SECURITYWEEK NETWORK:

- Information Security News
- Infosec Island
- Suits and Spooks

Security Experts:

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe (Free)
- Security White Papers
- ICS Cyber Security Conference
- Contact Us

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - White Papers
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
  - Whitepapers
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance
  - Risk Management
  - Compliance
  - Privacy
  - Whitepapers
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - White Papers
  - Network Security
  - Application Security
- Management & Strategy

Docker Boosts Security for Containerized Applications

By SecurityWeek News on November 17, 2015

Docker, makers of container technology that enables speedy deployment of applications, has unveiled new security enhancements to extend the protection of "Dockerized" distributed applications.

Docker is an open platform that allows developers and system administrators to build and run distributed applications that run the same, regardless of the environment they are running in.

Similar to virtual machines, containers benefit from resource isolation and allocation, but do not rely on an OS kernel, making them faster and more portable than virtual machines.

Included in the latest security protections unveiled by Docker are hardware signing of container images, content auditing through image scanning and vulnerability detection and granular access control policies with user namespaces.

Hardware signing and scanning of container images directly address the trust and integrity of application content, Docker said, as the new features verify the publisher of the content. Furthermore, the chain of trust is protected and containerized content is verified via image scanning.

"It has been our goal from the beginning to develop a framework that secures Dockerized distributed applications throughout the entire application lifecycle," said Solomon Hykes, CTO and Chief Architect of Docker. "With this latest set of capabilities, we continue to drive our users and ecosystem forward with industry-first innovations and best practices that advance the end-to-end security of distributed applications. Furthermore, we've enabled developers and IT ops to benefit from a more secure environment, without having to learn a new set of commands or to be trained on a deep set of security principles. Docker security works as part of an integrated component without any disruption to developer productivity while providing IT with the appropriate level of security controls."

The new security enhancement builds on Docker Content Trust, a framework that allows verification of the image publisher. Prior to Docker Content Trust, IT operations had no way to validate content, the company said. Docker Content Trust verifies the publisher and ensures the integrity of the content.

Docker Content Trust's hardware signing is done under a partnership with Yubico to roll out a "touch-to-sign" code signing system that leverages YubiKeys (hardware key), which enable secure software creation for Docker developers, sysadmin and third-party ISVs. With the YubiKey 4, Docker users can digitally sign code during initial development and through subsequent updates to ensure the integrity of the Dockerized application throughout the application pipeline, Docker said.

"This is an important milestone for Yubico and our community as we move beyond authentication to address another area in which the YubiKey shines, using our hardware to perform cryptographic sign operations," said Jerrod Chong, VP, Solutions Engineering, Yubico. "Having root keys stored in the secure element of the YubiKey means attackers cannot duplicate the keys and forge sign

operations; insecure storage of keys in software modules is often the root cause for many of the vulnerabilities found in software packages."

YubiKey 4 works on Microsoft Windows, Mac OS X, Linux operating systems and major Web browsers.

Docker also announced a new secure service for its Official Repos that provides direct visibility into the content security of ISV software that is part of this set of images.

Docker image scanning and vulnerability detection provides container-optimized capability for granular auditing of images, presenting the results to ISVs and sharing the final output for Docker users to make decisions on which content to use based on their security policies.

If the scanning service detects an issue, ISVs can fix vulnerabilities and upgrade the security profile of their content. Because Official Repos is also integrated with Docker Content Trust, users are able to establish the validity of the publisher as well as the integrity of the image content. The end result is that IT organizations can rely on Official Repos as a curated source for secure, high-integrity content.

“This new capability addresses IT operations concerns about getting information regarding what’s inside the container,” Docker explained. “Users for the first time are presented with automated insights that give them the instant visibility they need to determine if they want to use that image or not.”

Introduced as part of the 1.9 Experimental release, user namespaces gives users the ability to separate container and Docker daemon-level privileges to assign privileges for each container by user group. With the new levels of control, containers themselves don’t have access to root on the host - only the Docker daemon does. The new functionality also gives IT teams the ability lock down hosts to a restricted group of sysadmins.

Docker says its technology is used by millions of developers across thousands of organizations, including eBay, Baidu, the BBC, Goldman Sachs, Groupon, ING, Yelp, and Spotify.

While container adoption is likely to surge over the next few years, concerns around security, certification and adequate skills remain, according to the results of a survey released earlier this year by Red Hat.

Related Reading: Disrupting the Disruptor: Security of Docker Containers

Related Reading: IT Teams Question Security of App Containers: Survey

Previous Columns by SecurityWeek News:
Docker Boosts Security for Containerized Applications
Researcher Hijacks Android Phone via Chrome Vulnerability
Radiflow Launches New Intrusion Detection System for ICS/SCADA Networks
Majority of Top Android Apps Easily Reverse Engineered: Report
Most Enterprises Prone to Privileged Account Hacks: Report

Tags:
NEWS & INDUSTRY Cloud Security

Subscribe to SecurityWeek

Most Recent Most Read

- Attacks Revive Debate on Encryption, Surveillance
- Docker Boosts Security for Containerized Applications
- Changing the Economics of Cybersecurity
- State-Sponsored Attackers Use Web Analytics for Reconnaissance
- Anonymous Hackers Declare War on IS: Video
- Libpng Library Updated to Patch Vulnerabilities
- Thousands of Sites Infected With Linux Encryption Ransomware
- Conficker Worm Shipped With Police Body Cameras
- Gmail to Warn When Messages Take Unencrypted Routes
- Researcher Hijacks Android Phone via Chrome Vulnerability

Popular Topics

- Information Security News
- IT Security News
- Risk Management
- Cybercrime
- Cloud Security
- Application Security
- Smart Device Security

Security Community

- IT Security Newsletters
- IT Security White Papers
- Suits and Spooks
- ICS Cyber Security Conference
- CISO Forum
- InfosecIsland.Com

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group
- Cyber Weapon Discussion Group
- RSS Feed
- Submit Tip
- Security Intelligence Group

About SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us