Your cloud infrastructure is just as vulnerable to ransomware as your user endpoints, perhaps more so. With cloud IaaS spending forecast to grow 22% in 2022, this attack surface is only becoming more vital to the operation of the digital enterprise. Your cloud workloads, data, and intellectual property need multi-layered defenses from vulnerable images, ransomware, crypto-mining malware, and zero-day attacks.

The cost of doing nothing, or not enough, is pegged at $4.6 million USD. That is the average cost of a ransomware attack according to research from The Ponemon Institute published in the 2021 X-Force Threat Intelligence Index. The good news? There are many security steps an organization can take to harden their cloud footprint against these threats.

Linux, Containers, & Kubernetes: Ransomware Casts a Wider Net

With the persistent, multi-year growth of cloud IaaS, Linux has increasingly become a target of bad actors. The cloud is built on Linux, with over 90% of cloud compute instances based on the Linux OS. The summer of 2021 saw a prime example of Linux ransomware dubbed "DarkRadiation", which targeted two of the more widely used distributions, RHEL and CentOS, as well as Docker containers.

Speaking of containers, Kubernetes is the de facto standard for container orchestration, with over 90% share. Recognizing the critical importance of securing the Kubernetes attack surface, and in response to industry feedback from its first revision, CISA published a revision to its Kubernetes Hardening Guide in March 2022. This document illustrates several readily-implemented recommendations for securing Kubernetes, the first of which is scanning software images for known vulnerabilities.

Image Scanning

Several years ago, when speaking with prospects I would often find myself clarifying some fundamental misgivings about where their cloud service providers' security responsibilities ended and theirs began. Perhaps owing in small part to a steady drip of high-profile cloud data breaches, the market now largely understands that they are responsible for securing what they put *in* the cloud. Yet now, the objection often heard is, "We are good: we do image scanning."

Image scanning is great. Everyone should be doing it. Alone, however, image scanning is insufficient. Why do I say this? If it were sufficient, then we would not be challenged by the fact that 3 of every 4 production images are running with a critical or high severity vulnerability. Shifting-left is good, but when push comes to shove and a DevOps team has to choose between addressing a software vulnerability or shipping code on-schedule, it would seem that delivery wins 75% of the time. It's not surprising. After all, the old business school axiom goes, "You get what you measure," and software delivery is a key performance metric.

Software composition analysis is a well-served segment, with a wide array of solutions available, some of which are even open-source. Let image scanning be the first layer of defense in a cloud security strategy, and press forward.

Identity & Access Management

Cloud service providers have made IAM techniques widely available to their customers, and there are several best practices within. First and foremost, organizations must strictly guard the cloud management plane by limiting access to privileged accounts, using multi-factor authentication (MFA), and logging use of such accounts. Robust password policies and encryption key rotation are also a must.

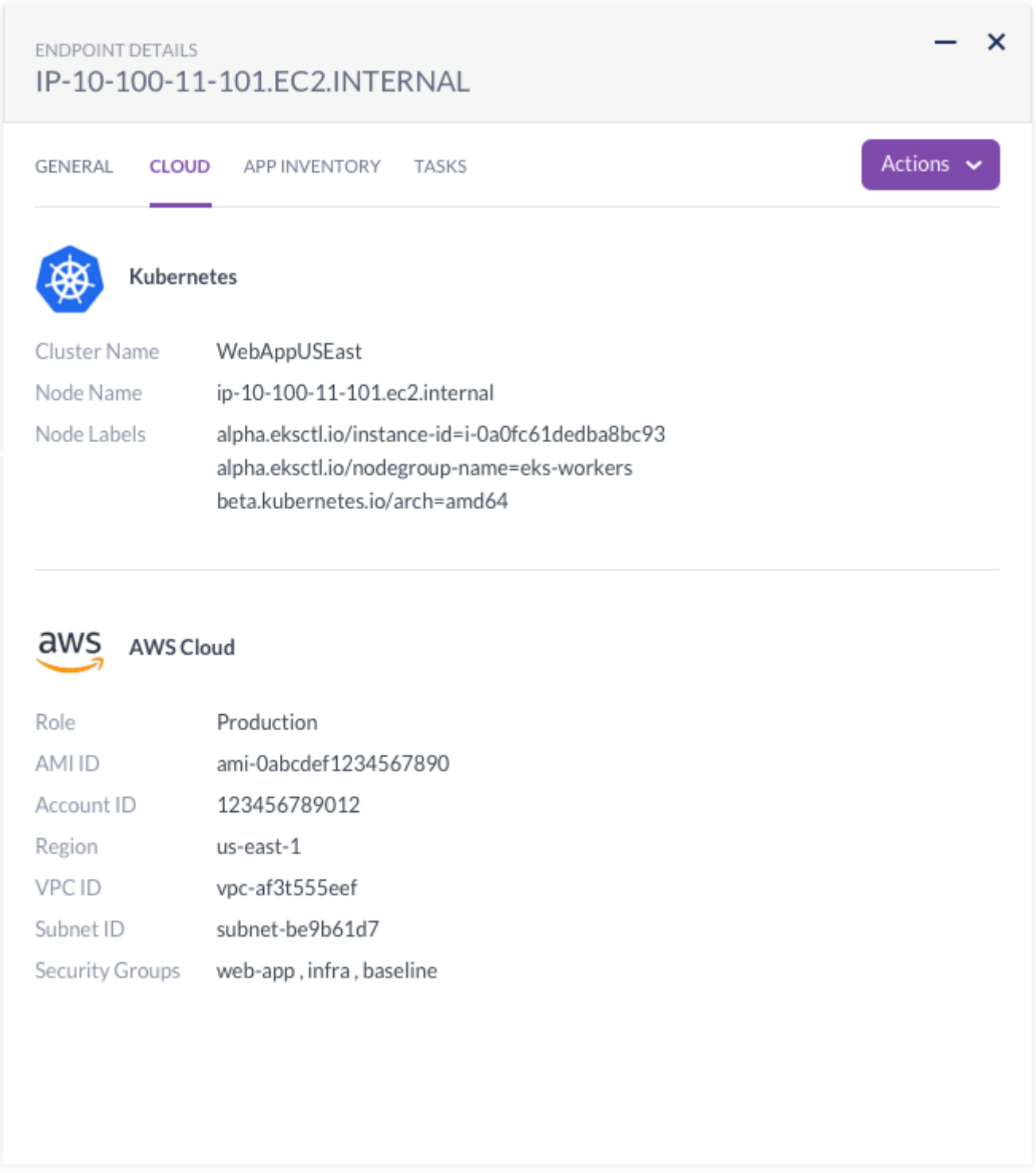
Extensive use of IAM roles under the principle of least privileges goes a long way to improve security, and use of such roles can be augmented with a well-planned workload architecture. For example, consider a cloud workload which processes a file uploaded by a user to an AWS account. The processing itself is conducted on an Amazon EC2 instance. Rather than expose the EC2 instance to the public internet, an S3 bucket can be configured to accept uploads. An IAM role allows the workload, and only the workload, to reach into this "drop bucket" and retrieve the file (presumably after having scanned the file for malware, but that's a topic for another blog). In this way, the EC2 remains safely within a VPC (virtual private cloud), accepting only input from a specific bucket and even then, only under certain conditions (e.g., the file has been scanned for malware and is clean). This is just a simple example of how architectural considerations can be used to further secure your cloud footprint.

Cloud Workload Protection & Response

Finally, cloud workload protection is your last line of defense against runtime threats. Behavioral AI detects unknown threats such as zero-day exploits and indicators of compromise consistent with novel ransomware. Ideally, a cloud workload protection platform can be managed from the same security console as your user endpoint protection; doing so facilitates triage and compresses incident response time.

In the United States, there is a new law which underscores the importance of CWP for securing the cloud footprint. Under the Cybersecurity Incident Response for Critical Infrastructure Act (CIRCIA), companies in 16 critical infrastructure industries — from Food & Agriculture to Finance, Defense, Healthcare, Utilities, and more — now have strict reporting requirements for material cybersecurity incidents. Such incidents must now be reported within 72 hours from the moment of awareness. A CWPP solution facilitates compliance to the new law. Without the extensive EDR data that a CWPP provides, compliance to the CIRCIA will be strenuous if not impossible, considering IR reports typically take upwards of 8 weeks.

When considering a CWPP solution such as Singularity Cloud, look for hybrid cloud support, ingestion of cloud metadata, and extensive support of Linux and Windows Server operating systems. AI and policy-driven automation should respond to threats in milliseconds: machine-speed attacks demand a machine-speed response. Protecting workload immutability is key: anything not in the workload image should be killed, ideally without any machine learning training periods to slow down agile innovation. Automated correlation of related events, such as with SentinelOne's patented Storyline™ technology, seamlessly stitches seemingly unrelated pieces of an attack sequence together, consolidating alerts, reducing noise, amplifying signal, and making SOC analysts far more productive in responding during crises.



Join Our Webinar

Cloud workload protection is your backstop, your last line of defense in a multi-layer defense-in-depth cloud security strategy. CWP protects cloud compute instances, containerized workloads, and Kubernetes clusters from runtime threats. Join KPMG, AWS, Recorded Future, and SentinelOne for our fireside chat on April 28, 2022, as we discuss ways and means to mitigate runtime threats such as cloud ransomware, and continuously protect your cloud workloads.

Defeat Ransomware: How to Mitigate Risk and Accelerate Your Enterprise Thursday, April 28, 2022 at 11 a.m. PDT Save Your Spot