Trend Micro

CLOUD ONE™ – CONTAINER SECURITY

Bảo vệ liên tục hình ảnh vùng chứa và các điểm đăng ký, tự hoạt động trong quy trình CI/CD của bạn

Phương thức phát triển ứng dụng ưu tiên hệ thống đám mây đã trở nên phổ biến hơn trong các công ty đang tìm cách cải tiến tốc độ chạy và hệ sinh thái ứng dụng tương quan. Tuy nhiên, các tổ chức hiện đang gặp khó khăn trong giải pháp bảo mật truyền thống, cách này cần đội ngũ DevOp và các phòng kinh doanh, lí do vì họ làm việc với nhiều nguồn và ưu tiên khác nhau. Trên hết, phương pháp chọn phát triển ứng dụng theo khối đang thay đổi cách tiếp cận của tổ chức khi chuyển sang hệ thống đám mây, vùng chứa và nền tảng không máy chủ.

ESG, hãng phân tích và nghiên cứu CNTT, gần đây đã thực hiện một cuộc khảo sát, cho thấy 39% công ty đang triển khai chiến lược ưu tiên hệ thống đám mây, theo đó các ứng dụng mới sử dụng dịch vụ đám mây công cộng để được tạo ra , trừ khi có trường hợp đáng chú ý cần được triển khai tại cơ sở.

Với quy trình công việc chuyển sang nền tảng đám mây gốc và đội ngũ DevOps áp dụng bảo mật trên khắp quy trình cũng như ứng dụng đám mây gốc của họ, giải pháp bảo mật cần được thiết kế để đạt thành công trên các môi trường (vật lý, ảo, đám mây, vùng chứa và không dây). Điều này cung cấp sức mạnh liên kết giữa bảo mật CNTT và việc của DevOps. Nó cũng thúc đẩy hợp nhất công cụ cũng như hợp tác của bảo mật và yêu cầu về tuân thủ, mà không can thiệp vào chu kỳ phát triển cài đặt/ chuyển tiếp liên tục (CI/CD) .

Trend Micro Cloud One™ – Container Security* cung cấp quy trình tự động tạo hình ảnh vùng chứa và quét điểm đăng ký. Được thiết kế cho nhà phát triển và đội điều hành, Container Security cho phép phát hiện phần mềm độc hại, tài liệu mật/ mã khóa, vi phạm tuân thủ cũng như lỗ hổng bảo mật sớm và nhanh chóng, bao gồm cả những lỗ hổng phụ thuộc mã code được tìm thấy trong nguồn mở. Ngoài ra, Container Security còn cung cấp khả năng phát hiện nguy hiểm trong gói quản lí ứng dụng đã được cài, cũng như ứng dụng cài trực tiếp, thông qua nguồn cung cấp quy tắc dữ liệu dẫn đầu ngành an ninh mạng của Trend Micro. Container Security giúp nhà phát triển tiếp cận trực tiếp hơn với nguồn tài nguyên dữ liệu lỗ hổng vảo mật của Snyk, cung cấp khả năng phát hiện sớm và giảm lỗ hổng trong phần mã code phụ thuộc vào nguồn mở. Với Container Security, các đội DevOp có thể liên tục cung cấp sản phẩm cũng như ứng dụng và đạt yêu cầu của doanh nghiệp mà không ảnh hưởng đến chu kỳ cấu tạo.

Điểm mạnh

Ngăn bị khai thác trước khi hoạt động

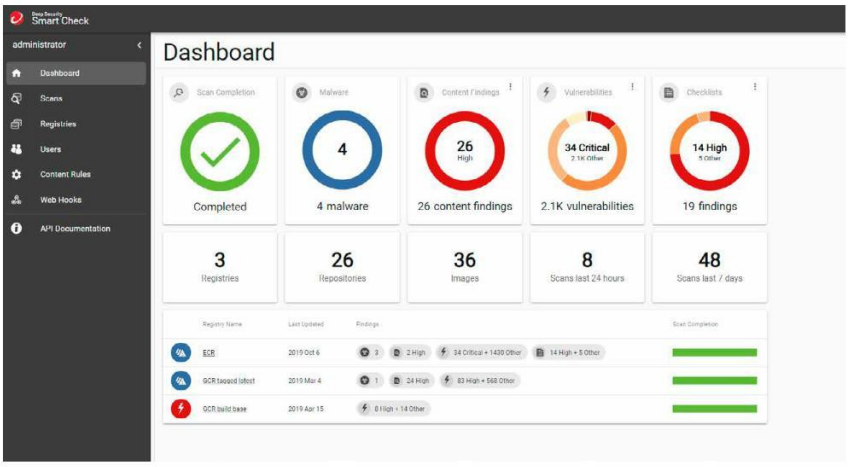
- Bảo vệ trước các phần mềm độc hại, lỗ hổng bảo mật và tài liệu mật với quét thời gian thực và điểm đăng ký của hình ảnh vùng chứa. Đảm bảo phát hiện mối đe dọa trước khi ứng dụng hoạt động.

Tối ưu hóa bảo mật cho DevOps

- Sớm triển khai bảo mật không va chạm trong CI/CD với việc bảo vệ như là mã code và bảo vệ tự động mà không làm chậm hoạt động của DecOps

Bảo vệ toàn chu kỳ của vùng chứa

- Trend Micro Cloud One™ – Workload Security đẩy mạnh Bảo vệ cho vùng chứa, mang đến biện pháp bảo vệ theo thời gian thực dẫn dầu, giúp vùng chứa của bạn được bảo vệ toàn chu kỳ



Liên tục tối ưu hóa chức năng quét cho DevOp

Container Security giúp đội ngũ DevOp áp dụng bảo mật không tiếp xúc với chức năng lập tức quét và liên tục quét các mối đe dọa, lỗ hổng bảo mật, tài liệu mật và vi phạm tuân thủ. Container Security cũng cung cấp độ hiển thị của bảng điều khiển, thông báo và nhật ký quét để hỗ trợ sự tuân thủ của thiết bị. Container Security được tối ưu hóa cho các nền tảng vùng chứa hàng đầu, nó có thể tích hợp vào chuỗi công cụ hiện có của bạn một cách dế dàng.

Quy trình tự động với API

Container Security cung cấp chức năng sản phẩm hoàn toàn tự động sử dụng danh mục API toàn diện, được cấu tạo với mục đích tích hợp vào quy trình CI/CD của bạn. Container Security cho phép kiến trúc sư và nhà phát triển ứng dụng đưa bảo mật dưới dạng mã code vào quy trình quét hình ảnh vùng chứa và điểm đăng ký của họ. Triển khai bảo mật sớm và hiệu quả trong quy trình cấu tạo phần mềm, giúp đạt được hiệu quả nhất quán nhanh hơn trong chu kỳ phát triển, cũng như giảm các bước bảo mật thủ công và thời gian ứng dụng phải ngừng hoạt động.

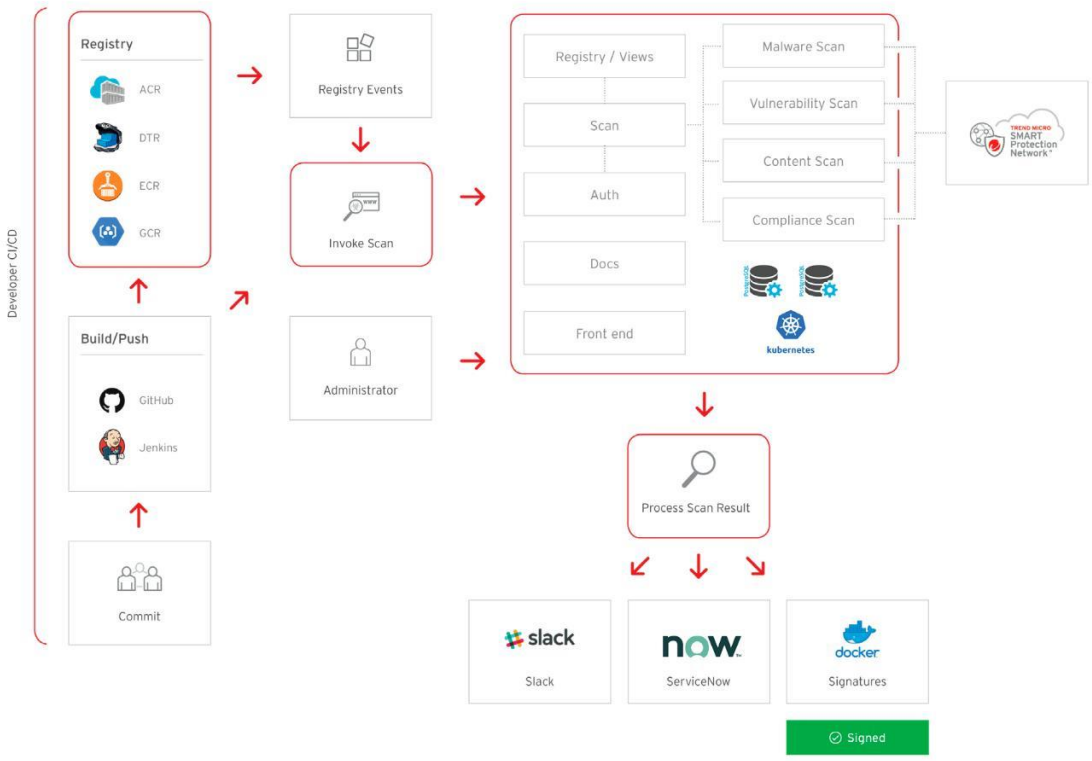
Bảo vệ thông minh

Container Security làm giảm sự gián đoạn khi nâng cấp và quy trình làm việc với khả năng nghiên cứu cũng như phát hiện mối đe dọa hàng đầu, bảo mật không xâm lấn cho quy trình CI/CD. Container Security loại bỏ sự phức tạp và lượng mối đe dọa bằng cách phát hiện lỗ hổng bảo mật, tài liệu mật và phần mềm độc hại zero-day sử dụng Trend Micro™ Smart Protection Network™.

Bảo mật sẵn sàng tuân thủ quy tắc

Container Security cho phép kỹ sư bảo mật đạt được yêu cầu tuân thủ mà không ảnh hưởng hiệu suất và can thiệp vào quy trình CI/CD. Không những vậy, nó còn cung cấp chức năng quét theo chính sách, với chính sách có thể tùy chỉnh để đạt yêu cầu tuân thủ và quản trị. Container Security cũng cung cấp nhật kí lịch sử chi tiết, giúp việc báo cáo và kiểm tra thuận tiện hơn.

Sơ đồ cấu tạo Container Security



NĂNG LỰC CỦA CONTAINER SECURITY

Quét hình ảnh nâng cao

Khi quét, Container Security sẽ mở từng lớp hình ảnh và thực hiện quét chi tiết trên từng nội dung. Đảm báo lỗi được sửa sớm và lọc ra kết quả giả bằng cách tương quan các lớp bản vá lỗi với các gói dễ bị tấn công trong cùng một hình ảnh. Container Security sẽ quét hình ảnh để tìm

- Phát hiện phần mềm độc hại
- Đánh giá lỗ hổng bảo mật
- Tài liệu mật như là mã khóa hoặc mật khẩu
- Độ tuân thủ chính sách
- Lỗ hổng mã nguồn bằng tính năng phát hiện của Snyk

Bảo vệ xuyên suốt

Chức năng quét của Container Security trở nên hữu dụng khi hình ảnh vừa được tạo và nó liên tục quét lượt đăng ký để tìm phần mềm độc hại cũng như lỗ hổng trong đó trước khi tiếp tục. Việc này đảm bảo cho hình ảnh của bạn được bảo vệ trước khi bắt đầu tạo và được bảo vệ khỏi các nguy hại trong tương lai. Ngoài ra, bạn có thể quét hình ảnh trong đa môi trường đám mây từ một lần chạy Container Security.

Quy trình bảo vệ tự động

Chức năng hoàn chỉnh của Container Security hiện có thông qua các API để hoàn toàn tích hợp tự động với quy trình CI/CD của bạn

- Thêm kênh đăng ký và nguồn chứa mục tiêu với các thẻ để quét
- Tự động bắt đầu quét lại hình ảnh để kiểm tra lỗ hổng bảo mật mới trước khi nhận bản cập nhật
- Thực hiện quét tại bất kì giai đoạn trong quy trình sửa dụng Container Security API
- Đảm bảo chỉ có hình ảnh an toàn được phép đi qua quy trinhg và chặn hình ảnh độc hại bằng quy trình xác nhận
- Lấy kết quả từ Container Security, thông qua Webhook, để phù hợp với luồng việc tự động cụ thể, Ví dụ, một dịch vụ ký trên hình ảnh Docker® có thể được phê duyệt và quảng bá dựa trên kết quả quét.

Nâng cao độ tuân thủ

Container Security cung cấp tính năng quét độ tuân thủ nâng cao, với chính sách có thể tùy chỉnh để đảm bảo đáp ứng yêu cầu nội bộ và bên ngoài của bạn. Nhật ký quét của Container Security hỗ trợ nhu cầu của doanh nghiệp và hoạt động audit với lịch sử cũng như kết quả quét chi tiết.

Quản lí bảng điều khiển và kiểm soát truy cập

Container Security cung cấp bảng điều khiển quản lí giao diện đồ họa cho người dùng (GUI) lớn, bao gồm cả quét bảng điều khiển phạm vi, kết quả quét và điều chỉnh mục tiêu quét (chế độ xem), cũng như quản lý người dùng và chế độ xem dành cho truy cập dựa kiểm soát vai trò của người dùng (RBAC).

- Nguồn nội dung: Hiển thị danh sách các điểm đăng ký đã được quét / giám sát
- Quét đang hoạt động: Hiển thị trạng thái mọi hoạt động quét
- Phạm vi bảo vệ: Hiển thị một phần trong tổng số hình ảnh của điểm đăng ký chỉ định đã được quét
- Cảnh báo: Hiển thị kết quả bao gồm phát hiện phần mềm độc hại, lỗ hổng và tài liệu mật.

Quét chi tiết hình ảnh

Container Security cung cấp cho DevOp chi tiết bảo mật và trả kết quả, cho phép phản hồi ngay lập tức với mọi vấn đề

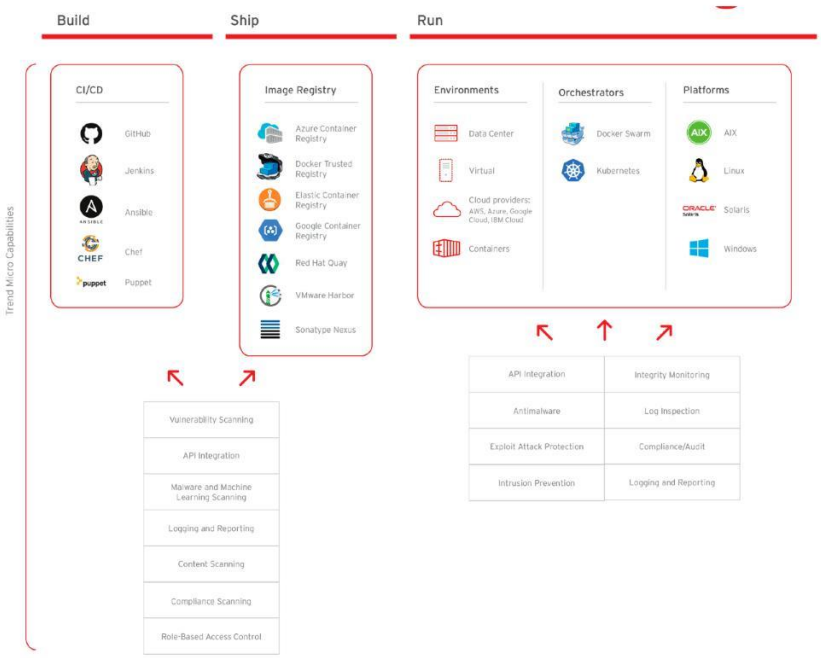
- Danh sách lớp hình ảnh đã quét
- Cảnh báo phần mềm độc hại, bao gồm tên và vị trí tập tin
- Truy vết nội dung, bao gồm tài liệu mật hoặc dấu hiệu xâm phạm (IOC)
- Chi tiết lỗ hổng, gồm có:
  - Số lượng lỗ hổng thường gặp và sự phơi nhiễm theo xếp hạng L/M/H CVSS
  - Thông tin về lớp và gói cho mỗi CVE
  - CVE và đường dẫn đến tập tin CVE
  - Phiên bản sửa/ vá lỗi

Nguồn thông tin mối đe dọa toàn cầu

Chức năng quét của Container Security được nhận nguồn thông tin mối đe dọa mới nhất từ cả nguồn riêng của Trend Micro và từ cộng đồng

- Chức năng phát hiện phần mềm độc hại được cung cấp bởi Trend Micro thông qua Trend Micro™ Smart Protection Network™
- Thuật toán trí tuệ nhân tạo để phát hiện mối nguy hiểm Zero-day

WORKLOAD SECURITY HỖ TRỢ SECURITY BẰNG CÁCH CUNG CẤP SỰ BẢO VỆ HÀNG ĐẦU CHO VÙNG CHỨA MÁY CHỦ CỦA HỆ THỐNG ĐIỀU HÀNH



Bảo vệ toàn bộ chu kỳ của vùng chứa

Bổ sung cho khả năng quét hình ảnh của Container Security, Workload Security cung cấp bảo mật nâng cao cho vùng chứa trong thời gian hoạt động, với chức năng đối phó phần mềm độc hại theo thời gian thực, che chắn vùng thiết yếu, kiểm tra lưu lượng vùng chứa, cùng như bảo vệ cho vùng chứ chính, các lớp Kubernetes® và hơn thế nữa.

Yêu cầu hệ thống:

- Kubernetes 1.8.7 trở lên
- Helm/Tiller 2.8.1 trở lên
- Docker 17.06 trở lên
- OpenShift 3.11.82

Đăng ký được hỗ trợ

Container Security hỗ trợ quét bất kỳ điểm đăng ký nào có API Docker V2 và cho phép liệt kê danh mục .

- Amazon Elastic Container Registry (ECR)
- Azure Container Registry (ACR)
- Docker Trusted Registry (DTR)
- Google Container Registry (GCR)
- VMware Harbor
- JFrog Artifactory
- Sonatype Nexus
- Red Hat Quay Container Registry

Để biết thêm thông tin vui lòng truy cập trendmicro.com/containersecurity

CẤU TẠO CỦA CONTAINER SECURITY

Cài đặt

Container Security được hỗ trợ trên nền tảng Kubernetes trong một cụm Kubernetes.

- Public: https://github.com/deep-security/smartcheck-helm

Người dùng Container Security được cấp quyền truy cập vào shell script và một bộ tài nguyên của Kubernetes trong Container Security GitHub® . Các hình ảnh trong ứng dụng hiện có tại Docker Hub.

CÁCH TRIỂN KHAI VÀ LÀM QUEN

Container Security cung cấp bước quan trọng trong quy trình CI/CD của bạn.

Hệ thống quét hình ảnh vùng chứa và điểm đăng ký bạn cần, chẳng hạn như Docker. Tất cả hoạt động của Container Security hiện có trên bộ tài liệu của API, đơn giản hóa cách để làm quen với hệ thống CI/CD của bạn. Ví dụ: API của nó có thể tự hoạt động bằng CI/CD của bạn để bắt đầu quét khi hình ảnh được đẩy sang đăng ký Docker riêng. Kết quả quét cũng hiển thị qua API.

API của Container Security bao gồm sơ sở webhook, cho phép thành phần CI/CD được đăng ký. Điều này cho phép bạn nhận thông tin về sự kiện quét, ví dụ như " quá trình quét đã hoàn thành", mạng lại khả năng tự động hóa luồng việc.

Container Security bao gồm bảng điều khiển quản trị viên và mang lại:

- Bảng điều khiển (tóm tắt thông tin quét, bao gồm cả số liệu, của toàn hệ thống)
- Bảng tóm tắt (bao gồm kết quả quét và số liệu)
- Quản lí người dùng
- Lượt đăng ký và hình trạng
- Nắm được kết quả quét
- Lịch sử quét.

THIẾT LẬP BẢO VỆ. GIAO HÀNG NHANH CHÓNG. HOẠT ĐỘNG MỌI NƠI.

Có mặt tại:

Kubernetes and Docker: Container Security chạy dưới dạng biểu đồ helm, thuận tiện cài đặt trong cụm Kubernetes, cung cấp thời gian cấu tạo nâng cao, cùng như quét hình ảnh điểm đăng ký tìm phần mềm độc hại, lỗ hổng, tài liệu mật và chính sách tuân thủ. Workload Security sẽ cung cấp thêm bảo vệ cho vùng chứa theo thời gian thực, cũng như giám sát thay đổi trong nền tảng, công cụ điều phối, tập tin và hoạt động của vùng chứa. Đảm bảo bảo vệ toàn diện xuyên suốt chu kỳ của vùng chứa.

Amazon Web Services (AWS): Container Security chạy dịch vụ Amazon Elastic Container Service cho Kubernetes (EKS) để quét hình ảnh vùng chứa, cùng với việc bổ sung Workload Security, bạn nhận được vùng chứa thời gian thực và bảo vệ luồng việc Amazon Machine Image (AMI) xuyên suốt môi trường AWS của bạn

---

Microsoft® Azure™: Container Security chạy quét hình ảnh vùng chứa, có thêm vùng chứa theo thời gian thực và bảo vệ máy ảo Azure (VM) thông qua Workload Security.

Google Cloud™: Chạy Container Security trên Google Kubernetes Engine (GKE) để quét hình ảnh quy trình cấu tạo, có thêm vùng chứa thời gian thực và sẵn sàng bảo vệ ngay lập tức VM thông qua Workload Security. Chạy Container Security trong GKE để cung cấp khả năng quét xuyên suốt nhiều môi trường đám mây.

Red Hat® OpenShift: Container Security có thể chạy trong môi trường OpenShift và bảo vệ ứng dụng của bạn với chức năng quét nâng cao trong quy trình cấu tạo phần mềm. Vùng chứa thời gian thực có thể được bảo vệ thông qua Container Security (trên máy chủ được hỗ trợ) để đảm bảo bảo mật toàn chu kỳ của vùng chứa.

VMware® Cloud™: Tích hợp mạnh mẽ của Workload Security trên khắp dịch vụ VMware® đảm bảo sự bảo vệ liên tục trên toàn bộ luồng việc ảo và dựa trên hệ thống đám mây của bạn, gồm cả vùng chứa, với nền tảng rộng và hỗ trợ hạt nhân, chính quản lí tự động và bảo mật dựa trên phần mềm giám sát máy ảo.

File Storage Security là một phần của Trend Micro Cloud One™, là nền tảng dịch vụ bảo mật dành cho tổ chức được xây dựng trên hệ thống đám mây, đồng thời cũng có:

- Trend Micro Cloud One – Workload Security: Bảo vệ thời gian thực cho luồng công việc (Ảo, vật lý, đám mây và vùng chứa)
- Trend Micro Cloud One – File Storage Security: Bảo vệ cho tệp tin trên đám mây và dịch vụ lưu trữ vật thể
- Trend Micro Cloud One – Application Security: Bảo vệ cho các chức năng, API và ứng dụng không máy chủ
- Trend Micro Cloud One – Network Security: Bảo vệ lớp IPS của hệ thống mạng đám mây.
- Trend Micro Cloud One – Conformity: Bảo vệ đám mây và quản lí độ tuân thủ.

*Bảo vệ vùng chứa của Trend Micro cung cấp tích hợp với Snyk và bao gồm cả Deep Security™ Smart Check™ – Container Image
Security and Trend Micro Cloud One™ - Container Security.

TREND MICRO™
Securing Your Connected World

[DS02_Cloud_One_Container_Security_200323US]