PRISMA™ CLOUD
BY PALO ALTO NETWORKS

Prisma Cloud Compute Edition

Проблемы безопасности в облачных средах

Традиционные инструменты и методологии безопасности не подходят для защиты облачных приложений, управляемых разработчиками и не привязанных к инфраструктуре:

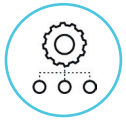
- Разработчики и команды DevOps играют жизненно важную роль в создании и развертывании облачных приложений, зачастую работая вне поля зрения традиционных технологий безопасности. Требуются решения по безопасности, которые интегрируются с инфраструктурой и инструментами разработчиков.
- Организации используют всё более разнородную инфраструктуру: физические сервера, частные облака, публичные облака или любые их комбинации.
- В облачных средах процесс изменений никогда не останавливается. От решений безопасности требуется автоматизация защиты растущего числа постоянно меняющихся микросервисов.

Комплексная защита хостов, контейнеров и функций

Prisma™ Cloud Compute Edition – это ведущая облачная платформа безопасности, обеспечивающая целостную защиту хостов, контейнеров и бессерверных вычислений на протяжении всего жизненного цикла приложений независимо от базовой вычислительной технологии или облака, в котором они работают.

Управление уязвимостями: Обнаруживает и блокирует уязвимости на уровне ОС, фреймворка приложений и отдельных сборок на протяжении всего жизненного цикла приложения (от процесса разработки до эксплуатации) .

Регуляторное соответствие: Обеспечивает регуляторное соответвствие на протяжении всего жизненного цикла приложения. Готовые шаблоны для HIPAA, PCI, GDPR и NIST SP 800-190, а также проверки для Docker, Kubernetes, Linux CIS Benchmarks, Istio®.



Интеграция с CI/CD : Полностью интегрируется в процесс разработки и доставки приложений. Автоматизированные и пользовательские политики могут блокировать сборку или публикацию на основании выявленных уязвимостей или несоответствий стандартам.

Runtime defense: Обеспечивает защиту инфраструктуры при помощи машинного обучения. Автоматически создаёт основанные на белых списках модели поведения приложений с минимально необходимыми привилегиями.

Cloud-native firewalls: Изучает топологию сетевого взаимодействия приложений и реализует необходимую изоляцию для каждого микросервиса, обеспечивая защиту на сетевом и прикладном уровне (WAF).

Контроль доступа: Позволяет управлять секретами, формировать и применять детализированные политики, регулирующие доступ пользователей к ресурсам Docker и Kubernetes с возможностью мониторинга их активностей.

PRISMA™ CLOUD
BY PALO ALTO NETWORKS

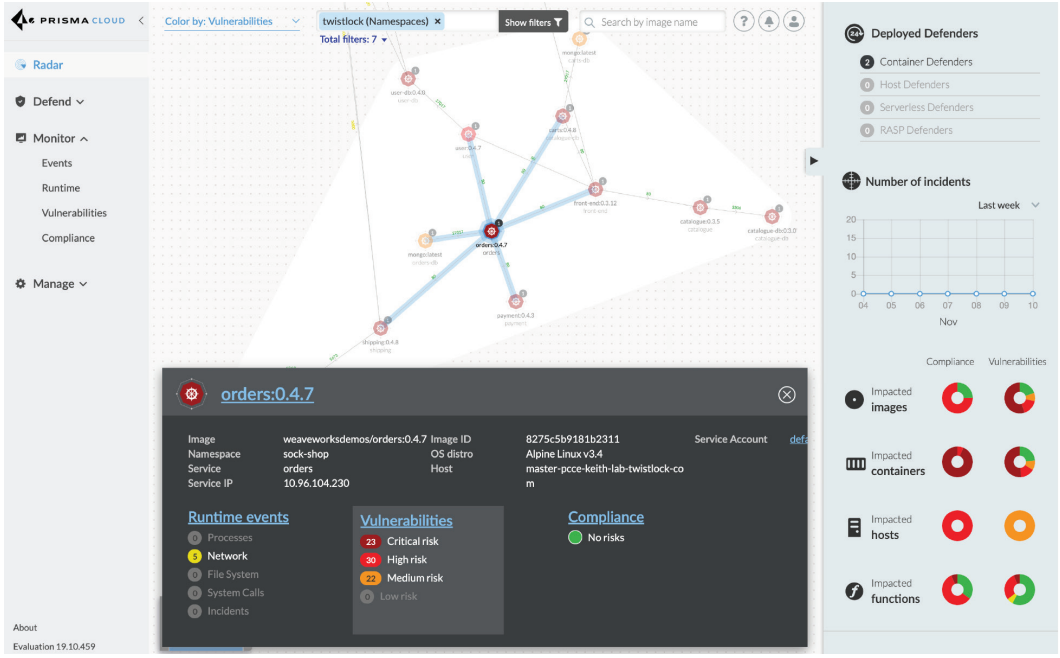
Архитектура

Prisma Cloud Compute Edition поставляется в виде образа контейнера и поддерживает множество вариантов развертывания: в публичных, частных (включая полностью изолированные) или гибридных облачных средах.

Defenders – это агенты, устанавливаемые внутри инфраструктуры, защищающие как виртуальные машины или физические хосты, так и контейнеры, кластеры Kubernetes, CaaS, PaaS и serverless приложения. Они изучают нормальное поведение приложений и предотвращают любые аномальные действия, а также обеспечивают комплексную защиту на основе технологий машинного обучения, комбинируя в моделях локальную активность и сетевое взаимодействие приложений.

Prisma Cloud Compute Edition позволяет управлять уязвимостями и регуляторным соответствием на протяжении полного жизненного цикла приложения путем интеграции с CI/CD процессом, реестром образов Docker, репозиторием кода и любой производственной средой, непрерывно оценивая факторы риска и приоритезируя события. Возможности разграничения доступа к системе и приложениям внутри нее по ролям позволяют безопасно и удобно управлять всей распределенной инфраструктурой, секретами, журналами Kubernetes, инструментами IAM.

Для получения дополнительной информации посетите www.paloaltonetworks.com.



Ключевые преимущества

- **Следуйте трендам и используйте любые облачные технологии.** Выберите подходящую архитектуру для своего приложения и будьте уверены, что Prisma Cloud обеспечит ее защиту.
- **Правильно приоритезируйте риски в облачных средах.** Используйте схемы взаимодействия и данные об угрозах для непрерывного анализа уязвимостей и определения приоритетов рисков во всей облачной инфраструктуре на протяжении всего жизненного цикла приложений.
- **Автоматизируйте безопасность на скорости DevOps.** Предоставьте командам разработчиков и DevOps возможность публикации приложений как можно быстрее, чтобы повысить эффективность бизнеса одновременно с повышением безопасности.