназначен для обнаружения вторжения с использованием механизма сигнатурного анализа трафика, базируется на продукте Suricata. Omnis IDS передает события информационной безопасности, сопоставляя их с базами данных Mitre Att&ck (расширенная функция), в модуль IDS Manager, в консоль Cyber Intelligence или SIEM/SOAR.
- **Arbor Edge Defense (AED)** – устройство используемое на границе сети, между оборудованием провайдера и FireWall, AED обнаруживает угрозы со стороны сети Интернет, такие как DDoS-атаки, сканирование портов, попытки перебора паролей, попытки проникновения вредоносного ПО и другие IoC. При обнаружении угроз события могут быть переданы на консоль Cyber Intelligence или в используемые SIEM/SOAR-системы.

Вместе все три продукта обеспечивают многоступенчатое обнаружение сетевых угроз и интегрируются в существующую экосистему информационной безопасности, способствуя реализации стратегии комплексной, многоступенчатой и эшелонированной защиты организации.

## Контекстное исследование угроз и их устранение на периметре

Простого “обнаружения” киберугроз недостаточно. Платформа расследования инцидентов для команды SOC является следующим важным шагом в защите от киберугроз Вашей компании. Omnis Security предлагает два мощных метода противодействия угрозам.

**Контекстное расследование** – используется обширный источник интеллектуальных данных компании NETSCOUT, Omnis® Cyber Intelligence не только обнаруживает угрозы, но и дает возможность специалистам SOC использовать источник метаданных и полной информации из сетевых пакетов для быстрого расследования любых инцидентов. Результаты расследований Cyber Intelligence могут помочь с приоритезацией оповещений или действий по устранению последствий.




**Защита периметра** – Предотвращение сетевых угроз на периметре сети является одним из средств противодействия уже известным или абсолютно новым киберугрозам. Однако, подобное блокирование киберугроз должно осуществляться только при гарантии отсутствия воздействия или влияния на работу бизнес-систем. Только полный доступ платформы Cyber Intelligence к метаданным и сетевым пакетам помогает Вашему SOC контролировать корректность блокирования сессий на периметре сети. Omnis Cyber Intelligence позволяет взаимодействовать и направлять информацию в такие устройства, как FireWall или NETSCOUT Arbor Edge Defense (AED), блокировать вредоносный трафик на периметре сети. AED также может автоматически обнаруживать и блокировать входящие и исходящие угрозы. В частности, AED предлагает проверенную и самую популярную в отрасли защиту от DDoS-атак. Платформа справляется со всеми типами DDoS-атак, а благодаря технологии обработки пакетов без статических данных AED может блокировать атаки с, которые угрожают доступности и производительности устройств обрабатывающих статические данные, таких как FireWall, UTM, VPN-шлюзы и балансировщики нагрузки. Используя данные об угрозах от NETSCOUT ATLAS или сторонних производителей, AED также может быть настроен на остановку исходящего трафика от скомпрометированных внутренних узлов, взаимодействующих с внешними известными нелегитимными сайтами - по сути, выступая в качестве первой и последней линии защиты периметра.

## Интеграция очень важна

NETSCOUT Omnis Security является максимально эффективной платформой для анализа и реагирования на современные угрозы информационной безопасности. NETSCOUT Omnis Security одновременно обрабатывает и систематизирует данные сетевых пакетов и и метаданных источником которых выступают NETSCOUT ISNG /vSTREAM. NETSCOUT уверен, что сетевые данные являются конечным источником объективной информации, но мы также знаем, что SOC использует технологии обнаружения вредоносных конечных точек ( устройств) и данные из SIEM. Именно поэтому NETSCOUT сделал своим главным приоритетом максимальное расширение интеграционных возможностей Omnis Security, в том числе для обеспечения внедрения в существующие стеки безопасности и процессы.

## Интеграционные возможности Omnis Security:

- Поддержка всех типов подключений и интерфейсов к существующей сети.
- Возможность захвата, декодирования и создания надежных метаданных для тысячи сетевых протоколов и приложений.
- Поддержка любой сетевой среды, включая виртуальные (например, Oracle Cloud Infrastructure, VMware NSX-V и NSX-T) или публичные облака (например, Amazon Web Services, Google Cloud, Microsoft Azure),
- Использование информации об угрозах сторонних производителей с помощью поддержки STIX и TAXII или пользовательских интерфейсов с TIP (например, Anomali или ThreatQuotient).
- Оповещение через распространенный формат SYSLOG.
- Использование открытых REST API.
- Использование систем обнаружения угроз с открытым исходным кодом (например, таких как Suricata) и развивающихся отраслевых систем (например, Mitre Att&ck).
- Интеграция с SIEM (например, Splunk, AWS Security Hub).
- Интеграция с межсетевыми экранами (например, PaloAlto Networks).

Все это позволяет Omnis Security стать полностью интегрированной и жизненно важной частью инфраструктуры кибербезопасности Вашей организации.

NETSCOUT

**Штаб-квартира компании**
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

**Коммерческая информация**
Бесплатно для США: 800-309-4804
(Информация о международных номерах ниже)

**Поддержка продукта**
Бесплатно для США: 888-357-7667
(Информация о международных номерах ниже)

NETSCOUT предлагает продажи, поддержку и услуги в более чем 32 странах. Глобальные адреса и международные номера указаны на веб-сайте NETSCOUT по адресу: www.netscout.com/company/contact-us



SECSB_029_RU-2102 12/2021