No.14
30th October 2018

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

Container Security the Red Hat Way

Red Hat – which looks set to be acquired by IBM – held a briefing on container security for IT security analysts last week. The following are the key take-aways:

- Red Hat has a substantial portfolio of security features for container environments. These are designed to protect both the application and the underlying infrastructure.
- Container security specialists Twistlock, Aqua Security and Sysdig are some of the ecosystem partners that add extra security to Red Hat container environments.
- Red Hat's security portfolio has a relatively low profile compared with competitors but the company now looks set to increase its communications around security.

Along with the likes of Google, Microsoft and VMware, Red Hat is among the leading software companies driving digital transformation. While it has been driving software innovation at a frenetic pace like competitors, Red Hat's security portfolio has had a comparatively low industry profile, especially with investors.

Red Hat appears to recognize this perception deficit now and is upping its communications on security accordingly. Last week the company hosted an analyst briefing on container security.

Red Hat delivers container security to enterprises via two main sources. The first is a baseline set of approaches to company-wide secure software development and security features that span its entire portfolio. The second is OpenShift, Red Hat's Kubernetes-based orchestration platform for developing, deploying and managing containers across multiple clouds.

OpenShift supports some nice features for accessing and managing external images securely.

Control of application security and defence of infrastructure

Red Hat presents its container security features in terms of what they do to enable control of application security; defence of infrastructure; and additional capabilities from security software partners that specialize in securing container environments.

Red Hat enhances an enterprise customer's security posture around application security in several ways. At a fundamental level, the adoption of containers tends to drive convergence of development and operations toward a DevOps model. That same discontinuity also creates an opportunity to integrate security and move straight to a DevSecOps model. Certainly not all organizations have the capability or security maturity to do that. But those that do give their security team the opportunity to write security as code rather than having to retro-fit it.

OpenShift integrates with multiple external registries and supports an integrated registry for management of both external and custom-built images. It supports some nice features for accessing and managing the external content securely:

- **External software repositories can be black-listed or white-listed**. This can be tailored to the unique security profile of separate development and production clusters within the organization.
- **A key Red Hat feature called ImageStream Events** helps monitor changes to external images that are stored in the repository. This monitoring allows customers to update images whenever security vulnerabilities are discovered.

- **The Red Hat Container Catalogue** gives teams access to a variety of Red Hat-produced container images as well as OpenShift-certified 3rd party ISV images. Images are assigned a security score. If that score changes as a result of a vulnerability being discovered, customers are notified, the score is updated in real-time, and a new image is made available.

With the acquisition of CoreOS, Red Hat is able to offer an enterprise container registry called Red Hat Quay which has an integrated vulnerability scanner. This gives visibility of vulnerabilities at the level of a single container image as well as each individual package within the image. Red Hat cites Cisco as a big customer for both OpenShift and Quay, citing a statistic that Cisco has 12 Terrabytes of container images on Quay.

OpenShift also helps organizations navigate the new security patching model that comes with adopting containers. With a container image being built in layers, responsibility for security patching of different layers can be distributed across different security, development or operations teams according to each enterprise's unique requirements.

Central to runtime security policies in an OpenShift environment are what Red Hat calls Security Context Constraints or SCCs.

Common Criteria certification with Linux Container Framework Support

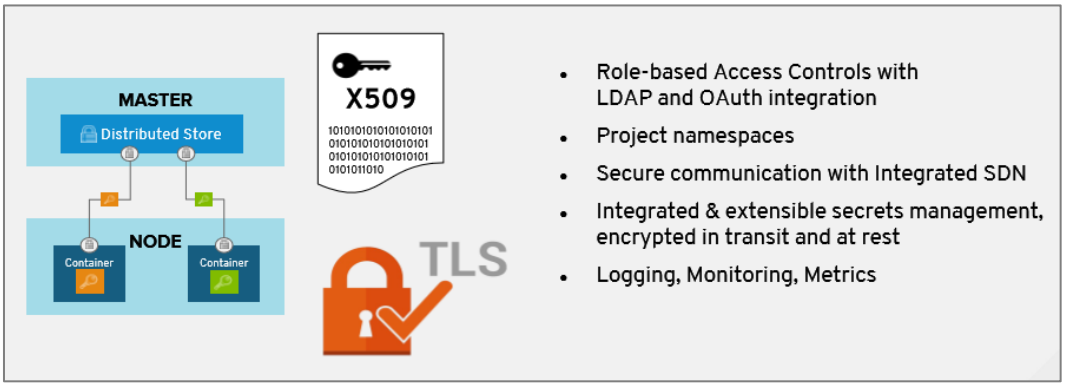
Red Hat draws most on its Linux heritage as a security differentiator for protecting the infrastructure when containers are deployed. As announced just under a year ago, Red Hat Enterprise Linux was the first OS to be Common Criteria-certified with Linux Container Framework Support.

Red Hat is able to secure the infrastructure as containers are deployed without requiring a high level of Linux-related expertise on the part of the OpenShift administrator. Red Hat Enterprise Linux (RHEL) effectively does the management of multi-tenancy to ensure that containers are appropriately isolated from one another. OpenShift works with Security Enhanced Linux (SE Linux) – a module that supports access control policies – on by default.

Central to runtime security policies in an OpenShift environment are what Red Hat calls Security Context Constraints (SCC). For example, one SCC mandates that no container can ever run in the compute space as privileged. Whilst they're set as a default, administrators can override them if they choose to by using a privileged or custom SCC.

Securing the Kubernetes orchestration tool itself within OpenShift is also important. As shown in **Figure 1,** Role Based Access Controls (RBAC) are built in to the OpenShift Master. This can be integrated with any from eight different Identity and Access Management (IAM) providers. Multi-tenancy to prevent teams from accessing one another's environments without authorization is provided by Project namespaces as well as the integrated OpenShift SDN.

Figure 1: Securing the Container Platform



Source: Red Hat

OpenShift SDN provides a unified cluster network that enables communication between containers across the OpenShift cluster. Multi-tenancy within that environment allows for project network level isolation. Granular, policy-based, isolation can also be provided with network policies – for example determining which pods can and can't talk to each other, on which specific ports, and in which specific direction. All access to the OpenShift Master is over TLS. Access to the API server is via X.509 certificates. Logging and audit capabilities are also built in. Integrated secrets management is provided and encrypted in transit as well as at rest.

Twistlock deploys on OpenShift to provide automated, whitelist-based defence against threats.

OpenShift provides plug-ins for a variety of different storage types for customers that need it to manage state. Here security is provided by SE Linux access controls, secure mounts and supplemental group IDs for shared storage. Lastly, Red Hat customers can secure the external APIs that provide access to their applications. In addition to ingress and egress controls that are built into OpenShift, Red Hat also offers its 3Scale API management solution which supports a number of security features.

Red Hat also draws on an ecosystem of specialist container security partners

No IT security company can deliver best in class security through its own efforts alone. Red Hat recognizes that. To that end, the OpenShift ecosystem of security partners covers areas such as vulnerability scanning, privileged access management, vaults, and networking. The company currently has partnerships in place with container security specialists, such as Twistlock, Aqua Security and Sysdig.

As an example, Twistlock deploys on OpenShift to provide automated, whitelist-based defence against threats as well as microservices-aware L3 and L7 firewalls. Twistlock also enables administrators to scan images stored in OpenShift Container Registry (OCR) or Quay for vulnerabilities or compliance violations. Also security partners like Black Duck by Synopsys have integrated with Image Stream Events ■

- HardenStance received no payment – direct or "in kind" – for publishing this Briefing.

- **Contact HardenStance's Principal Analyst:** patrick.donegan@hardenstance.com

- HardenStance received no payment – direct or "in kind" – for publishing this Briefing.

HardenStance Ltd Disclaimer of Warranty and Liability