Чеклист: Как Fortinet помогает директорам по ИТ противостоять быстро развивающимся угрозам

Для директора по ИТ кибербезопасность является всего лишь одной из множества обязанностей. Однако недостаточная защита угрожает успеху буквально всех других проектов ИТ-команды. Директора по ИТ часто не знают, с чего начать в условиях появления постоянно меняющихся угроз, не говоря уже об увеличении их объема, скорости распространения и изощренности.

6 способов обеспечения комплексной защиты от Fortinet

Глобальная архитектура безопасности Fortinet с консолидированными и полными базами данных об угрозах помогает директорам по ИТ принимать упреждающие меры защиты от возникающих угроз. Интеграция обеспечивает возможность отслеживания, централизованное управление и автоматизацию процессов безопасности во всей инфраструктуре.

☑ Комплексная интегрированная система безопасности

Архитектура сетевой безопасности Fortinet Security Fabric объединяет в себе обширный портфель решений для всей инфраструктуры безопасности, которые помогают снизить сложность и обеспечить защиту от продвинутых и появляющихся угроз. Полная интеграция предоставляет возможность централизованного отслеживания и контроля всей сети.

☑ Открытая экосистема

В рамках открытой экосистемы партнеры Fortinet могут разрабатывать решения для интеграции собственных инструментов с системой сетевой безопасности Fortinet. Для других решений безопасности компания Fortinet предлагает сценарии и инструменты для разработчиков, в том числе надежный API-интерфейс передачи состояния представления (REST API), для создания индивидуальных интеграционных решений с уникальной инфраструктурой организации.

☑ Автоматизированные рабочие процессы защиты

Глубокая интеграция открывает возможности для автоматизации всех процессов безопасности — в том числе для управления инцидентами и событиями безопасности (SIEM), развертывания в автоматическом режиме, контроля доступа к сети (NAC) и проверки на соответствие требованиям. Таким образом, это помогает устранить ручные процессы, которые отвлекают компетентных специалистов от решения стратегических задач.

☑ Высокая скорость обнаружения угроз

Своевременный сбор данных об угрозах является ключевым условием противодействия атакам, особенно когда большинство из них угрозы «нулевого дня». Служба FortiGuard Labs ежедневно анализирует миллионы файлов, используя технологии искусственного интеллекта (AI) и машинного обучения (ML), что обеспечивает максимальную точность анализа новых файлов. В качестве дополнительного уровня защиты FortiSandbox проверяет неизвестные файлы еще до того, как они попадут в сеть, чтобы определить, являются ли они вредоносными или нет.

☑ Комплексные инструменты анализа и составления отчетов

Служба оценки систем безопасности Fortinet Security определяет уровень безопасности организации и выполняет сравнительный анализ с показателями конкурентов и отраслевыми стандартами — в формате, который можно предоставить высшему руководству и совету директоров. Отчеты FortiManager и инструмент анализа FortiAnalyzer помогают упростить согласованное составление отчетов и стратегическое планирование.

☑ Упреждающий подход к управлению рисками

Поскольку вторжения неизбежны, директорам по ИТ необходим упреждающий подход, основанный на управлении рисками, чтобы оценивать, куда направлять ресурсы. Инструменты Fortinet для обнаружения и устранения угроз в реальном времени помогают сократить временные промежутки реагирования, а динамические панели мониторинга отображают процесс превращения уязвимости в угрозу.

Повышение эффективности защиты за счет комплексного интегрированного подхода

Решение Fortinet Security Fabric обеспечивает комплексную защиту благодаря интеграции широкого набора инструментов безопасности и использования надежной сети анализа данных об угрозах, которая помогает опережать злоумышленников и вредоносные угрозы, которые они создают.

FORTINET

www.fortinet.com/ru

октября 17, 2019 4:41 ПП

323490-0-1-RU

D:\Projekty\Fortinet (United Kingdom)\P-348531\06_DTP (Multi)\to correct\CIO\CIO\Checklist - CIO Threat Landscape SS-A4_RU-ru