Trend Micro™

DEEP DISCOVERY™ ANALYZER

Расширенная защита от направленных атак

Направленные атаки и сложные угрозы созданы таким образом, чтобы обходить ваши обычные средства защиты и оставаться скрытыми в момент кражи конфиденциальных данных или шифрования критических данных, за которые они требуют 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 защиты от современных угроз с обманными маневрами.

Deep Discovery Analyzer повышает ценность текущих инвестиций в системы безопасности от Trend Micro и сторонних производителей (через API для веб-служб) благодаря наличию настраиваемых «песочниц» и расширенному анализу. Другие продукты Trend Micro также могут воспользоваться расширенными возможностями «песочниц». Подозрительные объекты могут быть отправлены в «песочницу» модуля Analyzer для расширенного анализа с использованием нескольких методов обнаружения. Если обнаружена угроза, решения по безопасности могут обновляться автоматически.

КЛЮЧЕВЫЕ ФУНКЦИИ

Настраиваемый анализ с использованием «песочницы» использует виртуальные образы, которые настроены так, чтобы точно соответствовать конфигурациям вашей системы, драйверам, установленным приложениям и языковым версиям. Использование данного подхода увеличивает скорость обнаружения расширенных угроз, рассчитанных на обход стандартных виртуальных образов. Настраиваемая среда «песочницы» включает в себя безопасный внешний доступ для идентификации и анализа многоступенчатых загрузок, URL-адресов, командных центров, файлов и прочих объектов, которые могут быть переданы на анализ как в ручную, так и в автоматическом режиме.

Гибкое развертывание. Analyzer может быть развернут как в виде отдельной «песочницы», так и в составе более крупного развертывания Deep Discovery в качестве дополнительной «песочницы». Функция масштабирования обеспечивает поддержку до 60 «песочниц» в одном устройстве. В свою очередь, несколько устройств могут быть сгруппированы для обеспечения высокой отказоустойчивости или настроены для горячего или холодного резервного копирования.

Усовершенствованные методы обнаружения угроз. Комбинация таких методов, как статический анализ, эвристический анализ, анализ поведения, проверка репутации файлов и веб-служб позволяет быстро обнаруживать угрозы. Analyzer также обнаруживает многоступенчатые вредоносные файлы, исходящие соединения и повторяющиеся сеансы связи с командными центрами от подозрительных файлов.

- **Широкий спектр анализируемых файлов.** Благодаря использованию «песочниц» и нескольких механизмов обнаружения угроз, Deep Discovery Analyzer работает с большим количеством типов файлов: исполняемые файлы Windows, офисные файлы Microsoft® Office, PDF-файлы, интернет-содержимое и разнообразные архивные файлы. При этом каждому типу файлов могут быть определены собственные политики.
- **Обнаружение эксплойтов в документах.** Обнаружение вредоносных программ и эксплойтов в документах распространенных форматов с использованием специализированных методов обнаружения и «песочницы».
- **Анализ URL-адресов.** URL-адреса, содержащиеся в электронных письмах или набранные вручную, анализируются с использованием «песочницы».
- **API для веб-служб и самостоятельная отправка файлов.** Аналитики любых продуктов или вредоносных программ могут отправлять подозрительные образцы на анализ. Deep Discovery Analyzer автоматически предоставляет другим решениям Trend Micro и решениям сторонних поставщиков оперативные сведения о новых индикаторах компрометации.
- **Поддержка операционных систем Windows, Mac и Android.**

Обнаружение программ-вымогателей. Deep Discovery Analyzer 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. Настраиваемая «песочница» может обнаруживать массовые изменения в файлах, признаки шифрования данных и изменения в резервных копиях.

Основные преимущества

Улучшенное обнаружение угроз:

- Более эффективное обнаружение угроз по сравнению с обычными виртуальными средами.
- Более эффективное противодействие уклонению от обнаружения.

Существенная рентабельность инвестиций:

- Повышает ценность инвестиций за счет интеграции и обмена аналитической информацией об угрозах и совместного использования дополнительной вычислительной мощности в сетях с высоким уровнем трафика.
- Избавляет от необходимости выполнять трудоемкий ручной анализ подозрительных файлов.
- Защищает от программ-вымогателей и дорогостоящих процедур восстановления после их атак.
- Гибкость развертывания для централизованного или децентрализованного анализа.

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 новая модель кибербезопасности, которая позволит организациям быстро предотвращать, обнаруживать и реагировать на новые направленные угрозы, при этом повышая прозрачность и контроль сетей.

- **Защита:** 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 отклик благодаря обмену информацией об угрозах и получению обновлений безопасности в режиме реального времени всеми слоями безопасности Trend Micro, а также между решениями сторонних поставщиков, через механизмы YARA и STIX.
- **Мониторинг и управление:** Централизованный мониторинг всей сети и систем; анализ и оценка воздействия угроз.

СПЕЦИФИКАЦИЯ УСТРОЙСТВА DEEP DISCOVERY ANALYZER

	Аппаратная модель 1100
Производительность	45 000 образцов/день
Поддерживаемые типы файлов	cell, chm, class, dll, doc, docx, exe, gul, hwp, hwpx, jar, js, jse, jtd, lnk, mov, pdf, ppt, pptx, ps1, rtf, swf, vbs, vbe, xls, xlsx, xml
Поддерживаемые операционные системы	Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, Mac OS
Форм-фактор	2U для установки в стойку, 48,26 см (19 дюймов)
Вес	32,5 кг (71,65 фунтов)
Размеры	Ширина 48,2 см (18,98 дюйма) x Глубина 75,58 см (29,75 дюйма) x Высота 8,73 см (3,44 дюйма)
Порты управления	10/100/1000 BASE-T RJ45 порт x 1
Порты для обмена данными	10/100/1000 Base-T RJ45 x 3
Входное напряжение (переменный ток)	100–240 В переменного тока
Входной ток (переменный ток)	от 10 до 5 А
Жесткие диски	2 x 4 ТБ 3,5-дюймовых SATA-диска
Конфигурация RAID	RAID 1
Источник питания	750 Вт с резервированием
Потребление (макс.)	847 Вт (макс.)
Теплоотдача	2891 БТЕ/час (макс.)
Частота	50/60 Гц
Рабочая температура	50-95 °F (10 to 35 °C)
Гарантия на оборудование	3 года

ПРОЧИЕ ПРОДУКТЫ DEEP DISCOVERY

Deep Discovery Analyzer является частью платформы Deep Discovery и обеспечивает расширенную защиту от угроз самых важных элементов вашей организации — сети, электронной почты, конечных устройств, а также дополняет существующие решения безопасности.

- **Deep Discovery Inspector** — это физическое или виртуальное устройство, которое обеспечивает полный контроль сети и позволяет обнаруживать любые направленные атаки и сложные угрозы. 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, горизонтальное движение, а также скрытые действия злоумышленников, которые не фиксируются стандартными средствами обеспечения безопасности.
- **Deep Discovery Email Inspector** обеспечивает расширенное обнаружение вредоносных программ, включая использование «песочницы» для электронной почты. Email Inspector может быть настроен на блокирование доставки сложного вредоносного ПО по электронной почте.

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

POWERED BY XGen™ SECURITY

TREND MICRO™

Securing Your Journey to the Cloud