# Network Detection and Response

XDR без NDR — это просто EDR

## Устраните угрозы, прежде чем они нанесут удар

Обнаруживайте то, что невозможно выявить, и останавливайте скрытые атаки. Trellix Network Detection and Response (NDR) помогает вашей команде сосредоточиться на актуальных угрозах, быстро и с умом отражать вторжения, а также усилить слабые места вашей кибербезопасности.

**Автоматически адаптируйтесь к новым угрозам**

Выявляйте распространенные угрозы в сети и центрах обработки данных с возможностью автоматической адаптации, чтобы вы могли распознать непрерывно развивающиеся угрозы и своевременно реагировать на них.

**Защита от сети до облака**

Защитите свое облако, IoT, инструменты для совместной работы, конечные точки и инфраструктуру. Автоматизируйте свои действия, чтобы адаптироваться к изменяющейся среде безопасности.

**Подстраивайте решение под потребности вашей организации**

Интегрируйтесь с любым поставщиком и повышайте операционную эффективность, отображая только важные для вас оповещения.

# ПРОДУКТЫ TRELLIX ДЛЯ СЕТЕВОЙ БЕЗОПАСНОСТИ

## Trellix Network Security

- Автоматически выявляйте подозрительное поведение в сети и предотвращайте атаки, которые ускользают от традиционных сигнатурных систем безопасности.
- Выявляйте и блокируйте сложные угрозы и перемещение по периметру организации в режиме реального времени.
- Ускоряйте устранение обнаруженных угроз с помощью исчерпывающих доказательств и оперативных данных.

## Trellix Network Forensics

- Выявляйте и устраняйте широкий спектр угроз быстрее.
- Определяйте масштаб и влияние угроз, а также восстанавливайте защищенное состояние вашей сети.
- Визуализируйте события до, во время и после атаки, чтобы исключить возможность повторного заражения сети.

## Trellix Intrusion Prevention System

- Проверяйте весь сетевой трафик на наличие новых и неизвестных угроз.
- Оптимизируйте операции по обеспечению безопасности с корреляцией событий из всех источников в режиме реального времени.
- Отслеживайте свою сеть на предмет вредоносной активности и блокируйте вторжения в момент их обнаружения.

## Обнаруживайте возможные атаки и предотвращайте угрозы, незаметные для других продуктов

| ВОЗМОЖНОСТЬ | ФУНКЦИОНАЛ |
|---|---|
| Обнаружение угроз без сигнатур | Обнаруживает многопоточные, многоэтапные, полиморфные, Zero-Day-атаки, а также программы-вымогатели и другие продвинутые угрозы |
| Обнаружение в режиме реального времени «задним числом» | Отслеживает известные и неизвестные угрозы в режиме реального времени и в прошлом |
| Многовекторная корреляция | Автоматизирует проверку и блокирует атаки на электронную почту, конечные точки и другие векторы безопасности |
| Обнаружение движения по периметру организации | Обнаруживает ранее неизвестный подозрительный сетевой трафик внутри сети |
| Предотвращение DoS и DDoS | Предотвращает попадание вредоносного трафика в вашу сеть, не мешая проходить легальному трафику |
| Расшифровка входящего/исходящего SSL | Обнаруживает вредоносные программы и другие современные угрозы во входящем и исходящем зашифрованном трафике |
| Совместимость с многими ОС, форматами файлов и приложениями | Поддерживает гетерогенные среды конечных точек для широкого спектра приложений |
| Надежный гипервизор | Скрывает следы виртуализации, чтобы обойти техники уклонения от анализа |

## Проактивно реагируйте и быстро локализуйте инциденты

| ВОЗМОЖНОСТЬ | ФУНКЦИОНАЛ |
|---|---|
| Блокировка в режиме реального времени | Мгновенно останавливает атаки |
| Усовершенствованная система предотвращения вторжений | Выполняет глубокую проверку сетевого трафика (DPI) для обнаружения и защиты от ботнетов и других сложных угроз |
| Интегрированные рабочие процессы безопасности | Быстрый переход от обнаружения к расследованию и реагированию |
| Отказоустойчивость | Обеспечивает надежную бесперебойную защиту сети |
| Сигнатурное обнаружение вторжений без ложных срабатываний | Автоматизирует и ускоряет обработку оповещений для устранения избыточной ручной работы |
| Обнаружение и классификация потенциально опасного ПО | Классифицирует вредоносные программы на критические и некритические для определения приоритетов ресурсов реагирования |
| Эффективный контекстный интеллект | Ускоряет устранение продвинутых угроз, предоставляя подробную информацию об атаке и злоумышленнике |

## Определяйте масштаб последствий инцидента и повышайте качество реагирования

| ВОЗМОЖНОСТЬ | ФУНКЦИОНАЛ |
|---|---|
| Обширный контекст | Проверяет сетевые пакеты, соединения и сеансы до, во время и после атаки |
| Ретроспективный поиск угроз | Интегрирует аналитику угроз для исторического анализа IOC и оповещения об обнаруженных IOC, присутствующих в вашей сети днями или неделями ранее |
| Уменьшение ущерба от атак | Ускоряет процесс расследования благодаря единому рабочему пространству с мгновенным переходом из оповещений к данным о сеансах одним щелчком мыши |