LUNTRY

Карта механизмов предотвращения Runtime угроз в Kubernetes окружениях

Данные актуальны на 07.07.2025г.

Технология	seccomp	Linux Security Modules (LSM)		iptables	eBPF (tc, xdp)	eBPF_LSM
Реализация	seccomp профиль	AppArmor профиль	SeLinux политика	NetworkPolicy политика	NetworkPolicy политика	Luntry prevention политика
Краткое описание	Контроль на уровне системных вызовов	Контроль на уровне процессов. Mandatory Access Control (MAC)	Контроль на уровне процессов. Mandatory Access Control (MAC)	Контроль сетевого доступа	Контроль сетевого доступа	Контроль на уровне процессов
Основная цель	Усложнить побег из контейнера на хост через уязвимости ядра	Ограничить возможности контейнера для развития атаки и побега на хост	Усложнить побег из контейнера на хост через уязвимости ядра и некорректные конфигурации	Родной межсетевой экран для Pod в кластере	Родной межсетевой экран для Pod в кластере	Ограничить возможности контейнера для развития атаки и побега на хост
Контроль над	Любым системным вызовом	Доступами к файлам, каталогам, сетевым портам, ресурсам системы, capabilities и действиями процессов	Доступами к файлам, каталогам, сетевым портам, ресурсам системы и действиями процессов	Сетевыми соединениями (L3/L4/L7)	Сетевыми соединениями (L3/L4/L7)	Запуском процессов
Версия ядра	2.6.12	2.6.36	2.6.0	2.4	4.8-4.18	5.7
Версия Kubernetes для GA	1.19	1.30	1.12	1.7	1.7	Не зависит
Предоставляется	Средствами ОС	Средствами ОС	Средствами ОС	Плагин CNI Например, Calico, Antrea	Плагин CNI Например, Calico, Antrea	Сторонними средствами защиты. Например, Luntry
Интеграция с Kubernetes	Раздел SecurityContext.SeccompProfile	Раздел SecurityContext.AppArmorProfile	Раздел SecurityContext.SELinuxOptions	YAML ресурс NetworkPolicy. Возможны и кастомные реализации CNI	YAML ресурс NetworkPolicy. Возможны и кастомные реализации CNI	Не зависит
Применение	Файл на Node	Файл на Node	Файл на Node	YAML в etcd	YAML в etcd	UI/API
Режимы работы	Whitelist, Blacklist	Whitelist, Blacklist	Whitelist, Blacklist	Как правило Whitelist. В кастомных реализациях возможен Blacklist	Как правило Whitelist. В кастомных реализациях возможен Blacklist	Whitelist, Blacklist
Сложность описания и использования	Высокая (Из-за сложности хорошего покрытия)	Средняя	Высокая (Из-за сложности описания)	Средняя	Средняя	Низкая + возможность генерировать AppArmor профиль
Значения по умолчанию	Да - RuntimeDefault	Да - RuntimeDefault	Нет	Нет	Нет	Нет
Влияние на производительность	Минимальное	Минимальное	Среднее	Среднее	Минимальное	Минимальное
Комментарий/ограничения	Тяжело поддерживать для активно развивающихся приложений	Не совместим с SeLinux	Не совместим с AppArmor	Низкая скорость обработки по сравнению с eBPF, но более простая в отладке	Высокая скорость обработки по сравнению с iptables	Коммерческое решение

luntry.ru

luntry_official luntrysolution luntrysolution info@luntry.ru

В данном обзоре представлены только те **Linux**-технологии и реализации, которые имеют поддержку **Kubernetes**.
Такие механизмы **Linux**, как **Lockdown, landlock, yama** не рассматриваются.