aws modern apps

SentinelOne®

Modern cybersecurity for modern enterprises

Secure your containerized apps with SentinelOne and AWS

Contents

Driving business value through cloud and containers

Digital transformation is more than a buzzword. It's the process of evolving from rigid, legacy on-premises platforms to a modern, cloud-first IT environment equipped to rapidly adjust to changing business and customer needs. At the core, it's about driving business value throughout your organization.

For example, on average, migrating to the cloud with Amazon Web Services (AWS) delivers

- 69% reduction in unplanned downtime
- 43% fewer security incidents per year

While those benefits have real bottom-line impact, coupling cloud migration with application modernization (rehosting, refactoring, rearchitecting, and rebuilding your applications to take full advantage of the cloud) offers even more:

- **Elasticity:** the ability to respond to spikes in customer demand
- **Availability:** the ability to serve customer requests wherever and whenever
- **Agility:** the ability to quickly fix a problem or deploy a new functionality that customers want

But how do you modernize your applications as easily and efficiently as possible? How do you minimize business disruption and maximize return on investment?

For many companies, the answer is containers. According to the 2020 Cloud Native Computing Foundation Survey, the use of containers in production has increased by 300 percent since 2016. Gartner predicts that by 2022, more than 75 percent of global organizations will be running containerized apps.

Why containers? Containers are more than a packaging mechanism; they enable flexibility and scale that simply isn't possible with monolithic applications. While containers address several critical concerns of application developers, including the need for faster delivery, portability, modernization, and lifecycle management, they also empower organizations to deliver innovation at scale.

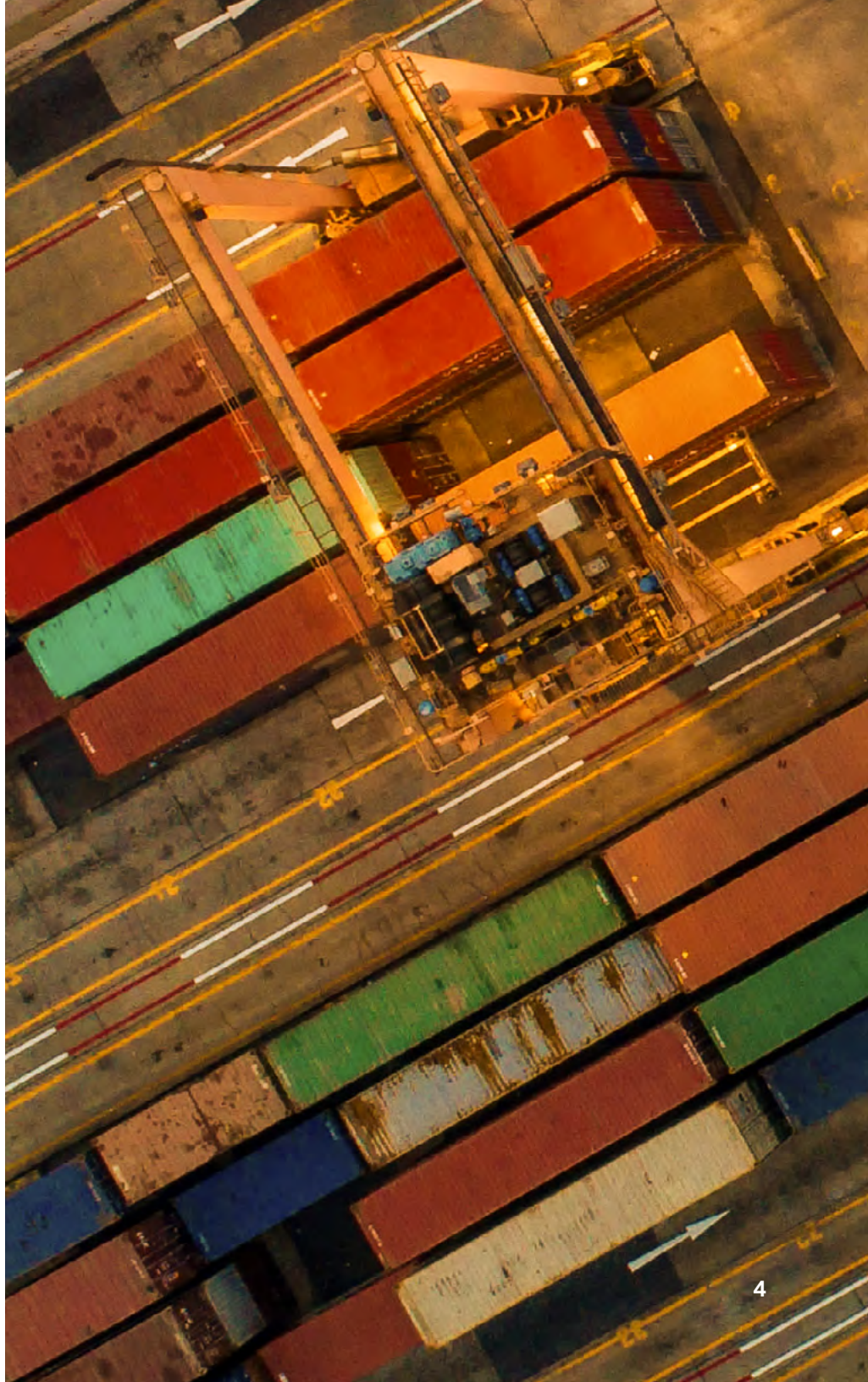
Containers:

Improve productivity: Containers provide pre-made platforms that developers can easily spin up and use, slashing development time.

Increase operational efficiency: Because containers decouple applications from the underlying infrastructures, applications can be patched independently of the infrastructure without disrupting either.

Improve time to market and customer satisfaction: Improved productivity and increased efficiency translate into delivering new solutions customers want faster.

Lower total cost of ownership (TCO): Containers eliminate the overhead costs of operating systems and their maintenance, substantially reducing TCO for almost any application.



AWS knows containers

Nearly 80 percent of all containers in the cloud today run on AWS. AWS services make it easy to containerize and manage your underlying infrastructure, whether on premises or in the cloud, so you can focus on your business. Customers such as Samsung, Expedia, KPMG, GoDaddy, and Snap rely on AWS container services for security, reliability, and scalability.

AWS provides the solutions you need to make containerization seamless:

Provisioning: For serverless compute for your containers, choose AWS Fargate and let AWS manage your infrastructure provisioning. Or, use Amazon Elastic Compute Cloud (Amazon EC2) for full control over your compute environment.

Orchestration: Container orchestration automates the deployment, management, scaling, and networking of containers. Use Amazon Elastic Container Registry (Amazon ECR) to build and store images, then choose from Amazon Elastic Container Service (Amazon ECS) or Amazon Elastic Kubernetes Service (Amazon EKS) to run your containerized applications.

Security: AWS and its partners offer solutions to secure, scan, and detect vulnerabilities in containers:

- Enable container security with AWS Identity and Access Management (IAM) by associating an IAM role with an Amazon ECS task definition or run task API definition.
- Use image scanning solutions to detect vulnerabilities in container images.
- Deploy solutions from AWS partner SentinelOne for scalable and resource-efficient workload protection, detection, and response.

Networking and connectivity: A key component of containerization is distributing and routing application traffic:

- Distribute application traffic across containers and serverless environments with AWS Elastic Load Balancing (ELB).
- Route traffic for globally distributed applications running on containers and improve application performance with AWS Global Accelerator.
- Manage service-to-service communication and security with AWS App Mesh.

Automation: The automated AWS environment eliminates the task of manual code deployment, empowering automatic code deployment with continuous integration/continuous delivery (CI/CD):

- Create a source code repository using AWS CodeCommit.
- Configure a CI/CD pipeline using AWS CodePipeline.
- Deploy AWS CodeBuild to build your container image.
- Build, deploy, and run containerized web applications with AWS App Runner.

Observation and monitoring: Finally, AWS helps ensure your containerized applications are healthy and communicating with each other as expected:

- Deploy AWS App Mesh to provide visibility into logging, metrics, and tracing, as well as to enable load balancing and traffic shaping.
- Run a health check of container images to confirm your containers are running and your app is working.
- Use Amazon CloudWatch Application Insights to monitor health and wellness of applications running in containers deployed in Amazon ECS, Amazon EKS, or Kubernetes on Amazon EC2.

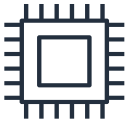
The shifting landscape of cybersecurity

While the operational and bottom-line benefits of containers are clear, they bring new and evolving security challenges that even the most tech-savvy organizations find challenging. Here are five considerations for securing your containerized apps:

On-premises security solutions don't necessarily translate to the cloud: When you migrate to the cloud, what happens to your current security solution? Can you still deploy it once your application is containerized?

The cybersecurity skill shortage demands automation: The global cybersecurity skills shortage shows no sign of abating—in fact, 95 percent of respondents to a recent survey say the skill shortage will stay the same or get worse over time. Given that cybersecurity professionals are in short supply, do you have an automated security solution that eliminates (or at least reduces) the need for in-house cybersecurity staff?

The regulatory environment is constantly changing: Recently, the federal government has intensified its focus on cybersecurity. For example, the National Security Agency issued Kubernetes Hardening Guidance designed to help organizations address the risks of using Kubernetes in the face of supply chain risks, malicious threat actors, and insider threats. While it's difficult to know what new requirements might be coming, things are likely to change. Is your security solution able to respond to changing compliance mandates?



Ransomware remains a threat: Ransomware is malicious code designed to gain unauthorized access to systems and data and encrypt that data to block access by legitimate users. Once ransomware has locked users out of their systems and encrypted their sensitive data, cybercriminals demand a ransom before providing a decryption key to unlock the blocked systems and decrypt data. Do you have a comprehensive approach to fighting ransomware, including protection, detection, and response?

With great containers comes great responsibility: A modern, containerized application requires many different tools and container images. This varied landscape can introduce complexity into your environment, making it difficult to assess the full scope of your cloud workloads. Will your security solution provide a single view to support consistency?

SentinelOne: autonomous cybersecurity for the future of cloud computing

When it comes to securing your organization against evolving security threats, you need a partner that:

- provides industry-leading protection, detection, and response, with third-party test results to back up its claims
- secures workloads running on virtual machines or containers, whether on-premises or in AWS
- is resource-efficient
- auto-deploys and auto-scales with fluctuating workload demand
- secures Kubernetes-orchestrated workloads, whether self-managed or as a managed service in the cloud
- operates in user space to prevent Linux kernel panics and allow maximum flexibility to upgrade a host OS image without fear of agent conflict
- protects the immutable state of cloud workloads
- is easy to use, so that cybersecurity teams spend their time productively
- is multi-tenant, to support a wide-ranging enterprise hybrid cloud footprint

At SentinelOne, we deliver the defenses you need to prevent, detect, and undo known and unknown cybersecurity threats. Three of the Fortune 10 and hundreds of the global 2000 count on us as their trusted cybersecurity partner.

SentinelOne provides:

Better protection of cloud workloads: We protect the host for 10 major Linux distributions and 12 years of Windows Server, as well as containers orchestrated via Kubernetes and standalone Docker containers. Our MITRE ATT&CK 2020 Results, which included Linux, prove the point: zero missed detections, zero configuration changes, and the most analytic enrichment two years running.

Autonomous, real-time detection of security incidents: We use Behavioral AI to evaluate threats in real-time, delivering high-quality detections without human intervention. Our solution automatically correlates individual events into context-rich Storylines™ to reconstruct the attack and easily integrates threat intelligence to increase detection efficacy.

Faster triage and investigation: Storylines detect and prevent threats while accelerating triage and incident response. Alerts and telemetry data are also auto-correlated to the MITRE Engenuity ATT&CK framework, specifically for the tactics and techniques that a given threat exhibits. According to Forrester, by reducing the time needed to resolve endpoint issues, we save users an average of $1.2 million.

Streamlined remediation: We remediate all affected endpoints with a single click, without the need to write any new scripts, simplifying and reducing mean time to respond.

Simplified, powerful, and proactive threat hunting: Our up-level security operations center (SOC) resources enable proactive threat hunting with automated hunting rules and intel-driven hunting packs, along with support for MITRE ATT&CK tactic and technique hunting. What's more, our easy-to-use search and pivoting features lighten analyst load when hunting across large volumes (up to 365 days) of endpoint detection and response (EDR) telemetry.

Consolidated security platform: We provide complete endpoint protection by combining EPP and EDR capabilities into a single platform with a single agent. Forrester Consulting calculates that by consolidating various legacy systems into a single agent solution, we save users $3 million. SentinelOne solutions are designed for organizations seeking enterprise-grade prevention, detection, response, and hunting across endpoint, cloud, and IoT.

SentinelOne Singularity Cloud Workload Security

The SentinelOne Singularity Cloud Workload Security solution extends security and visibility to assets running in AWS environments. Your security team can manage both Linux and Windows servers in Amazon EC2, as well as containers running on self-managed Kubernetes or managed container services like Amazon EKS and Amazon ECS.

A single resource-efficient Sentinel agent delivers autonomous runtime protection, detection, and response across the hybrid cloud estate. SentinelOne brings runtime security to Amazon EKS, Amazon EKS Anywhere, Amazon ECS, and Amazon ECS Anywhere, with automated kill and quarantine, application control, and complete remote shell forensics.

Singularity Cloud Workload Security features include:

Enterprise-grade EDR for Amazon EC2 and Containers: Delivers full-featured EDR directly to your AWS workloads.

- Pivot and hunt from Storylines by MITRE ATT&CK technique.
- Query endpoint telemetry securely stored in the SentinelOne Cloud built on AWS with industry-leading historical EDR data retention options.
- Mark findings as threats and resolve with a click.
- Automate further with a single API with 350+ functions

DevOps friendly: A single, resource-efficient container Sentinel agent protects the Kubernetes worker, its pods, and its containers without any container instrumentation to complicate your efforts. Our agent operates entirely in user space giving you the freedom to update your container image or AMI at will without worrying about compatibility.

Storyline connects the dots automatically: Storyline observes all concurrent processes within all major operating systems and cloud workloads, connects the dots, and builds context. Distributed intelligence watches each Storyline to drive instantaneous protection against advanced attacks. Each Storyline is preserved in an Amazon Simple Storage Service (Amazon S3) bucket to fuel EDR activity.

SentinelOne cybersecurity in action

Thousands of leading enterprises across the globe trust SentinelOne as their cybersecurity provider. Here are the stories of just two:

Cengage: modernizing cloud security

Business challenge: Cengage, a global education technology company serving millions of learners, realized its legacy antivirus solution couldn't keep up with the dynamic threat landscape. When a threat occurred, it took multiple teams several days to respond. Cengage had long trusted SentinelOne with its user endpoints and recognized the need to extend SentinelOne's visibility, detection, and response solutions to its AWS workloads.

Solution: As Cengage continued its journey to a cloud-native architecture on Kubernetes, it chose to use SentinelOne to secure its containerized workloads. Auto-scaling and auto-deployed, SentinelOne's Singularity Cloud Workload Security brings enterprise-grade protection and EDR directly to cloud workloads running on Amazon EC2, Amazon EKS, and Amazon ECS.

Results: Since deploying SentinelOne, Cengage has closed gaps and increased efficiency in its security program. When an attack on a cloud account occurs, a single security team can respond in minutes, not days. Thanks to context-rich Storyline forensics, the security team can offer prescriptive guidance to the cloud team on what is being targeted and how to fix it.

R.R. Donnelley: reinventing security at scale

Business challenge: R.R. Donnelley (RRD), a Fortune 500 provider of multichannel marketing and communication solutions, had a legacy antivirus solution that couldn't adapt to the organization's cloud and endpoint modernization strategy. To stay ahead of risks and take a proactive posture against threats, RRD knew it needed a more modern and holistic security solution that still supported its remaining legacy infrastructure.

Solution: After rigorous field testing, RRD deployed SentinelOne Singularity Complete and Singularity Cloud in parallel with the team's legacy solution. SentinelOne's compatibility made it easy to deploy: RRD was able to do a full rollout to all 50,000+ endpoints and servers in under a month, which was five months sooner than expected. Within a month of deployment, RRD prevented an outbreak of WannaCry ransomware stemming from a contractor's laptop overseas.

Results: SentinelOne has become RRD's new corporate standard for endpoint security, delivering equal protection across all endpoints and servers regardless of whether they reside on-premises or in AWS. When an incident occurs, the security team can coordinate a response by killing malicious processes and quarantining affected machines, quickly identifying and protecting against attacks on RRD's critical systems and services.

SentinelOne and AWS: modern cybersecurity meets modern cloud

SentinelOne is redefining cybersecurity by pushing the boundaries of autonomous technology. AWS is the world's most comprehensive and broadly adopted cloud platform. Together, they're leading the way in cloud and container security.

AWS's Shared Responsibly Model means that when you run on AWS, AWS is responsible for security OF the cloud—protecting the infrastructure that runs all the services offered by AWS. You're responsible for security IN the cloud—including the guest operating system (updates and security patches), other associated application software, and configuration of your AWS footprint—and SentinelOne stands ready to support you in meeting your responsibilities.

As an AWS Advanced Technology Partner, SentinelOne is fully committed to AWS:

- **SentinelOne runs on AWS:** 99 percent of SentinelOne's customers run on AWS.
- **SentinelOne sells on AWS Marketplace:** We make it easy to purchase SentinelOne solutions using your existing channel partners.
- **SentinelOne provides security solution for AWS services:** We deliver added security features for all AWS container services—Amazon ECS, Amazon ECS Anywhere, Amazon EKS, and Amazon EKS Anywhere.
- **SentinelOne is trusted:** We've achieved the AWS Security Competency, recognizing our deep technical expertise and proven customer success in protecting user endpoints and securing cloud adoption.

aws modern apps

SentinelOne

Ready to get started?

If you'd like to learn more about how SentinelOne secures your containerized workloads on AWS, visit s1.ai/AWS or view SentinelOne on AWS Marketplace.

Are you ready to see for yourself?
Let us show you a demo of SentinelOne and how it secures AWS environments.