Trend Micro™

DEEP DISCOVERY™ INSPECTOR

Обнаружение направленных атак, сложных угроз и программ-вымогателей по всей сети

Направленные атаки и сложные угрозы созданы таким образом, чтобы обходить ваши обычные средства защиты и оставаться скрытыми в момент кражи корпоративных данных, интеллектуальной собственности или переписки. Также они могут зашифровать критические данные и требовать за них выкуп. Аналитики и эксперты по безопасности сходятся во мнении, что для обнаружения направленных атак и сложных угроз организации должны использовать передовые технологии обнаружения в рамках единой расширенной стратегии.

Deep Discovery Inspector — это физическое или виртуальное сетевое устройство, которое всесторонне наблюдает за вашей сетью и обнаруживает любые проявления направленных атак, сложных угроз и программ-вымогателей. Специализированные модули обнаружения и настраиваемые «песочницы» Deep Discovery Inspector позволяют выявлять и анализировать сложные и неизвестные вредоносные программы, программы-вымогатели, эксплойты нулевого дня, сеансы обмена данными с командными центрами, а также скрытые действия злоумышленников, которые не фиксируются стандартными средствами обеспечения безопасности. Все это дополняется всесторонним мониторингом всех видов трафика — горизонтального и вертикального, физических и виртуальных узлов. Эти функциональные возможности позволяют компании Trend Micro занимать верхнюю строчку в рейтинге наиболее эффективных систем обнаружения угроз в течение уже двух лет, по оценке компании NSS Labs.

КЛЮЧЕВЫЕ ФУНКЦИИ

Всесторонний мониторинг сети. Deep Discovery Inspector контролирует весь трафик как физических, так и виртуальных сегментов сети, а также отслеживает трафик на всех сетевых портах по более чем 100 протоколам, идентифицируя направленные атаки, сложные угрозы и программы-вымогатели. Наш независимый подход к анализу сетевого трафика позволяет Deep Discovery обнаруживать направленные атаки, сложные угрозы и программы-вымогатели во входящем и исходящем трафике, а также горизонтальное движение, командные центры и другие действия злоумышленников на всех этапах атаки.

Расширенные методы обнаружения угроз включают проверку репутации файлов, сетей, IP-адресов и мобильных приложений, эвристический анализ, сканирование сложных угроз, индивидуальный анализ с использованием «песочницы» и анализ коррелированной аналитической информации об угрозах для обнаружения программ-вымогателей, эксплойтов нулевого дня, сложного вредоносного ПО и иного поведения злоумышленников.

Анализ с использованием настраиваемой «песочницы» подразумевает создание виртуальных образов, которые настроены так, чтобы точно соответствовать конфигурациям вашей системы, драйверам, установленным приложениям и языковым версиям. Использование данного подхода увеличивает скорость обнаружения расширенных угроз и программ-вымогателей, рассчитанных на обход стандартных виртуальных образов.

Всесторонний анализ информации об угрозах использует глобальные данные об угрозах из системы Trend Micro™ Smart Protection Network™ для понимания локальных угроз, что обеспечивает мгновенную защиту данных, где бы они ни находились.

Высокая рентабельность инвестиций достигается за счет гибкой архитектуры, подразумевающей развертывание системы в виде единого аппаратного или виртуального устройства на основе пропускной способности сети. Повышает ценность текущих инвестиций в системы NGFW/IPS, SIEM и шлюзы путем обмена аналитической информацией об угрозах.

Повсеместное обнаружение программ-вымогателей. Deep Discovery Inspector способен обнаруживать эмуляции скриптов, эксплойты нулевого дня, а также целевые и защищенные паролем вредоносные программы, ассоциируемые с программами-вымогателями. Система также использует информацию об известных угрозах для обнаружения программ-вымогателей посредством анализа шаблонов и репутационных списков.

Ключевые преимущества

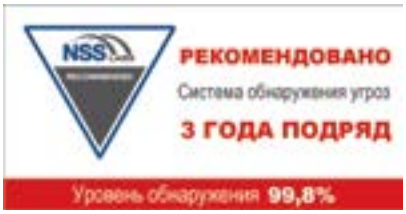
Улучшенное обнаружение угроз

- Множественные методы обнаружения.
- Всесторонний мониторинг трафика.
- Анализ «песочницы».
- Комплексный анализ информации об угрозах.

Существенная рентабельность инвестиций

- Исследование показывает рентабельность инвестиций на уровне 145% за 10 месяцев.
- Повышение ценности текущих инвестиций.
- Гибкие варианты развертывания.
- Автоматизация задач, выполняемых вручную.

[1] ESG, Оценка экономической ценности: Октябрь 2015



КЛЮЧЕВАЯ ЧАСТЬ СИСТЕМЫ CONNECTED THREAT DEFENSE ОТ TREND MICRO

Для создания адекватной защиты от текущего ландшафта угроз вам понадобится многоуровневая платформа защиты, обеспечивающая полный жизненный цикл защиты от угроз. Trend Micro Connected Threat Defense — это многоуровневый подход к безопасности, который позволит вашей организации быстро предотвращать, обнаруживать и реагировать на новые направленные угрозы, при этом повышая прозрачность и контроль вашей сети.

- **Предотвращение:** оценка потенциальных уязвимостей и превентивная защита конечных устройств, серверов и приложений.
- **Обнаружение:** обнаружение сложных вредоносных программ, поведения и обмена информацией, которые не фиксируются стандартными средствами обеспечения безопасности.
- **Реагирование:** быстрый ответ благодаря обмену информацией об угрозах и получению обновлений безопасности в режиме реального времени.
- **Мониторинг и управление:** обеспечение централизованного мониторинга всей сети и систем; анализ и оценка воздействия угроз.

СПЕЦИФИКАЦИЯ УСТРОЙСТВА DEEP DISCOVERY INSPECTOR

	Модель 500/1000	Модель 4000
Модель устройства	510/1100	4100
Поддерживаемые «песочницы»	2 (500), 4 (1000)	20
Форм-фактор	1U для установки в стойку, 48,26 см (19”)	2U для установки в стойку, 48,26 см (19”)
Вес	19,9 кг (43,87 фунта)	31,5 кг (69,45 фунта)
Размеры (Ш x Г x В)	43,4 (17,09”) x 64,2 (25,28”) 4,28 (1,69”) см	48,2 см (18,98”) x 75,58 см (29,75”) x 8.73 см (3,44”)
Порты управления	10/100/1000 BASE-T RJ45 порт x 1 iDrac Enterprise RD45 x 1	10/100/1000 BASE-T RJ45 порт x 1 iDrac Enterprise RD45 x 1
Порты для обмена данными	10/100/1000 BASE-T RJ45 порт x 5	10Gb SFP+ с приемопередатчиком SX x 4 10/100/1000 Base-T RJ45 x 5
Входное напряжение (переменный ток)	от 100 до 240 В переменного тока	от 100 до 240 В переменного тока
Входной ток (переменный ток)	от 7,4 до 3,7 А	от 10 до 5 А
Жесткие диски	2 x 1 ТБ 3,5-дюймовых SATA-диска	44 x 1 ТБ 3,5-дюймовых NLSAS-диска
Конфигурация RAID	RAID 1	RAID 1+0
Источник питания	550 Вт с резервированием	750 Вт с резервированием
Энергопотребление (макс.)	604Вт	847Вт (макс.)
Теплоотдача	2133 БТЕ/час (макс.)	2891 БТЕ/час (макс.)
Частота	50/60 Гц	50/60 Гц
Рабочая температура	10–35 °C (50–95 °F)	10–35 °C (50–95 °F)
Гарантия	3 года	3 года

Виртуальные устройства Deep Discovery Inspector доступны при пропускной способности 100/250/500/1000 Мбит/с и развертываются в VMware vSphere 5 и выше, а также в KVM.

ПРОЧИЕ ПРОДУКТЫ DEEP DISCOVERY

Deep Discovery Inspector обеспечивает защиту от сложных угроз самых уязвимых мест вашей организации — сети, электронной почты, конечных устройств, а также дополняет имеющиеся решения по обеспечению безопасности.

- **Deep Discovery Analyzer** выполняет расширенный анализ с использованием «песочницы», таким образом повышая ценность прочих систем безопасности, включая системы защиты конечных устройств, интернет-шлюзы и почтовые шлюзы, решения для обеспечения сетевой безопасности и другие продукты Deep Discovery. Deep Discovery Analyzer способен обнаруживать программы-вымогатели, сложное вредоносное ПО, эксплойты нулевого дня, сеансы обмена данными с командными центрами, а также многоэтапные загрузки данных через вредоносные вложения или с неблагонадежных URL-адресов в системах Windows и Mac.
- **Deep Discovery Email Inspector** обеспечивает расширенное обнаружение вредоносных программ, в том числе с помощью «песочницы» для электронной почты. Email Inspector может быть настроен на блокирование доставки сложного вредоносного ПО по электронной почте. Доставка такого вредоносного ПО часто является первым этапом атаки с помощью программы-вымогателя.

Deep Discovery Inspector является частью решения Trend Micro Network Defense с технологиями XGen™ Security.

Обнаружение и защита

- Направленные атаки и сложные угрозы.
- Целевые и известные атаки программ-вымогателей.
- Вредоносные программы нулевого дня и эксплойты в документах.
- Признаки действий злоумышленника и иная сетевая активность.
- Веб-угрозы, включая эксплойты и скрытые загрузки.
- Фишинг, целевой фишинг и другие угрозы электронной почты.
- Внедрение вредоносного кода.
- Боты, трояны, черви, клавиатурные шпионы.
- Неблагонадежные приложения.

TREND MICRO™

Securing Your Journey to the Cloud