CROWDSTRIKE

CLOUD SECURITY BEST PRACTICES

From an Industry Expert

ANDRAS CSER

Vice President and Principal Analyst,
Security and Risk at Forrester Research

CrowdStrike recently hosted a webinar featuring guest speaker Andras Cser from Forrester. We are continuing that conversation with this Q&A in which we ask him about cloud security best practices.

CAN YOU OVERVIEW THE CURRENT CLOUD THREAT LANDSCAPE AND THE TRENDS YOU FORESEE?

The underlying issues behind the proliferation of threats include: 1) more workloads in the cloud, 2) more desirable data (PII, PHI, IP, sensitive) in the cloud, 3) an increase in the complexity of cloud workloads (new storage, instances and network objects often without adequate protection), and 4) an increase in the number of workloads in the cloud. Add containerization and the fact that most cloud and containerized environments are built out by scripts, aka infrastructure as code (IaC), and you have a perfect storm on your hands.

Current cloud threat landscape:
Threats are proliferating

WHAT'S YOUR VIEW ON WORKLOAD PROTECTION AND COMPLIANCE FOR DEVOPS AND SECOPS?

Workload protection should be a multilayered set of detections and defenses. Organizations need protection, detection, interception and policy remediation at five levels: 1) the hypervisor/virtualization layer, 2) operating system (typically, but not only, Linux and Windows), 3) container runtime (Docker, etc.), 4) container orchestration (Kubernetes, etc.), and 5) serverless. The build pipeline's IaC configuration is also vulnerable and should be protected against unauthorized changes and drifts.

WHAT VALUE DO YOU SEE IN BRINGING TOGETHER CLOUD WORKLOAD PROTECTION PLATFORMS (CWPPS) AND CLOUD SECURITY POSTURE MANAGEMENT (CSPM)?

CWPPs and CSPM are applicable to the layers described in the previous response. CWPP mainly refers to the reactive, runtime, post-deployment aspect, while CSPM refers to the proactive, configuration-time, pre-deployment of defenses. CWPP and CSPM (covering the five areas outlined above) form a continuum of protections against threats. Sharing access and activity logs between CWPP and CSPM also further strengthens protections pre-and post-deployment in the DevOps lifecycle.

CWPPs + CSPM

WHICH BEST PRACTICES CAN YOU OFFER FOR SECURING CLOUD ENVIRONMENTS?

We see leading organizations adhering to the following guidelines and best practices: 1) Do not let any environments get out of hand. Ensure that your organization has and maintains proper controls and procedures for creating and managing new environments. This includes IaC build scripts and OS and container images and configurations. 2) Maintain scanning procedures for images (shift left) and runtime (shift right). 3) Resist pressures from operations teams to apply legacy processes (patching, manual configuration management, etc.) to containers and IaC script-built workloads.

Guidelines and best practices

Learn about CrowdStrike cloud security solutions

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**