**No.2**
*5th February 2018*

HardenStance Briefing

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

# Container Security: A Twistlock Update

During CyberTech 2018 in Tel Aviv last week, HardenStance met with Dima Stopel, one of the co-founders of Twistlock, and learnt the following:

- Runtime protection is the biggest security concern that Twistlock's customers have.
- Twistlock is pushing new firewalls for the container environment.

Last September, Twistlock (John Morello) and Scarfone Cybersecurity (Karen Scarfone) were credited as the two companies that co-authored the new NIST Application Container Security Guide. This can be downloaded via the link at the foot of this page.

- Twistlock reports its customers following the market's rapid acceleration away from Docker to Kubernetes for deploying and managing containers. Fully 80% of its customers are now using Kubernetes, with only 20% now using Swarm or Docker.

*Runtime protection is currently the biggest security concern that Twistlock's customes have.*

- The company has a handful of customers that have more than 50,000 hosts running containers.
- As of now, the number one security concern among Twistlock's customers is runtime protection. Vulnerability management, which was the main worry eighteen months ago, is now the second biggest concern. The third biggest issue is compliance (hence the NIST guidelines).
- Twistlock is pushing its own firewalls for the container environment that can determine that a given cluster can communicate with this other cluster but not that one. The capabilities have been internally developed leveraging some open source components and external threat feeds.
- The first firewall variant is a Cloud Native Network Firewall (CNNF), an automated TCP-level solution that automatically learns which clusters should talk to each other and blocks unauthorized associations.
- The second is a Cloud Native Application Firewall (CNAF). This is a form of Web Application Firewall (WAF) for the container environment to spot threats. It relies initially on manual provisioning.
- As well as providing container security, the company has been turning the roadmap of its core platform to securing serverless computing environments as well as containers. This is to ensure that serverless functions are not exposing critical resources to exploitation. By scanning functions during the build process, Twistlock is creating a feedback loop to developers. By continuously monitoring the existing serverless functions it is looking to protect against new and emerging threats to serverless computing.
- A couple of U.S telecom operators that are already deploying containers are Twistlock customers. Telcos don't rank among Twistlock's largest customers, though. They don't feature among those that have 50.000 hosts running containers.

The NIST Application Security Guide, September 2017 (SP 800-190)

To automatically receive notifications of new HardenStance content register here

***HardenStance received no payment – direct or "in kind" – for publishing this briefing.***

## HardenStance Ltd Disclaimer of Warranty and Liability

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.