RESEARCH

Tripwire State of Container Security Report

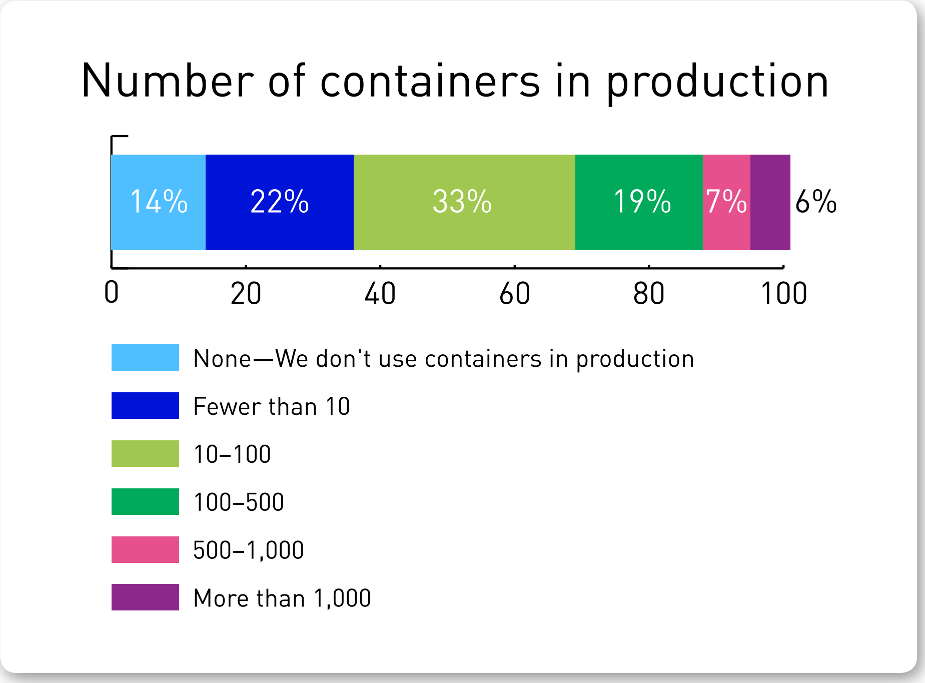
January 2019

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

As DevOps continues to drive increased use of containers, security teams are struggling to secure these new assets and processes. This report explores the challenges that organizations actively using containers today are facing, as well as the real consequences they have experienced.

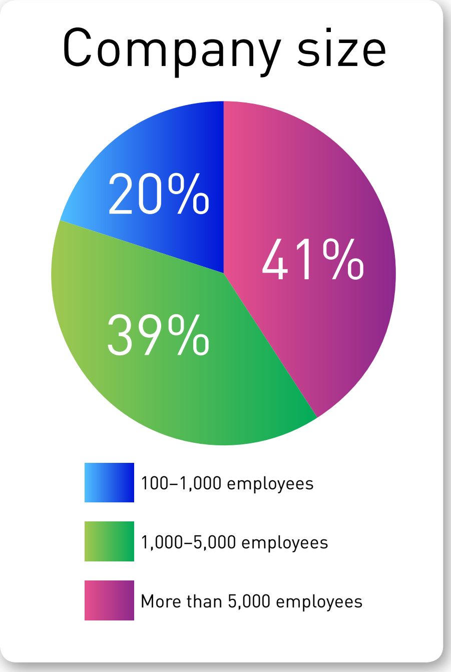
Highlights include:

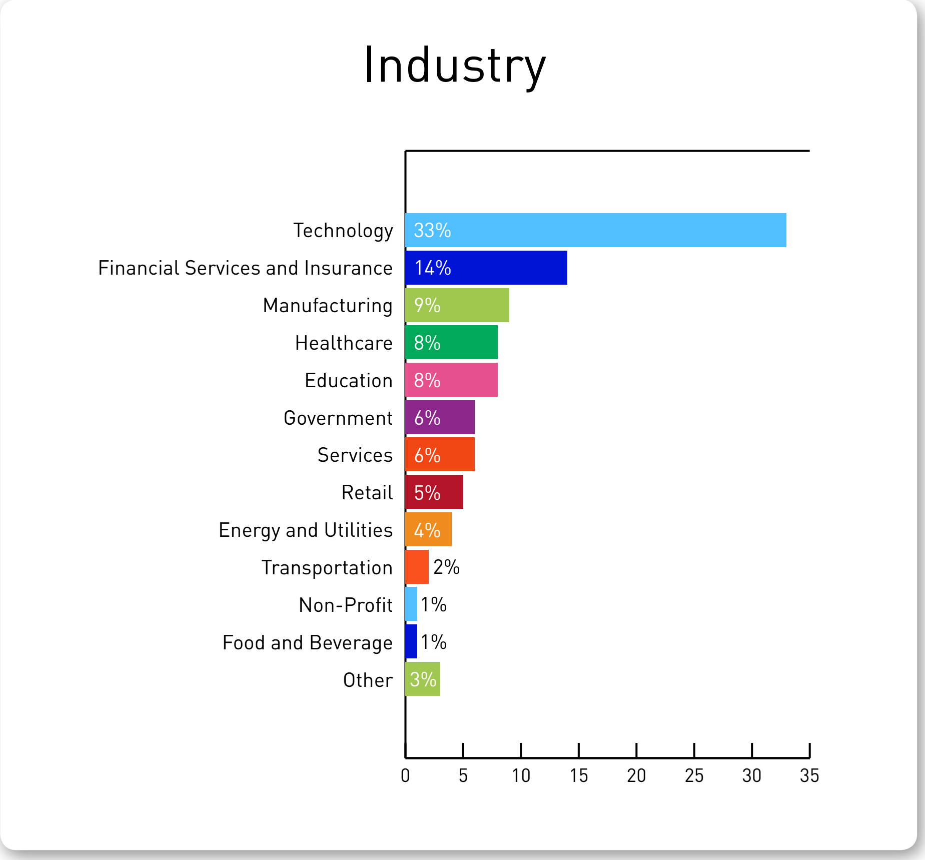
- 94% are concerned about container security
- 60% have had container security incidents in the past year
- 47% have vulnerable containers in production and 46% don't know if they do


Number of containers in production

Demographics

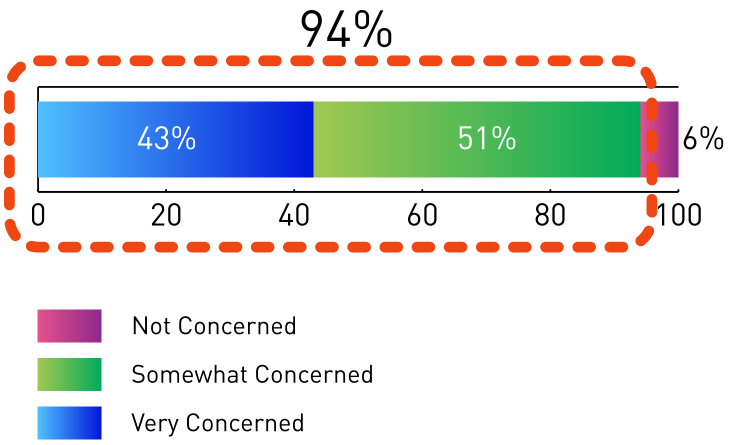
Survey respondents included 311 IT security professionals who manage environments with containers at companies with over 100 employees. Eight-six percent (269) had containers inproduction.


Company size


Industry

94% are concerned about container security

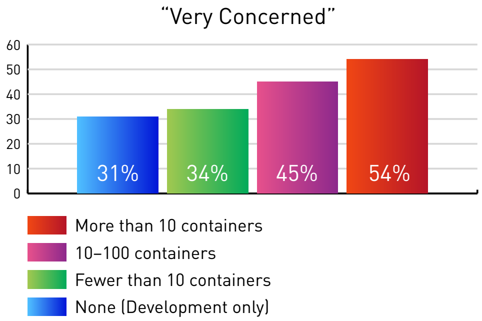
How concerned are you about security in container environments?



The concern increases with the number of containers in production, and is higher among those with more container security expertise.

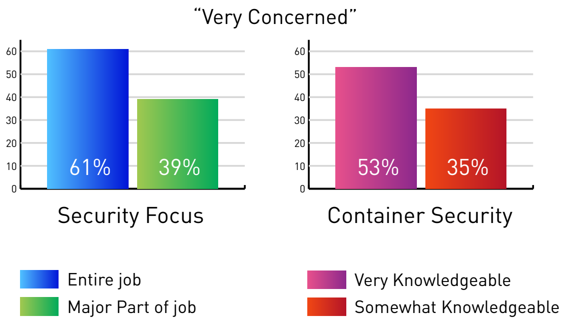
By # of containers in production

How concerned are you about security in container environments?



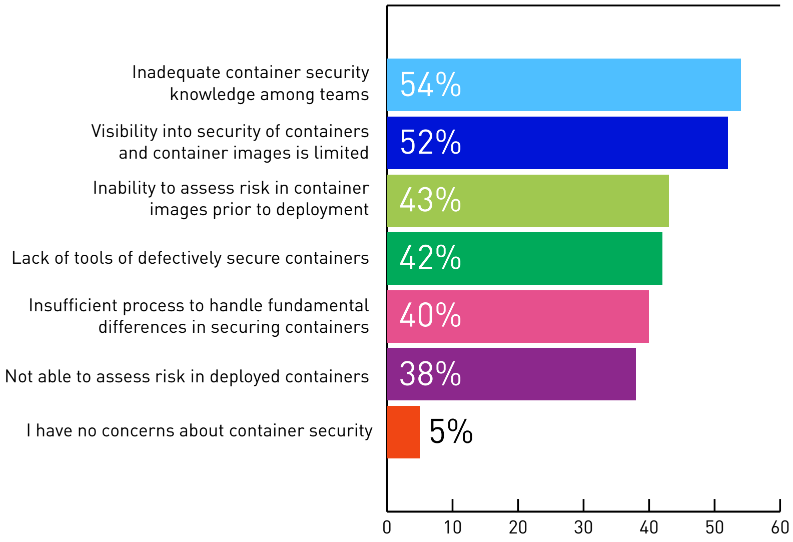
By security focus and knowledge of containers

How concerned are you about security in container environments?



Top concerns about container security

What specific security concerns do you have about containers?

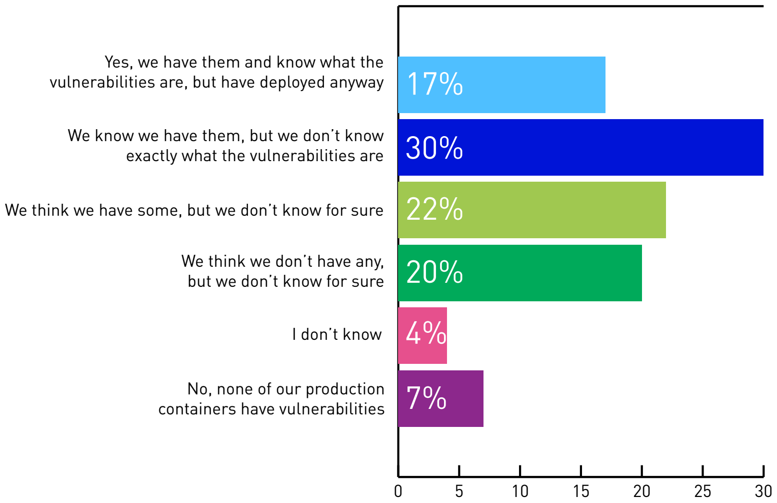


Organizations are accepting risk and facing consequences

Of the 269 respondents with containers in production:

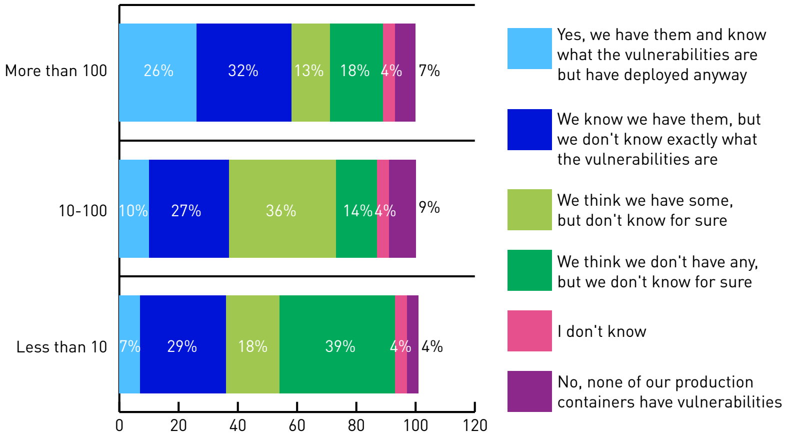
47% have vulnerable containers in production and 46% don't know if they do

Do you currently have vulnerable containers deployed in production at this time?



Those with the most containers in production have ignored security issues

Do you currently have vulnerable containers deployed in production at this time?
By # of containers in production



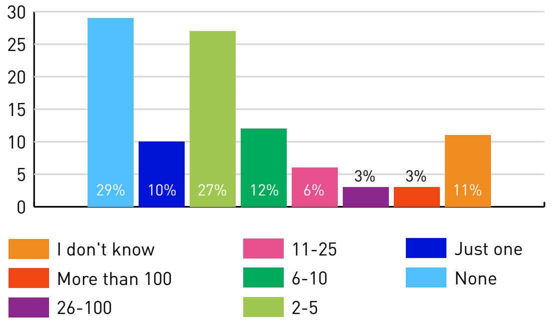
Those with the most containers in production were more likely to acknowledge that some of those containers are vulnerable.

“With the increased growth and adoption of containers, security practitioners are feeling the pressure to speed their deployment. To keep up with the demand, teams are accepting unnecessary risks by not securing containers.”

—**Tim Erlin**, Vice President of Product Management and Strategy at Tripwire

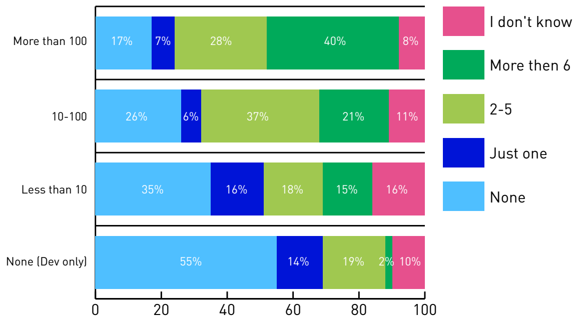
60% have had container security incidents in the past year

Approximately how many security incidents have occurred in your container infrastructure in the past 12 months?



The more containers deployed, the more likely there had been a container security incident.

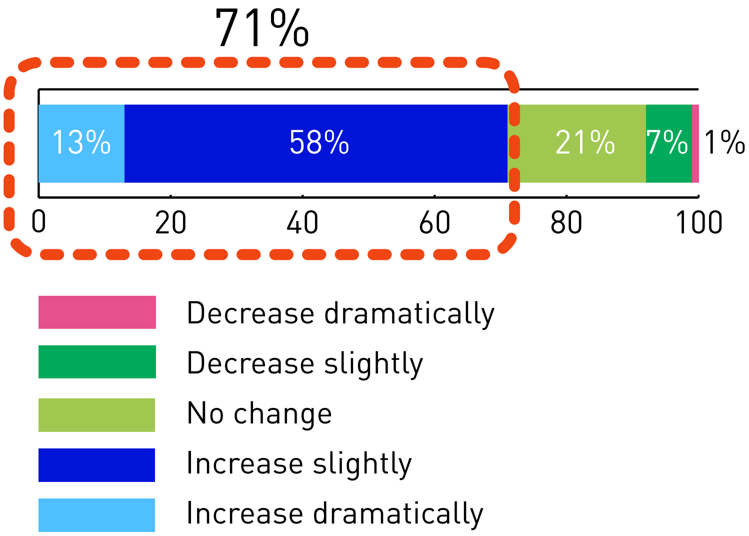
Approximately how many security incidents have occurred in your container infrastructure in the past 12 months?
(By # of containers in production)



Organizations are bracing for a rise in container-related security incidents.

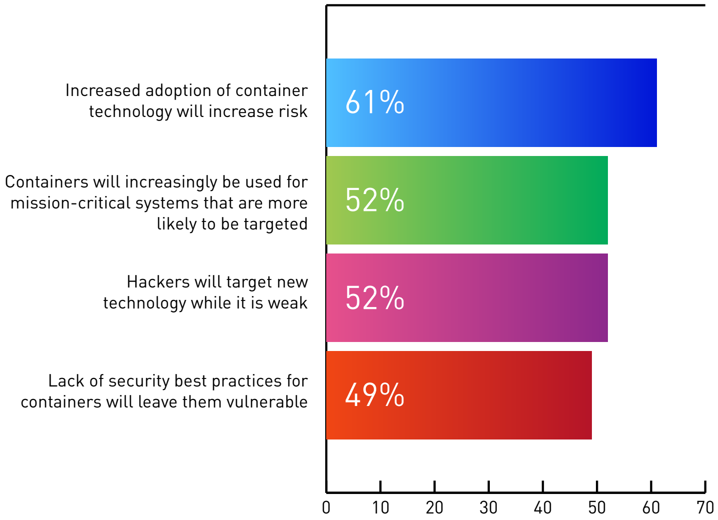
Most expect rate of security-related security incidents to increase in the coming year

How do you expect the rate of container-related security incidents to change in the coming year?



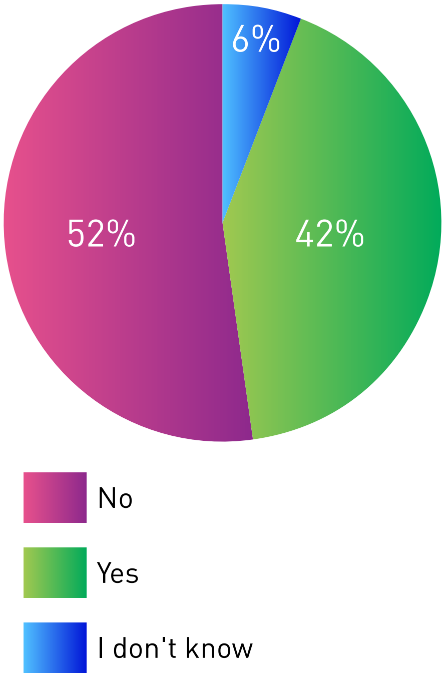
Top reasons for increased security incidents

n = expect security incidents to increase



42% are limiting container adoption because of security risks

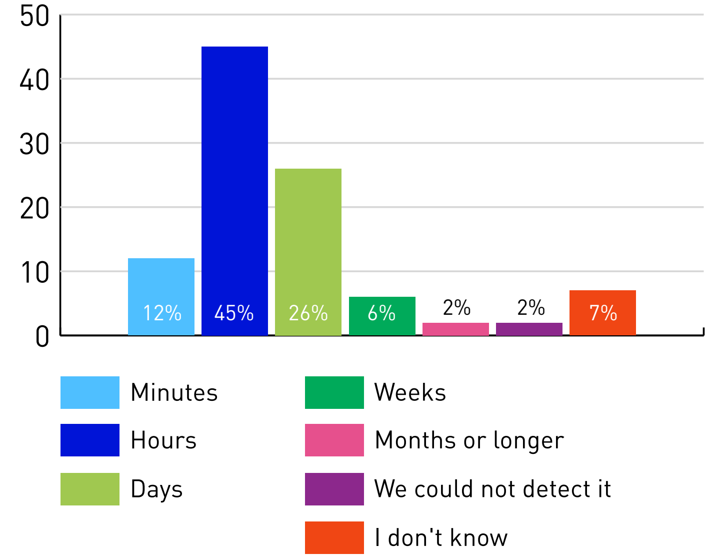
Has your company delayed or limited container adoption because of security concerns?



> "There's a belief that you have to accept a significant amount of risk to take advantage of containers, but that's not true. Security can and should be embedded into the DevOps life cycle, incorporating vulnerability and configuration assessment of container infrastructure to monitor risks from build to production."
> —**Tim Erlin**

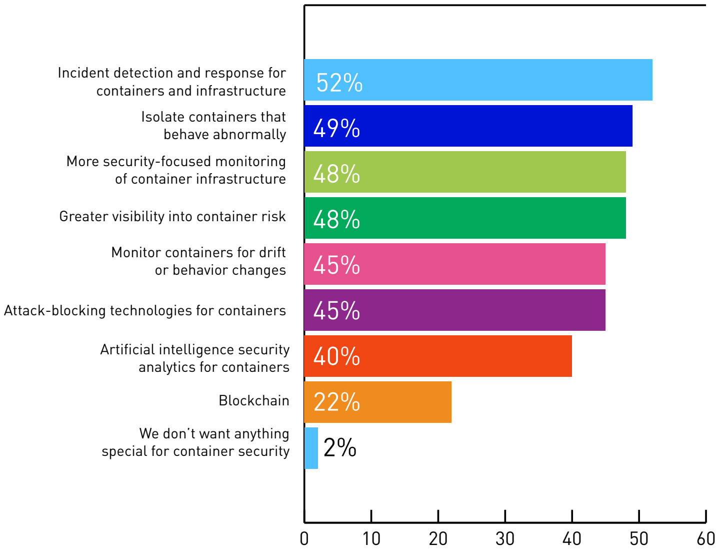
Only a few believe they could detect a compromised container within minutes

Approximately how long would it take to detect a compromised container or container image?



98% want additional security capabilities for container environments

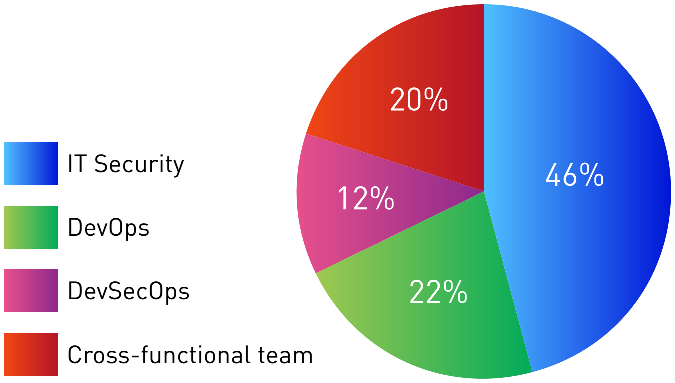
What additional security management tools or capabilities would your organization want for container environments?



Who’s in charge?

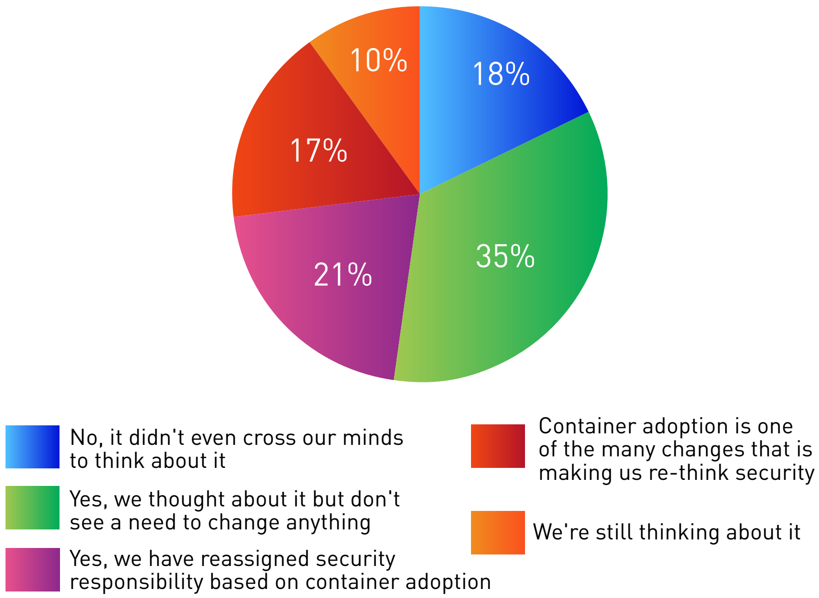
IT security is most likely team to have primary responsibility for container security

What organization owns primary responsibility for container security?



Because of containers, 82% are rethinking security responsibilities—with varying results

Has container adoption caused your organization to think about restructuring security responsibilities?



Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at tripwire.com**

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » Watch us at youtube.com/TripwireInc