5 способов обеспечить всеобъемлющую безопасность

Угрозы окружают нас повсюду, еще никогда они не были столь изощрены. Cisco предлагает пять способов защиты в среде распределенной сети.

> «Операторы вредоносного ПО, например программ-вымогателей, нанимают и финансируют группы профессиональных разработчиков, стремясь тем самым гарантировать прибыльность своей деятельности».
>
> *– Отчет Cisco по информационной безопасности за первое полугодие 2015 года*

1

Используйте сеть в качестве индикатора.

Вредоносная деятельность может маскироваться в потоках обычных оповещений, генерируемых вашей системой. Технология Cisco IOS® Flexible NetFlow, реализованная на новых коммутаторах, маршрутизаторах и беспроводных решениях Cisco®, повышает прозрачность и предоставляет контекстуальную информацию, позволяя вам определять базовые показатели трафика и своевременно выявлять случаи подозрительного поведения в любой точке вашей повседневной рабочей среды.

2

Выявляйте реальные угрозы среди множества транзакций.

Собирая метаданные NetFlow и других источников, Lancope StealthWatch System анализирует и документирует все транзакции, выполняемые в сети. Используя эти данные, StealthWatch идентифицирует аномальное поведение и признаки вредоносной деятельности.[1]

> «90 % компаний уверены в надежности своих политик безопасности. 54 % этих компаний были подвергнуты общественному контролю после нарушения данных».
>
> *– Отчет Cisco по информационной безопасности за 2015 год*

3

Предоставляйте доступ только проверенным устройствам.

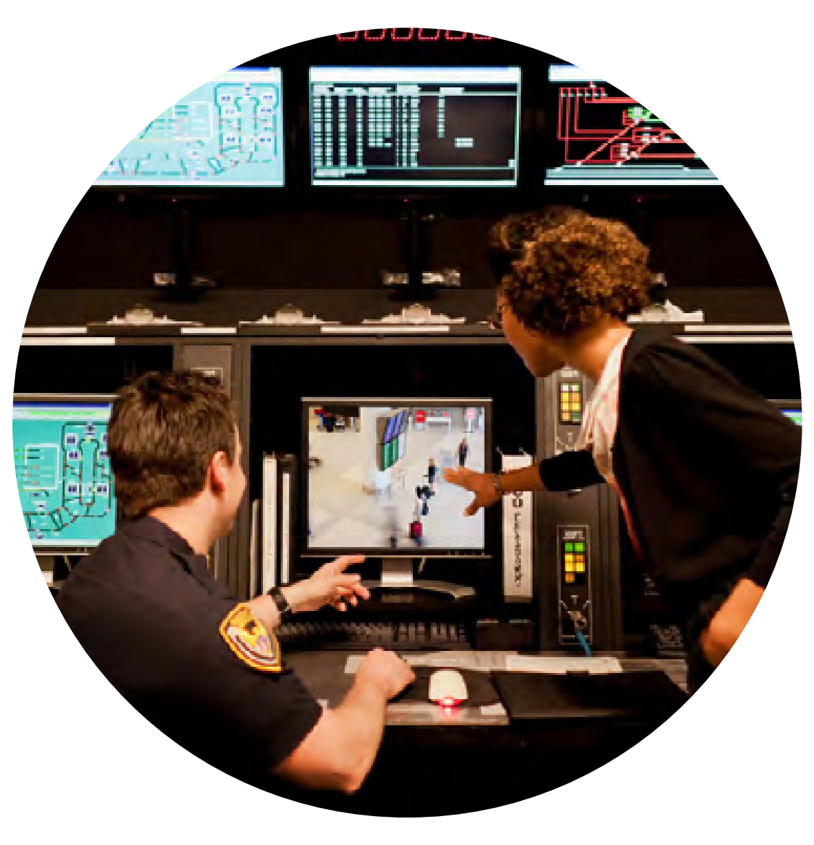
По мере усложнения структуры вашей распределенной сети и роста количества устройств, пытающихся получить к ней доступ, уровень вашей защиты снизится, и угрозы смогут незаметно проникнуть в среду вашей сети. Используйте решение контроля доступа Cisco Identity Services Engine (ISE) для минимизации зоны поражения, чтобы только проверенные устройства могли получить доступ в сеть.

> «Технология Cisco TrustSec® повышает безопасность ИТ-среды и снижает эксплуатационные расходы, обеспечивая рентабельность инвестиций на уровне 405 % с полной окупаемостью в течение 4,7 месяцев».
>
> – Forrester, *Total Economic Impact Study: Cisco TrustSec*

4

Установите правила и обеспечьте их соблюдение.

Угрозы могут существовать на любом участке вашей сети. Используйте свою сеть в качестве средства контроля, реализовав программно-определяемую сегментацию на базе технологии Cisco TrustSec для последовательного соблюдения прав доступа в среде всей сети. TrustSec интерпретирует политику ISE для обеспечения соблюдения необходимого уровня доступа для пользователей, предотвращения обходных маневров злоумышленников и ограничения воздействия нарушений.



> «На данный момент уже можно заявить, что в 2015 году инновационность, качество и эффективность маскирования кибератак вышли на беспрецедентный уровень».
>
> *– Отчет Cisco по информационной безопасности за первое полугодие 2015 года*

5

Расширьте поддержку своих филиалов.

Даже сеть комплекса зданий защитить весьма непросто, а сети филиалов ставят перед вами новые задачи и расширяют зону поражения. Cisco Intelligent WAN (IWAN) позволяет защитить распределенную сеть с обеспечением шифрования, прозрачности и удобного управления, характерных для сетей центрального комплекса зданий. Cisco ONE для WAN предлагает весь пакет этих расширенных программных функций, что существенно упрощает их приобретение и развертывание.

> «Если компания намерена использовать свои инвестиции с максимальной эффективностью, систему защиты необходимо интегрировать в среду всей сетевой инфраструктуры».
>
> – Кевин Филлипс (Kevin Phillips), директор по ИТ-операциям, K&L Gates LLP

Подготовьте свою сеть.

Если вы готовы обеспечить всеобъемлющую безопасность, мы можем вам помочь.

Подробнее

Дополнительные ресурсы

Получить *отчет Cisco по информационной безопасности за первое полугодие 2015 года.*

5 лучших способов реализовать интеллектуальный потенциал вашей сети

---

[1] *Cisco & Lancope Partnership*, Lancope, 2015.