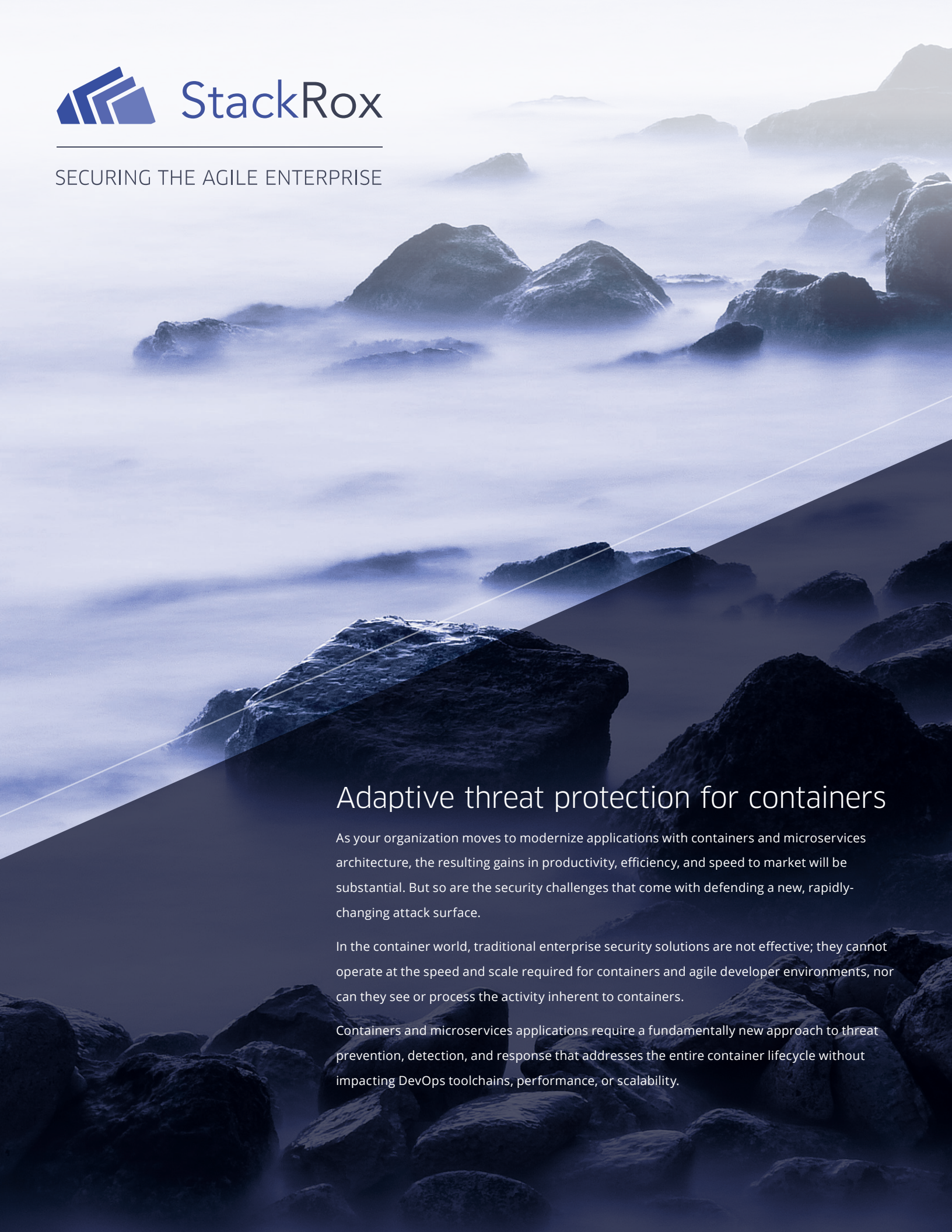


StackRox

SECURING THE AGILE ENTERPRISE

Adaptive threat protection for containers

As your organization moves to modernize applications with containers and microservices architecture, the resulting gains in productivity, efficiency, and speed to market will be substantial. But so are the security challenges that come with defending a new, rapidly-changing attack surface.

In the container world, traditional enterprise security solutions are not effective; they cannot operate at the speed and scale required for containers and agile developer environments, nor can they see or process the activity inherent to containers.

Containers and microservices applications require a fundamentally new approach to threat prevention, detection, and response that addresses the entire container lifecycle without impacting DevOps toolchains, performance, or scalability.

Introducing the industry's only container security platform with adaptive threat protection

With StackRox, you're not just solving one aspect of your container security problem, you're building a comprehensive security foundation that addresses the whole container lifecycle.

SEE YOUR CONTAINERS IN HIGH-RESOLUTION

Automatically discover all containers and organize them by their microservices

Establish full operational visibility and auditability

ADAPT YOUR DEFENSES AGAINST EVOLVING THREATS

Configure and apply sophisticated machine learning to your environment in two clicks

Auto-tune threat prevention, detection, and response at container speed

UNIFY CYBERSECURITY FOR CONTAINER ENVIRONMENTS

Benefit from IDS/IPS, WAF, and EDR capabilities within a single platform

Reduce cost, complexity, and manual effort

"We have not found another security solution – legacy or new – that offers adaptive threat protection for containers. StackRox has already unified a handful of major product areas into a single security engine, so moving to containers means positive ROI."

—Gene Yoo
SVP & Head of InfoSec

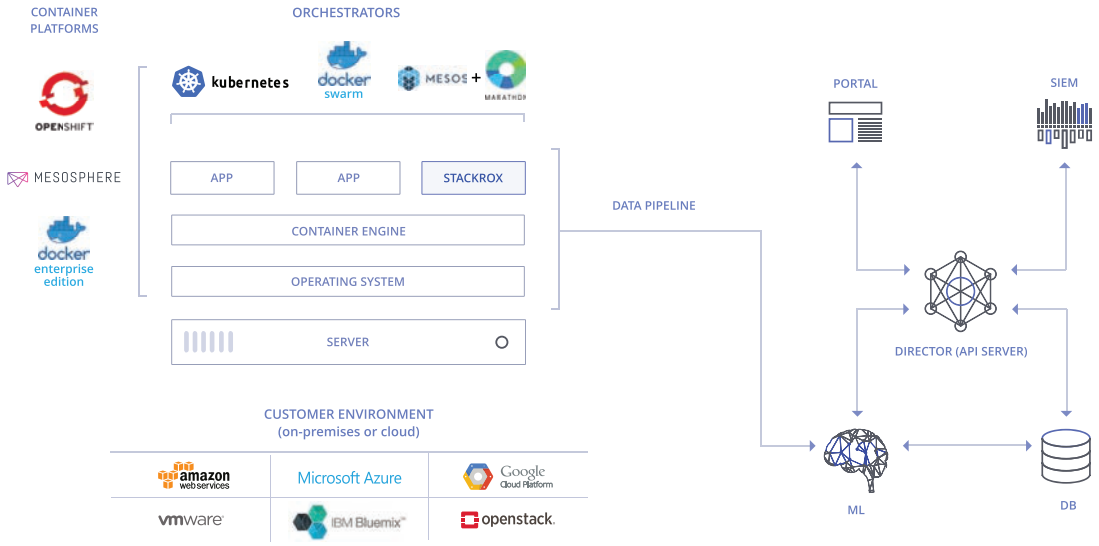
CITY NATIONAL BANK

Global enterprises across finance, media, technology, and government are using StackRox to discover assets, protect cloud workloads, and hunt threats across their environments.

The StackRox approach: instrumentation, insight, action.

Built-in security architecture

StackRox combines a new, highly scalable security architecture with deep instrumentation and machine learning to protect containers from evolving threats. StackRox deploys across cloud, virtual, and bare metal environments as a set of container-based security microservices that collects signals, performs machine learning, and automates prevention and response. It works as a single integrated platform that scales automatically and interfaces seamlessly with container platforms and your existing security infrastructure.



High-resolution visibility

Robust security begins with complete visibility. StackRox's unique instrumentation captures millions of signals to enable deep insights into container activity with dramatically less noise.

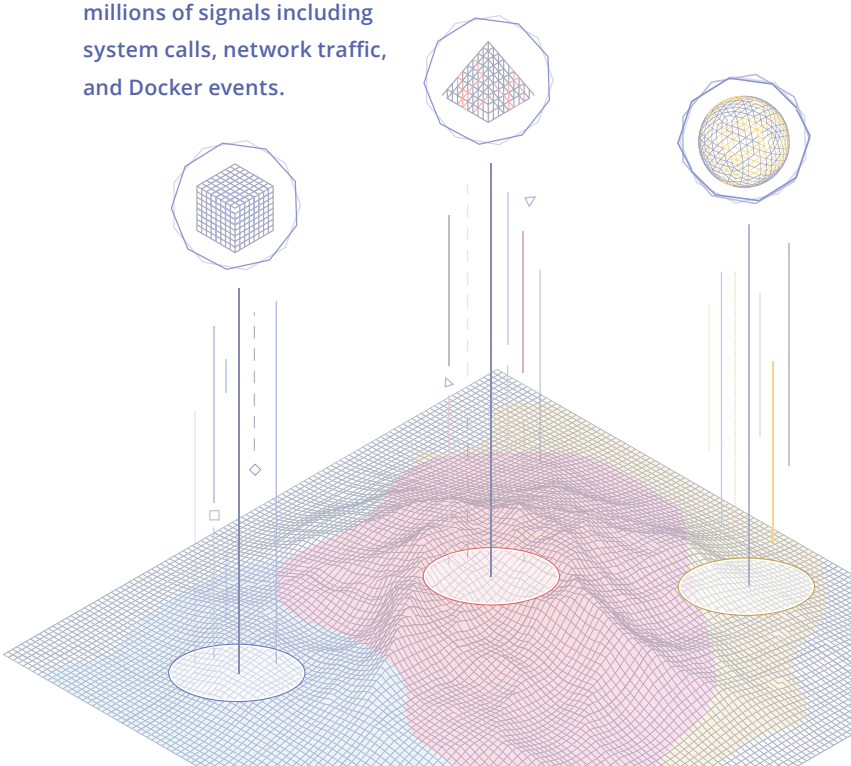
CONTAINER AUTO-DISCOVERY WITH FINGERPRINTING

StackRox auto-discovers every container across your environment. Patent-pending microservice fingerprinting technology enables rapid, reliable identification of both known and rogue containers, giving you a concisely organized view of your applications.

ADVANCED NETWORK VISUALIZATIONS

StackRox renders interactive, detailed visualizations of your container network in real time, giving you a clear depiction of connections between containers, microservices, and applications.

StackRox continuously monitors millions of signals including system calls, network traffic, and Docker events.



Adaptive defenses

StackRox's adaptive threat protection is the result of multiple machine learning (ML) models working in parallel to continuously protect containers from threats such as code injection, privilege escalation, malicious lateral movement, and data exfiltration.

TWO-CLICK BEHAVIOR MODELING

With just two clicks, you can train StackRox's powerful machine learning models to generate a complete behavioral context of your applications.

ADVANCED EVENT CORRELATION

StackRox correlates indicators of compromise and security events across your entire environment, swiftly alerting you to attacks and policy violations.

AUTO-TUNING MACHINE LEARNING MODELS

StackRox's ML models dynamically auto-tune based on application and environment changes. This in turn enables a high-fidelity understanding of application behaviors.

IMAGE VULNERABILITY SCANNING

Conveniently scan container images for known vulnerabilities.

SMART FILTERS

StackRox puts hundreds of preconfigured data filters at your fingertips. Quickly zero in on the event data that's most meaningful, or use them to create your own filters.

ATTACK PROFILE LIBRARY

StackRox provides a library of attack types and techniques based on patterns of anomalous or malicious behaviors across a variety of threat vectors.

POLICY-DRIVEN PREVENTION AND RESPONSE

Automatically prevent and respond to threats according to your policies. Actions include blocking unauthorized Docker commands, blocking system calls, and quarantining, isolating, or instantly pausing compromised or rogue containers.

Simple deployment, management, and integration

StackRox's intuitive web-based interface puts interactive visualizations, actionable dashboards and reports, and powerful search features at your fingertips. Focus security operators on the information most relevant to them via role-based and application-based access controls. Through fully-developed native integrations and APIs, StackRox is built for production environments and interfaces with the following platforms and tools:

Container engine	Docker
Container orchestration	Docker Swarm, Kubernetes, Mesos/Marathon
Container platforms	Amazon EC2 Container Service (ECS), Azure Container Service (ACS), Docker Enterprise Edition, Google Container Engine (GKE), IBM Bluemix Container Service, Mesosphere DC/OS, Red Hat OpenShift
Operating systems	CentOS, Debian, Red Hat Enterprise Linux (RHEL), Ubuntu
Infrastructure	Amazon Web Services (AWS), Google Cloud Platform (GCP), IBM Bluemix, Microsoft Azure, OpenStack, virtual machines (KVM, Xen, VMware, Hyper-V), bare metal
Image delivery	Amazon EC2 Container Registry (ECR), Artifactory, Azure Container Registry (ACR), Docker Hub, Docker Trusted Registry (DTR), Google Container Registry (GCR)
Identity management	SAML 2.0-compliant identity providers including Google, Okta, Ping Identity
Incident alerting	PagerDuty, Slack

Let's get started

Request a demo to see how StackRox can secure your container environments.

sales@stackrox.com | +1 (650) 489-6769 | www.stackrox.com | 700 E. El Camino Real, Suite 200, Mountain View, CA 94040